The 5G-AKA Authentication Protocol Privacy (Technical Report)

Adrien Koutsos
LSV, CNRS, ENS Paris-Saclay, Université Paris-Saclay
Cachan, France
adrien.koutsos@lsv.fr

***Abstract*—We study the 5G-AKA authentication protocol described in the 5G mobile communication standards. This version of AKA tries to achieve a better privacy than the 3G and 4G versions through the use of asymmetric randomized encryption. Nonetheless, we show that except for the IMSI-catcher attack, all known attacks against 5G-AKA privacy still apply.**

Next, we modify the 5G-AKA protocol to prevent these attacks, while satisfying 5G-AKA efficiency constraints as much as possible. We then formally prove that our protocol is σ-unlinkable. This is a new security notion, which allows for a fine-grained quantification of a protocol privacy. Our security proof is carried out in the Bana-Comon indistinguishability logic. We also prove mutual authentication as a secondary result.

***Index Terms*—AKA, Unlinkability, Privacy, Formal Methods.**

I. Introduction

Mobile communication technologies are widely used for voice, text and Internet access. These technologies allow a subscriber's device, typically a mobile phone, to connect wirelessly to an antenna, and from there to its service provider. The two most recent generations of mobile communication standards, the 3G and 4G standards, have been designed by the 3GPP consortium. The *fifth generation* (5G) of mobile communication standards is being finalized, and drafts are now available [1]. These standards describe protocols that aim at providing security guarantees to the subscribers and service providers. One of the most important such protocol is the *Authentication and Key Agreement* (AKA) protocol, which allows a subscriber and its service provider to establish a shared secret key in an authenticated fashion. There are different variants of the AKA protocol, one for each generation.

In the 3G and 4G-AKA protocols, the subscriber and its service provider share a long term secret key. The subscriber stores this key in a cryptographic chip, the *Universal Subscriber Identity Module* (*USIM*), which also performs all the cryptographic computations. Because of the *USIM* limited computational power, the protocols only use symmetric key cryptography without any pseudo-random number generation on the subscriber side. Therefore the subscriber does not use a random challenge to prevent replay attacks, but instead relies on a sequence number SQN. Since the sequence number has to be tracked by the subscriber and its service provider, the AKA protocols are stateful.

Because a user could be easily tracked through its mobile phone, it is important that the AKA protocols provide privacy guarantees. The 3G and 4G-AKA protocols try to do that using temporary identities. While this provides some privacy against a *passive adversary*, this is not enough against an *active adversary*. Indeed, these protocols allow an antenna to ask for a user permanent identity when it does not know its temporary identity (this naturally happens in roaming situations). This mechanism is abused by IMSI-catchers [2] to collect the permanent identities of all mobile devices in range.

The IMSI-catcher attack is not the only known attack against the privacy of the AKA protocols. In [3], the authors show how an attacker can obtain the least significant bits of a subscriber's sequence number, which allows the attacker to monitor the user's activity. The authors of [4] describe a linkability attack against the 3G-AKA protocol. This attack is similar to the attack on the French e-passport [5], and relies on the fact that 3G-AKA protocol uses different error messages if the authentication failed because of a bad Mac or because a de-synchronization occurred.

The 5G standards include changes to the AKA protocol to improve its privacy guarantees. In 5G-AKA, a user never sends its permanent identity in plain-text. Instead, it encrypts it using a *randomized asymmetric encryption* with its service provider public key. While this prevents the IMSI-catcher attack, this is not sufficient to get unlinkability. Indeed, the attacks from [3], [4] against the 3G and 4G-AKA protocols still apply. Moreover, the authors of [6] proposed an attack against a variant of the AKA protocol introduced in [4], which uses the fact that an encrypted identity can be replayed. It turns out that their attack also applies to 5G-AKA.

a) Objectives: Our goal is to improve the privacy of 5G-AKA while satisfying its design and efficiency constraints. In particular, our protocol should be as efficient as the 5G-AKA protocol, have a similar communication complexity and rely on the same cryptographic primitives. Moreover, we want formal guarantees on the privacy provided by our protocol.

b) Formal Methods: Formal methods are the best way to get a strong confidence in the security provided by a protocol. They have been successfully applied to prove the security of crucial protocols, such as Signal [7] and TLS [8], [9]. There exist several approaches to formally prove a protocol security.

In the *symbolic* or *Dolev-Yao* (DY) model, protocols are modeled as members of a formal process algebra [10]. In this model, the attacker controls the network: he reads all messages and he can forge new messages using capabilities granted to him through a fixed set of rules. While security in this model can be automated (e.g. [11]–[14]), it offers limited guarantees: we only prove security against an attacker that has the designated capabilities.

The *computational model* is more realistic. The attacker also controls the network, but is not limited by a fixed set of rules. Instead, the attacker is any Probabilistic Polynomial-time Turing Machine (PPTM for short). Security proofs in this model are typically sequences of game transformations [15] between a game stating the protocol security and cryptographic hypotheses. This model offers strong security guarantees, but proof automation is much harder. For instance, CRYPTOVERIF [16] cannot prove the security of stateful cryptographic protocols (such as the AKA protocols).

There is a third model, the *Bana-Comon* (BC) model [17], [18]. In this model, messages are terms and the security property is a first-order formula. Instead of granting the attacker capabilities through rules, as in the symbolic approach, we state what the adversary *cannot* do. This model has several advantages. First, since security in the BC model entails computational security, it offers strong security guarantees. Then, there is no ambiguity: the adversary can do anything which is not explicitly forbidden. Finally, this approach is well-suited to model stateful protocols.

c) Related Work: There are several formal analysis of AKA protocols in the symbolic models. In [12], the authors use the DEEPSEC tool to prove unlinkability of the protocol for three sessions. In [4] and [19], the authors use PROVERIF to prove unlinkability of AKA variants for, respectively, three sessions and an unbounded number of sessions. In these three works, the authors abstracted away several key features of the protocol. Because DEEPSEC and PROVERIF do not support the xor operator, they replaced it with a symmetric encryption. Moreover, sequence numbers are modeled by nonces in [4] and [12]. While [19] models the sequence number update, they assume it is always incremented by one, which is incorrect. Finally, none of these works modeled the re-synchronization or the temporary identity mechanisms. Because of these inaccuracies in their models, they all miss attacks.

In [20], the authors use the TAMARIN prover to analyse multiple properties of 5G-AKA. For each property, they either find a proof, or exhibit an attack. To our knowledge, this is the most precise symbolic analysis of an AKA protocol. For example, they correctly model the xor and the re-synchronization mechanisms, and they represent sequence numbers as integers (which makes their model stateful). Still, they decided not to include the temporary identity mechanism. Using this model, they successfully rediscover the linkability attack from [4].

We are aware of two analysis of AKA protocols in the computational model. In [6], the authors present a significantly modified version of AKA, called PRIV-AKA, and claim it is unlinkable. However, we discovered a linkability attack against the protocol, which falsifies the authors claim. In [21], the authors study the 4G-AKA protocol *without its first message*. They show that this reduced protocol satisfies a form of anonymity (which is weaker than unlinkability). Because they consider a weak privacy property for a reduced protocol, they fail to capture the linkability attacks from the literature.

To summarize, there is currently no computational security proof of a complete version of an AKA protocol.

d) Contributions: Our contributions are:

- We study the privacy of the 5G-AKA protocol described in the 3GPP draft [1]. Thanks to the introduction of asymmetric encryption, the 5G version of AKA is not vulnerable to the IMSI-catcher attack. However, we show that the linkability attacks from [3], [4], [6] against older versions of AKA still apply to 5G-AKA.
- We present a new linkability attack against PRIV-AKA, a significantly modified version of the AKA protocol introduced and claimed unlinkable in [6]. This attack exploits the fact that, in PRIV-AKA, a message can be delayed to yield a state update later in the execution of the protocol, where it can be detected.
- We propose the AKA^+ protocol, which is a modified version of 5G-AKA with better privacy guarantees and satisfying the same design and efficiency constraints.
- We introduce a new privacy property, called σ-unlinkability, inspired from [22] and Vaudenay's Privacy [23]. Our property is parametric and allows us to have a fine-grained quantification of a protocol privacy.
- We formally prove that AKA^+ satisfies the σ-unlinkability property in the computational model. Our proof is carried out in the BC model, and holds for any number of agents and sessions that are not related to the security parameter. We also show that AKA^+ provides mutual authentication.

e) Outline: In Section II and III we describe the 5G-AKA protocol and the known linkability attacks against it. We present the AKA^+ protocol in Section IV, and we define the σ-unlinkability property in Section V. Finally, we show how we model the AKA^+ protocol using the BC logic in Section VI, and we state and sketch the proofs of the mutual authentication and σ-unlinkability of AKA^+ in Section VII. The full proofs are in Appendix.

II. THE 5G-AKA PROTOCOL

We present the 5G-AKA protocol described in the 3GPP standards [1]. This is a three-party authentication protocol between:

- The *User Equipment* (*UE*). This is the subscriber's physical device using the mobile communication network (e.g. a mobile phone). Each *UE* contains a cryptographic chip, the *Universal Subscriber Identity Module* (*USIM*), which stores the user confidential material (such as secret keys).
- The *Home Network* (*HN*), which is the subscriber's service provider. It maintains a database with the necessary data to authenticate its subscribers.
- The *Serving Network* (*SN*). It controls the base station (the antenna) the *UE* is communicating with through a wireless channel.

If the *HN* has a base station nearby the *UE*, then the *HN* and the *SN* are the same entity. But this is not always the case (e.g. in roaming situations). When no base station from the user's *HN* are in range, the *UE* uses another network's base station.

The *UE* and its corresponding *HN* share some confidential key material and the *Subscription Permanent Identifier* (SUPI), which uniquely identifies the *UE*. The *SN* does not have access to the secret key material. It follows that all cryptographic computations are performed by the *HN*, and sent to the *SN* through a secure channel. The *SN* also forwards all the information it gets from the *UE* to the *HN*. But the *UE* permanent identity is not kept hidden from the *SN*: after a successful authentication, the *HN* sends the SUPI to the *SN*. This is not technically needed, but is done for legal reasons. Indeed, the *SN* needs to know whom it is serving to be able to answer to *Lawful Interception* requests.

Therefore, privacy requires to trust both the *HN* and the *SN*. Since, in addition, they communicate through a secure channel, we decided to model them as a single entity and we include the *SN* inside the *HN*. A description of the protocol with three distinct parties can be found in [20].

A. Description of the Protocol

The 5G standard proposes two authentication protocols, EAP-AKA′ and 5G-AKA. Since their differences are not relevant for privacy, we only describe the 5G-AKA protocol.

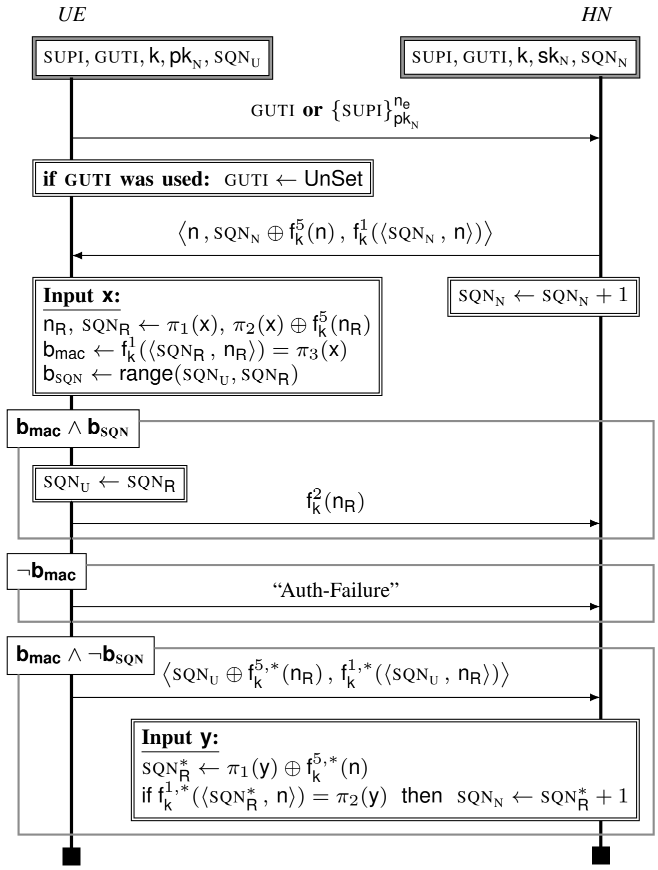
a) Cryptographic Primitives: As in the 3G and 4G variants, the 5G-AKA protocol uses several keyed cryptographic one-way functions: f^1, f^2, f^5, $f^{1,*}$ and $f^{5,*}$. These functions are used both for integrity and confidentiality, and take as input a long term secret key k (which is different for each subscriber).

A major novelty in 5G-AKA is the introduction of an asymmetric randomized encryption $\{\cdot\}_{pk}^{n_e}$. Here pk is the public key, and n_e is the encryption randomness. Previous versions of AKA did not use asymmetric encryption because the *USIM*, which is a cryptographic micro-processor, had no randomness generation capabilities. The asymmetric encryption is used to conceal the identity of the *UE*, by sending $\{\text{SUPI}\}_{pk}^{n_e}$ instead of transmitting the SUPI in clear (as in 3G and 4G-AKA).

b) Temporary Identities: After a successful run of the protocol, the *HN* may issue a temporary identity, a *Globally Unique Temporary Identity* (GUTI), to the *UE*. Each GUTI can be used in *at most one session* to replace the encrypted identity $\{\text{SUPI}\}_{pk}^{n_e}$. It is renewed after each use. Using a GUTI allows to avoid one asymmetric encryption. This saves a pseudo-random number generation and the expensive computation of an asymmetric encryption.

c) Sequence Numbers: The 5G-AKA protocol prevents replay attacks using a sequence number SQN instead of a random challenge. This sequence number is included in the messages, incremented after each successful run of the protocol, and must be tracked and updated by the *UE* and the *HN*. As it may get de-synchronized (e.g. because a message is lost), there are two versions of it: the *UE* sequence number SQN_U, and the *HN* sequence number SQN_N.

d) State: The *UE* and *HN* share the *UE* identity SUPI, a long-term symmetric secret key k, a sequence number SQN_U and the *HN* public key pk_N. The *UE* also stores in GUTI the value of the last temporary identity assigned to it (if there is one). Finally, the *HN* stores the secret key sk_N corresponding to pk_N, its version SQN_N of every *UE*'s sequence number and a mapping between the GUTIs and the SUPIs.



Conventions: $\leftarrow$ is used for assignments, and has a lower priority than the equality comparison operator $=$.

Fig. 1. The 5G-AKA Protocol

e) Authentication Protocol: The 5G-AKA protocol is represented in Fig. 1. We now describe an honest execution of the protocol. The *UE* initiates the protocol by identifying itself to the *HN*, which it can do in two different ways:

- It can send a temporary identity GUTI, if one was assigned to it. After sending the GUTI, the *UE* sets it to UnSet to ensure that it will not be used more than once. Otherwise, it would allow an adversary to link sessions together.
- It can send its concealed permanent identity $\{\text{SUPI}\}_{pk_N}^{n_e}$, using the *HN* public key pk_N and a fresh randomness n_e.

Upon reception of an identifying message, the *HN* retrieves the permanent identity SUPI: if it received a temporary identity GUTI, this is done through a database look-up; and if a concealed permanent identity was used, it uses sk_N to decrypt it. It can then recover SQN_N and the key k associated to the identity SUPI from its memory. The *HN* then generates a fresh nonce n. It masks the sequence number SQN_N by xoring it with $f_k^5(n)$, and mac the message by computing $f_k^1(\langle \text{SQN}_N , n\rangle)$ (we use $\langle \dots \rangle$ for tuples). It then sends the message $\langle n , \text{SQN}_N \oplus f_k^5(n) ,\ f_k^1(\langle \text{SQN}_N , n\rangle)\rangle$.

When receiving this message, the *UE* computes $f^5_k(n)$. With it, it unmasks SQN_N and checks the authenticity of the message by re-computing $f^1_k(\langle \text{SQN}_\text{N}, n\rangle)$ and verifying that it is equal to the third component of the message. It also checks whether SQN_N and SQN_U are in range[1]. If both checks succeed, the *UE* sets SQN_U to SQN_N, which prevents this message from being accepted again. It then sends $f^2_k(n)$ to prove to *HN* the knowledge of k. If the authenticity check fails, an "Auth-Failure" message is sent. Finally, if the authenticity check succeeds but the range check fails, *UE* starts the re-synchronization sub-protocol, which we describe below.

f) Re-synchronization: The re-synchronization protocol allows the *HN* to obtain the current value of SQN_U. First, the *UE* masks SQN_U by xoring it with $f^{5,*}_k(n)$, mac the message using $f^{1,*}_k(\langle \text{SQN}_\text{U}, n\rangle)$ and sends the pair $\langle \text{SQN}_\text{U} \oplus f^{5,*}_k(n), f^{1,*}_k(\langle \text{SQN}_\text{U}, n\rangle)\rangle$. When receiving this message, the *HN* unmasks SQN_U and checks the mac. If the authentication test is successful, *HN* sets the value of SQN_N to $\text{SQN}_\text{U} + 1$. This ensures that *HN* first message in the next session of the protocol is in the correct range.

g) GUTI *Assignment:* There is a final component of the protocol which is not described in Fig. 1 (as it is not used in the privacy attacks we present later). After a successful run of the protocol, the *HN* generates a new temporary identity GUTI and links it to the *UE*'s permanent identity in its database. Then, it sends the masked fresh GUTI to the *UE*.

III. Unlinkability Attacks Against 5G-AKA

We present in this section several attacks against AKA that appeared in the literature. All these attacks but one (the IMSI-catcher attack) carry over to 5G-AKA. Moreover, several fixes of the 3G and 4G versions of AKA have been proposed. We discuss the two most relevant fixes, the first by Arapinis et al. [4], and the second by Fouque et al. [6].

None of these fixes are satisfactory. The modified AKA protocol given in [4] has been shown flawed in [6]. The authors of [6] then propose their own protocol, called PRIV-AKA, and claim it is unlinkable (they only provide a proof sketch). While analyzing the PRIV-AKA protocol, we discovered an attack allowing to permanently de-synchronize the *UE* and the *HN*. Since a de-synchronized *UE* can be easily tracked (after being de-synchronized, the *UE* rejects all further messages), our attack is also an unlinkability attack. This is in direct contradiction with the security property claimed in [6]. This is a novel attack that never appeared in the literature.

A. IMSI-*Catcher Attack*

All the older versions of AKA (4G and earlier) are vulnerable to the IMSI-catcher attack [2]. This attack simply relies on the fact that, in these versions of AKA, the permanent identity (called the *International Mobile Subscriber Identity* or IMSI in the 4G specifications) is not encrypted but sent in plain-text. Moreover, even if a temporary identity is used (a *Temporary Mobile Subscriber Identity* or TMSI), an attacker can simply send a Permanent-ID-Request message to obtain the *UE*'s permanent identity. The attack is depicted in Fig. 2.

[1]The specification is loose here: it only requires that $\text{SQN}_\text{U} < \text{SQN}_\text{N} \leq \text{SQN}_\text{U} + C$, where C is some constant chosen by the *HN*.

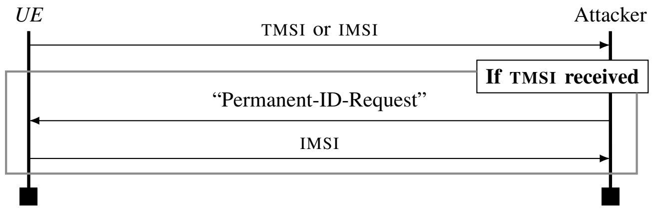


Fig. 2. An IMSI-Catcher Attack

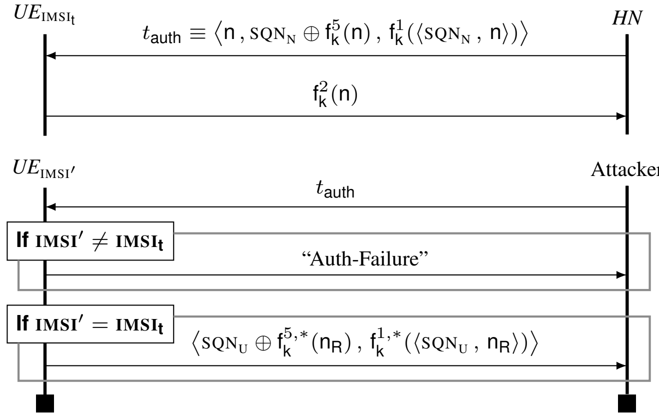


Fig. 3. The Failure Message Attack by [4]

This necessitates an active attacker with its own base station. At the time, this required specialized hardware, and was believed to be too expensive. This is no longer the case, and can be done for a few hundreds dollars (see [24]).

B. *The Failure Message Attack*

In [4], Arapinis et al. propose to use an asymmetric encryption to protect against the IMSI-catcher attack: each *UE* carries the public-key of its corresponding *HN*, and uses it to encrypt its permanent identity. This is basically the solution that was adopted by 3GPP for the 5G version of AKA. Interestingly, they show that this is not enough to ensure privacy, and give a linkability attack that does not rely on the identification message sent by *UE*. While their attack is against the 3G-AKA protocol, it is applicable to the 5G-AKA protocol.

a) The Attack: The attack is depicted in Fig. 3, and works in two phases. First, the adversary eavesdrops a successful run of the protocol between the *HN* and the target *UE* with identity IMSI_t, and stores the authentication message t_{auth} sent by *HN*. In a second phase, the attacker $\mathcal{A}$ tries to determine whether a *UE* with identity IMSI' is the initial *UE* (i.e. whether $\text{IMSI}' = \text{IMSI}_t$). To do this, $\mathcal{A}$ initiates a new session of the protocol and replays the message t_{auth}. If $\text{IMSI}' \neq \text{IMSI}_t$, then the mac test fails, and $UE_{\text{IMSI}'}$ answers "Auth-Failure". If $\text{IMSI}' = \text{IMSI}_t$, then the mac test succeeds but the range test fails, and $UE_{\text{IMSI}'}$ sends a re-synchronization message.

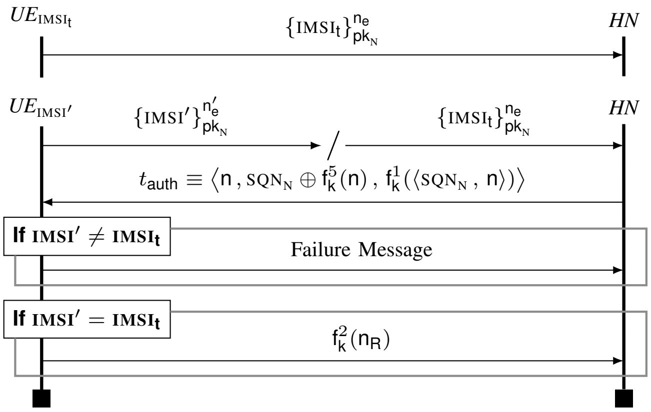


Fig. 4. The Encrypted IMSI Replay Attack by [6]

The adversary can distinguish between the two messages, and therefore knows if it is interacting with the original or a different *UE*. Moreover, the second phase of the attack can be repeated every time the adversary wants to check for the presence of the tracked user IMSI_t in its vicinity.

b) Proposed Fix: To protect against the failure message attack, the authors of [4] propose that the *UE* encrypts both error messages using the public key pk_N of the *HN*, making them indistinguishable. To the adversary, there is no distinctions between an authentication and a de-synchronization failure. The fixed AKA protocol, *without the identifying message* $\{\text{IMSI}\}^{n_e}_{pk_N}$, was formally checked in the symbolic model using the PROVERIF tool. Because this message was omitted in the model, an attack was missed. We present this attack next.

C. The Encrypted IMSI Replay Attack

In [6], Fouque et al. give an attack against the fixed AKA proposed by Arapinis et al. in [4]. Their attack, described in Fig. 4, uses the fact the identifying message $\{\text{IMSI}_t\}^{n_e}_{pk_N}$ in the proposed AKA protocol by Arapinis et al. can be replayed.

In a first phase, the attacker $\mathcal{A}$ eavesdrops and stores the identifying message $\{\text{IMSI}_t\}^{n_e}_{pk_N}$ of an honest session between the user UE_{IMSI_t} it wants to track and the *HN*. Then, every time $\mathcal{A}$ wants to determine whether some user $UE_{\text{IMSI}'}$ is the tracked user UE_{IMSI_t}, it intercepts the identifying message $\{\text{IMSI}'\}^{n'_e}_{pk_N}$ sent by $UE_{\text{IMSI}'}$, and replaces it with the stored message $\{\text{IMSI}_t\}^{n_e}_{pk_N}$. Finally, $\mathcal{A}$ lets the protocol continue without further tampering. We have two possible outcomes:

- If $\text{IMSI}' \neq \text{IMSI}_t$ then the message t_{auth} sent by *HN* is mac-ed using the wrong key, and the *UE* rejects the message. Hence the attacker observes a failure message.
- If $\text{IMSI}' = \text{IMSI}_t$ then t_{auth} is accepted by $UE_{\text{IMSI}'}$, and the attacker observes a success message.

Therefore the attacker can deduce whether it is interacting with UE_{IMSI_t} or not, which breaks unlinkability.

D. Attack Against The PRIV-AKA Protocol

The authors of [6] then propose the PRIV-AKA protocol, which is a significantly modified version of AKA. The authors claim that their protocol achieves authentication and client unlinkability. But we discovered a de-synchronization attack: it is possible to permanently de-synchronize the *UE* and the *HN*. Our attack uses the fact that in PRIV-AKA, the *HN* sequence number is incremented only upon reception of the confirmation message from the *UE*. Therefore, by intercepting the last message from the *UE*, we can prevent the *HN* from incrementing its sequence number. We now describe the attack.

We run a session of the protocol, but we intercept the last message and store it for later use. Note that the *HN*'s session is not closed. At that point, the *UE* and the *HN* are de-synchronized by one. We re-synchronize them by running a full session of the protocol. We then re-iterate the steps described above: we run a session of the protocol, prevent the last message from arriving at the *HN*, and then run a full session of the protocol to re-synchronize the *HN* and the *UE*. Now the *UE* and the *HN* are synchronized, and we have two stored messages, one for each uncompleted session. We then send the two messages to the corresponding *HN* sessions, which accept them and increment the sequence number. In the end, it is incremented by *two*.

The problem is that the *UE* and the *HN* cannot recover from a de-synchronization by two. We believe that this was missed by the authors of [6][2]. Remark that this attack is also an unlinkability attack. To attack some user UE_{IMSI}'s privacy, we permanently de-synchronize it. Then each time UE_{IMSI} tries to run the PRIV-AKA protocol, it will abort, which allows the adversary to track it.

Remark 1. Our attack requires that the *HN* does not close the first session when we execute the second session. At the end of the attack, before sending the two stored messages, there are two *HN* sessions simultaneously opened for the same *UE*. If the *HN* closes any un-finished sessions when starting a new session with the same *UE*, our attack does not work.

But this make another unlinkability attack possible. Indeed, closing a session because of some later session between the *HN* and the same *UE* reveals a link between the two sessions. We describe the attack. First, we start a session i between a user UE_A and the *HN*, but we intercept and store the last message t_A from the user. Then, we let the *HN* run a full session with some user UE_X. Finally, we complete the initial session i by sending the stored message t_A to the *HN*. Here, we have two cases. If $X = A$, then the *HN* closed the first session when it completed the second. Hence it rejects t_A. If $X \neq A$, then the first session is still opened, and it accepts t_A.

Closing a session may leak information to the adversary. Protocols which aim at providing unlinkability must explicit when sessions can safely be closed. By default, we assume a session stays open. In a real implementation, a timeout *tied to the session* (and not the user identity) could be used to avoid keeping sessions opened forever.

[2]"the two sequence numbers may become desynchronized by one step [...]. Further desynchronization is prevented [...]" (p. 266 [6])

E. Sequence Numbers and Unlinkability

We conjecture that it is not possible to achieve functionality (i.e. honest sessions eventually succeed), authentication and unlinkability at the same time when using a sequence number based protocol with no random number generation capabilities in the *UE* side. We briefly explain our intuition.

In any sequence number based protocol, the agents may become de-synchronized because they cannot know if their last message has been received. Furthermore, the attacker can cause de-synchronization by blocking messages. The problem is that we have contradictory requirements. On the one hand, to ensure authentication, an agent must reject a replayed message. On the other hand, in order to guarantee unlinkability, an honest agent has to behave the same way when receiving a message from a synchronized agent or from a de-synchronized agent. Since functionality requires that a message from a synchronized agent is accepted, it follows that a message from a de-synchronized agent must be accepted. Intuitively, it seems to us that an honest agent cannot distinguish between a protocol message which is being replayed and an honest protocol message from a de-synchronized agent. It follows that a replayed message should be both rejected and accepted, which is a contradiction.

This is only a conjecture. We do not have a formal statement, or a proof. Actually, it is unclear how to formally define the set of protocols that rely on sequence numbers to achieve authentication. Note however that all requirements can be satisfied simultaneously if we allow *both* parties to generate random challenges in each session (in AKA, only *HN* uses a random challenge). Examples of challenge based unlinkable authentication protocols can be found in [25].

IV. The AKA$^+$ Protocol

We now describe our principal contribution, which is the design of the AKA$^+$ protocol. This is a fixed version of the 5G-AKA protocol offering some form of privacy against an *active* attacker. First, we explicit the efficiency and design constraints. We then describe the AKA$^+$ protocol, and explain how we designed this protocol from 5G-AKA by fixing all the previously described attacks. As we mentioned before, we think unlinkability cannot be achieved under these constraints. Nonetheless, our protocol satisfies some weaker notion of unlinkability that we call σ-unlinkability. This is a new security property that we introduce. Finally, we will show a subtle attack, and explain how we fine-tuned AKA$^+$ to prevent it.

A. Efficiency and Design Constraints

We now explicit the protocol design constraints. These constraints are necessary for an efficient, in-expensive to implement and backward compatible protocol. Observe that, in a mobile setting, it is very important to avoid expensive computations as they quickly drain the *UE*'s battery.

a) Communication Complexity: In 5G-AKA, authentication is achieved using only three messages: two messages are sent by the *UE*, and one by the *HN*. We want our protocol to have a similar communication complexity. While we did not manage to use only three messages in all scenarios, our protocol achieves authentication in less than four messages.

b) Cryptographic primitives: We recall that all cryptographic primitives are computed in the *USIM*, where they are implemented in hardware. It follows that using more primitives in the *UE* would make the *USIM* more voluminous and expensive. Hence we restrict AKA$^+$ to the cryptographic primitives used in 5G-AKA: we use only symmetric keyed one-way functions and asymmetric encryption. Notice that the *USIM* cannot do asymmetric *decryption*. As in 5G-AKA, we use some in-expensive functions, e.g. xor, pairs, by-one increments and boolean tests. We believe that relying on the same cryptographic primitives helps ensuring backward compatibility, and would simplify the protocol deployment.

c) Random Number Generation: In 5G-AKA, the *UE* generates at most one nonce per session, which is used to randomize the asymmetric encryption. Moreover, if the *UE* was assigned a GUTI in the previous session then there is no random number generation. Remark that when the *UE* and the *HN* are de-synchronized, the authentication fails and the *UE* sends a re-synchronization message. Since the session fails, no fresh GUTI is assigned to the *UE*. Hence, the next session of the protocol has to conceal the SUPI using $\{\text{SUPI}\}^{\mathsf{n_e}}_{\mathsf{pk_N}}$, which requires a random number generation. Therefore, we constrain our protocol to use at most one random number generation by the *UE* per session, and only if no GUTI has been assigned or if the *UE* and the *HN* have been de-synchronized.

d) Summary: We summarize the constraints for AKA$^+$:

- It must use at most four messages per sessions.
- The *UE* may use only keyed one-way functions and asymmetric *encryption*. The *HN* may use these functions, plus asymmetric *decryption*.
- The *UE* may generate at most one random number per session, and only if no GUTI is available, or if re-synchronization with the *HN* is necessary.

B. Key Ideas

In this section, we present the two key ideas used in the design of the AKA$^+$ protocol.

a) Postponed Re-Synchronization Message: We recall that whenever the *UE* and the *HN* are de-synchronized, the authentication fails and the *UE* sends a re-synchronization message. The problem is that this message can be distinguished from a mac failure message, which allows the attack presented in Section III-B. Since the session fails, no GUTI is assigned to the *UE*, and the next session will use the asymmetric encryption to conceal the SUPI. The first key idea is to piggy-back on the randomized encryption of the *next session* to send a concealed re-synchronization message. More precisely, we replace the message $\{\text{SUPI}\}^{\mathsf{n_e}}_{\mathsf{pk_N}}$ by $\{\langle \text{SUPI}\,,\ \text{SQN}_\text{U}\rangle\}^{\mathsf{n_e}}_{\mathsf{pk_N}}$. This has several advantages:

- We can remove the re-synchronization message that lead to the unlinkability attack presented in Section III-B. In AKA$^+$, whenever the mac check or the range check fails, the same failure message is sent.

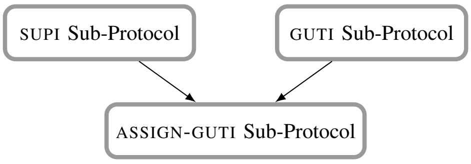


Fig. 5. General Architecture of the AKA$^+$ Protocol

- This does not require more random number generation by the *UE*, since a random number is already being generated to conceal the SUPI in the next session.

The 3GPP technical specification (see [1], Annex C) requires that the asymmetric encryption used in the 5G-AKA protocol is the ECIES encryption scheme, which is an hybrid encryption scheme. Hybrid encryption schemes use a randomized asymmetric encryption to conceal a temporary key. This key is then used to encrypt the message using a symmetric encryption, which is in-expensive. Hence encrypting the pair $\langle \mathrm{SUPI}, \mathrm{SQN}_\mathrm{U} \rangle$ is almost as fast as encrypting only SUPI, and requires the *UE* to generate the same amount of randomness.

b) HN Challenge Before Identification: To prevent the Encrypted IMSI Replay Attack of Section III-C, we add a random challenge n from the *HN*. The *UE* initiates the protocol by requesting a challenge without identifying itself. When requested, the *HN* generates and sends a fresh challenge n to the *UE*, which includes it in its response by mac-ing it with the SUPI using a symmetric one-way function Mac^1 with key $\mathsf{k}_\mathsf{m}^{\mathrm{ID}}$. The *UE* response is now:

$$\Big\langle \{\langle \mathsf{SUPI}, \mathrm{SQN}_\mathrm{U} \rangle\}_{\mathsf{pk}_\mathrm{N}}^{\mathsf{n_e}}, \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\mathrm{ID}}}(\langle \{\langle \mathsf{SUPI}, \mathrm{SQN}_\mathrm{U} \rangle\}_{\mathsf{pk}_\mathrm{N}}^{\mathsf{n_e}}, \mathsf{n} \rangle) \Big\rangle$$

This challenge is only needed when the encrypted permanent identity is used. If the *UE* uses a temporary identity GUTI, then we do not need to use a random challenge. Indeed, temporary identities can only be used once before being discarded, and are therefore not subject to replay attacks. By consequence we split the protocol in two sub-protocols:

- The SUPI sub-protocol uses a random challenge from the *HN*, encrypts the permanent identity and allows to re-synchronize the *UE* and the *HN*.
- The GUTI sub-protocol is initiated by the *UE* using a temporary identity.

In the SUPI sub-protocol, the *UE*'s answer includes the challenge. We use this to save one message: the last confirmation step from the *UE* is not needed, and is removed. The resulting sub-protocol has four messages. Observe that the GUTI sub-protocol is faster, since it uses only three messages.

C. Architecture and States

Instead of a monolithic protocol, we have three sub-protocols: the SUPI and GUTI sub-protocols, which handle authentication; and the ASSIGN-GUTI sub-protocol, which is run after authentication has been achieved and assigns a fresh temporary identity to the *UE*. A full session of the AKA$^+$ protocol comprises a session of the SUPI or GUTI sub-protocols, followed by a session of the ASSIGN-GUTI sub-protocol. This is graphically depicted in Fig. 5.

Since the GUTI sub-protocol uses only three messages and does not require the *UE* to generate a random number or compute an asymmetric encryption, it is faster than the SUPI sub-protocol. By consequence, the *UE* should always use the GUTI sub-protocol if it has a temporary identity available.

The *HN* runs concurrently an arbitrary number of sessions, but a subscriber cannot run more than one session at the same time. Of course, sessions from *different* subscribers may be concurrently running. We associate a unique integer, the session number, to every session, and we use $HN(j)$ and $UE_{\mathrm{ID}}(j)$ to refer to the j-th session of, respectively, the *HN* and the *UE* with identity ID.

a) One-Way Functions: We separate functions that are used only for confidentiality from functions that are also used for integrity. We have two confidentiality functions f and f^r, which use the key k, and five integrity functions Mac^1–Mac^5, which use the key $\mathsf{k_m}$. We require that f and f^r (resp. Mac^1–Mac^5) satisfy jointly the PRF assumption.

This is a new assumption, which requires that these functions are *simultaneously* computationally indistinguishable from random functions.

Definition 1 (Jointly PRF Functions)**.** *Let $H_1(\cdot,\cdot), \ldots, H_n(\cdot,\cdot)$ be a finite family of keyed hash functions from $\{0,1\}^* \times \{0,1\}^\eta$ to $\{0,1\}^\eta$. The functions $H_1, \ldots, H_n$ are* Jointly Pseudo Random Functions *if, for any PPTM adversary $\mathcal{A}$ with access to oracles $\mathcal{O}_{f_1}, \ldots, \mathcal{O}_{f_n}$:*

$$|\mathbf{Pr}(k: \ \mathcal{A}^{\mathcal{O}_{H_1(\cdot,k)},\ldots,\mathcal{O}_{H_n(\cdot,k)}}(1^\eta) = 1) - \mathbf{Pr}(g_1, \ldots, g_n: \ \mathcal{A}^{\mathcal{O}_{g_1(\cdot)},\ldots,\mathcal{O}_{g_n(\cdot)}}(1^\eta) = 1)|$$

is negligible, where:

- *k is drawn uniformly in $\{0,1\}^\eta$.*
- *$g_1, \ldots, g_n$ are drawn uniformly in the set of all functions from $\{0,1\}^*$ to $\{0,1\}^\eta$.*

Observe that if $H_1, \ldots, H_n$ are jointly PRF then, in particular, every individual H_i is a PRF.

Remark 2. While this is a non-usual assumption, it is simple to build a set of functions $H_1, \ldots, H_n$ which are jointly PRF from a single PRF H. For example, let $\mathsf{tag}_1, \ldots, \mathsf{tag}_n$ be non-ambiguous tags, and let $H_i(m, \mathsf{k}) = H(\mathsf{tag}_i(m), \mathsf{k})$. Then, $H_1, \ldots, H_n$ are jointly PRF whenever H is a PRF (see Appendix I-B).

b) UE Persistent State: Each UE_{ID} with identity ID has a state $\mathsf{state}_\mathrm{U}^{\mathrm{ID}}$ persistent across sessions. It contains the following immutable values: the permanent identity $\mathrm{SUPI} = \mathrm{ID}$, the confidentiality key k^{ID}, the integrity key $\mathsf{k}_\mathsf{m}^{\mathrm{ID}}$ and the *HN*'s public key pk_N. The states also contain mutable values: the sequence number SQN_U, the temporary identity GUTI_U and the boolean $\mathsf{valid\text{-}guti}_\mathrm{U}$. We have $\mathsf{valid\text{-}guti}_\mathrm{U} = \mathsf{false}$ whenever no valid temporary identity is assigned to the *UE*. Finally, there are mutable values that are not persistent across sessions. E.g.

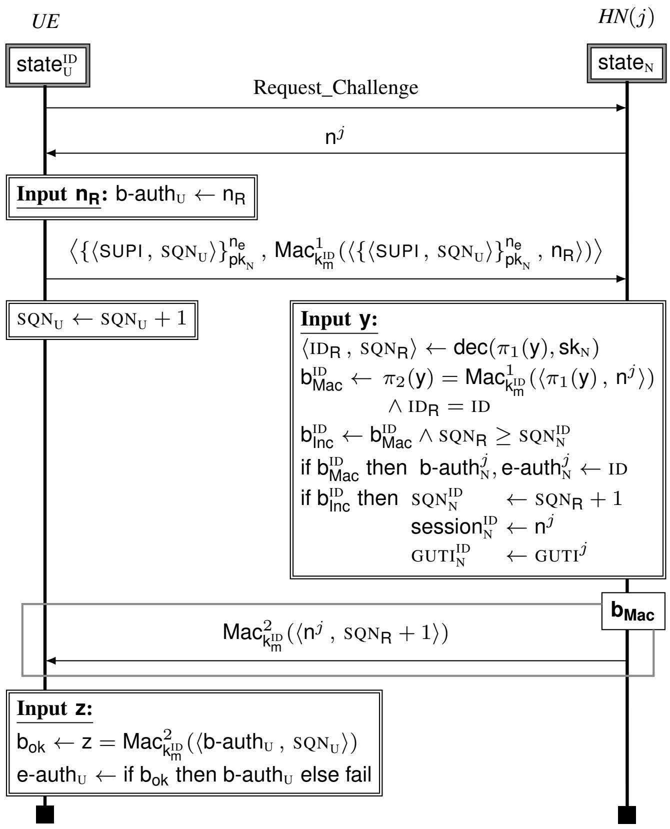


Fig. 6. The SUPI Sub-Protocol of the AKA$^+$ Protocol

b-auth$_U$ stores *HN*'s random challenge, and e-auth$_U$ stores *HN*'s random challenge *when the authentication is successful.*

c) HN Persistent State: The *HN* state state$_N$ contains the secret key sk_N corresponding to the public key pk_N. Also, for every subscriber with identity ID, it stores the keys k^{ID} and k_m^{ID}, the permanent identity SUPI = ID, the *HN* version of the sequence number SQN_N^{ID} and the temporary identity GUTI_N^{ID}. It stores in session$_N^{ID}$ the random challenge of the last session that was either a successful SUPI session which modified the sequence number, or a GUTI session which authenticated ID. This is used to detect and prevent some subtle attacks, which we present later. Finally, every session $HN(j)$ stores in b-auth$_N^j$ the identity claimed by the *UE*, and in e-auth$_N^j$ the identity of the *UE* it authenticated.

D. The SUPI, GUTI *and* ASSIGN-GUTI *Sub-Protocols*

We describe honest executions of the three sub-protocols of the AKA$^+$ protocol. An honest execution is an execution where the adversary dutifully forwards the messages without tampering. Each execution is between a *UE* and $HN(j)$.

a) The SUPI *Sub-Protocol:* This protocol uses the *UE*'s permanent identity, re-synchronizes the *UE* and the *HN* and is expensive to run. The protocol is sketched in Fig. 6.

The *UE* initiates the protocol by requesting a challenge from the network. When asked, $HN(j)$ sends a fresh random challenge n^j. After receiving n^j, the *UE* stores it in b-auth$_U$, and answers with the encryption of its permanent identity together with the current value of its sequence number, using the *HN* public key pk_N. It also includes the mac of this encryption and of the challenge, which yields the message:

$$\langle \{\langle \text{SUPI}, \text{SQN}_U \rangle\}_{pk_N}^{n_e}, \mathsf{Mac}^1_{k_m^{ID}}(\langle \{\langle \text{SUPI}, \text{SQN}_U\rangle\}_{pk_N}^{n_e}, n^j\rangle)\rangle$$

Then the *UE* increments its sequence number by one. When it gets this message, the *HN* retrieves the pair $\langle \text{SUPI}, \text{SQN}_U\rangle$ by decrypting the encryption using its secret key sk_N. For every identity ID, it checks if SUPI = ID and if the mac is correct. If this is the case, *HN* authenticated ID, and it stores ID in b-auth$_N^j$ and e-auth$_N^j$. After having authenticated ID, *HN* checks whether the sequence number SQN_U it received is greater than or equal to SQN_N^{ID}. If this holds, it sets SQN_N^{ID} to $\text{SQN}_U + 1$, stores n^j in session$_N^{ID}$, generates a fresh temporary identity GUTI^j and stores it into GUTI_N^{ID}. This additional check ensures that the *HN* sequence number is always increasing, which is a crucial property of the protocol.

If the *HN* authenticated ID, it sends a confirmation message $\mathsf{Mac}^2_{k_m^{ID}}(\langle n^j, \text{SQN}_U + 1\rangle)$ to the *UE*. This message is sent even if the received sequence number SQN_U is smaller than SQN_N^{ID}. When receiving the confirmation message, if the mac is valid then the *UE* authenticated the *HN*, and it stores in e-auth$_U$ the initial random challenge (which it keeps in b-auth$_U$). If the mac test fails, it stores in e-auth$_U$ the special value fail.

b) The GUTI *Sub-Protocol:* This protocol uses the *UE*'s temporary identity, requires synchronization to succeed and is inexpensive. The protocol is sketched in Fig. 7.

When valid-guti$_U$ is true, the *UE* can initiate the protocol by sending its temporary identity GUTI_U. The *UE* then sets valid-guti$_U$ to false to guarantee that this temporary identity is not used again. When receiving a temporary identity x, *HN* looks if there is an ID such that GUTI_N^{ID} is equal to x and is not UnSet. If the temporary identity belongs to ID, it sets GUTI_N^{ID} to UnSet and stores ID in b-auth$_N^j$. Then it generates a random challenge n^j, stores it in session$_N^{ID}$, and sends it to the *UE*, together with the xor of the sequence number SQN_N^{ID} with $f_{k^{ID}}(n^j)$, and a mac:

$$\langle n^j, \text{SQN}_N^{ID} \oplus f_{k^{ID}}(n^j), \mathsf{Mac}^3_{k_m^{ID}}(\langle n^j, \text{SQN}_N^{ID}, \text{GUTI}_N^{ID}\rangle)\rangle$$

When it receives this message, the *UE* retrieves the challenge n^j at the beginning of the message, computes $f_{k^{ID}}(n^j)$ and uses this value to unconceal the sequence number SQN_N^{ID}. It then computes $\mathsf{Mac}^3_{k_m^{ID}}(\langle n^j, \text{SQN}_N^{ID}, \text{GUTI}_U\rangle)$ and compares it to the mac received from the network. If the macs are not equal, or if the range check $\mathsf{range}(\text{SQN}_U, \text{SQN}_N^{ID})$ fails, it puts fail into b-auth$_U$ and e-auth$_U$ to record that the authentication was not successful. If both tests succeed, it stores in b-auth$_U$ and e-auth$_U$ the random challenge, increments SQN_U by one and sends the confirmation message $\mathsf{Mac}^4_{k_m^{ID}}(n^j)$. When receiving this message, the *HN* verifies that the mac is correct. If this is the case then the *HN* authenticated the *UE*, and stores ID into e-auth$_N^{ID}$. Then, *HN* checks whether session$_N^{ID}$ is still equal to the challenge n^j stored in it at the beginning of the session. If this is true, the *HN* increments SQN_N^{ID} by one, generates a fresh temporary identity GUTI^j and stores it into GUTI_N^{ID}.

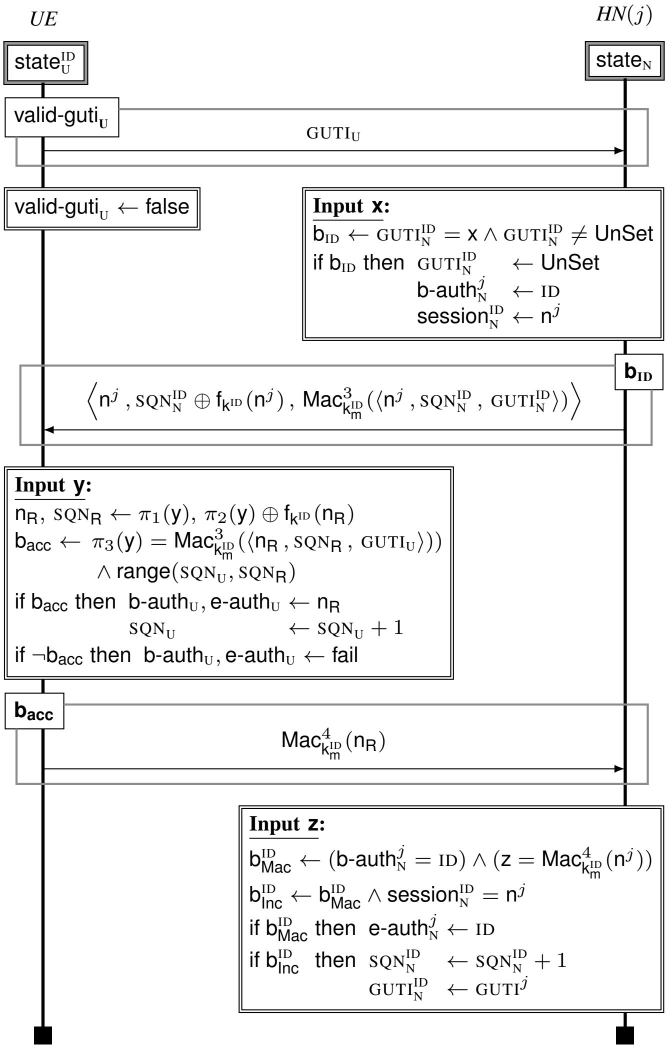


Fig. 7. The GUTI Sub-Protocol of the AKA$^+$ Protocol

c) The ASSIGN-GUTI *Sub-Protocol:* The ASSIGN-GUTI sub-protocol is run after a successful authentication, regardless of the authentication sub-protocol used. It assigns a fresh temporary identity to the *UE* to allow the next AKA$^+$ session to run the faster GUTI sub-protocol. It is depicted in Fig. 8.

The *HN* conceals the temporary identity GUTI^j generated by the authentication sub-protocol by xoring it with $\mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\text{ID}}}(\mathsf{n}^j)$, and macs it. When receiving this message, *UE* unconceals the temporary identity $\text{GUTI}^{\text{ID}}_{\text{N}}$ by xoring its first component with $\mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{e\text{-}auth}_{\text{U}})$ (since $\mathsf{e\text{-}auth}_{\text{U}}$ contains the *HN*'s challenge after authentication). Then *UE* checks that the mac is correct and that the authentication was successful. If it is the case, it stores $\text{GUTI}^{\text{ID}}_{\text{N}}$ in GUTI_{U} and sets $\mathsf{valid\text{-}guti}_{\text{U}}$ to true.

V. UNLINKABILITY

We now define the unlinkability property we use, which is inspired from [22] and Vaudenay's privacy [23].

a) Definition: The property is defined by a game in which an adversary tries to link together some subscriber's sessions. The adversary is a PPTM which interacts, through oracles, with N different subscribers with identities $\text{ID}_1, \ldots, \text{ID}_N$, and with the *HN*. The adversary cannot use a subscriber's permanent identity to refer to it, as it may not know it. Instead, we associate a virtual handler vh to any subscriber currently running a session of the protocol. We maintain a list l_{free} of all subscribers that are ready to start a session. We now describe the oracles $\mathcal{O}_b$:

- `StartSession()`: starts a new *HN* session and returns its session number j.
- `SendHN`(m, j) (resp. `SendUE`(m, vh)): sends the message m to *HN*(j) (resp. the *UE* associated with vh), and returns *HN*(j) (resp. vh) answer.
- `ResultHN`(j) (resp. `ResultUE`(vh)): returns true if *HN*(j) (resp. the *UE* associated with vh) has made a successful authentication.
- `DrawUE`$(\text{ID}_{i_0}, \text{ID}_{i_1})$: checks that ID_{i_0} and ID_{i_1} are both in l_{free}. If that is the case, returns a new virtual handler pointing to ID_{i_b}, depending on an internal secret bit b. Then, it removes ID_{i_0} and ID_{i_1} from l_{free}.
- `FreeUE`(vh): makes the virtual handler vh no longer valid, and adds back to l_{free} the two identities that were removed when the virtual handler was created.

We recall that a function is negligible if and only if it is asymptotically smaller than the inverse of any polynomial. An adversary $\mathcal{A}$ interacting with $\mathcal{O}_b$ is winning the q-unlinkability game if: $\mathcal{A}$ makes less than q calls to the oracles; and it can guess the value of the internal bit b with a probability better than $1/2$ by a non-negligible margin, i.e. if the following quantity is non negligible in η:

$$\left|2 \times \mathbf{Pr}\left(b : \mathcal{A}^{\mathcal{O}_b}(1^\eta) = b\right) - 1\right|$$

Finally, a protocol is q-unlinkable if and only if there are no winning adversaries against the q-unlinkability game.

b) Corruption: In [22], [23], the adversary is allowed to corrupt some tags using a `Corrupt` oracle. Several classes of adversary are defined by restricting its access to the corruption

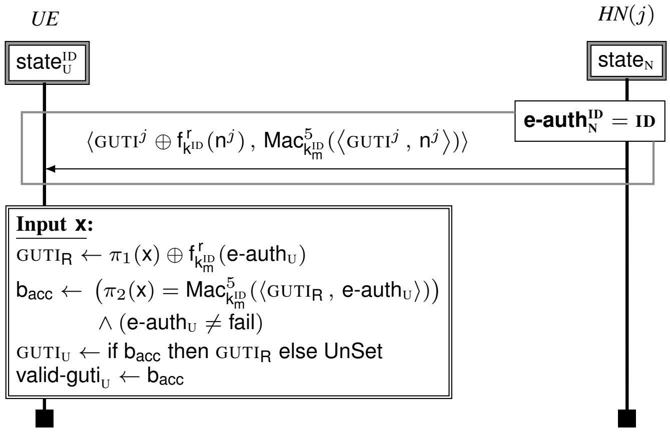


Fig. 8. The ASSIGN-GUTI Sub-Protocol of the AKA$^+$ Protocol

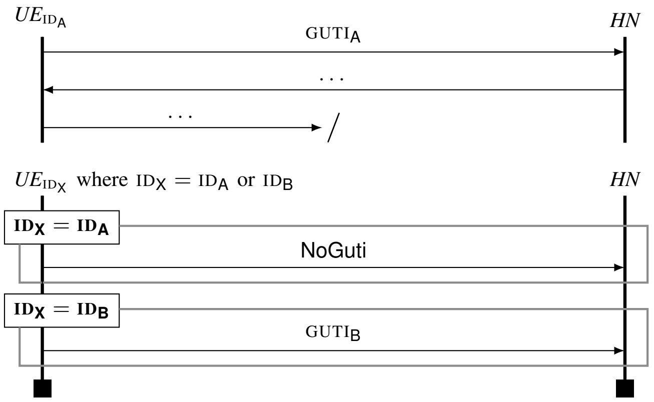


Fig. 9. Consecutive GUTI Sessions of AKA$^+$ Are Not Unlinkable.

oracle. A *strong* adversary has unrestricted access, a *destructive* adversary can no longer use a tag after corrupting it (it is destroyed), a *forward* adversary can only follow a `Corrupt` call by further `Corrupt` calls, and finally a *weak* adversary cannot use `Corrupt` at all. A protocol is $\mathcal{C}$ unlinkable if no adversary in $\mathcal{C}$ can win the unlinkability game. Clearly, we have the following relations:

$$\textit{strong} \Rightarrow \textit{destructive} \Rightarrow \textit{forward} \Rightarrow \textit{weak}$$

The 5G-AKA protocol does not provide forward secrecy: indeed, obtaining the long-term secret of a *UE* allows to decrypt all its past messages. By consequence, the best we can hope for is *weak* unlinkability. Since such adversaries cannot call `Corrupt`, we removed the oracle from our definition.

c) Wide Adversary: Note that the adversary knows if the protocol was successful or not using the `ResultUE` and `ResultHN` oracles (such an adversary is called *wide* in Vaudenay's terminology [23]). Indeed, in an authenticated key agreement protocol, this information is always available to the adversary: if the key exchange succeeds then it is followed by another protocol using the newly established key; while if it fails then either a new key-exchange session is initiated, or no message is sent. Hence the adversary knows if the key exchange was successful by passive monitoring.

A. σ-Unlinkability

In accord with our conjecture in Section III-E, the AKA$^+$ protocol is not unlinkable. Indeed, an adversary $\mathcal{A}$ can easily win the linkability game. First, $\mathcal{A}$ ensures that $\mathrm{ID_A}$ and $\mathrm{ID_B}$ have a valid temporary identity assigned: $\mathcal{A}$ calls $\mathtt{DrawUE}(\mathrm{ID_A}, \mathrm{ID_A})$ to obtain a virtual handler for $\mathrm{ID_A}$, and runs a SUPI and ASSIGN-GUTI sessions between $\mathrm{ID_A}$ and the *HN* with no interruptions. This assigns a temporary identity to $\mathrm{ID_A}$. We use the same procedure for $\mathrm{ID_B}$.

Then, $\mathcal{A}$ executes the attack described in Fig. 9. It starts a GUTI session with $\mathrm{ID_A}$, and intercepts the last message. At that point, $\mathrm{ID_A}$ no longer has a temporary identity, while $\mathrm{ID_B}$ still does. Then, it calls $\mathtt{DrawUE}(\mathrm{ID_A}, \mathrm{ID_B})$, which returns a virtual handler vh to $\mathrm{ID_A}$ or $\mathrm{ID_B}$. The attacker then start a

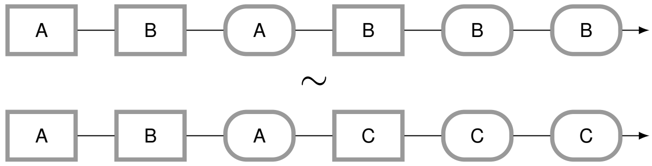


Fig. 10. Two indistinguishable executions. Square (resp. round) nodes are executions of the SUPI (resp. GUTI) sub-protocol. Each time the SUPI sub-protocol is used, we can change the subscriber's identity.

new GUTI session with vh. If vh is a handler for $\mathrm{ID_A}$, the *UE* returns NoGuti. If vh aliases $\mathrm{ID_B}$, the *UE* returns the temporary identity $\mathrm{GUTI_A}$. The adversary $\mathcal{A}$ can distinguish between these two cases, and therefore wins the game.

a) σ-unlinkability: To prevent this, we want to forbid `DrawUE` to be called on de-synchronized subscribers. We do this by modifying the state of the user chosen by `DrawUE`. We let σ be an update on the state of the subscribers. We then define the oracle $\mathtt{DrawUE}_\sigma(\mathrm{ID}_{i_0}, \mathrm{ID}_{i_1})$: it checks that $\mathrm{ID_A}$ and $\mathrm{ID_B}$ are both free, then *applies the update* σ to ID_{i_b}'s state, and returns a new virtual handler pointing to ID_{i_b}. The (q, σ)-unlinkability game is the q-unlinkability game in which we replace `DrawUE` with $\mathtt{DrawUE}_\sigma$. A protocol is (q, σ)-unlinkable if and only if there is no winning adversary against the (q, σ)-unlinkability game. Finally, a protocol is σ-unlinkable if it is (q, σ)-unlinkable for any q.

b) Application to AKA$^+$*:* The privacy guarantees given by the σ-unlinkability depend on the choice of σ. The idea is to choose a σ that allows to establish privacy in *some scenarios* of the standard unlinkability game[3].

We illustrate this on the AKA$^+$ protocol. Let $\sigma_{\mathsf{ul}} = \mathsf{valid\text{-}guti}_{\mathrm{U}} \mapsto \mathsf{false}$ be the function that makes the *UE*'s temporary identity not valid. This simulates the fact that the GUTI has been used and is no longer available. If the *UE*'s temporary identity is not valid, then it can only run the SUPI sub-protocol. Hence, if the AKA$^+$ protocol is σ_{ul}-unlinkable, then no adversary can distinguish between a normal execution and an execution where we change the identity of a subscriber each time it runs the SUPI sub-protocol. We give in Fig. 10 an example of such a scenario. We now state our main result:

Theorem 1. *The* AKA$^+$ *protocol is* σ_{ul}*-unlinkable for an arbitrary number of agents and sessions when the asymmetric encryption* $\{\_\}_{-}^{-}$ *is* IND-CCA1 *secure and* f *and* $\mathsf{f^r}$ *(resp.* Mac^1*–*Mac^5*) satisfy jointly the* PRF *assumption.*

This result is shown later in the paper. Still, the intuition is that no adversary can distinguish between two sessions of the SUPI protocol. Moreover, the SUPI protocol has two important properties. First, it re-synchronizes the user with the *HN*, which prevents the attacker from using any prior de-synchronization. Second, the AKA$^+$ protocol is designed in such a way that no message sent by the *UE* before a successful SUPI session can modify the *HN*'s state after the SUPI session.

[3]Remark that when σ is the empty state update, the σ-unlinkability and unlinkability properties coincide.

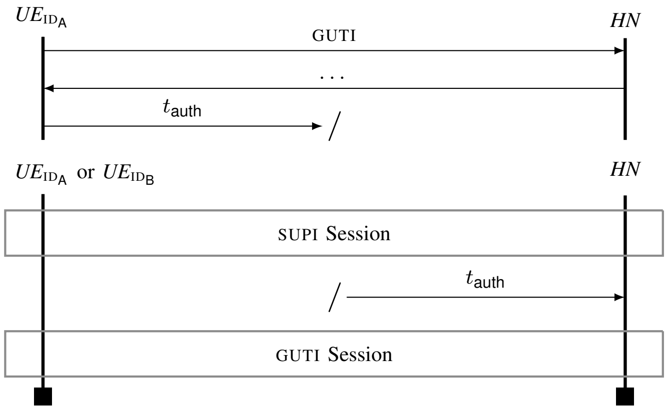


Fig. 11. A Subtle Attack Against The $\text{AKA}^{+}_{\textsf{no-inc}}$ Protocol

Therefore, any time the SUPI protocol is run, we get a "clean slate" and we can change the subscriber's identity. Note that we have a trade-off between efficiency and privacy: the SUPI protocol is more expensive to run, but provides more privacy.

B. A Subtle Attack

We now explain what is the role of $\mathsf{session}^{\text{ID}}_{\text{N}}$, and how it prevents a subtle attack against the σ_{ul}-unlinkability of AKA^{+}. We let $\text{AKA}^{+}_{\textsf{no-inc}}$ be the AKA^{+} protocol where we modify the GUTI sub-protocol we described in Fig. 7: in the state update of the *HN*'s last input, we remove the check $\mathsf{session}^{\text{ID}}_{\text{N}} = \mathsf{n}^j$ (i.e. $\mathsf{b}^{\text{ID}}_{\mathsf{Inc}} = \mathsf{b}^{\text{ID}}_{\mathsf{Mac}}$). The attack is described in Fig. 11.

First, we run a session of the GUTI sub-protocol between $UE_{\text{ID}_\mathsf{A}}$ and the *HN*, but we do not forward the last message t_{auth} to the *HN*. We then call $\texttt{DrawUE}_{\sigma_{\mathsf{ul}}}(\text{ID}_\mathsf{A}, \text{ID}_\mathsf{B})$, which returns a virtual handler vh to ID_A or ID_B. We run a full session using the SUPI sub-protocol with vh, and then send the message t_{auth} to the *HN*. We can check that, because we removed the condition $\mathsf{session}^{\text{ID}}_{\text{N}} = \mathsf{n}^j$ from $\mathsf{b}^{\text{ID}}_{\mathsf{Inc}}$, this message causes the *HN* to increment $\text{SQN}^{\text{ID}_\mathsf{A}}_{\text{N}}$ by one. At that point, $UE_{\text{ID}_\mathsf{A}}$ is desynchronized but $UE_{\text{ID}_\mathsf{B}}$ is synchronized. Finally, we run a session of the GUTI sub-protocol. The session has two possible outcomes: if vh aliases to A then it fails, while if vh aliases to B, it succeeds. This leads to an attack.

When we removed the condition $\mathsf{session}^{\text{ID}}_{\text{N}} = \mathsf{n}^j$, we broke the "clean slate" property of the SUPI sub-protocol: we can use a message from a session that started *before* the SUPI session to modify the state *after* the SUPI session. $\mathsf{session}^{\text{ID}}_{\text{N}}$ allows to detect whether another session has been executed since the current session started, and to prevent the update of the sequence number when this is the case.

VI. Modeling in The Bana-Comon Logic

We prove Theorem 1 using the Bana-Comon model introduced in [18]. This is a first order logic, in which protocol messages are represented by terms using special function symbols for the adversary's inputs. It has only one predicate, $\sim$, which represents computational indistinguishability. To use this model, we first build a set of axioms Ax specifying what the adversary *cannot* do. This set of axiom comprises computationally valid properties, cryptographic hypotheses and implementation assumptions. Then, given a protocol and a security property, we compute a formula ϕ expressing the protocol security. Finally, we show that the security property ϕ can be deduced from the axioms Ax. If this is the case, this entails *computational security*.

A. Syntax and Semantics

We quickly recall the syntax and semantics of the logic.

a) Terms: Terms are built using function symbols in $\mathcal{F}$, names in $\mathcal{N}$ (representing random samplings) and variables in $\mathcal{X}$. The set $\mathcal{F}$ of function symbols contains a countable set of *adversarial* function symbols $\mathcal{G}$, which represent the adversary inputs, and protocol function symbols. The protocol function symbols are the functions used in the protocol, e.g. the pair $\langle \_\, , \_ \rangle$, the i-th projection π_i, encryption $\{\_\}^{\_}_{\_}$, decryption $\mathsf{dec}(\_, \_)$, $\mathsf{if\_then\_else\_}$, true, false, equality $\mathsf{eq}(\_, \_)$, integer greater or equal $\mathsf{geq}(\_, \_)$ and length $\mathsf{len}(\_)$.

b) Formulas: For every integer n, we have one predicate symbol $\sim_n$ of arity $2n$, which represents equivalence between two vectors of terms of length n. We use an infix notation for $\sim_n$, and omit n when not relevant. Formulas are built using the usual Boolean connectives and first-order quantifiers.

c) Semantics: We use the classical semantics of first-order logic. Given an interpretation domain, we interpret terms, function symbols and predicates as, respectively, elements, functions and relations of this domain.

We focus on a particular class of models, called the *computational models* (see [18] for a formal definition). In a computational model $\mathcal{M}_c$, terms are interpreted in the set of PPTMs equipped with a working tape and two random tapes ρ_1, ρ_2. The tape ρ_1 is used for the protocol random values, while ρ_2 is for the adversary's random samplings. The adversary cannot access directly the random tape ρ_1, although it may obtain part of ρ_1 through the protocol messages. A key feature is to let the interpretation of an adversarial function g be *any* PPTM, which soundly models an attacker *arbitrary probabilistic polynomial time computation*. Moreover, the predicates $\sim_n$ are interpreted using *computational indistinguishability* $\approx$. Two families of distributions of bit-string sequences $(m_\eta)_\eta$ and $(m'_\eta)_\eta$, indexed by η, are indistinguishable iff for every PPTM $\mathcal{A}$ with random tape ρ_2, the following quantity is negligible in η:

$$\big|\,\mathbf{Pr}(\rho_1, \rho_2 :\ \mathcal{A}(m_\eta(\rho_1, \rho_2), \rho_2) = 1) - \mathbf{Pr}(\rho_1, \rho_2 :\ \mathcal{A}(m'_\eta(\rho_1, \rho_2), \rho_2) = 1)\,\big|$$

B. Modeling of the AKA^{+} Protocol States and Messages

We now use the Bana-Comon logic to model the σ_{ul}-unlinkability of the AKA^{+} protocol. We consider a setting with N identities $\text{ID}_1, \dots, \text{ID}_N$, and we let $\mathcal{S}_{\mathsf{id}}$ be the set of all identities. To improve readability, protocol descriptions often omit some details. For example, in Section IV we sometimes omitted the description of the error messages. The failure message attack of [4] demonstrates that such details may be crucial for security. An advantage of the Bana-Comon model is that it requires us to fully formalize the protocol, and to make all assumptions explicit.

a) Symbolic State: For every identity $\text{ID} \in \mathcal{S}_{\mathsf{id}}$, we use several variables to represent UE_{ID}'s state. E.g., $\text{SQN}_{\text{U}}^{\text{ID}}$ and $\text{GUTI}_{\text{U}}^{\text{ID}}$ store, respectively, UE_{ID}'s sequence number and temporary identity. Similarly, we have variables for *HN*'s state, e.g. $\text{SQN}_{\text{N}}^{\text{ID}}$. We let $\mathcal{S}_{\mathsf{var}}$ be the set of variables used in AKA^+:

$$\bigcup_{\substack{j\in\mathbb{N},\text{A}\in\{\text{U},\text{N}\}\\ \text{ID}\in\mathcal{S}_{\mathsf{id}}}} \left\{ \begin{array}{l} \text{SQN}_{\text{A}}^{\text{ID}}, \text{GUTI}_{\text{A}}^{\text{ID}}, \mathsf{e\text{-}auth}_{\text{U}}^{\text{ID}}, \mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}}, \mathsf{e\text{-}auth}_{\text{N}}^{j} \\ \mathsf{b\text{-}auth}_{\text{N}}^{j}, \mathsf{s\text{-}valid\text{-}guti}_{\text{U}}^{\text{ID}}, \mathsf{valid\text{-}guti}_{\text{U}}^{\text{ID}}, \mathsf{session}_{\text{N}}^{\text{ID}} \end{array} \right\}$$

A symbolic state σ is a mapping from $\mathcal{S}_{\mathsf{var}}$ to terms. Intuitively, $\sigma(\mathsf{x})$ is a term representing (the distribution of) the value of x.

Example 1. To avoid confusion with the *semantic* equality $=$, we use $\equiv$ to denote *syntactic* equality. Then, we can express the fact that $\text{GUTI}_{\text{U}}^{\text{ID}}$ is unset in a symbolic state σ by having $\sigma(\text{GUTI}_{\text{U}}^{\text{ID}}) \equiv \mathsf{UnSet}$. Also, given a state σ, we can state that σ' is the state σ in which we incremented $\text{SQN}_{\text{U}}^{\text{ID}}$ by having $\sigma'(\mathsf{x})$ be the term $\sigma(\text{SQN}_{\text{U}}^{\text{ID}}) + 1$ if x is $\text{SQN}_{\text{U}}^{\text{ID}}$, and $\sigma(\mathsf{x})$ otherwise.

b) Symbolic Traces: We explain how to express $(q, \sigma_{\mathsf{ul}})$-unlinkability in the BC model. In the $(q, \sigma_{\mathsf{ul}})$-unlinkability game, the adversary chooses dynamically which oracle it wants to call. This is not convenient to use in proofs, as we do not know statically the i-th action of the adversary. We prefer an alternative point-of-view, in which the trace of oracle calls is fixed (w.l.o.g., as shown later in Proposition 1). Then, there are no winning adversaries against the σ_{ul}-unlinkability game with a fixed trace of oracle calls if the adversary's interactions with the oracles when $b = 0$ are indistinguishable from the interactions with the oracles when $b = 1$.

We use the following action identifiers to represent symbolic calls to the oracle of the $(q, \sigma_{\mathsf{ul}})$-unlinkability game:

- $\text{NS}_{\text{ID}}(j)$ represents a call to $\mathtt{DrawUE}_{\sigma_{\mathsf{ul}}}(\text{ID}, \_)$ when $b = 0$ or $\mathtt{DrawUE}_{\sigma_{\mathsf{ul}}}(\_, \text{ID})$ when $b = 1$.
- $\text{PU}_{\text{ID}}(j, i)$ (resp. $\text{TU}_{\text{ID}}(j, i)$) is the i-th user message in the session $UE_{\text{ID}}(j)$ of the SUPI (resp. GUTI) sub-protocol.
- $\text{FU}_{\text{ID}}(j)$ is the only user message in the session $UE_{\text{ID}}(j)$ of the ASSIGN-GUTI sub-protocol.
- $\text{PN}(j, i)$ (resp. $\text{TN}(j, i)$) is the i-th network message in the session $HN(j)$ of the SUPI (resp. GUTI) sub-protocol.
- $\text{FN}(j)$ is the only network message in the session $HN(j)$ of the ASSIGN-GUTI sub-protocol.

The remaining oracle calls either have no outputs and do not modify the state (e.g. `StartSession`), or can be simulated using the oracles above. E.g., since the *HN* sends an error message whenever the protocol is not successful, the output of `ResultHN` can be deduced from the protocol messages.

A *symbolic trace* τ is a finite sequence of action identifiers. We associate, to any execution of the $(q, \sigma_{\mathsf{ul}})$-unlinkability game with a fixed trace of oracle calls, a pair of symbolic traces (τ_l, τ_r), which corresponds to the adversary's interactions with the oracles when b is, respectively, 0 and 1. We let $\mathcal{R}_{\mathsf{ul}}$ be the set of such pairs of traces.

Example 2. We give the symbolic traces corresponding to the honest execution of AKA^+ between $UE_{\text{ID}}(i)$ and $HN(j)$. If the SUPI protocol is used, we have the trace $\tau_{\text{SUPI}}^{i,j}(\text{ID})$:

$$\text{PU}_{\text{ID}}(i, 0),\ \text{PN}(j, 0), \text{PU}_{\text{ID}}(i, 1), \text{PN}(j, 1), \text{PU}_{\text{ID}}(i, 2), \text{FN}(j), \text{FU}_{\text{ID}}(i)$$

And if the GUTI sub-protocol is used, the trace $\tau_{\text{GUTI}}^{i,j}(\text{ID})$:

$$\text{TU}_{\text{ID}}(i, 0), \text{TN}(j, 0), \text{TU}_{\text{ID}}(i, 1), \text{TN}(j, 1), \text{FN}(j), \text{FU}_{\text{ID}}(i)$$

Which such notations, the left trace τ_l of the attack described in Fig. 11, in which the adversary only interacts with A, is:

$$\text{TU}_{\mathsf{A}}(0, 0), \text{TN}(0, 0), \text{TU}_{\mathsf{A}}(0, 1), \tau_{\text{SUPI}}^{1,1}(\mathsf{A}), \text{TN}(0, 1), \tau_{\text{GUTI}}^{2,2}(\mathsf{A})$$

Similarly, we can give the right trace τ_r in which the adversary interacts with A and B:

$$\text{TU}_{\mathsf{A}}(0, 0), \text{TN}(0, 0), \text{TU}_{\mathsf{A}}(0, 1), \tau_{\text{SUPI}}^{0,1}(\mathsf{B}), \text{TN}(0, 1), \tau_{\text{GUTI}}^{1,2}(\mathsf{B})$$

c) Symbolic Messages: We define, for every action identifier ai, the term representing the output observed by the adversary when ai is executed. Since the protocol is stateful, this term is a function of the prefix trace of actions executed since the beginning. We define by mutual induction, for any symbolic trace $\tau = \tau_0, \mathsf{ai}$ whose last action is ai:

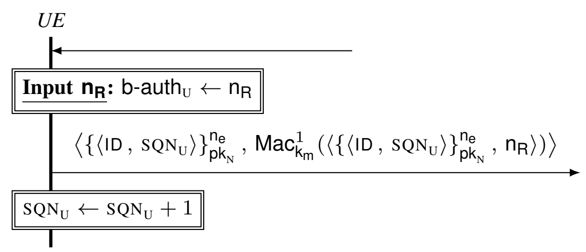
- The term t_τ representing the last message observed during the execution of τ.
- The symbolic state σ_τ representing the state after the execution of τ.
- The frame ϕ_τ representing the sequence of all messages observed during the execution of τ.

Some syntactic sugar: we let $\sigma_\tau^{\mathsf{in}} = \sigma_{\tau_0}$ be the symbolic state before the execution of the last action; and $\phi_\tau^{\mathsf{in}} = \phi_{\tau_0}$ be the sequence of all messages observed during the execution of τ, except for the last message.

The frame ϕ_τ is simply the frame ϕ_τ^{in} extended with t_τ, i.e. $\phi_\tau \equiv \phi_\tau^{\mathsf{in}}, t_\tau$. Moreover the initial frame contains only pk_{N}, i.e. $\phi_\epsilon \equiv \mathsf{pk}_{\text{N}}$. When executing an action ai, only a subset of the symbolic state is modified. For example, if the adversary interacts with UE_{ID} then the state of the *HN* and of all the other users is unchanged. Therefore instead of defining σ_τ, we define the *symbolic state update* $\sigma_\tau^{\mathsf{up}}$, which is a *partial* function from $\mathcal{S}_{\mathsf{var}}$ to terms. Then σ_τ is the function:

$$\sigma_\tau(\mathsf{x}) \equiv \begin{cases} \sigma_\tau^{\mathsf{in}}(\mathsf{x}) & \text{if } \mathsf{x} \notin \mathsf{dom}(\sigma_\tau^{\mathsf{up}}) \\ \sigma_\tau^{\mathsf{up}}(\mathsf{x}) & \text{if } \mathsf{x} \in \mathsf{dom}(\sigma_\tau^{\mathsf{up}}) \end{cases}$$

where dom gives the domain of a function. Now, for every action ai, we define t_τ and $\sigma_\tau^{\mathsf{up}}$ using ϕ_τ^{in} and $\sigma_\tau^{\mathsf{in}}$. As an example, we describe the second message and state update of the session $UE_{\text{ID}}(j)$ for the SUPI sub-protocol, which corresponds to the action $\text{PU}_{\text{ID}}(j, 1)$. We recall the relevant part of Fig. 6:



First, we need a term representing the value inputted by UE_{ID} from the network. As we have an active adversary, this value can be anything that the adversary can compute using the knowledge it accumulated since the beginning of the protocol. The knowledge of the adversary, or the frame, is the sequence of all messages observed during the execution of τ, except for the last message. This is exactly ϕ_τ^{in}. Finally, we use a special function symbol $g \in \mathcal{G}$ to represent the arbitrary polynomial time computation done by the adversary. This yields the term $g(\phi_\tau^{\mathsf{in}})$, which symbolically represents the input.

We now need to build a term representing the asymmetric encryption of the pair containing the *UE*'s permanent identity ID and its sequence number. The permanent identity ID is simply represented using a constant function symbol ID (we omit the parenthesis ()). UE_{ID}'s sequence number is stored in the variable $\text{SQN}_{\text{U}}^{\text{ID}}$. To retrieve its value, we just do a look-up in the symbolic state $\sigma_\tau^{\mathsf{in}}$, which yields $\sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})$. Finally, we use the asymmetric encryption function symbol to build the term $t_\tau^{\mathsf{enc}} \equiv \{\langle \text{ID}\,,\, \sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}$. Notice that the encryption is randomized using a nonce $\mathsf{n}_{\mathsf{e}}^{j}$, and that the freshness of the randomness is guaranteed by indexing the nonce with the session number j. Finally, we can give t_τ and $\sigma_\tau^{\mathsf{up}}$:

$$t_\tau \equiv \langle t_\tau^{\mathsf{enc}}\,,\, \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}(\langle t_\tau^{\mathsf{enc}}\,,\, g(\phi_\tau^{\mathsf{in}})\rangle)\rangle$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \text{SQN}_{\text{U}}^{\text{ID}} \mapsto \mathsf{suc}(\sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})) & \mathsf{e\text{-}auth}_{\text{U}}^{\text{ID}} \mapsto \mathsf{fail} \\ \mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}} \mapsto g(\phi_\tau^{\mathsf{in}}) & \text{GUTI}_{\text{U}}^{\text{ID}} \mapsto \mathsf{UnSet} \\ \mathsf{valid\text{-}guti}_{\text{U}}^{\text{ID}} \mapsto \mathsf{false} & \end{cases}$$

Remark that we omitted some state updates in the description of the protocol in Fig. 6. For example, UE_{ID} temporary identity $\text{GUTI}_{\text{U}}^{\text{ID}}$ is reset when starting the SUPI sub-protocol. In the BC model, these details are made explicit.

The description of t_τ and $\sigma_\tau^{\mathsf{up}}$ for the other actions can be found in Fig. 12 and Fig. 13. Observe that we describe one more message for the SUPI and GUTI protocols than in Section IV . This is because we add one message ($\text{PU}_{\text{ID}}(j, 2)$ for SUPI and $\text{TN}(j, 1)$ for GUTI) for proof purposes, to simulate the `ResultUE` and `ResultHN` oracles. Also, notice that in the GUTI protocol, when *HN* receives a GUTI that is not assigned to anybody, it sends a decoy message to a special dummy identity ID_{dum}.

The following soundness theorem states that security in the BC model implies computationally security:

Proposition 1. *The* AKA^+ *protocol is* σ_{ul}*-unlinkable in any computational model satisfying the axioms* Ax *if, for every* $(\tau_l, \tau_r) \in \mathcal{R}_{ul}$*, we can derive* $\phi_{\tau_l} \sim \phi_{\tau_r}$ *using* Ax*.*

The proof of this result is basically the proof that Fixed Trace Privacy implies Bounded Session Privacy in [26]. We omit the details.

C. Axioms

Using Proposition 1, we know that to prove Theorem 1 we need to derive $\phi_{\tau_l} \sim \phi_{\tau_r}$, for every $(\tau_l, \tau_r) \in \mathcal{R}_{\mathsf{ul}}$, using a set of inference rules Ax. Moreover, we need the axioms Ax to be valid in any computational model where the asymmetric encryption $\{\_\}_{\_}^{\_}$ is IND-CCA1 secure and f and f^{r} (resp. Mac^1–Mac^5) satisfy jointly the PRF assumption.

<u>**Case** $\mathsf{ai} = \text{PU}_{\text{ID}}(j, 0)$.</u> $t_\tau \equiv$ Request_Challenge

<u>**Case** $\mathsf{ai} = \text{PN}(j, 0)$.</u> $t_\tau \equiv \mathsf{n}^j$

<u>**Case** $\mathsf{ai} = \text{PU}_{\text{ID}}(j, 1)$.</u> Let $t_\tau^{\mathsf{enc}} \equiv \{\langle \text{ID}\,,\, \sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}}$, then:

$$t_\tau \equiv \langle t_\tau^{\mathsf{enc}}\,,\, \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}(\langle t_\tau^{\mathsf{enc}}\,,\, g(\phi_\tau^{\mathsf{in}})\rangle)\rangle$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \text{SQN}_{\text{U}}^{\text{ID}} \mapsto \mathsf{suc}(\sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})) & \mathsf{e\text{-}auth}_{\text{U}}^{\text{ID}} \mapsto \mathsf{fail} \\ \mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}} \mapsto g(\phi_\tau^{\mathsf{in}}) & \text{GUTI}_{\text{U}}^{\text{ID}} \mapsto \mathsf{UnSet} \\ \mathsf{valid\text{-}guti}_{\text{U}}^{\text{ID}} \mapsto \mathsf{false} & \end{cases}$$

<u>**Case** $\mathsf{ai} = \text{PN}(j, 1)$.</u> Let $t_{\mathsf{dec}} \equiv \mathsf{dec}(\pi_1(g(\phi_\tau^{\mathsf{in}})), \mathsf{sk}_{\text{N}})$, and let:

$$\begin{aligned} \mathsf{accept}_\tau^{\text{ID}_i} &\equiv \mathsf{eq}(\pi_2(g(\phi_\tau^{\mathsf{in}})), \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\text{ID}_i}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}}))\,,\, \mathsf{n}^j\rangle)) \\ &\qquad \wedge\ \mathsf{eq}(\pi_1(t_{\mathsf{dec}}), \text{ID}_i) \\ \mathsf{inc\text{-}accept}_\tau^{\text{ID}_i} &\equiv \mathsf{accept}_\tau^{\text{ID}_i} \wedge \mathsf{geq}(\pi_2(t_{\mathsf{dec}}), \sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}_i})) \\ t_\tau &\equiv \mathsf{if}\ \mathsf{accept}_\tau^{\text{ID}_1}\ \mathsf{then}\ \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\text{ID}_1}}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\pi_2(t_{\mathsf{dec}}))\rangle) \\ &\qquad \mathsf{else\ if}\ \mathsf{accept}_\tau^{\text{ID}_2}\ \mathsf{then}\ \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\text{ID}_2}}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\pi_2(t_{\mathsf{dec}}))\rangle) \\ &\qquad \dots \\ &\qquad \mathsf{else\ UnknownId} \end{aligned}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \mathsf{session}_{\text{N}}^{\text{ID}_i} \mapsto \mathsf{if\ inc\text{-}accept}_\tau^{\text{ID}_i}\ \mathsf{then}\ \mathsf{n}^j\ \mathsf{else}\ \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\text{N}}^{\text{ID}_i}) \\ \text{GUTI}_{\text{N}}^{\text{ID}_i} \mapsto \mathsf{if\ inc\text{-}accept}_\tau^{\text{ID}}\ \mathsf{then}\ \text{GUTI}^j\ \mathsf{else}\ \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}_i}) \\ \text{SQN}_{\text{N}}^{\text{ID}_i} \mapsto \mathsf{if\ inc\text{-}accept}_\tau^{\text{ID}_i}\ \mathsf{then}\ \mathsf{suc}(\pi_2(t_{\mathsf{dec}}))\ \mathsf{else}\ \sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}_i}) \\ \mathsf{b\text{-}auth}_{\text{N}}^{j}, \mathsf{e\text{-}auth}_{\text{N}}^{j} \mapsto \mathsf{if}\ \mathsf{accept}_\tau^{\text{ID}_1}\ \mathsf{then}\ \text{ID}_1 \\ \qquad \mathsf{else\ if}\ \mathsf{accept}_\tau^{\text{ID}_2}\ \mathsf{then}\ \text{ID}_2 \\ \qquad \dots \\ \qquad \mathsf{else\ UnknownId} \end{cases}$$

<u>**Case** $\mathsf{ai} = \text{PU}_{\text{ID}}(j, 2)$.</u>

$$\begin{aligned} \mathsf{accept}_\tau^{\text{ID}} &\equiv \mathsf{eq}(g(\phi_\tau^{\mathsf{in}}), \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}(\langle \sigma_\tau^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}})\,,\, \sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle)) \\ t_\tau &\equiv \mathsf{if}\ \mathsf{accept}_\tau^{\text{ID}}\ \mathsf{then\ ok\ else\ error} \\ \sigma_\tau^{\mathsf{up}} &\equiv \mathsf{e\text{-}auth}_{\text{U}}^{\text{ID}} \mapsto \mathsf{if}\ \mathsf{accept}_\tau^{\text{ID}}\ \mathsf{then}\ \sigma_\tau^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}})\ \mathsf{else\ fail} \end{aligned}$$

Fig. 12. The Symbolic Terms and State Updates for the SUPI Sub-Protocol.

Remark that the AKA^+ protocol described in Section IV is under-specified. E.g., we never specified how the $\langle \_\,,\, \_\rangle$ function should be implemented. Instead of giving a complex specification of the protocol, we are going to put requirements on AKA^+ implementations through the set of axioms Ax. Then, if we can derive $\phi_{\tau_l} \sim \phi_{\tau_r}$ using Ax for every $(\tau_l, \tau_r) \in \mathcal{R}_{\mathsf{ul}}$, we know that any implementation of AKA^+ satisfying the axioms Ax is secure.

Our axioms are of two kinds. First, we have *structural axioms*, which are properties that are valid in any computational model. For example, we have axioms stating that $\sim$ is an equivalence relation. Second, we have *implementation axioms*, which reflect implementation assumptions on the protocol functions. For example, we can declare that different identity symbols are never equal by having an axiom $\mathsf{eq}(\text{ID}_1, \text{ID}_2) \sim \mathsf{false}$ for every $\text{ID}_1 \not\equiv \text{ID}_2$. For space reasons, we only describe a few of them here (the full set of axioms Ax is given in Appendix I).

a) Equality Axioms: If $\mathsf{eq}(s, t) \sim \mathsf{true}$ holds in any computational model then we know that the interpretations of s and t are always equal except for a negligible number of samplings. Let $s \doteq t$ be a shorthand for $\mathsf{eq}(s, t) \sim \mathsf{true}$.

Case ai $=$ NS$_{\text{ID}}(j)$. $\sigma_\tau^{\mathsf{up}} \equiv$ valid-guti$_{\text{U}}^{\text{ID}} \mapsto$ false

Case ai $=$ TU$_{\text{ID}}(j,0)$.

$$t_\tau \equiv \text{if } \sigma_\tau^{\mathsf{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}}) \text{ then } \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) \text{ else NoGuti}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \text{valid-guti}_{\text{U}}^{\text{ID}} \mapsto \text{false} & \text{e-auth}_{\text{U}}^{\text{ID}} \mapsto \text{fail} \\ \text{s-valid-guti}_{\text{U}}^{\text{ID}} \mapsto \sigma_\tau^{\mathsf{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}}) & \text{b-auth}_{\text{U}}^{\text{ID}} \mapsto \text{fail} \end{cases}$$

Case ai $=$ TN$(j,0)$. Let $t_\oplus^{\text{ID}_i} \equiv \sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}_i}) \oplus \mathsf{f}_{\mathsf{k}^{\text{ID}_i}}(\mathsf{n}^j)$, then:

$$\text{msg}_\tau^{\text{ID}_i} \equiv \langle \mathsf{n}^j, t_\oplus^{\text{ID}_i}, \mathsf{Mac}^3_{\mathsf{k}_\mathsf{m}^{\text{ID}_i}}(\langle \mathsf{n}^j, \sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}_i}), \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}_i})\rangle)\rangle$$

$$\text{accept}_\tau^{\text{ID}_i} \equiv \mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}_i}), g(\phi_\tau^{\mathsf{in}})) \wedge \neg\mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}_i}), \text{UnSet})$$

$$\begin{aligned} t_\tau \equiv\ & \text{if accept}_\tau^{\text{ID}_1} \text{ then msg}_\tau^{\text{ID}_1} \\ & \text{else if accept}_\tau^{\text{ID}_2} \text{ then msg}_\tau^{\text{ID}_2} \\ & \quad \cdots \\ & \text{else msg}_\tau^{\text{ID}_{\text{dum}}} \end{aligned}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \text{GUTI}_{\text{N}}^{\text{ID}_i} \mapsto \text{if accept}_\tau^{\text{ID}_i} \text{ then UnSet else } \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}_i}) \\ \text{session}_{\text{N}}^{\text{ID}_i} \mapsto \text{if accept}_\tau^{\text{ID}_i} \text{ then } \mathsf{n}^j \text{ else } \sigma_\tau^{\mathsf{in}}(\text{session}_{\text{N}}^{\text{ID}_i}) \\ \text{b-auth}_{\text{N}}^j \mapsto \text{if accept}_\tau^{\text{ID}_1} \text{ then ID}_1 \\ \qquad\qquad \text{else if accept}_\tau^{\text{ID}_2} \text{ then ID}_2 \\ \qquad\qquad \cdots \\ \qquad\qquad \text{else UnknownId} \end{cases}$$

Case ai $=$ TU$_{\text{ID}}(j,1)$. Let $t_{\text{SQN}} \equiv \pi_2(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f}_{\mathsf{k}^{\text{ID}}}(\pi_1(g(\phi_\tau^{\mathsf{in}})))$, then:

$$\begin{aligned} \text{accept}_\tau^{\text{ID}} \equiv\ & \mathsf{eq}(\pi_3(g(\phi_\tau^{\mathsf{in}})), \mathsf{Mac}^3_{\mathsf{k}_\mathsf{m}^{\text{ID}}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}})), t_{\text{SQN}}, \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})\rangle)) \\ & \wedge\ \sigma_\tau^{\mathsf{in}}(\text{s-valid-guti}_{\text{U}}^{\text{ID}}) \ \wedge\ \text{range}(\sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}}), t_{\text{SQN}}) \end{aligned}$$

$$t_\tau \equiv \text{if accept}_\tau^{\text{ID}} \text{ then } \mathsf{Mac}^4_{\mathsf{k}_\mathsf{m}^{\text{ID}}}(\pi_1(g(\phi_\tau^{\mathsf{in}}))) \text{ else error}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \text{b-auth}_{\text{U}}^{\text{ID}}, \text{e-auth}_{\text{U}}^{\text{ID}} \mapsto \text{if accept}_\tau^{\text{ID}} \text{ then } \pi_1(g(\phi_\tau^{\mathsf{in}})) \text{ else fail} \\ \text{SQN}_{\text{U}}^{\text{ID}} \mapsto \text{if accept}_\tau^{\text{ID}} \text{ then suc}(\sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})) \text{ else } \sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}}) \end{cases}$$

Case ai $=$ TN$(j,1)$.

$$\text{accept}_\tau^{\text{ID}_i} \equiv \mathsf{eq}(g(\phi_\tau^{\mathsf{in}}), \mathsf{Mac}^4_{\mathsf{k}_\mathsf{m}^{\text{ID}_i}}(\mathsf{n}^j)) \wedge \mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\text{b-auth}_{\text{N}}^j), \text{ID}_i)$$

$$\text{inc-accept}_\tau^{\text{ID}_i} \equiv \text{accept}_\tau^{\text{ID}_i} \wedge \mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\text{session}_{\text{N}}^{\text{ID}_i}), \mathsf{n}^j)$$

$$t_\tau \equiv \text{if } \textstyle\bigvee_i \text{accept}_\tau^{\text{ID}_i} \text{ then ok else error}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \text{SQN}_{\text{N}}^{\text{ID}_i} \mapsto \text{if inc-accept}_\tau^{\text{ID}_i} \text{ then suc}(\sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}_i})) \\ \qquad\qquad\qquad \text{else } \sigma_\tau^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}_i}) \\ \text{GUTI}_{\text{N}}^{\text{ID}_i} \mapsto \text{if inc-accept}_\tau^{\text{ID}_i} \text{ then GUTI}^j \text{ else } \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}_i}) \\ \text{e-auth}_{\text{N}}^j \mapsto \text{if accept}_\tau^{\text{ID}_1} \text{ then ID}_1 \\ \qquad\qquad \text{else if accept}_\tau^{\text{ID}_2} \text{ then ID}_2 \\ \qquad\qquad \cdots \\ \qquad\qquad \text{else UnknownId} \end{cases}$$

Case ai $=$ FN(j).

$$\text{msg}_\tau^{\text{ID}_i} \equiv \langle \text{GUTI}^j \oplus \mathsf{f}^\mathsf{r}_{\mathsf{k}^{\text{ID}_i}}(\mathsf{n}^j), \mathsf{Mac}^5_{\mathsf{k}_\mathsf{m}^{\text{ID}_i}}(\langle \text{GUTI}^j, \mathsf{n}^j\rangle)\rangle$$

$$\begin{aligned} t_\tau \equiv\ & \text{if } \mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\text{N}}^j), \text{ID}_1) \text{ then msg}_\tau^{\text{ID}_1} \\ & \text{else if } \mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\text{N}}^j), \text{ID}_2) \text{ then msg}_\tau^{\text{ID}_2} \\ & \quad \cdots \\ & \text{else UnknownId} \end{aligned}$$

Case ai $=$ FU$_{\text{ID}}(j)$. Let $t_{\text{GUTI}} \equiv \pi_1(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f}^\mathsf{r}_{\mathsf{k}^{\text{ID}}}(\sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\text{U}}^{\text{ID}}))$, then:

$$\begin{aligned} \text{accept}_\tau^{\text{ID}} \equiv\ & \mathsf{eq}(\pi_2(g(\phi_\tau^{\mathsf{in}})), \mathsf{Mac}^5_{\mathsf{k}_\mathsf{m}^{\text{ID}}}(\langle t_{\text{GUTI}}, \sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\text{U}}^{\text{ID}})\rangle)) \\ & \wedge\ \neg\mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\text{U}}^{\text{ID}}), \text{fail}) \ \wedge\ \neg\mathsf{eq}(\sigma_\tau^{\mathsf{in}}(\text{e-auth}_{\text{U}}^{\text{ID}}), \bot) \end{aligned}$$

$$t_\tau \equiv \text{if accept}_\tau^{\text{ID}} \text{ then ok else error}$$

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \text{valid-guti}_{\text{U}}^{\text{ID}} \mapsto \text{accept}_\tau^{\text{ID}} \\ \text{GUTI}_{\text{U}}^{\text{ID}} \mapsto \text{if accept}_\tau^{\text{ID}} \text{ then } t_{\text{GUTI}} \text{ else UnSet} \end{cases}$$

Fig. 13. The Symbolic Terms and State Updates for NS$_{\text{ID}}(j)$ and the GUTI and ASSIGN-GUTI Sub-Protocols.

We use $\doteq$ to specify functional correctness properties of the protocol function symbols. For example, the following rules state that the i-th projection of a pair is the i-th element of the pair, and that the decryption with the correct key of a cipher-text is equal to the message in plain-text:

$$\frac{}{\pi_i(\langle x_1, x_2\rangle) \doteq x_i} \quad \text{for } i \in \{1,2\} \qquad \frac{}{\mathsf{dec}(\{x\}^z_{\mathsf{pk}(y)}, \mathsf{sk}(y)) \doteq x}$$

b) Structural Axioms: Structural axioms are axioms which are valid in any computational model, e.g.:

$$\frac{\vec{u}_1, \vec{v}_1 \sim \vec{u}_2, \vec{v}_2}{f(\vec{u}_1), \vec{v}_1 \sim f(\vec{u}_2), \vec{v}_2}\ \mathsf{FA} \qquad \frac{\vec{u}, t \sim \vec{v} \quad s \doteq t}{\vec{u}, s \sim \vec{v}}\ R$$

The axiom FA states that to show that two function applications are indistinguishable, it is sufficient to show that their arguments are indistinguishable. The axiom R states that if $s \doteq t$ holds then we can safely replace s by t.

c) Cryptographic Assumptions: We now explain how cryptographic assumptions are translated into axioms. We illustrate this on the unforgeability property of the functions Mac^1–Mac^5. Recall that UE_{ID} uses the same secret key $\mathsf{k}_\mathsf{m}^{\text{ID}}$ for these five functions. Therefore, instead of the standard PRF assumption, we assume that these functions are *jointly* PRF, i.e. Mac^1–Mac^5 are *simultaneously* computationally indistinguishable from random functions.

It is well-known that if H is a PRF then H is unforgeable against an adversary with oracle access to $H(\cdot, \mathsf{k_m})$. Similarly, we can show that if $H, H_1, \dots, H_l$ are jointly PRF, then no adversary can forge a mac of $H(\cdot, \mathsf{k_m})$, even if it has oracle access to $H(\cdot, \mathsf{k_m}), H_1(\cdot, \mathsf{k_m}), \dots, H_l(\cdot, \mathsf{k_m})$. We translate this property as follows: let s, m be ground terms where $\mathsf{k_m}$ appears only in subterms of the form $\mathsf{Mac}^{-}_{\mathsf{k_m}}(\_)$, then for every $1 \leq j \leq 5$, if S is the set of subterms of s, m of the form $\mathsf{Mac}^j_{\mathsf{k_m}}(\_)$ then we have an instance of EUF-MAC^j:

$$\frac{}{s = \mathsf{Mac}^j_{\mathsf{k_m}}(m) \rightarrow \bigvee_{u \in S} s = \mathsf{Mac}^j_{\mathsf{k_m}}(u)} \qquad (\text{EUF-MAC}^j)$$

where $u = v$ denotes the term $\mathsf{eq}(u, v)$. Basically, if s is a valid Mac then s must have been honestly generated. Similarly, we can build a set of axioms reflecting the fact that some functions are jointly collision-resistant. Indeed, if $H, H_1, \dots, H_l$ are jointly PRF, then no adversary can build a collision for $H(\cdot, \mathsf{k_m})$, even if it has oracle access to $H(\cdot, \mathsf{k_m}), H_1(\cdot, \mathsf{k_m}), \dots, H_l(\cdot, \mathsf{k_m})$. This translates as follows: let m_1, m_2 be ground terms, if $\mathsf{k_m}$ appears only in subterms of the form $\mathsf{Mac}^{-}_{\mathsf{k_m}}(\_)$ then we have an instance of CR^j:

$$\frac{}{\mathsf{Mac}^j_{\mathsf{k_m}}(m_1) = \mathsf{Mac}^j_{\mathsf{k_m}}(m_2) \rightarrow m_1 = m_2} \qquad (\text{CR}^j)$$

These axioms are sound (the proof is given in Appendix I-B).

Proposition 2. *For every $1 \leq j \leq 5$, the* EUF-MAC^j *and* CR^j *axioms are valid in any computational model where the $(\mathsf{Mac}^i)_i$ functions are interpreted as jointly* PRF *functions.*

VII. Security Proofs

We now state the authentication and σ_{ul}-unlinkability lemmas. For space reasons, we only sketch the proofs (the full proofs are given in Appendix III and IV).

A. *Mutual Authentication of the* AKA$^+$ *Protocol*

Authentication is modeled by a correspondence property [27] of the form "in any execution, if event A occurs, then event B occurred". This can be translated in the BC logic.

a) Authentication of the User by the Network: AKA$^+$ guarantees authentication of the user by the network if in any execution, if $HN(j)$ believes it authenticated UE_{ID}, then UE_{ID} stated earlier that it had initiated the protocol with $HN(j)$.

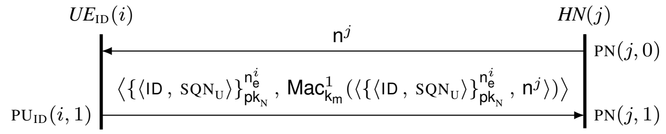
We recall that $\mathsf{e\text{-}auth}_{\text{N}}^{j}$ stores the identity of the *UE* authenticated by $HN(j)$, and that UE_{ID} stores in $\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}}$ the random challenge it received. Moreover, the session $HN(j)$ is uniquely identified by its random challenge n^j. Therefore, authentication of the user by the network is modeled by stating that, for any symbolic trace $\tau \in \mathsf{dom}(\mathcal{R}_{\mathsf{ul}})$, if $\sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\text{N}}^{j}) = \text{ID}$ then there exists some prefix τ' of τ such that $\sigma_{\tau'}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}}) = \mathsf{n}^j$. Let $\preceq$ be the prefix ordering on symbolic traces, then:

Lemma 1. *For every $\tau \in \mathsf{dom}(\mathcal{R}_{ul})$, $\text{ID} \in \mathcal{S}_{id}$ and $j \in \mathbb{N}$, there is derivation using Ax of:*

$$\sigma_\tau^{in}(\mathsf{e\text{-}auth}_{\text{N}}^{j}) = \text{ID} \;\rightarrow\; \bigvee_{\tau' \preceq \tau} \sigma_{\tau'}^{in}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}}) = \mathsf{n}^j$$

The key ingredients to show this lemma are *necessary conditions* for a message to be accepted by the network. Basically, a message can be accepted only if it was honestly generated by a subscriber. These necessary conditions rely on the unforgeability and collision-resistance of $(\mathsf{Mac}^j)_{1 \le j \le 5}$.

b) Necessary Acceptance Conditions: Using the EUF-MAC^j and CR^j axioms, we can find necessary conditions for a message to be accepted by a user. We illustrate this on the *HN*'s second message in the SUPI sub-protocol. We depict a part of the execution between session $UE_{\text{ID}}(i)$ and session $HN(j)$ below:



We then prove that if a message is accepted by $HN(j)$ as coming from UE_{ID}, then the first component of this message must have been honestly generated by a session of UE_{ID}. Moreover, we know that this session received the challenge n^j.

Lemma 2. *Let $\text{ID} \in \mathcal{S}_{id}$ and $\tau \in \mathsf{dom}(\mathcal{R}_{ul})$ be a trace ending with $\text{PN}(j,1)$. There is a derivation using Ax of:*

$$\mathsf{accept}_\tau^{\text{ID}} \rightarrow \bigvee_{\tau_1 = \_,\text{PU}_{\text{ID}}(\_,1) \preceq \tau} \left(\pi_1(g(\phi_\tau^{in})) = t_{\tau_1}^{enc} \wedge g(\phi_{\tau_1}^{in}) = \mathsf{n}^j\right)$$

Proof sktech. Let t_{dec} be the term $\mathsf{dec}(\pi_1(g(\phi_\tau^{\mathsf{in}})), \mathsf{sk_N})$. Then $HN(j)$ accepts the last message iff the following test succeeds:

$$\underline{\pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^1(\langle \pi_1(g(\phi_\tau^{\mathsf{in}}))\,,\, \mathsf{n}^j \rangle)} \wedge \pi_1(t_{\mathsf{dec}}) = \text{ID}$$

By applying EUF-MAC^1 to the underlined part above, we know that if the test holds then $\pi_2(g(\phi_\tau^{\mathsf{in}}))$ is equal to one of the honest $\mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^1$ subterms of $\pi_2(g(\phi^{\mathsf{in}}(\tau)))$, which are the terms:

$$\left(\mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^1(\langle t_{\tau_1}^{\mathsf{enc}}\,,\, g(\phi_{\tau_1}^{\mathsf{in}}) \rangle)\right)_{\tau_1 = \_,\text{PU}_{\text{ID}}(\_,1) \prec \tau} \quad (1)$$

$$\left(\mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^1(\langle \pi_1(g(\phi_{\tau_1}^{\mathsf{in}}))\,,\, \mathsf{n}^{j_1} \rangle)\right)_{\tau_1 = \_,\text{PN}(j_1,1) \prec \tau} \quad (2)$$

Where $\prec$ is the strict version of $\preceq$. We know that $\text{PN}(j,1)$ cannot appear twice in τ. Hence for every $\tau_1 = \_, \text{PN}(j_1,1) \prec \tau$, we know that $j_1 \neq j$. Using the fact that two distinct nonces are never equal except for a negligible number of samplings, we can derive that $\mathsf{eq}(\mathsf{n}^{j_1}, \mathsf{n}^j) = \mathsf{false}$. Using an axiom stating that the pair is injective and the CR^1 axiom, we can show that $\pi_2(g(\phi_\tau^{\mathsf{in}}))$ cannot by equal to one of the terms in (2).

Finally, for every $\tau_1 = \_, \text{PU}_{\text{ID}}(\_,1) \prec \tau$, using the CR^1 and the pair injectivity axioms we can derive that:

$$\mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^1(\langle \pi_1(g(\phi_\tau^{\mathsf{in}}))\,,\, \mathsf{n}^j \rangle) = \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^1(\langle t_{\tau_1}^{\mathsf{enc}}\,,\, g(\phi_{\tau_1}^{\mathsf{in}}) \rangle)$$
$$\rightarrow \pi_1(g(\phi_\tau^{\mathsf{in}})) = t_{\tau_1}^{\mathsf{enc}} \wedge \mathsf{n}^j = g(\phi_{\tau_1}^{\mathsf{in}}) \quad \blacksquare$$

We prove a similar lemma for $\text{TN}(j,1)$. The proof of Lemma 1 is straightforward using these two properties.

c) Authentication of the Network by the User: The AKA$^+$ protocol also provides authentication of the network by the user. That is, in any execution, if UE_{ID} believes it authenticated session $HN(j)$ then $HN(j)$ stated that it had initiated the protocol with UE_{ID}. Formally:

Lemma 3. *For every $\tau \in \mathsf{dom}(\mathcal{R}_{ul})$, $\text{ID} \in \mathcal{S}_{id}$ and $j \in \mathbb{N}$, there is derivation using Ax of:*

$$\sigma_\tau^{in}(\mathsf{e\text{-}auth}_{\text{U}}^{\text{ID}}) = \mathsf{n}^j \;\rightarrow\; \bigvee_{\tau' \preceq \tau} \sigma_{\tau'}^{in}(\mathsf{b\text{-}auth}_{\text{N}}^{j}) = \text{ID}$$

This is shown using the same techniques than for Lemma 1.

B. *σ-Unlinkability of the* AKA$^+$ *Protocol*

Lemma 2 gives a necessary condition for a message to be accepted by $\text{PN}(j,1)$ as coming from ID. We can actually go further, and show that a message is accepted by $\text{PN}(j,1)$ as coming from ID *if and only if* it was honestly generated by a session of UE_{ID} which received the challenge n^j.

Lemma 4. *Let $\text{ID} \in \mathcal{S}_{id}$ and $\tau \in \mathsf{dom}(\mathcal{R}_{ul})$ be a trace ending with $\text{PN}(j,1)$. There is a derivation using Ax of:*

$$\mathsf{accept}_\tau^{\text{ID}} \leftrightarrow \bigvee_{\tau_1 = \_,\text{PU}_{\text{ID}}(\_,1) \preceq \tau} \left(g(\phi_\tau^{in}) = t_{\tau_1} \wedge g(\phi_{\tau_1}^{in}) = \mathsf{n}^j\right)$$

We prove similar lemmas for most actions of the AKA$^+$ protocol. Basically, these lemmas state that a message is accepted if and only if it is part of an honest execution of the protocol between UE_{ID} and *HN*. This allow us to replace each acceptance conditional $\mathsf{accept}_\tau^{\text{ID}}$ by a disjunction over all possible honest partial transcripts of the protocol.

We now state the σ_{ul}-unlinkability lemma:

Lemma 5. *For every $(\tau_l, \tau_r) \in \mathcal{R}_{ul}$, there is a derivation using Ax of the formula $\phi_{\tau_l} \sim \phi_{\tau_r}$.*

The full proof is long and technical. It is shown by induction over τ. Let $(\tau_l, \tau_r) \in \mathcal{R}_{\mathsf{ul}}$, we assume by induction that there is a derivation of $\phi^{\mathsf{in}}_{\tau_l} \sim \phi^{\mathsf{in}}_{\tau_r}$. We want to build a derivation of $\phi^{\mathsf{in}}_{\tau_l}, t_{\tau_l} \sim \phi^{\mathsf{in}}_{\tau_r}, t_{\tau_r}$ using the inference rules in Ax.

First, we rewrite t_{τ_l} using the acceptance characterization lemmas such as Lemma 4. This replaces each $\mathsf{accept}^{\mathrm{ID}}_{\tau_l}$ by a case disjunction over all honest executions *on the left side*. Similarly, we rewrite t_{τ_r} as a case disjunction over honest executions *on the right side*. Our goal is then to find a matching between left and right transcripts such that matched transcripts are indistinguishable. If a left and right transcript correspond to the same trace of oracle calls, this is easy. But since the left and right traces of oracle calls may differ, this is not always possible. E.g., some left transcript may not have a corresponding right transcript. When this happens, we have two possibilities: instead of a one-to-one match we build a many-to-one match, e.g. matching a left transcript to several right transcripts; or we show that some transcripts always result in a failure of the protocol. Showing the latter is complicated, as it requires to precisely track the possible values of $\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}$ and $\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}$ across multiple sessions of the protocol to prove that some transcripts always yield a desynchronization between UE_{ID} and *HN*.

VIII. Conclusion

We studied the privacy provided by the 5G-AKA authentication protocol. While this protocol is not vulnerable to IMSI catchers, we showed that several privacy attacks from the literature apply to it. We also discovered a novel desynchronization attack against PRIV-AKA, a modified version of AKA, even though it had been claimed secure.

We then proposed the AKA^{+} protocol. This is a fixed version of 5G-AKA, which is both efficient and has improved privacy guarantees. To study AKA^{+}'s privacy, we defined the σ-unlinkability property. This is a new parametric privacy property, which requires the prover to establish privacy only for a subset of the standard unlinkability game scenarios. Finally, we formally proved that AKA^{+} provides mutual authentication and σ_{ul}-unlinkability for any number of agents and sessions. Our proof is carried out in the Bana-Comon model, which is well-suited to the formal analysis of stateful protocols.

Acknowledgment

This research has been partially funded by the French National Research Agency (ANR) under the project TECAP (ANR-17-CE39-0004-01).

References

[1] *TS 33.501: Security architecture and procedures for 5G system*, 3GPP Technical Specification, Rev. 15.2.0, September 2018.

[2] D. Strobel, "IMSI catcher," *Ruhr-Universität Bochum, Seminar Work*, 2007.

[3] R. Borgaonkar, L. Hirshi, S. Park, A. Shaik, A. Martin, and J.-P. Seifert, "New adventures in spying 3G & 4G users: Locate, track, monitor," 2017, briefing at BlackHat USA 2017. [Online]. Available: https://www.blackhat.com/us-17/briefings.html#new-adventures-in-spying-3g-and-4g-users-locate-track-and-monitor

[4] M. Arapinis, L. I. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar, "New privacy issues in mobile telephony: fix and verification," in *the ACM Conference on Computer and Communications Security, CCS'12*. ACM, 2012, pp. 205–216.

[5] M. Arapinis, T. Chothia, E. Ritter, and M. Ryan, "Analysing unlinkability and anonymity using the applied pi calculus," in *Proceedings of the 23rd IEEE Computer Security Foundations Symposium, CSF 2010*. IEEE Computer Society, 2010, pp. 107–121.

[6] P. Fouque, C. Onete, and B. Richard, "Achieving better privacy for the 3gpp AKA protocol," *PoPETs*, vol. 2016, no. 4, pp. 255–275, 2016.

[7] N. Kobeissi, K. Bhargavan, and B. Blanchet, "Automated verification for secure messaging protocols and their implementations: A symbolic and computational approach," in *2017 IEEE European Symposium on Security and Privacy, EuroS&P*. IEEE, 2017, pp. 435–450.

[8] K. Bhargavan, C. Fournet, and M. Kohlweiss, "mitls: Verifying protocol implementations against real-world attacks," *IEEE Security & Privacy*, vol. 14, no. 6, pp. 18–25, 2016.

[9] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. van der Merwe, "A comprehensive symbolic analysis of TLS 1.3," in *ACM Conference on Computer and Communications Security, CCS'17*. ACM, 2017, pp. 1773–1788.

[10] M. Abadi, B. Blanchet, and C. Fournet, "The applied pi calculus: Mobile values, new names, and secure communication," *J. ACM*, vol. 65, no. 1, pp. 1:1–1:41, 2018.

[11] B. Blanchet, ProVerif*: Cryptographic protocols verifier in the formal model*, available at http://proseccco.gforge..inria.fr/personal/bblanchet/proverif/.

[12] V. Cheval, S. Kremer, and I. Rakotonirina, "DEEPSEC: deciding equivalence properties in security protocols theory and practice," in *2018 IEEE Symposium on Security and Privacy, SP 2018*. IEEE, 2018, pp. 529–546.

[13] S. Meier, B. Schmidt, C. Cremers, and D. Basin, "The tamarin prover for the symbolic analysis of security protocols," in *25th International Conference on Computer Aided Verification, CAV'13*. Springer-Verlag, 2013, pp. 696–701.

[14] V. Cortier, N. Grimm, J. Lallemand, and M. Maffei, "A type system for privacy properties," in *ACM Conference on Computer and Communications Security, CCS'17*. ACM, 2017, pp. 409–423.

[15] V. Shoup, "Sequences of games: a tool for taming complexity in security proofs," *IACR Cryptology ePrint Archive*, vol. 2004, p. 332, 2004.

[16] B. Blanchet, "A computationally sound mechanized prover for security protocols," *IEEE Trans. Dependable Sec. Comput.*, vol. 5, no. 4, pp. 193–207, 2008.

[17] G. Bana and H. Comon-Lundh, "Towards unconditional soundness: Computationally complete symbolic attacker," in *Principles of Security and Trust, 2012*, ser. LNCS, vol. 7215. Springer, 2012, pp. 189–208.

[18] G. Bana and H. Comon-Lundh, "A computationally complete symbolic attacker for equivalence properties," in *2014 ACM Conference on Computer and Communications Security, CCS '14*. ACM, 2014, pp. 609–620.

[19] F. van den Broek, R. Verdult, and J. de Ruiter, "Defeating IMSI catchers," in *ACM Conference on Computer and Communications Security, CCS'15*. ACM, 2015, pp. 340–351.

[20] D. A. Basin, J. Dreier, L. Hirschi, S. Radomirovi'c, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *the ACM Conference on Computer and Communications Security, CCS'18*. ACM, 2018.

[21] M. Lee, N. P. Smart, B. Warinschi, and G. J. Watson, "Anonymity guarantees of the UMTS/LTE authentication and connection protocol," *Int. J. Inf. Sec.*, vol. 13, no. 6, pp. 513–527, 2014.

[22] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel, "A new RFID privacy model," in *ESORICS*, ser. Lecture Notes in Computer Science, vol. 6879. Springer, 2011, pp. 568–587.

[23] S. Vaudenay, "On privacy models for RFID," in *ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security*, ser. LNCS. Springer, 2007, pp. 68–87.

[24] A. Shaik, J. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," in *23rd Annual Network and Distributed System Security Symposium, NDSS*. The Internet Society, 2016.

[25] L. Hirschi, D. Baelde, and S. Delaune, "A method for verifying privacy-type properties: The unbounded case," in *IEEE Symposium on Security and Privacy, SP 2016*. IEEE Computer Society, 2016, pp. 564–581.

[26] H. Comon and A. Koutsos, "Formal computational unlinkability proofs of RFID protocols," in *30th Computer Security Foundations Symposium, 2017*. IEEE Computer Society, 2017, pp. 100–114.

[27] T. Y. C. Woo and S. S. Lam, "A semantic model for authentication protocols," in *Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, May 1993, pp. 178–194.

[28] O. Goldreich, *The Foundations of Cryptography - Volume 1, Basic Techniques*. Cambridge University Press, 2001.

[29] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *J. ACM*, vol. 33, no. 4, pp. 792–807, 1986.

[30] G. Barthe, M. Daubignard, B. M. Kapron, Y. Lakhnech, and V. Laporte, "On the equality of probabilistic terms," in *Logic for Programming, Artificial Intelligence, and Reasoning - 16th International Conference, LPAR-16, Dakar, Senegal, April 25-May 1, 2010, Revised Selected Papers*, ser. LNCS, E. M. Clarke and A. Voronkov, Eds., vol. 6355. Springer, 2010, pp. 46–63.

Contents

Appendix I
Axioms

In this section, we define the set of axioms Ax. We split our set of axioms in three parts, $\mathsf{Ax} = \mathsf{Ax}_{\mathsf{struct}} \cup \mathsf{Ax}_{\mathsf{impl}} \cup \mathsf{Ax}_{\mathsf{crypto}}$, where $\mathsf{Ax}_{\mathsf{struct}}$ is the set of structural axioms, $\mathsf{Ax}_{\mathsf{impl}}$ is the set of implementation axioms and $\mathsf{Ax}_{\mathsf{crypto}}$ is the set of cryptographic axioms.

Definitions: We give some definitions used to define the cryptographic axioms.

Definition 2. *For any subset $\mathcal{S}$ of $\mathcal{F}, \mathcal{N}$ and $\mathcal{X}$, we let $\mathcal{T}(\mathcal{S})$ be the set of terms built upon $\mathcal{S}$.*

Definition 3. *A* position *is a word in $\mathbb{N}^*$. The value of a term t at a position p, denoted by $(t)_{|p}$, is the partial function defined inductively as follows:*

$$
\begin{aligned}
(t)_{|\epsilon} &= t \\
(f(u_0, \dots, u_{n-1}))_{|i.p} &= \begin{cases} (u_i)_{|p} & \textit{if } i < n \\ \textit{undefined} & \textit{otherwise} \end{cases}
\end{aligned}
$$

We say that a position in valid *is t if $(t)_{|p}$ is defined. The set of positions $\mathsf{pos}(t)$ of a term is the set of positions which are valid in t. Moreover, given two position p, p', we have $p \leq p'$ if and only if p is a prefix of p'.*

Definition 4. *A context $D[]_{\vec{x}}$ (sometimes written D when there is no confusion) is a term in $\mathcal{T}(\mathcal{F}, \mathcal{N}, \{[]_y \mid y \in \vec{x}\})$ where $\vec{x}$ are distinct special variables called holes.*

For all contexts $D[]_{\vec{x}}, C_0, \dots, C_{n-1}$ with $|\vec{x}| = n$, we let $D[(C_i)_{i<n}]$ be the context $D[]_{\vec{x}}$ in which we substitute, for every $0 \leq i < n$, all occurrences of the hole $[]_{x_i}$ by C_i.

A one-holed context is a context with one hole (in which case we write $D[]$ where $[]$ is the only variable).

Definition 5. *Given a term t, we let $\mathsf{st}(t)$ be the set of subterms of t. We extend this to sequences of terms by having $\mathsf{st}(u_1, \dots, u_n) = \mathsf{st}(u_1) \cup \dots \cup \mathsf{st}(u_n)$.*

Definition 6. *For every terms b, t, we let $[b]t$ be the term $\mathsf{if}\, b\ \mathsf{then}\ t\ \mathsf{else}\ \bot$.*

Definition 7. *Let $s, \vec{u}$ be ground terms and $C_{\vec{x},\cdot}$ be a context with one distinguished hole variable $\cdot$, and we require that the hole variable $\cdot$ appears exactly once in $C_{\vec{x},\cdot}$. Then we let $s \sqsubseteq_{C_{\vec{x},\cdot}} \vec{u}$ holds whenever s appears in $\vec{u}$ only in subterms of the form $C[\vec{w}, s]$. Formally:*

$$\forall u \in \vec{u}, \forall p \in \mathsf{pos}(u), u_{|p} \equiv s \rightarrow \exists \vec{w} \in \mathcal{T}(\mathcal{F}, \mathcal{N}), \exists q \in \mathsf{pos}(u) \textit{ s.t. } q \leq p \wedge u_{|q} \equiv C[\vec{w}, s]$$

Given n contexts $C_1, \dots, C_n$, we let $s \sqsubseteq_{C_1,\dots,C_n} \vec{u}$ if and only if for all $1 \leq i \leq n$, $s \sqsubseteq_{C_i} \vec{u}$.

Example 3. For example, $\mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{sk}(\cdot)} \vec{u}$ states that the nonce n appears only in terms of the form $\mathsf{pk}(\mathsf{n})$ or $\mathsf{sk}(\mathsf{n})$ in $\vec{u}$.

Similarly, $\mathsf{sk}(\mathsf{n}) \sqsubseteq_{\mathsf{dec}(\_,\cdot)} \vec{u}$ states that the secret key $\mathsf{sk}(\mathsf{n})$ appears only in decryption position in $\vec{u}$.

A. *CCA1* Axioms

a) The $\mathsf{CCA1}_s$ Axioms: To prove that the AKA$^+$ protocol is σ_{ul}-unlinkable, we need the encryption scheme to be IND-CCA1 secure. We define first set of axioms $\mathsf{CCA1}_s$:

Definition 8. *We let $\mathsf{CCA1}_s$ be the set of axioms:*

$$\frac{\mathsf{len}(s) \doteq \mathsf{len}(t)}{\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{u}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}}\ \mathsf{CCA1}_s \qquad \textit{when} \begin{cases} \mathsf{fresh}(\mathsf{n_e}; \vec{u}, s, t) \\ \mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{sk}(\cdot)} \vec{u}, s, t \ \wedge\ \mathsf{sk}(\mathsf{n}) \sqsubseteq_{\mathsf{dec}(\_,\cdot)} \vec{u}, s, t \end{cases}$$

This set of axioms $\mathsf{CCA1}_s$ is very similar to the one used in [18]. The only difference is that in [18], the length equality requirement is not a premise of the axiom. Instead, if the length are not equal they return a error message. We found our version of the axiom simpler to use.

We have the following soundness property:

Proposition 3. *The $\mathsf{CCA1}_s$ axioms are valid in any computational model where $(\{\_\}^{\_}_{\_}, \mathsf{dec}(\_,\_), \mathsf{pk}(\_), \mathsf{sk}(\_))$ is interpreted as a* IND-CCA1 *secure encryption scheme.*

Proof. The proof is by contradiction, and is sketched below:

We assume that there is a computational model $\mathcal{M}_c$ where the encryption scheme is IND-CCA1 secure, and such that there is an instance $\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}$ of the axioms $\mathsf{CCA1}_s$ which is not valid. We deduce that there exists an attacker $\mathcal{A}$ that can distinguish between the left and right terms, i.e. the following quantity is non-negligible:

$$\left| \mathbf{Pr}\left(\vec{w} \xleftarrow{\$} [\![\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c} : \mathcal{A}(1^\eta, \vec{w}) = 1\right) - \mathbf{Pr}\left(\vec{w} \xleftarrow{\$} [\![\vec{u}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c} : \mathcal{A}(1^\eta, \vec{w}) = 1\right) \right| \tag{3}$$

Where $\xleftarrow{\$}$ denotes a uniform random sampling. Using $\mathcal{A}$, we can build an adversary $\mathcal{B}$ with a non-negligible advantage against the IND-CCA1 game. First, $\mathcal{B}$ samples a vector of bit-strings $\vec{u}_s, s_s, t_s$ from $[\![\vec{u}, s, t]\!]_{\mathcal{M}_c}$, querying the decryption oracle whenever $\mathcal{B}$ needs to compute a subterm of the from $\mathsf{dec}(\_, \mathsf{sk}(\mathsf{n}))$. Remark that the syntactic side-conditions:

$$\mathsf{n} \sqsubseteq_{\mathsf{pk}(\cdot),\mathsf{sk}(\cdot)} \vec{u}, s, t \qquad\qquad \mathsf{sk}(\mathsf{n}) \sqsubseteq_{\mathsf{dec}(\_,\cdot)} \vec{u}, s, t$$

guarantee that this is always possible. Afterward, $\mathcal{B}$ queries the left-or-right oracle with (s_s, t_s) to get a value a. Here, we need the side-condition $\mathsf{fresh}(\mathsf{n_e}; \vec{u}, s, t)$ to guarantee that the random value $\mathsf{n_e}$ has not been sampled by $\mathcal{B}$. Indeed, the value $\mathsf{n_e}$ is sampled by the challenger, and is not available to $\mathcal{B}$. If the challenger internal bit b is 0 then $\vec{u}_s, a$ has been sampled from $[\![\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c}$, and if the challenger internal bit is 1 then $\vec{u}_s, a$ has been sampled from $[\![\vec{u}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c}$:

$$\vec{u}_s, a \xleftarrow{\$} \begin{cases} [\![\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c} & \text{if } b = 0 \\ [\![\vec{u}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}]\!]_{\mathcal{M}_c} & \text{if } b = 1 \end{cases}$$

Then $\mathcal{B}$ returns $\mathcal{A}(\vec{u}_s, a)$. It is easy to check that the advantage of $\mathcal{B}$ against the IND-CCA1 game is exactly the advantage of $\mathcal{A}$ against $\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{u}, \{t\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}$ This advantage is the quantity in Equation 3, which we assumed non-negligible. Hence $\mathcal{B}$ is a winning adversary against the IND-CCA1 game. Contradiction. ■

b) The CCA1 Axioms: We now define the set of axioms CCA1, which is more convenient to use than $\mathsf{CCA1}_s$:

Definition 9. *We let CCA1 be the set of axioms:*

$$\frac{\vec{u} \sim \vec{v} \qquad \mathit{len}(s) \doteq \mathit{len}(t)}{\vec{u}, \{s\}^{n_e}_{pk(n)}, \mathit{len}(s) \sim \vec{v}, \{t\}^{n'_e}_{pk(n')}, \mathit{len}(s)}\ \mathit{CCA1} \qquad \textit{when} \begin{cases} \mathit{fresh}(n_e, n'_e; \vec{u}, \vec{v}, s, t) \\ \vec{u} \equiv \mathit{pk}(n), \_ \ \wedge\ \vec{v} \equiv \mathit{pk}(n'), \_ \\ n \sqsubseteq_{pk(\cdot),sk(\cdot)} \vec{u}, s \ \wedge\ \mathit{sk}(n) \sqsubseteq_{dec(\_,\cdot)} \vec{u}, s \\ n' \sqsubseteq_{pk(\cdot),sk(\cdot)} \vec{v}, t \ \wedge\ \mathit{sk}(n') \sqsubseteq_{dec(\_,\cdot)} \vec{v}, t \end{cases}$$

We now state the following soundness theorem:

Proposition 4. *The CCA1 axioms are valid in any computational model where* $(\{\_\}^{\_}_{\_}, \mathit{dec}(\_,\_), \mathit{pk}(\_), \mathit{sk}(\_))$ *is interpreted as a* IND-CCA1 *secure encryption scheme.*

Proof. The proof relies on the transitivity axiom Trans and the $\mathsf{CCA1}_s$ axioms, which are valid are valid in any computational model where $(\{\_\}^{\_}_{\_}, \mathsf{dec}(\_,\_), \mathsf{pk}(\_), \mathsf{sk}(\_))$ is interpreted as a IND-CCA1 secure encryption scheme using Proposition 3.

$$\dfrac{\dfrac{\overline{\mathsf{len}(s) = \mathsf{len}(0^{\mathsf{len}(s)})}}{\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{u}, \{0^{\mathsf{len}(s)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}}\ \mathsf{CCA1}_s \qquad \vec{u}, \{0^{\mathsf{len}(s)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{0^{\mathsf{len}(t)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \qquad \dfrac{\overline{\mathsf{len}(t) = \mathsf{len}(0^{\mathsf{len}(t)})}}{\vec{v}, \{0^{\mathsf{len}(t)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}\ \mathsf{CCA1}_s}{\vec{u}, \{s\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{t\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}}\ \mathsf{Trans}$$

And:

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{\vec{u}, \mathsf{len}(s) \sim \vec{v}, \mathsf{len}(s)}}{\vec{u}, \mathsf{len}(s), \mathsf{n_e} \sim \vec{v}, \mathsf{len}(s), \mathsf{n_e}}\ \mathsf{Fresh}}{\vec{u}, \mathsf{len}(s), \mathsf{pk(n)}, \mathsf{n_e} \sim \vec{v}, \mathsf{len}(s), \mathsf{pk(n)}, \mathsf{n_e}}\ \mathsf{Dup} \qquad \overline{\mathsf{len}(s) = \mathsf{len}(t)}}{\vec{u}, \mathsf{len}(s), \mathsf{pk(n)}, \mathsf{n_e} \sim \vec{v}, \mathsf{len}(t), \mathsf{pk(n)}, \mathsf{n_e}}\ R}{\vec{u}, \{0^{\mathsf{len}(s)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}} \sim \vec{v}, \{0^{\mathsf{len}(t)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}}\ \mathsf{FA}^3$$

■

B. PRF-MAC *Axioms*

Definition 10 (PRF Function [28], [29])**.** *Let* $H(\cdot,\cdot) : \{0,1\}^* \times \{0,1\}^\eta \to \{0,1\}^\eta$ *be a keyed hash functions. The function* H *is a* Pseudo Random Function *if, for any PPTM adversary* $\mathcal{A}$ *with access to an oracle* $\mathcal{O}_f$*:*

$$|\mathbf{Pr}(k:\ \mathcal{A}^{\mathcal{O}_{H(\cdot,k)}}(1^\eta) = 1) - \mathbf{Pr}(g:\ \mathcal{A}^{\mathcal{O}_{g(\cdot)}}(1^\eta) = 1)|$$

is negligible. Where

- k *is drawn uniformly in* $\{0,1\}^\eta$.
- g *is drawn uniformly in the set of all functions from* $\{0,1\}^*$ *to* $\{0,1\}^\eta$.

The authors of [26] already gave axioms for this property (and proved soundness). We recall their axiom schema below, using our notations:

$$\frac{}{\begin{array}{r}\vec{u}, \mathsf{if}\ \bigvee_{i\in I} \mathsf{eq}(m, m_i)\ \mathsf{then}\ \mathbf{0}\ \mathsf{else}\ H(m,\mathsf{k}) \\ \sim\ \vec{u}, \mathsf{if}\ \bigvee_{i\in I} \mathsf{eq}(m, m_i)\ \mathsf{then}\ \mathbf{0}\ \mathsf{else}\ \mathsf{n}\end{array}} \quad \text{when} \begin{cases}\mathsf{fresh}(\mathsf{n}; \vec{u}, m) \\ \mathsf{k} \sqsubseteq_{H(\_,\cdot)} \vec{u}, m \\ \{m_i \mid i \in I\} = \{u \mid H(u, \mathsf{k}) \in \mathsf{st}(\vec{u}, m)\} \\ \forall u, v.\ \text{if}\ H(u,v) \in \mathsf{st}(\vec{u}, m)\ \text{then}\ v \equiv \mathsf{k}\end{cases}$$

We simplify this axiom schema by dropping the last syntactical requirement. Indeed, it is not necessary to require that every occurrence of H in $\vec{u}, m$ uses the key k. We prove that this is valid.

Proposition 5. *The following set of axioms is valid in any computational model where the H is interpreted as a* PRF *function:*

$$\frac{}{\begin{array}{r}\vec{u}, \mathsf{if}\ \bigvee_{i\in I} \mathsf{eq}(m, m_i)\ \mathsf{then}\ \mathbf{0}\ \mathsf{else}\ H(m,\mathsf{k}) \\ \sim\ \vec{u}, \mathsf{if}\ \bigvee_{i\in I} \mathsf{eq}(m, m_i)\ \mathsf{then}\ \mathbf{0}\ \mathsf{else}\ \mathsf{n}\end{array}} \quad \textit{when} \begin{cases}\mathsf{fresh}(\mathsf{n}; \vec{u}, m) \\ \mathsf{k} \sqsubseteq_{H(\_,\cdot)} \vec{u}, m \\ \{m_i \mid i \in I\} = \{u \mid H(u, \mathsf{k}) \in \mathsf{st}(\vec{u}, m)\}\end{cases}$$

Proof. We consider an instance of the axiom schema:

$$\frac{}{\begin{array}{r}\vec{u}, \mathsf{if}\ \bigvee_{i\in I} \mathsf{eq}(m, m_i)\ \mathsf{then}\ \mathbf{0}\ \mathsf{else}\ H(m,\mathsf{k}) \\ \sim\ \vec{u}, \mathsf{if}\ \bigvee_{i\in I} \mathsf{eq}(m, m_i)\ \mathsf{then}\ \mathbf{0}\ \mathsf{else}\ \mathsf{n}\end{array}}$$

Let $\vec{h} \equiv (H(m_i, \mathsf{k}))_{i\in I}$ and $\vec{v}[], b[]$ be contexts such that $\vec{v}[\vec{h}] \equiv \vec{u}$ and $b[\vec{h}] \equiv \bigvee_{i\in I} \mathsf{eq}(m, m_i)$ and such that $\mathsf{k} \notin \mathsf{st}(\vec{v}, b)$. Let $\mathcal{M}_c{}^0$ be a computational model and $\mathcal{A}$ be an adversary. We need to show that:

$$\mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{h}], [b[\vec{h}]]H(m,\mathsf{k})\right]\!\right]_{\mathcal{M}_c{}^0}\right) = 1\right) \approx \mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{h}], [b[\vec{h}]]\mathsf{n}\right]\!\right]_{\mathcal{M}_c{}^0}\right) = 1\right)$$

Let $\mathcal{M}_c$ be an extension of $\mathcal{M}_c{}^0$ where we added two function symbols g, g' which are interpreted as random functions. Then we know that it is sufficient to show that:

$$\mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{h}], [b[\vec{h}]]H(m,\mathsf{k})\right]\!\right]_{\mathcal{M}_c}\right) = 1\right) \approx \mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{h}], [b[\vec{h}]]\mathsf{n}\right]\!\right]_{\mathcal{M}_c}\right) = 1\right) \tag{4}$$

Let $\vec{r} \equiv (g(m_i))_{i\in I}$. It is straightforward to check that, thanks to the PRF assumption of H, we have:

$$\mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{h}], [b[\vec{h}]]H(m,\mathsf{k})\right]\!\right]_{\mathcal{M}_c}\right) = 1\right) \approx \mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{r}], [b[\vec{r}]]g(m)\right]\!\right]_{\mathcal{M}_c}\right) = 1\right)$$

Moreover, using the fact that the subterm $g(m)$ is guarded by $b[\vec{r}]$, we know that, except for a negligible number of samplings, m is never queried to the random function g except once, in $[b[\vec{r}]]g(m)$. It follows that we can safely replace the last call to $g(m)$ by a call to $g'(m)$, which yields:

$$\mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{r}], [b[\vec{r}]]g(m)\right]\!\right]_{\mathcal{M}_c}\right) = 1\right) \approx \mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{r}], [b[\vec{r}]]g'(m)\right]\!\right]_{\mathcal{M}_c}\right) = 1\right)$$

Now, using again the PRF property of H, we know that:

$$\mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{r}], [b[\vec{r}]]g'(m)\right]\!\right]_{\mathcal{M}_c}\right) = 1\right) \approx \mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{h}], [b[\vec{h}]]g'(m)\right]\!\right]_{\mathcal{M}_c}\right) = 1\right)$$

Finally, since g' appears only once in $\vec{v}[\vec{h}], [b[\vec{h}]]g'(m)$, we can replace $g'(m)$ by a fresh nonce. Hence:

$$\mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{h}], [b[\vec{h}]]g'(m)\right]\!\right]_{\mathcal{M}_c}\right) = 1\right) \approx \mathbf{Pr}\left(\mathcal{A}\left(\left[\!\left[\vec{v}[\vec{h}], [b[\vec{h}]]\mathsf{n}\right]\!\right]_{\mathcal{M}_c}\right) = 1\right)$$

This concludes the proof of (4). ■

This can be extended to have a finite family of functions being jointly PRF. A finite family of functions $H_1(\cdot, k), \dots, H_n(\cdot, k)$ are jointly PRF if they are jointly computationally indistinguishable from random functions. Formally:

Definition 11 (Jointly PRF Functions). *Let $H_1(\cdot,\cdot), \dots, H_n(\cdot,\cdot)$ be a finite family of keyed hash functions such that for every $1 \le i \le n$, $H_i(\cdot,\cdot) : \{0,1\}^* \times \{0,1\}^\eta \to \{0,1\}^\eta$. The functions $H_1, \dots, H_n$ are* Jointly Pseudo Random Functions *if, for any PPTM adversary $\mathcal{A}$ with access to oracles $\mathcal{O}_{f_1}, \dots, \mathcal{O}_{f_n}$:*

$$|\mathbf{Pr}(k:\ \mathcal{A}^{\mathcal{O}_{H_1(\cdot,k)},\dots,\mathcal{O}_{H_n(\cdot,k)}}(1^\eta) = 1) - \mathbf{Pr}(g_1, \dots, g_n:\ \mathcal{A}^{\mathcal{O}_{g_1(\cdot)},\dots,\mathcal{O}_{g_n(\cdot)}}(1^\eta) = 1)|$$

is negligible. Where

- *k is drawn uniformly in $\{0,1\}^\eta$.*
- *$g_1, \dots, g_n$ are drawn uniformly in the set of all functions from $\{0,1\}^*$ to $\{0,1\}^\eta$.*

Remark 3. It is easy to build a family $H_1, \dots, H_n$ of jointly pseudo random functions from a pseudo random function $H(\cdot,\cdot)$. First, let $(\mathsf{tag}_i(\cdot))_{1\le i\le n}$ be a set of tagging functions. We require that these functions are unambiguous, i.e. for all bit-strings u, v and $i \neq j$ we must have $\mathsf{tag}_i(u) \neq \mathsf{tag}_j(v)$. Then for every $1 \le i \le n$, we let $H_i(x,y) = H(\mathsf{tag}_i(x), y)$. It is straightforward to show that if H is a PRF then $H_1, \dots, H_n$ are jointly PRF.

Now, we translate this property for f and $\mathsf{f^r}$ (resp. Mac^1–Mac^5) in the logic.

Definition 12. *We let $\mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(u)$ be the set of Mac^j terms under key $\mathsf{k_m}$ in u:*

$$\mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(u) = \{m \mid \mathsf{Mac}^j_{\mathsf{k_m}}(m) \in \mathsf{st}(u)\}$$

Definition 13. *For every $1 \le j \le 5$, we let PRF-MAC^j be the set of axioms:*

$$\frac{}{\begin{array}{l}\vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{Mac}^j_{\mathsf{k_m}}(m)\\ \sim\ \vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{n}\end{array}}\ \text{PRF-MAC}^j \qquad \textit{when} \begin{cases}\mathsf{fresh}(\mathsf{n}; \vec{u}, m)\\ \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} \vec{u}, m\\ \{m_i \mid i \in I\} = \mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(\vec{u}, m)\end{cases}$$

Definition 14. *Let $g \in \{\mathsf{f}, \mathsf{f^r}\}$. We let $\mathsf{set\text{-}prf}^g_{\mathsf{k}}(u)$ be the set of g terms under key k in u:*

$$\mathsf{set\text{-}prf}^g_{\mathsf{k}}(u) = \{m \mid g_{\mathsf{k}}(m) \in \mathsf{st}(u)\}$$

Definition 15. *For every $g \in \{\mathsf{f}, \mathsf{f^r}\}$, we let PRF-$g$ be the set of axioms:*

$$\frac{}{\begin{array}{l}\vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } g_{\mathsf{k}}(m)\\ \sim\ \vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{n}\end{array}}\ \text{PRF-}g \qquad \textit{when} \begin{cases}\mathsf{fresh}(\mathsf{n}; \vec{u}, m)\\ \mathsf{k} \sqsubseteq_{\mathsf{f}_{\cdot}(\_), \mathsf{f^r_{\cdot}}(\_)} \vec{u}, m\\ \{m_i \mid i \in I\} = \mathsf{set\text{-}prf}^g_{\mathsf{k}}(\vec{u}, m)\end{cases}$$

Proposition 6. *The (PRF-MAC^j) (resp. PRF-f and PRF-$\mathsf{f^r}$) axiom schemes are valid in any computational model where the (Mac^j) (resp. f and $\mathsf{f^r}$) function symbols are interpreted as jointly PRF functions.*

Proof. This is an extension of the axiom schema given in Proposition 5. The soundness proof follows the same step, by replacing every call $H_j(\_, \mathsf{k})$ with a call to a random function $g_i(\_)$, where $(g_i)_{1\le i\le n}$ are independent random functions. We omit the details. ■

Remark 4. If we have a valid instance of PRF-MAC^j:

$$\frac{}{\begin{array}{l}\vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{Mac}^j_{\mathsf{k_m}}(m)\\ \sim\ \vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{n}\end{array}}\ \text{PRF-MAC}^j$$

then using transitivity we know that:

$$\frac{\dfrac{}{\begin{array}{l}\vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{Mac}^j_{\mathsf{k_m}}(m)\\ \sim\ \vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{n}\end{array}}\ \text{PRF-MAC}^j \qquad \vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{n} \sim \vec{v}}{\vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{Mac}^j_{\mathsf{k_m}}(m) \sim \vec{v}}\ \mathsf{Trans}$$

Therefore the following axiom schema is admissible using PRF-MAC^j + Trans:

$$\frac{\vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{n} \sim \vec{v}}{\vec{u}, \text{if } \bigvee_{i\in I} \mathsf{eq}(m, m_i) \text{ then } \mathbf{0} \text{ else } \mathsf{Mac}^j_{\mathsf{k_m}}(m) \sim \vec{v}} \quad \text{when} \begin{cases}\mathsf{fresh}(\mathsf{n}; \vec{u}, m)\\ \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} \vec{u}, m\\ \{m_i \mid i \in I\} = \mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(\vec{u}, m)\end{cases}$$

We will prefer the axiom schema above over the axiom schema given in Definition 13. By a notation abuse, we refer also to the axiom above as PRF-MAC^j. The same remark applies to PRF-f and PRF-$\mathsf{f^r}$.

C. EUF-MAC *Axioms*

a) The SIMP-EUF-MAC *Axioms:*

Definition 16. *We let* $\mathsf{set\text{-}mac}_{\mathsf{k_m}}(u)$ *be the set of* Mac *terms under key* $\mathsf{k_m}$ *in* u*:*

$$\mathsf{set\text{-}mac}_{\mathsf{k_m}}(u) = \{m \mid \mathsf{Mac}_{\mathsf{k_m}}(m) \in \mathsf{st}(u)\}$$

Definition 17. *A function* Mac *is* EUF-MAC *secure if for every PPTM* $\mathcal{A}$*, the following quantity is negligible in* η*:*

$$\mathbf{Pr}\left(\mathsf{k_m} \leftarrow \{0,1\}^\eta : (m,\sigma) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Mac}}(\mathsf{k_m})}(1^\eta), m \text{ not queried to } \mathcal{O}_{\mathsf{Mac}}(\mathsf{k_m}) \text{ and } \sigma = \mathsf{Mac}_{\mathsf{k_m}}(m)\right)$$

This can be modeled using the following axioms:

Definition 18. *We let* SIMP-EUF-MAC *be the set of axioms:*

$$\overline{s = \mathsf{Mac}_{\mathsf{k_m}}(m) \rightarrow \bigvee_{u \in S} s = \mathsf{Mac}_{\mathsf{k_m}}(u)} \qquad when \begin{cases} \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}_{\cdot}(\_)} s, m \\ S = \mathsf{set\text{-}mac}_{\mathsf{k_m}}(s, m) \end{cases} \qquad \text{(SIMP-EUF-MAC)}$$

Proposition 7. *The* SIMP-EUF-MAC *axioms are valid in any computational model where the* Mac *function is interpreted as an* EUF-MAC *secure function.*

The proof is similar to the proof of Proposition 3. We omit the details.

b) The EUF-MAC *Axioms:* It is well-know that if a function H is a PRF then H is EUF-MAC secure. We give here the counterpart of this result for a family of functions $H, H_1, \dots, H_l$ which are jointly PRF.

If $H, H_1, \dots, H_l$ which are jointly PRF, then no adversary can forge a mac of $H(\cdot, \mathsf{k_m})$, even if the adversary has oracle access to $H(\cdot, \mathsf{k_m}), H_1(\cdot, \mathsf{k_m}), \dots, H_l(\cdot, \mathsf{k_m})$. First, we define what it means for a function to be EUF-MAC secure with a key jointly used by other functions:

Definition 19. *A function* H *is* EUF-MAC *secure with a key jointly used by* $H_1, \dots, H_l$ *if for every PPTM* $\mathcal{A}$*, the following quantity is negligible in* η*:*

$$\mathbf{Pr}\left(\mathsf{k_m} \leftarrow \{0,1\}^\eta : (m,\sigma) \leftarrow \mathcal{A}^{\mathcal{O}_{H(\cdot,\mathsf{k_m})}, \mathcal{O}_{H_1(\cdot,\mathsf{k_m})}, \dots, \mathcal{O}_{H_l(\cdot,\mathsf{k_m})}}(1^\eta), m \text{ not queried to } \mathcal{O}_{H(\cdot,\mathsf{k_m})} \text{ and } \sigma = H(m, \mathsf{k_m})\right)$$

Proposition 8. *If* $H, H_1, \dots, H_l$ *are jointly* PRF *then* H *is* EUF-MAC *secure with a key jointly used by* $H_1, \dots, H_l$*.*

Proof. The proof is almost the same than the proof showing that if a function H is a PRF then H is EUF-MAC secure, and is by reduction. If H is not EUF-MAC secure with a key jointly used by $H_1, \dots, H_l$ then there exists an adversary $\mathcal{A}$ winning the corresponding game with a non-negligible probability. It is simple to build from $\mathcal{A}$ an adversary $\mathcal{B}$ against the joint PRF property of $H, H_1, \dots, H_l$.

First, $\mathcal{B}$ runs the adversary $\mathcal{A}$, forwarding and logging its the oracle calls. Eventually, $\mathcal{A}$ returns a pair (m, σ). Then, $\mathcal{B}$ queries the first oracle on m, which returns a value σ'. Finally, $\mathcal{B}$ returns 1 if and only if $\mathcal{A}$ never queried the first oracle on m and $\sigma' = \sigma$. Then:

- If $\mathcal{B}$ is interacting with the oracles $\mathcal{O}_{H(\cdot,\mathsf{k_m})}, \mathcal{O}_{H_1(\cdot,\mathsf{k_m})}, \dots, \mathcal{O}_{H_l(\cdot,\mathsf{k_m})}$, its probability of returning 1 is exactly the advantage of $\mathcal{A}$ against the EUF-MAC game with key jointly used.
- If $\mathcal{B}$ is interacting with the oracles $\mathcal{O}_{g(\cdot)}, \mathcal{O}_{g_1(\cdot)}, \dots, \mathcal{O}_{g_l(\cdot)}$ where $g, g_1, \dots, g_l$ are random functions, then its probability of returning 1 is the probability of having $g(m) = \sigma$ knowing that m was never queried to g. Since g is a random function, this is less than $1/2^\eta$.

Since $\mathcal{A}$ has a non-negligible advantage against the EUF-MAC game with key jointly used, we deduce that $\mathcal{B}$ has a non-negligible advantage against the joint PRF-fgame. ∎

We translate this cryptographic property in the logic to obtain the sets of axioms $(\text{EUF-MAC}^j)_{1 \leq j \leq 5}$.

Definition 20. *We let* EUF-MAC^j *be the set of axioms:*

$$\overline{s = \mathsf{Mac}^j_{\mathsf{k_m}}(m) \rightarrow \bigvee_{u \in S} s = \mathsf{Mac}^j_{\mathsf{k_m}}(u)} \qquad when \begin{cases} \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} s, m \\ S = \mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(s, m) \end{cases} \qquad (\text{EUF-MAC}^j)$$

Proposition 9. *The* EUF-MAC^j *axioms are valid in any computational model where the* Mac^j *function is interpreted as a* EUF-MAC *secure function with a key jointly used by the interpretations of* $(\mathsf{Mac}^i)_{1 \leq i \leq 5, i \neq j}$*.*

Remark that it is easy to prove Proposition 2 using Proposition 8 and Proposition 9.

Proof of Proposition 9. The proof is straightforward and has the same structure than the proof of Proposition 3.

We assume that there is a computational model $\mathcal{M}_c$ where the Mac^j function is interpreted as a EUF-MAC secure function with a key jointly used by the interpretations of $(\mathsf{Mac}^i)_{1\leq i\leq 5, i\neq j}$. Moreover, we assume that there is an instance:

$$\overline{s = \mathsf{Mac}^j_{\mathsf{k_m}}(m) \rightarrow \bigvee_{u\in S} s = \mathsf{Mac}^j_{\mathsf{k_m}}(u)}$$

of the EUF-MAC^j which is not valid in $\mathcal{M}_c$, and such that:

$$\mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} s, m \qquad\qquad S = \mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(s, m)$$

Therefore we know that the following quantity is not negligible in η:

$$\mathbf{Pr}\left(\rho_1, \rho_2 : [\![s = \mathsf{Mac}^j_{\mathsf{k_m}}(m)]\!]^\eta_{\rho_1,\rho_2} \wedge \neg[\![\bigvee_{u\in S} s = \mathsf{Mac}^j_{\mathsf{k_m}}(u)]\!]^\eta_{\rho_1,\rho_2}\right)$$

Or equivalently the following quantity is not negligible in η:

$$\mathbf{Pr}\left(\rho_1, \rho_2 : [\![s]\!]^\eta_{\rho_1,\rho_2} = [\![\mathsf{Mac}^j_{\mathsf{k_m}}(m)]\!]^\eta_{\rho_1,\rho_2} \wedge \bigwedge_{u\in S}[\![s]\!]^\eta_{\rho_1,\rho_2} \neq [\![\mathsf{Mac}^j_{\mathsf{k_m}}(u)]\!]^\eta_{\rho_1,\rho_2}\right) \tag{5}$$

Using $\mathcal{M}_c$ we can build a adversary $\mathcal{A}$ against the EUF-MAC game with key jointly used. The adversary $\mathcal{A}$ simply samples two values a_s, a_{Mac} from $[\![s]\!]^\eta_{\rho_1,\rho_2}$ and $[\![\mathsf{Mac}^j_{\mathsf{k_m}}(m)]\!]^\eta_{\rho_1,\rho_2}$ by sampling a value from all the subterms of s and m in a bottom-up fashion. The adversary calls the $(\mathcal{O}_{\mathsf{Mac}^i})_{1\leq i\leq 5}$ whenever he need to sample a value from a subterm of the form $\mathsf{Mac}^i_{\mathsf{k_m}}(\_)$. Remark that the side-condition $\mathsf{k_m} \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} s, m$ ensures that this is always possible. Then $\mathcal{A}$ returns a_s, a_{Mac}. One can check that the advantage of $\mathcal{A}$ against the EUF-MAC game with key jointly used by $(\mathsf{Mac}^i)_{1\leq i\leq 5, i\neq j}$ is exactly the quantity in 5. It follows that $\mathcal{A}$ has a non-negligible probability of winning the game. Contradiction. ■

D. CR Axioms

We recall the definition of Collision-Resistance:

Definition 21. *A function H is* CR *secure if for every PPTM $\mathcal{A}$, the following quantity is negligible in η:*

$$\mathbf{Pr}\left(k_m \leftarrow \{0,1\}^\eta : (m_1, m_2) \leftarrow \mathcal{A}^{\mathcal{O}_{H(\cdot,k_m)}}(1^\eta), m_1 \neq m_2 \text{ and } H(m_1, k_m) = H(m_2, k_m)\right)$$

As for unforgeability, we generalize this to allow the key $\mathsf{k_m}$ to be jointly used by others functions. Formally:

Definition 22. *A function H is* CR *secure with a key jointly used by $H_1, \dots, H_l$ if for every PPTM $\mathcal{A}$, the following quantity is negligible in η:*

$$\mathbf{Pr}\left(k_m \leftarrow \{0,1\}^\eta : (m_1, m_2) \leftarrow \mathcal{A}^{\mathcal{O}_{H(\cdot,k_m)},\mathcal{O}_{H_1(\cdot,k_m)},\dots,\mathcal{O}_{H_l(\cdot,k_m)}}(1^\eta), m_1 \neq m_2 \text{ and } H(m_1, k_m) = H(m_2, k_m)\right)$$

It is well-known that a EUF-MAC secure function is also CR secure. Similarly we have that:

Proposition 10. *If H is* EUF-MAC *secure with a key jointly used by $H_1, \dots, H_l$ then H is* CR *secure with a key jointly used by $H_1, \dots, H_l$.*

Proof. We can easily build an adversary $\mathcal{B}$ against the EUF-MAC game with a key jointly from any adversary $\mathcal{A}$ against the CR game with a key jointly such that $\mathcal{A}$ and $\mathcal{B}$ have the same advantage against their respective games. The result follows. ■

We translate this game in the logic as follows:

Definition 23. *We let* CR^j *be the set of axioms:*

$$\overline{\mathsf{Mac}^j_{k_m}(m_1) = \mathsf{Mac}^j_{k_m}(m_2) \rightarrow m_1 = m_2} \qquad \text{when } k_m \sqsubseteq_{\mathsf{Mac}^{\cdot}_{\cdot}(\_)} m_1, m_2 \tag{CR^j}$$

Proposition 11. *The* CR^j *axioms are valid in any computational model where the Mac^j function is interpreted as a* CR *secure function with a key jointly used by the interpretations of $(\mathsf{Mac}^i)_{1\leq i\leq 5, i\neq j}$.*

Proof. The proof works exactly like the proof of Proposition 3 and Proposition 9. We omit the details. ■

E. Cryptographic Axioms

Definition 24. *We let Ax_{crypto} be the set of cryptographic axioms:*

$$\mathsf{Ax}_{crypto} = \mathsf{CCA1} \cup \left(\text{PRF-MAC}^j\right)_{1\leq j\leq 5} \cup \text{PRF-}\mathsf{f} \cup \text{PRF-}\mathsf{f}^{\mathsf{r}} \cup \left(\text{EUF-MAC}^j\right)_{1\leq j\leq 5} \cup \left(\text{CR}^j\right)_{1\leq j\leq 5}$$

Proposition 12. *The axioms in Ax_{crypto} are valid in any computational model where the asymmetric encryption $\{\_\}^{\_}_{\_}$ is* IND-CCA1 *secure and f and f^{r} (resp. Mac^1–Mac^5) satisfy jointly the* PRF-f*assumption.*

Proof. This is a direct consequence of the Propositions 4, 6, 9 and 11. ■

$$\frac{\vec{v} \sim \vec{u}}{\vec{u} \sim \vec{v}}\ \mathsf{Sym} \qquad \frac{}{\vec{u} \sim \vec{u}}\ \mathsf{Refl} \qquad \frac{\vec{u} \sim \vec{w} \quad \vec{w} \sim \vec{v}}{\vec{u} \sim \vec{v}}\ \mathsf{Trans} \qquad \frac{(x_{\pi(i)})_{i \le n} \sim (y_{\pi(i)})_{i \le n}}{(x_i)_{i \le n} \sim (y_i)_{i \le n}}\ \mathsf{Perm} \qquad \frac{\vec{u}, t \sim \vec{v}, t'}{\vec{u}, t, t \sim \vec{v}, t', t'}\ \mathsf{Dup}$$

$$\frac{\vec{u}, t \sim \vec{v}, t'}{\vec{u} \sim \vec{v}}\ \mathsf{Restr} \qquad \frac{\vec{x}, \vec{y} \sim \vec{x'}, \vec{y'}}{f(\vec{x}), \vec{y} \sim f(\vec{x'}), \vec{y'}}\ \mathsf{FA} \qquad \frac{\vec{u}, s \sim \vec{v} \qquad s \doteq t}{\vec{u}, t \sim \vec{v}}\ R \qquad \frac{\vec{u} \sim \vec{v}}{\vec{u}, \mathsf{n} \sim \vec{v}, \mathsf{n}}\ \mathsf{Fresh}\ \text{ when } \mathsf{n} \notin \mathsf{st}(\vec{u}, \vec{v})$$

$$\frac{\vec{u}, \mathsf{n} \sim \vec{v}}{\vec{u}, t \oplus \mathsf{n} \sim \vec{v}}\ \oplus\text{-}\mathsf{indep}\ \text{ when } \mathsf{n} \notin \mathsf{st}(\vec{u}, t) \qquad \frac{\vec{w}, b, (u_i)_i \sim \vec{w}', b', (u'_i)_i \qquad \vec{w}, b, (v_i)_i \sim \vec{w}', b', (v'_i)_i}{\vec{w}, (\text{if } b \text{ then } u_i \text{ else } v_i)_i \sim \vec{w}', (\text{if } b' \text{ then } u'_i \text{ else } v'_i)_i}\ \mathsf{CS}$$

Conventions: π is a permutation of $\{1, \dots, n\}$ and $f \in \mathcal{F}$.

Fig. 14. The Structural Axioms $\mathsf{Ax}_{\mathsf{struct}}$.

F. Structural and Implementation Axioms

We present the structural axioms $\mathsf{Ax}_{\mathsf{struct}}$, which are given in Fig. 14. All these axioms have been introduced in the literature (e.g. see [18], [26]). Still, we informally describe them: the axioms Sym, Refl and Trans states that computational indistinguishability is an equivalence relation; the Perm axiom is used to change the order of the terms using a permutation π on both side of $\sim$; Dup is used to remove duplicate; Restr allows to strengthen the goal; FA states that to show that two function applications are indistinguishable, it is sufficient to show that their arguments are indistinguishable; the axiom R allow to rewrite any occurrence of s into t if we can show that $s = t$; Fresh allows to remove a random sampling appearing if it is not used; $\oplus$-indep is the optimistic sampling rule (see [30]); and finally, CS states that to show that two if_then_else_ are indistinguishable, it is sufficient to show that their then branches and else branches are indistinguishable, when giving the value of the branching conditional to the adversary.

We then have the following soundness result:

Proposition 13. *The axioms in $\mathsf{Ax}_{\mathsf{struct}}$ are valid in any computational model.*

Proof. The soundness proofs can be found in [18], [26]. ∎

We can now define the set of axioms Ax:

Definition 25. *We let Ax be the set inference rules:*

$$\mathsf{Ax} = \mathsf{Ax}_{\mathsf{struct}} \cup \mathsf{Ax}_{\mathsf{impl}} \cup \mathsf{Ax}_{\mathsf{crypto}}$$

Definition 26. *We let Simp denote a sequence of applications of R, FA and Dup, i.e.:*

$$\frac{\vec{s} \sim \vec{t}}{\vec{u} \sim \vec{v}}\ \mathsf{Simp} \quad \textit{when} \quad \frac{\vec{s} \sim \vec{t}}{\vec{u} \sim \vec{v}}\ (R + \mathsf{FA} + \mathsf{Dup})^*$$

Implementation Axioms: We describe the implementation axioms $\mathsf{Ax}_{\mathsf{impl}}$ given in Fig. 15. The set of implementation axioms is the union of the following sets of axioms:

- The set $\mathsf{Ax}_{\mathsf{ite}}$ of equalities satisfied by the if_then_else_ function symbols.
- The set $\mathsf{Ax}_{\mathsf{eq}}$ of axioms satisfied by the equality function symbol eq(_, _). This includes functional properties of projections and decryption, equality properties such as reflexivity and dis-equalities.
- The set $\mathsf{Ax}_{\mathsf{len}}$ of axioms satisfied by the length function len(_).
- The set $\mathsf{Ax}_{\mathsf{inj}}$ of injectivity axioms.
- The set $\mathsf{Ax}_{\mathrm{SQN}}$ of axioms satisfied by the range((, _), _) function on sequence numbers.

G. P-EUF-MAC$_s$ *Axioms*

We can refine the unforgeability axioms EUF-MAC^j using a finite partition of the outcomes.

Definition 27. *A finite family of conditionals $(b_i)_{i \in I}$ is a valid CS partition if:*

$$\left(\bigvee_i b_i \wedge \bigwedge_{i \neq j} b_i \neq b_j\right) \doteq \mathit{true}$$

We can have a more precise axiom, by considering a valid CS partition $(b_i)_{i \in I}$ and applying the EUF-MAC^j axiom once for each element of the partition.

Definition 28. *We let* P-EUF-MAC$_s^j$ *be the set of axioms:*

$$\frac{}{s = \mathit{Mac}^j_{\mathsf{k_m}}(m) \rightarrow \bigvee_{i \in I} b_i \wedge \bigvee_{u \in S_i} s = \mathit{Mac}^j_{\mathsf{k_m}}(u)} \quad \textit{when} \begin{cases} \mathit{k_m} \sqsubseteq_{\mathit{Mac}_\cdot(\_)} s, m \\ (b_i)_{i \in I} \textit{ is a valid } \mathit{CS} \textit{ partition} \\ \textit{There exists } (s_i, m_i)_{i \in I} \textit{ s.t. for every } i \in I \\ \qquad [b_i]s_i \doteq [b_i]s \wedge [b_i]m_i \doteq [b_i]m \\ \qquad S_i = \mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(s_i, m_i) \end{cases} \qquad (\text{P-EUF-MAC}_s^j)$$

Proposition 14. *The* P-EUF-MAC$_s^j$ *axioms are logical consequences of the axioms* *Ax*.

Proof. The proof is pretty straightforward:

$$\begin{aligned} s = \mathsf{Mac}^j_{\mathsf{k_m}}(m) &\rightarrow \bigvee_{i \in I} \left(b_i \wedge s = \mathsf{Mac}^j_{\mathsf{k_m}}(m)\right) && \text{(Since } (b_i)_{i \in I} \text{ is a valid CS partition)} \\ &\rightarrow \bigvee_{i \in I} \left(b_i \wedge s_i = \mathsf{Mac}^j_{\mathsf{k_m}}(m_i)\right) \\ &\rightarrow \bigvee_{i \in I} b_i \wedge \bigvee_{u \in S_i} s_i = \mathsf{Mac}^j_{\mathsf{k_m}}(u) && \text{(Using EUF-MAC}^j \text{ for every } i \in I) \\ &\rightarrow \bigvee_{i \in I} b_i \wedge \bigvee_{u \in S_i} s = \mathsf{Mac}^j_{\mathsf{k_m}}(u) \end{aligned}$$

■

H. P-EUF-MAC *Axioms*

We can further refine the unforgeability axioms, by noticing that macs appearing only in boolean conditionals can be ignored.

Definition 29. *For every term u, we let* *strict-st*(u) *be the set of subterms of u appearing outside a conditional:*

$$\textit{strict-st}(\textit{if } b \textit{ then } u \textit{ else } v) = \{\textit{strict-st}(\textit{if } b \textit{ then } u \textit{ else } v)\} \cup \textit{strict-st}(u) \cup \textit{strict-st}(v)$$

$$\textit{strict-st}(f(\vec{u})) = \{f(\vec{u})\} \cup \bigcup_{u \in \vec{u}} \textit{strict-st}(u) \textit{ when } f \neq \textit{if\_then\_else\_}$$

Definition 30. *We let* strict-set-mac$^j_{\mathsf{k_m}}(u)$ *be the set of mac-ed terms under key* $\mathit{k_m}$ *and tag j in u appearing outside a conditional:*

$$\mathsf{strict\text{-}set\text{-}mac}^j_{\mathsf{k_m}}(u) = \{m \mid \mathsf{Mac}^j_{\mathsf{k_m}}(m) \in \mathsf{strict\text{-}st}(u)\}$$

Definition 31. *We let* P-EUF-MAC^j *be the set of axioms:*

$$\frac{}{s = \mathit{Mac}^j_{\mathsf{k_m}}(m) \rightarrow \bigvee_{i \in I} b_i \wedge \bigvee_{u \in S_i} s = \mathit{Mac}^j_{\mathsf{k_m}}(u)} \quad \textit{when} \begin{cases} \mathit{k_m} \sqsubseteq_{\mathit{Mac}_\cdot(\_)} s, m \\ (b_i)_{i \in I} \textit{ is a valid } \mathit{CS} \textit{ partition} \\ \textit{There exists } (s_i, m_i)_{i \in I} \textit{ s.t. for every } i \in I \\ \qquad [b_i]s_i \doteq [b_i]s \wedge [b_i]m_i \doteq [b_i]m \\ \qquad S_i = \mathsf{strict\text{-}set\text{-}mac}^j_{\mathsf{k_m}}(s_i, m_i) \end{cases} \qquad (\text{P-EUF-MAC}^j)$$

Proposition 15. *The* P-EUF-MAC^j *axioms are logical consequences of the axioms* *Ax*.

Proof. First, we are going to show that the following axioms are consequences of the axioms Ax:

$$\frac{}{s = \mathsf{Mac}^j_{\mathsf{k_m}}(m) \rightarrow \bigvee_{u \in S} s = \mathsf{Mac}^j_{\mathsf{k_m}}(u)} \quad \text{when} \begin{cases} \mathsf{k_m} \sqsubseteq_{\mathsf{Mac}_\cdot(\_)} s, m \\ S \equiv \mathsf{strict\text{-}set\text{-}mac}^j_{\mathsf{k_m}}(s, m) \end{cases} \tag{6}$$

Assuming the axioms above are valid, it is easy to conclude by repeating the proof of Proposition 14, but using the axiom above instead of EUF-MAC^j.

To show that the axioms in (6) are valid, we are going to pull out all conditionals using the properties of the if_then_else_ function symbols. This yields a term of the form $C[\vec{\beta} \diamond (\vec{e})]$ where $\vec{e}$ themselves of the form $s' = \mathsf{Mac}^j_{\mathsf{k_m}}(u')$. We then apply the EUF-MAC^j axioms to every $e \in \vec{e}$. Finally, we rewrite back the conditionals.

To be able to do this last step, we need, when we pull out the conditionals, to remember which conditional appeared where. We do this by replacing a conditional b with either true_b or false_b, where the b lower-script is a label that we attach to the term.

This motivates the following definition: for every boolean term b, we let $\mathsf{Val}_b = \{\mathsf{true}_b, \mathsf{false}_b\}$. We extend this to vector of conditionals by having $\mathsf{Val}_{u_0,\dots,u_l} = \mathsf{Val}_{u_0} \times \cdots \times \mathsf{Val}_{u_l}$. Basically, for every vector of conditionals $\vec{\beta}$, choosing a vector of terms $\vec{\nu} \in \mathsf{Val}_{\vec{\beta}}$ correspond to choosing a valuation of $\vec{\beta}$.

We can start showing the validity of (6). Let $\vec{\beta}$ be the set of conditionals appearing in s, m, and C be an if-context such that:

$$\left(s = \mathsf{Mac}^j_{\mathsf{k_m}}(m)\right) \leftrightarrow \left(C\left[\vec{\beta} \diamond \left(s[\vec{\nu}/\vec{\beta}] = \mathsf{Mac}^j_{\mathsf{k_m}}(m[\vec{\nu}/\vec{\beta}])\right)_{\vec{\nu}\in\mathsf{Val}_{\vec{\beta}}}\right]\right)$$

where $t[\vec{u}/\vec{v}]$ denotes the substitution of every occurrence of $\vec{v}$ by $\vec{u}$ in t. Then:

$$s = \mathsf{Mac}^j_{\mathsf{k_m}}(m) \;\rightarrow\; \left(C\left[\vec{\beta} \diamond \left(s[\vec{\nu}/\vec{\beta}] = \mathsf{Mac}^j_{\mathsf{k_m}}(m[\vec{\nu}/\vec{\beta}])\right)_{\vec{\nu}\in\mathsf{Val}_{\vec{\beta}}}\right]\right)$$

For every $\vec{\nu} \in \mathsf{Val}_{\vec{\beta}}$, let $S_{\vec{\nu}} = \mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(s[\vec{\nu}/\vec{\beta}], m[\vec{\nu}/\vec{\beta}])$. By applying EUF-MAC^j

$$\rightarrow \left(C\left[\vec{\beta} \diamond \left(\bigvee_{u\in S_{\vec{\nu}}} s[\vec{\nu}/\vec{\beta}] = \mathsf{Mac}^j_{\mathsf{k_m}}(u)\right)_{\vec{\nu}\in\mathsf{Val}_{\vec{\beta}}}\right]\right)$$

Since any conditional of $s[\vec{\nu}/\vec{\beta}]$ or $m[\vec{\nu}/\vec{\beta}]$ is of the form true_x or false_x for some label x, we know that:

$$S_{\vec{\nu}} = \mathsf{set\text{-}mac}^j_{\mathsf{k_m}}(s[\vec{\nu}/\vec{\beta}], m[\vec{\nu}/\vec{\beta}]) = \mathsf{strict\text{-}set\text{-}mac}^j_{\mathsf{k_m}}(s[\vec{\nu}/\vec{\beta}], m[\vec{\nu}/\vec{\beta}])$$

Moreover, we can check that:

$$\mathsf{strict\text{-}set\text{-}mac}^j_{\mathsf{k_m}}(s[\vec{\nu}/\vec{\beta}], m[\vec{\nu}/\vec{\beta}]) = \left(\mathsf{strict\text{-}set\text{-}mac}^j_{\mathsf{k_m}}(s, m)\right)[\vec{\nu}/\vec{\beta}]$$

Let $S = \mathsf{strict\text{-}set\text{-}mac}^j_{\mathsf{k_m}}(s, m)$. Hence:

$$\begin{aligned}\left(C\left[\vec{\beta} \diamond \left(\bigvee_{u\in S_{\vec{\nu}}} s[\vec{\nu}/\vec{\beta}] = \mathsf{Mac}^j_{\mathsf{k_m}}(u)\right)_{\vec{\nu}\in\mathsf{Val}_{\vec{\beta}}}\right]\right) &\rightarrow \left(C\left[\vec{\beta} \diamond \left(\bigvee_{u\in S[\vec{\nu}/\vec{\beta}]} s[\vec{\nu}/\vec{\beta}] = \mathsf{Mac}^j_{\mathsf{k_m}}(u)\right)_{\vec{\nu}\in\mathsf{Val}_{\vec{\beta}}}\right]\right)\\ &\rightarrow \left(C\left[\vec{\beta} \diamond \left(\left(\bigvee_{u\in S} s = \mathsf{Mac}^j_{\mathsf{k_m}}(u)\right)[\vec{\nu}/\vec{\beta}]\right)_{\vec{\nu}\in\mathsf{Val}_{\vec{\beta}}}\right]\right)\\ &\rightarrow \bigvee_{u\in S} s = \mathsf{Mac}^j_{\mathsf{k_m}}(u)\end{aligned}$$

This concludes this proof. ■

I. Additional Axioms

We present additional axioms, and show that they are logical consequences of the axioms Ax.

An if-context is a context build using only the if_then_else_ function symbol, and hole variables. We also require that no if_then_else_ function symbol appears in a conditional position of another if_then_else_ function symbol. Moreover, we split the hole variables in two disjoint sets: the set $\vec{x}$ of hole variables appearing in a conditional position, and the set $\vec{y}$ of variables appearing in leave position. Formally:

Definition 32. *For all distinct variables $\vec{x}, \vec{y}$, an if-context $D[]_{\vec{x}\diamond\vec{y}}$ is a context in $\mathcal{T}(\textit{if \_ then \_ else \_}, \{[]_z \mid z \in \vec{x} \cup \vec{y}\})$ such that for all position p, $D_{|p} \equiv \textit{if } b \textit{ then } u \textit{ else } v$ implies:*

- $b \in \{[]_z \mid z \in \vec{x}\}$
- $u, v \notin \{[]_z \mid z \in \vec{x}\}$

Definition 33. *For every nonces $\mathsf{n}_0, \dots, \mathsf{n}_l$, for every ground terms $\vec{u}$, we let $\mathit{fresh}(\mathsf{n}_0, \dots, \mathsf{n}_l; \vec{u})$ holds if and only if for every $0 \le i \le l$, $\mathsf{n}_i \notin \mathit{st}(\vec{u})$.*

a) The indep-branch *Axioms:* This is useful to define the indep-branch axiom. Let $\vec{u}, \vec{b}$ be ground terms, C an if-context and $\mathsf{n}, (\mathsf{n}_i)_{i\in I}$ nonces. If $\mathsf{n}, (\mathsf{n}_i)_{i\in I}$ are distinct and such that $\mathsf{fresh}(\mathsf{n}, (\mathsf{n}_i)_{i\in I}; \vec{u}, \vec{b}, C[])$. Then the following inference rule is an instance of the indep-branch axiom:

$$\frac{}{\vec{u}, C\left[\vec{b} \diamond (\mathsf{n}_i)_{i\in I}\right] \sim \vec{u}, \mathsf{n}}\ \textsf{indep-branch}$$

Proposition 16. *The* indep-branch *axioms are a consequence of the* Ax *axioms.*

Proof. TO prove this, we first introduce the if-context C on the right to match the shape of the left side. We then split the proof using CS, and conclude by applying Fresh. This yields the derivation:

$$\dfrac{\dfrac{\dfrac{}{\forall i \in I, \vec{u}, \vec{b}, \mathsf{n}_i \sim \vec{u}, \vec{b}, \mathsf{n}}\ \textsf{Fresh}}{\vec{u}, C\left[\vec{b} \diamond (\mathsf{n}_i)_{i\in I}\right] \sim \vec{u}, C\left[\vec{b} \diamond (\mathsf{n})_{i\in I}\right]}\ \textsf{CS}^*}{\vec{u}, C\left[\vec{b} \diamond (\mathsf{n}_i)_{i\in I}\right] \sim \vec{u}, \mathsf{n}}\ R$$

■

b) Function Application Under Context: It is often convenient to apply the FA axiom under an if-context C. Formally, let $\vec{v}, \vec{b}, (u_{i,j})_{i\in I, 1\le j\le n}, (u'_{i,j})_{i\in I, 1\le j\le n}$ be terms and C an if-context. Then the following inference rule is an instance of the $\mathsf{FA_c}$ axiom:

$$\frac{\vec{v}, \left(C\left[\vec{b} \diamond (u_{i,j})_{i\in I}\right]\right)_{1\le j\le n} \sim \vec{v}', \left(C\left[\vec{b}' \diamond (u'_{i,j})_{i\in I}\right]\right)_{1\le j\le n}}{\vec{v}, C\left[\vec{b} \diamond \left(f((u_{i,j})_{1\le j\le n})\right)_{i\in I}\right] \sim \vec{v}', C\left[\vec{b}' \diamond \left(f((u'_{i,j})_{1\le j\le n})\right)_{i\in I}\right]}\ \mathsf{FA_c}$$

Proposition 17. *The $\mathsf{FA_c}$ axioms are a consequence of the* Ax *axioms.*

Proof. First, we pull the f function outside of the if-context C using the homomorphism properties if if_then_else_. Finally we apply the FA axiom. This yields the derivation:

$$\dfrac{\dfrac{\vec{v}, \left(C\left[\vec{b} \diamond (u_{i,j})_{i\in I}\right]\right)_{1\le j\le n} \sim \vec{v}', \left(C\left[\vec{b}' \diamond (u'_{i,j})_{i\in I}\right]\right)_{1\le j\le n}}{\vec{v}, f\left(C\left[\vec{b} \diamond (u_{i,j})_{i\in I}\right]\right)_{1\le j\le n} \sim \vec{v}', f\left(C\left[\vec{b}' \diamond (u'_{i,j})_{i\in I}\right]\right)_{1\le j\le n}}\ \textsf{FA}}{\vec{v}, C\left[\vec{b} \diamond \left(f((u_{i,j})_{1\le j\le n})\right)_{i\in I}\right] \sim \vec{v}', C\left[\vec{b}' \diamond \left(f((u'_{i,j})_{1\le j\le n})\right)_{i\in I}\right]}\ R$$

■

c) Program Constants:

Definition 34. *We define the set $\mathcal{S}_{cst}$ to be the set of program constant, with includes the set of agent names $\mathcal{S}_{id}$ and the constants UnknownId and fail:*

$$\mathcal{S}_{cst} \ := \ \mathcal{S}_{id} \cup \{\bot, \mathit{UnknownId}, \mathit{fail}, 0, 1\}$$

Proposition 18. *For every term u, v we have, the following axiom is a consequence of the axioms* Ax*:*

$$\frac{\mathit{len}(u) \doteq \mathit{len}(v) \qquad \mathit{len}(u) \neq 0}{\mathit{eq}(\{u\}^{n_e}_{pk(n)}, \{v\}^{n'_e}_{pk(n)}) \doteq \mathit{false}} \qquad \text{when} \begin{cases} n_e \not\equiv n'_e \\ \mathit{fresh}(n_e, n'_e; u, v) \\ n \sqsubseteq_{pk(\cdot), sk(\cdot)} u, v \ \wedge \ sk(n) \sqsubseteq_{dec(\_,\cdot)} u, v \end{cases}$$

Proof. We give directly the derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathsf{pk(n)}, \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \mathsf{len}(v) \sim \mathsf{pk(n)}, \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \mathsf{len}(v)}\ \textsf{Refl} \qquad \dfrac{\dfrac{}{\mathsf{len}(v) \doteq \mathsf{len}(v)}\ \textsf{Refl}}{\mathsf{len}(v) \doteq \mathsf{len}(1^{\mathsf{len}(v)})}}{\mathsf{pk(n)}, \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{v\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}} \sim \mathsf{pk(n)}, \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}}\ \textsf{CCA1}}{\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{v\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}} \sim \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}}\ \textsf{Restr}}{\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{v\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}})}\ \textsf{FA} \qquad \mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}{\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{v\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}\ \textsf{Trans}$$

To show $\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}$, we apply again transitivity:

$$\frac{\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \qquad \mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}{\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}\ \mathsf{Trans}$$

Now, we give the derivation of the left premise:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathsf{pk(n)}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}, \mathsf{len}(u) \sim \mathsf{pk(n)}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}, \mathsf{len}(u)}\ \mathsf{Refl} \qquad \dfrac{\dfrac{}{\mathsf{len}(u) \doteq \mathsf{len}(u)}\ \mathsf{Refl}}{\mathsf{len}(u) \doteq \mathsf{len}(0^{\mathsf{len}(u)})}}{\mathsf{pk(n)}, \{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}\{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}} \sim \mathsf{pk(n)}, \{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}\{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}}\ \mathsf{CCA1}}{\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}\{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}} \sim \{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}\{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}}\ \mathsf{Restr}}{\mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}})}\ \mathsf{FA}$$

And finally we prove the right premise $\mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}$:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{eq}(0,1) \doteq \mathsf{false}}\ \mathsf{EQConst} \qquad \dfrac{}{\mathsf{len}(0) \neq 0} \qquad \mathsf{len}(u) \neq 0}{\mathsf{eq}(0^{\mathsf{len}(u)}, 1^{\mathsf{len}(v)}) \doteq \mathsf{false}}\ \mathsf{l\text{-}neq}}{\mathsf{eq}(\{0^{\mathsf{len}(u)}\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{1^{\mathsf{len}(v)}\}^{\mathsf{n'_e}}_{\mathsf{pk(n)}}) \doteq \mathsf{false}}\ \mathsf{EQInj}(\{\cdot\}^{\_}_{\_}) + R$$

■

- *The set Ax_{ite} of equality axioms related to the $\mathsf{if\_then\_else\_}$ function symbol:*

$$\frac{}{f(\vec{u}, \mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ y, \vec{v}) \doteq \mathsf{if}\ b\ \mathsf{then}\ f(\vec{u}, x, \vec{v})\ \mathsf{else}\ f(\vec{u}, y, \vec{v})} \quad \text{for any } f \in \mathcal{F}_s$$

$$\frac{}{\mathsf{if}\ (\mathsf{if}\ b\ \mathsf{then}\ a\ \mathsf{else}\ c)\ \mathsf{then}\ x\ \mathsf{else}\ y \doteq \mathsf{if}\ b\ \mathsf{then}\ (\mathsf{if}\ a\ \mathsf{then}\ x\ \mathsf{else}\ y)\ \mathsf{else}\ (\mathsf{if}\ c\ \mathsf{then}\ x\ \mathsf{else}\ y)} \qquad \frac{}{\mathsf{if}\ \mathsf{true}\ \mathsf{then}\ x\ \mathsf{else}\ y \doteq x}$$

$$\frac{}{\mathsf{if}\ \mathsf{false}\ \mathsf{then}\ x\ \mathsf{else}\ y \doteq y} \qquad \frac{}{\mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ x \doteq x} \qquad \frac{}{\mathsf{if}\ b\ \mathsf{then}\ (\mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ y)\ \mathsf{else}\ z \doteq \mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ z}$$

$$\frac{}{\mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ (\mathsf{if}\ b\ \mathsf{then}\ y\ \mathsf{else}\ z) \doteq \mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ z}$$

$$\frac{}{\mathsf{if}\ b\ \mathsf{then}\ (\mathsf{if}\ a\ \mathsf{then}\ x\ \mathsf{else}\ y)\ \mathsf{else}\ z \doteq \mathsf{if}\ a\ \mathsf{then}\ (\mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ z)\ \mathsf{else}\ (\mathsf{if}\ b\ \mathsf{then}\ y\ \mathsf{else}\ z)}$$

$$\frac{}{\mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ (\mathsf{if}\ a\ \mathsf{then}\ y\ \mathsf{else}\ z) \doteq \mathsf{if}\ a\ \mathsf{then}\ (\mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ y)\ \mathsf{else}\ (\mathsf{if}\ b\ \mathsf{then}\ x\ \mathsf{else}\ z)}$$

- *The set Ax_{eq} of equality and disequality axiom:*

$$\frac{}{\pi_i(\langle x_1\,,\, x_2\rangle) \doteq x_i} \ \text{for } i \in \{1,2\} \qquad \frac{}{\pi_i(\langle x_1\,, x_2\,,\, x_3\rangle) \doteq x_i} \ \text{for } i \in \{1,2,3\} \qquad \frac{}{\mathsf{dec}(\{x\}^z_{\mathsf{pk}(y)}, \mathsf{sk}(y)) \doteq x}$$

$$\frac{}{\mathsf{eq}(x,x) \doteq \mathsf{true}} \qquad \frac{}{\mathsf{eq}(\mathsf{A},\mathsf{B}) \doteq \mathsf{false}}\ \neq\text{-Const} \ \ \text{for every } \mathsf{A},\mathsf{B} \in \mathcal{S}_{\mathsf{cst}} \text{ s.t. } \mathsf{A} \neq \mathsf{B} \qquad \frac{}{\mathsf{eq}(t,\mathsf{n}) \doteq \mathsf{false}}\ \text{EQIndep} \ \ \text{if } \mathsf{n} \notin \mathsf{st}(t)$$

- *The set Ax_{len} of length axioms:*

$$\frac{\mathsf{len}(u) \doteq \mathsf{len}(s) \qquad \mathsf{len}(v) \doteq \mathsf{len}(t)}{\mathsf{len}(\langle u\,,\, v\rangle) \doteq \mathsf{len}(\langle s\,,\, t\rangle)} \qquad \frac{}{\mathsf{len}(\mathrm{ID}_1) \doteq \mathsf{len}(\mathrm{ID}_2)} \ \text{for every } \mathrm{ID}, \mathrm{ID}' \in \mathcal{S}_{\mathsf{id}}$$

$$\frac{}{\mathsf{len}(\mathsf{suc}(\mathsf{sqn\text{-}init}^{\mathrm{ID}}_{\mathrm{U}})) \doteq \mathsf{len}(\mathsf{sqn\text{-}init}^{\mathrm{ID}}_{\mathrm{U}})} \qquad \frac{}{\mathsf{len}(\mathsf{sqn\text{-}init}^{\mathrm{ID}_1}_{\mathrm{U}}) \doteq \mathsf{len}(\mathsf{sqn\text{-}init}^{\mathrm{ID}_2}_{\mathrm{U}})} \qquad \frac{}{\mathsf{len}(0^x) \doteq x} \qquad \frac{}{\mathsf{len}(1^x) \doteq x}$$

$$\frac{}{\mathsf{len}(\mathsf{x}) \neq 0} \ \text{when } \mathsf{x} \in \mathcal{S}_{\mathsf{cst}} \qquad \frac{\mathsf{len}(u) \neq 0}{\mathsf{len}(\langle u\,,\, v\rangle) \neq 0} \qquad \frac{\mathsf{len}(v) \neq 0}{\mathsf{len}(\langle u\,,\, v\rangle) \neq 0} \qquad \frac{A \neq B \qquad \mathsf{len}(A) \neq 0 \qquad x \neq 0}{A^x \neq B^y}\ \text{l-neq}$$

- *The set Ax_{inj} of injectivity axioms:*

$$\frac{}{\neg\mathsf{eq}(u,s) \wedge \mathsf{eq}(\langle u\,,\, v\rangle\,, \langle s\,,\, t\rangle) \doteq \mathsf{false}}\ \text{EQInj}(\langle \cdot\,,\, \_\rangle) \qquad \frac{}{\neg\mathsf{eq}(v,t) \wedge \mathsf{eq}(\langle u\,,\, v\rangle\,, \langle s\,,\, t\rangle) \doteq \mathsf{false}}\ \text{EQInj}(\langle \_\,,\, \cdot\rangle)$$

$$\frac{}{\neg\mathsf{eq}(u,v) \wedge \mathsf{eq}(\{u\}^{\mathsf{n_e}}_{\mathsf{pk(n)}}, \{v\}^{\mathsf{n'_e}}_{\mathsf{pk(n')}}) \doteq \mathsf{false}}\ \text{EQInj}(\{\cdot\}_{\_}^{\_})$$

- *The set $\mathsf{Ax}_{\mathrm{SQN}}$ of sequence number axioms:*

$$\frac{}{\mathsf{range}(u,v) \doteq \mathsf{eq}(u,v)} \qquad \frac{}{\mathsf{suc}(u) \doteq u + 1} \qquad \frac{}{\mathsf{sqn\text{-}init}^{\mathrm{ID}}_{\mathrm{N}} \leq \mathsf{sqn\text{-}init}^{\mathrm{ID}}_{\mathrm{U}}}\ \text{SQN-ini}$$

$$\frac{}{\phi[\vec{u}] \doteq \mathsf{true}} \quad \text{when } \vec{u} \text{ are ground terms and } \mathrm{Th}(\mathbb{Z}, 0, +, -, =, \leq) \models \phi[\vec{x}\,]$$

Fig. 15. The Set of Axiom $\mathsf{Ax}_{\mathsf{impl}} = \mathsf{Ax}_{\mathsf{ite}} \cup \mathsf{Ax}_{\mathsf{eq}} \cup \mathsf{Ax}_{\mathsf{len}} \cup \mathsf{Ax}_{\mathsf{inj}} \cup \mathsf{Ax}_{\mathrm{SQN}}$.

Appendix II
Protocol

A. Symbolic Protocol

In this section we formally define the symbolic traces of the AKA^+ protocol, as well as some functions and properties of these traces.

We recall that $\mathcal{S}_{\mathsf{id}} = \{\text{ID}_1, \dots, \text{ID}_N\}$ is the set of identities used in the protocol. We split these identities between base identities, which are used by the normal protocol, and copies of the base identities, which we use to express the σ_{ul}-unlinkability of the protocol. We have B base identities $\mathsf{A}_1, \dots, \mathsf{A}_B$, and we let $\mathcal{S}_{\mathsf{bid}}$ be the set of base identities. Then, for every base identity A_i, we have C copies $\mathsf{A}_i = \mathsf{A}_{i,1}, \dots, \mathsf{A}_{i,C}$ of A_i. In total we use $N = B \times C$ distinct identities, and $\text{ID}_1, \dots, \text{ID}_N$ is an arbitrary enumeration of all the identities.

a) Valid Symbolic Trace: We recall that an symbolic trace is a sequence of action identifiers, which symbolically represents calls from the adversary to the oracles. Remark that some sequence of action identifiers do not correspond to a valid execution of the protocol. E.g., since the session $\mathit{UE}_{\text{ID}}(j)$ cannot execute both the SUPI and the GUTI protocols, a *valid symbolic trace* cannot contain both $\text{PU}_{\text{ID}}(j, \_)$ and $\text{TU}_{\text{ID}}(j, \_)$. Similarly, the *HN*'s second message in the SUPI protocol cannot be sent before the first message, hence $\text{PN}(j, 1)$ cannot appear before $\text{PN}(j, 0)$ in τ. Formally:

Definition 35. *Let $(\mathcal{Q}_{\text{U}}^{\text{ID}})_{\text{ID} \in \mathcal{S}_{id}}$ and $(\mathcal{Q}_{\text{N}}^{j})_{j \in \mathbb{N}}$ be the automatas given in Fig. 16. A symbolic trace $\tau = \mathsf{ai}_0, \dots, \mathsf{ai}_n$ is a* valid *symbolic trace iff τ is an inter-leaving of the words $w_{\text{ID}^1}, \dots, w_{\text{ID}^N}, w_{\text{N}}^0, \dots, w_{\text{N}}^l, \dots$ where:*

- *for every $1 \leq j \leq N$, w_{ID}^j is a run of $\mathcal{Q}_{\text{U}}^{\text{ID}_j}$.*
- *for every $j \in \mathbb{N}$, w_{N}^j is a run of $\mathcal{Q}_{\text{N}}^j$.*
- *for every $j \in \mathbb{N}$ and $1 \leq i \leq n$, if ai_i is a state of $\mathcal{Q}_{\text{N}}^j$ then there exists $i_0 < i$ such that ai_{i_0} is a state of $\mathcal{Q}_{\text{N}}^{j-1}$*

Furthermore, τ is said to be basic *if for all $1 \leq j \leq N$, if $w_{\text{ID}}^j \neq \epsilon$ then ID_j is a base identity (i.e. $\text{ID}_j \in \{\mathsf{A}_1, \dots, \mathsf{A}_B\}$).*

Since we only informally describe the AKA^+ protocol, we cannot formally prove that every $\tau \in \mathsf{dom}(\mathcal{R}_{\mathsf{ul}})$, τ is a valid symbolic trace. Instead, we put as an assumption that any implementation of the AKA^+ protocol must ensures that messages are processed as described in $\mathcal{Q}_{\text{U}}^{\text{ID}}$ and $\mathcal{Q}_{\text{N}}^j$.

Assumption 1. *For every $\tau \in \mathsf{dom}(\mathcal{R}_{ul})$, τ is a valid symbolic trace*

b) Modeling Unlinkability: Given a symbolic trace $\tau \in \mathsf{dom}(\mathcal{R}_{\mathsf{ul}})$, there is a particular and unique symbolic trace $\underline{\tau}$ which is the "most anonymised trace" corresponding to τ. Intuitively, $\underline{\tau}$ is the trace τ where we changed a user identity every time we could (i.e. every time $\text{NS}_{\text{ID}}(\_)$ appears). This is useful to prove that the 5G-AKA protocol is σ_{ul}-unlinkable, as it reduces the number of cases we have to consider: we only need to show that we can derive $\phi_\tau \sim \phi_{\underline{\tau}}$ for every $\tau \in \mathsf{dom}(\mathcal{R}_{\mathsf{ul}})$.

Definition 36. *Given an identity $\mathsf{A}_{b,c}$ where $c < C$, we let $\mathsf{fresh\text{-}id}(\mathsf{A}_{b,c}) = \mathsf{A}_{b,c+1}$, and given a base identity $\mathsf{A}_{b,1}$ we let $\mathsf{copies\text{-}id}(\mathsf{A}_{b,1}) = \{\mathsf{A}_{b,1} \mid 1 \leq i \leq C\}$.*

Definition 37. *We define some functions on symbolic traces:*

- *We let h be the function that, given a symbolic trace τ, returns the last action in τ (or ϵ is τ is empty):*

$$\mathsf{h}(\tau) \;=\; \begin{cases} \mathsf{ai}_n & \text{if } \tau = \mathsf{ai}_0, \dots, \mathsf{ai}_n \text{ and } n \geq 0 \\ \epsilon & \text{if } \tau = \epsilon \end{cases}$$

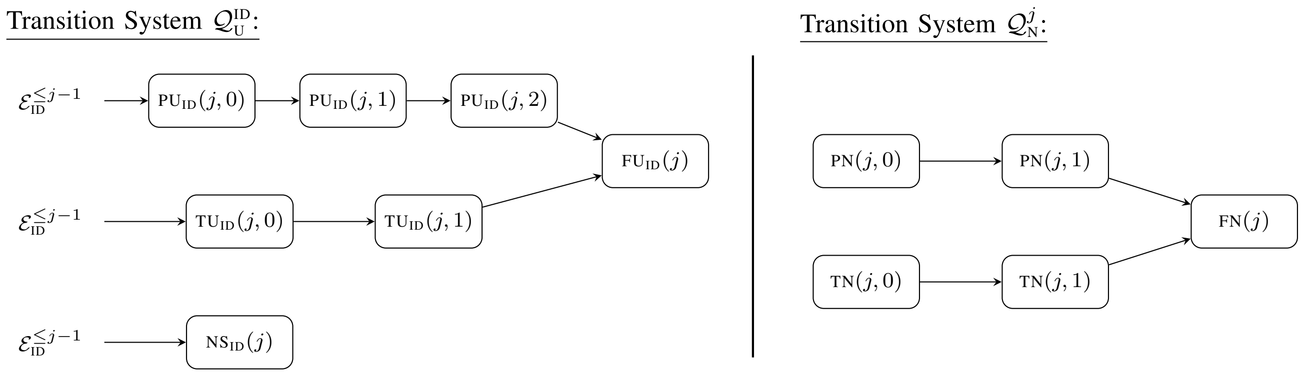
- *Given a symbolic trace τ, we let $\prec_\tau$ be the restriction of $\prec$ to the set of strict prefixes of τ, i.e. $\tau_2 \prec_\tau \tau_1$ iff $\tau_2 \prec \tau_1$ and $\tau_1 \prec \tau$.*
- *We extend $\prec_\tau$ to symbolic actions as follows: we have $\mathsf{ai} \prec_\tau \tau_1$ (resp. $\tau_1 \prec_\tau \mathsf{ai}$) iff there exists τ_2 such that $\mathsf{h}(\tau_2) = \mathsf{ai}$ and $\tau_2 \prec_\tau \tau_1$ (resp. $\tau_1 \prec_\tau \tau_2$).*

Definition 38. *Given a symbolic trace τ with less than C actions $\text{NS}_{\text{ID}}(\_)$ for every ID, we define the symbolic trace $\underline{\tau}$ where each time we encounter a action $\text{NS}_{\text{ID}}(j)$, we replace all subsequent action with agent ID by action with agent $\mathsf{fresh\text{-}id}(\text{ID})$:*

$$\underline{\tau} = \begin{cases} \text{NS}_{\nu\text{ID}}(j), \underline{\tau_0[\nu\text{ID}/\text{ID}]} & \text{when } \tau = \text{NS}_{\text{ID}}(j), \tau_0 \text{ and } \nu\text{ID} = \mathsf{fresh\text{-}id}(\text{ID}) \\ \mathsf{ai}, \underline{\tau_0} & \text{when } \tau = \mathsf{ai}, \tau_0 \text{ and } \mathsf{ai} \notin \{\text{NS}_{\text{ID}}(j) \mid \text{ID} \in \mathcal{S}_{id}, j \in \mathbb{N}\} \end{cases}$$

One can easily check that $\mathcal{R}_{\mathsf{ul}}(\tau, \underline{\tau})$. Besides, remark that for every $(\tau_l, \tau_r) \in \mathcal{R}_{\mathsf{ul}}$ we have $\underline{\tau_l} = \underline{\tau_r}$. Moreover, $\sim$ is a transitive relation. Therefore, instead of proving that for every $\mathcal{R}_{\mathsf{ul}}(\tau_l, \tau_r)$ the formula $\sigma_{\tau_l} \sim \sigma_{\tau_r}$ can be derived using Ax, it is sufficient to show that for every $\tau \in \mathsf{dom}(\mathcal{R}_{\mathsf{ul}})$, we can derive $\sigma_\tau \sim \sigma_{\underline{\tau}}$ using Ax. Formally:

Proposition 19. *The 5G-AKA protocol is σ_{ul}-unlinkable in any computational model satisfying some axioms Ax if for every $\tau \in \mathsf{dom}(\mathcal{R}_{ul})$, there is a derivation using Ax of $\phi_\tau \sim \phi_{\underline{\tau}}$.*



Convention: where $\mathcal{E}_{\text{ID}}^{\leq j} = \{\text{PU}_{\text{ID}}(j_0, i), \text{TU}_{\text{ID}}(j_0, i), \text{FU}_{\text{ID}}(j_0), \text{NS}_{\text{ID}}(j_0) \mid j_0 \leq j\}$, the initial states of $\mathcal{Q}_{\text{U}}^{\text{ID}}$ are $\text{PU}_{\text{ID}}(0,1)$ and $\text{TU}_{\text{ID}}(0,0)$, and the initial states of $\mathcal{Q}_{\text{N}}^{j}$ are $\text{PN}(j,0)$ and $\text{TN}(j,0)$. Every state of $\mathcal{Q}_{\text{U}}^{\text{ID}}$ or $\mathcal{Q}_{\text{N}}^{j}$ is final.

Fig. 16. The transition systems used to define valid symbolic traces.

Proof. Assume that for every $\tau \in \mathsf{dom}(\mathcal{R}_{\mathsf{ul}})$, we can derive using Ax the formula $\phi_\tau \sim \phi_{\underline{\tau}}$. Then, using Proposition 1 we know that 5G-AKA protocol is σ_{ul}-unlinkable in any computational model satisfying axioms Ax if for every $(\tau_l, \tau_r) \in \mathcal{R}_{\mathsf{ul}}$, we can derive $\phi_{\tau_l} \sim \phi_{\tau_r}$. If AKA$^+$ is σ_{ul}-unlinkable with N identities then it is σ_{ul}-unlinkable with N' identities if $N' \leq N$. Therefore, w.l.o.g. we can always assume that we have more identities than actions $\text{NS}_{\text{ID}}(\_)$ in τ. Hence $\underline{\tau}$ is well-defined, and we know that $(\tau_l, \underline{\tau_l}) \in \mathcal{R}_{\mathsf{ul}}$ and $(\tau_r, \underline{\tau_r}) \in \mathcal{R}_{\mathsf{ul}}$. By hypothesis, we have derivations of $\phi_{\tau_l} \sim \phi_{\underline{\tau_l}}$ and $\phi_{\tau_r} \sim \phi_{\underline{\tau_r}}$. Since $\underline{\tau_l} = \underline{\tau_r}$, and using the transitivity and symmetry axioms Trans and Sym, we get a derivation of $\phi_{\tau_l} \sim \phi_{\tau_r}$. This concludes this proof. ■

Proposition 20. *If τ is a valid basic symbolic trace with less than C actions* NS *then $\underline{\tau}$ is a valid symbolic trace.*

Proof. The proof is straightforward by induction over τ. ■

Definition 39. *Given a basic trace τ and a basic identity $\text{ID} = A_{i,0}$, we let $\nu_\tau(\text{ID})$ be the identity $A_{i,l}$ where l is the number of occurrences of $\text{NS}_{\text{ID}}(\_)$ in τ.*

Definition 40. *Let τ be a symbolic trace of actions $\mathsf{ai}_0, \dots, \mathsf{ai}_n$. Then for all $0 \leq i < n$, $\mathsf{suc}_\tau(\mathsf{ai}_i) = \mathsf{ai}_{i+1}$.*

Definition 41. *We define the partial* $\mathsf{session}$ *function:*

$$\mathsf{session}_{\text{N}}(\mathsf{ai}) = j \text{ when } \mathsf{ai} = \text{X}(j,\_), \text{X} \in \{\text{PN}, \text{TN}, \text{FN}\}$$

Definition 42. *We let $\mathsf{session\text{-}started}_j(\tau)$ be true if and only if there exists $\mathsf{ai} \in \tau$ s.t. $\mathsf{session}(\mathsf{ai}) = j$.*

B. The AKA$^+$ *Protocol*

To show that the AKA$^+$ protocol is σ_{ul}-unlinkable, we need to know, for every identity $\text{ID} \in \mathcal{S}_{\mathsf{id}}$, if there was a successful SUPI session since the last $\text{NS}_{\text{ID}}(\_)$. To do this, we extend the set of variables $\mathcal{S}_{\mathsf{var}}$ by adding a phantom variable $\mathsf{sync}_{\text{U}}^{\text{ID}}$ for every $\text{ID} \in \mathcal{S}_{\mathsf{id}}$. We also extend the symbolic state updates of $\text{NS}_{\text{ID}}(\_)$ and $\text{PU}_{\text{ID}}(j,2)$ as follows:

- For $\mathsf{ai} = \text{NS}_{\text{ID}}(j)$:

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \mathsf{valid\text{-}guti}_{\text{U}}^{\text{ID}} \mapsto \mathsf{false} \\ \mathsf{sync}_{\text{U}}^{\text{ID}} \mapsto \mathsf{false} \end{cases}$$

- For $\mathsf{ai} = \text{PU}_{\text{ID}}(j,2)$:

$$\sigma_\tau^{\mathsf{up}} \equiv \begin{cases} \mathsf{e\text{-}auth}_{\text{U}}^{\text{ID}} \mapsto \mathsf{if}\ \mathsf{accept}_\tau^{\text{ID}}\ \mathsf{then}\ \sigma_\tau^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}})\ \mathsf{else\ fail} \\ \mathsf{sync}_{\text{U}}^{\text{ID}} \mapsto \sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\text{U}}^{\text{ID}}) \vee \mathsf{accept}_\tau^{\text{ID}} \end{cases}$$

Remark that the variable $\mathsf{sync}_{\text{U}}^{\text{ID}}$ is read only to update its value. It is not used in the actual protocol. By consequence, the AKA$^+$ protocol is σ_{ul}-unlinkable if and only if the extended AKA$^+$ protocol is σ_{ul}-unlinkable.

We now give the definition of the initial symbolic state σ_ϵ, which we omitted in the body:

Definition 43. *The symbolic state σ_ϵ is the function from $\mathcal{S}_{var}$ to terms defined by having, for every $\text{ID} \in \mathcal{S}_{id}$ and $j \in \mathbb{N}$:*

$$\sigma_\epsilon(\text{SQN}_{\text{U}}^{\text{ID}}) \equiv \textit{sqn-init}_{\text{U}}^{\text{ID}} \qquad \sigma_\epsilon(\text{SQN}_{\text{N}}^{\text{ID}}) \equiv \textit{sqn-init}_{\text{N}}^{\text{ID}} \qquad \sigma_\epsilon(\text{GUTI}_{\text{X}}^{\text{ID}}) \equiv \textit{UnSet} \qquad \sigma_\epsilon(\textit{e-auth}_{\text{U}}^{\text{ID}}) \equiv \textit{fail} \qquad \sigma_\epsilon(\textit{b-auth}_{\text{U}}^{\text{ID}}) \equiv \textit{fail}$$

$$\sigma_\epsilon(\textit{e-auth}_{\text{N}}^{j}) \equiv \textit{fail} \qquad \sigma_\epsilon(\textit{b-auth}_{\text{N}}^{j}) \equiv \textit{fail} \qquad \sigma_\epsilon(\text{s-valid-guti}_{\text{U}}^{\text{ID}}) \equiv \text{false} \qquad \sigma_\epsilon(\text{valid-guti}_{\text{U}}^{\text{ID}}) \equiv \text{false}$$

$$\sigma_\epsilon(\text{session}_{\text{N}}^{\text{ID}}) \equiv \text{false} \qquad \sigma_\epsilon(\text{sync}^{\text{ID}}) \equiv \text{false}$$

C. Invariants and Necessary Acceptance Conditions

a) Notations: From now on, the set of axioms Ax is fixed, and we stop specify the set of axioms used: we say that we have a derivation of a formula ϕ to mean that ϕ can be deduced from Ax. Furthermore, we say that ϕ holds when there is a derivation of ϕ.

Moreover, we abuse notations and write $u = v$ instead of $u \doteq v$. We can always disambiguate using the context: if we expect a term, then $u = v$ stands for the term $\mathsf{eq}(u, v)$, whereas if a formula is expected then $u = v$ stands for $\mathsf{eq}(u, v) \sim \mathsf{true}$. We extends this to any boolean term: if b is a boolean term then we say that b holds if we can show that $b \sim \mathsf{true}$ holds. For example, $\sigma_\tau(\text{SQN}_{\text{U}}^{\text{ID}}) \geq \sigma_\tau(\text{SQN}_{\text{N}}^{\text{ID}})$ holds if we can show that $\mathsf{geq}(\sigma_\tau(\text{SQN}_{\text{U}}^{\text{ID}}), \sigma_\tau(\text{SQN}_{\text{N}}^{\text{ID}})) \sim \mathsf{true}$.

b) Properties: We now start to state and prove properties of the AKA$^+$ protocol.

Proposition 21. *For every valid symbolic trace τ, for every $\text{ID}_1, \text{ID}_2 \in \mathcal{S}_{id}$, we have a derivation of:*

$$\overline{\textit{len}(\sigma_\tau^{\textit{in}}(\text{SQN}_{\text{U}}^{\text{ID}_1})) = \textit{len}(\sigma_\tau^{\textit{in}}(\text{SQN}_{\text{U}}^{\text{ID}_2}))}$$

Proof. It is easy to show by induction over τ that for every $\text{ID} \in \mathcal{S}_{\text{id}}$, there exists an if-context C, terms $\vec{b}$ and integers $(k_i)_i$ such that:

$$\sigma_\tau^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}) = C[\vec{b} \diamond (\text{suc}^{k_i}(\text{sqn-init}_{\text{U}}^{\text{ID}}))_i)]$$

Therefore, let C_1, C_2, $\vec{b}_1, \vec{b}_2$ and $(k_i^1)_i, (k_j^2)_j$ be such that:

$$\sigma_\tau^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}_1}) = C_1[\vec{b}_1 \diamond (\text{suc}^{k_i^1}(\text{sqn-init}_{\text{U}}^{\text{ID}_1}))_i)] \qquad \sigma_\tau^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}_2})) = C_2[\vec{b}_2 \diamond (\text{suc}^{k_j^2}(\text{sqn-init}_{\text{U}}^{\text{ID}_2}))_j)]$$

Moreover, it is trivial to show using the axioms in $\mathsf{Ax}_{\mathsf{len}}$ that for every i, i', j, j':

$$\text{len}(\text{suc}^{k_i^1}(\text{sqn-init}_{\text{U}}^{\text{ID}_1})) = \text{len}(\text{suc}^{k_{i'}^1}(\text{sqn-init}_{\text{U}}^{\text{ID}_1})) = \text{len}(\text{suc}^{k_j^2}(\text{sqn-init}_{\text{U}}^{\text{ID}_2})) = \text{len}(\text{suc}^{k_{j'}^2}(\text{sqn-init}_{\text{U}}^{\text{ID}_2}))$$

It is then easy, using R, to get a derivation of:

$$\overline{\text{len}(\sigma_\tau^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}_1})) = \text{len}(\sigma_\tau^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}_2}))}$$ ∎

The following proposition states that n_{N} appears only in the *HN* public key $\mathsf{pk}(\mathsf{n}_{\text{N}})$ and secret key $\mathsf{sk}(\mathsf{n}_{\text{N}})$, and that for every $\text{ID} \in \mathcal{S}_{\text{id}}$, the keys k^{ID} and $\mathsf{k}_{\mathsf{m}}^{\text{ID}}$ appear only in key position in Mac^1–Mac^5. These properties will be useful to apply the cryptographic axioms later.

Proposition 22 (Invariant (INV-KEY))**.** *For all valid symbolic trace τ, we have:*

$$\begin{aligned} & \textit{n}_{\text{N}} \sqsubseteq_{\textit{pk}(\cdot),\textit{sk}(\cdot)} \phi_\tau \ \wedge\ \textit{sk}(\textit{n}_{\text{N}}) \sqsubseteq_{\textit{dec}(\_,\cdot)} \phi_\tau \\ \forall 1 \leq i \leq N, \quad & \textit{k}_m^{\text{ID}_i} \sqsubseteq_{\textit{Mac}_\cdot(\_)} \phi_\tau \\ \forall 1 \leq i \leq N, \quad & \textit{k}^{\text{ID}_i} \sqsubseteq_{f_\cdot(\_),f'_\cdot(\_)} \phi_\tau \end{aligned}$$

Proof. The proof is straightforward by induction on τ. ∎

Proposition 23. *For every valid symbolic trace τ, for every $\tau_2 \prec_\tau \tau_i$ and identity $\text{ID} \in \mathcal{S}_{id}$, we have:*

$$\left(\sigma_{\tau_2}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \textit{UnSet} \wedge \bigwedge_{\substack{\tau_1 = \_,\text{FU}_{\text{ID}}(j_1) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \neg\text{accept}_{\tau_1}^{\text{ID}} \right) \rightarrow \sigma_{\tau_i}^{\textit{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \textit{UnSet}$$

Proof. The proof is straightforward by induction on τ_i. ∎

We now state several simple properties of our system.

Proposition 24. *Let $\tau = \_, \textsf{ai}$ be a valid symbolic trace, then:*

1) **(A1)** *If $\neg\textit{session-started}_j(\tau)$ then $n^j \notin \textit{st}(\phi_\tau)$.*

2) *(A2) For all* $\tau_0 = \_, \text{PU}_{\text{ID}}(j_0, 2) \preceq \tau$ *and* $\tau_1 = \_, \text{PU}_{\text{ID}}(j_1, 2) \preceq \tau$*, if* $\tau_0 \neq \tau_1$ *then:*

$$\sigma^{in}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) \neq \sigma^{in}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})$$

3) *(A3) For every* $\tau_0 = \_, \text{PU}_{\text{ID}}(j_0, 2)$*,* $\tau_1 = \_, \text{PU}_{\text{ID}}(j_1, 1)$ *such that* $\tau_1 \prec_\tau \tau_0$*, if* $j_0 \neq j_1$ *then:*

$$\sigma^{in}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) \neq \mathsf{suc}(\sigma^{in}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))$$

4) *(A4) For all* $\text{ID}_0 \neq \text{ID}_1$*,*

$$\left(\sigma^{in}_{\tau}(\text{GUTI}^{\text{ID}_0}_{\text{N}}) \neq \mathsf{UnSet} \wedge \sigma^{in}_{\tau}(\text{GUTI}^{\text{ID}_1}_{\text{N}}) \neq \mathsf{UnSet}\right) \;\rightarrow\; \sigma^{in}_{\tau}(\text{GUTI}^{\text{ID}_0}_{\text{N}}) \neq \sigma^{in}_{\tau}(\text{GUTI}^{\text{ID}_1}_{\text{N}})$$

5) *(A5) , (A6) , (A7) If* $\mathsf{h}(\tau) = \text{PN}(j, 1), \text{TN}(j, 0)$ *or* $\text{TN}(j, 1)$*, then for every* $\text{ID}_0 \neq \text{ID}_1$*,*

$$\left(\neg\mathsf{accept}^{\text{ID}_0}_{\tau}\right) \vee \left(\neg\mathsf{accept}^{\text{ID}_1}_{\tau}\right)$$

6) *(A8) For every* $\text{ID} \in \mathcal{S}_{id}$*,* $j \in \mathbb{N}$*,* $\sigma^{in}_{\tau}(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^j \rightarrow \sigma^{in}_{\tau}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^j$.

Proof. All these properties are simple to show:

(A1) is trivial by induction over τ.

- **(A2)** and **(A3)** both follow from the fact that if $\tau = \_, \text{PU}_{\text{ID}}(j, 1)$ then $\sigma_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) \equiv \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}))$, and therefore $\sigma_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) > \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}})$.
- **(A5)** and **(A7)** follow easily from the unforgeability axioms EUF-MAC.
- To prove **(A4)**, we first observe that for every $\text{ID} \in \mathcal{S}_{\mathsf{id}}$, we initially have $\sigma_\epsilon(\text{GUTI}^{\text{ID}}_{\text{N}}) \equiv \mathsf{UnSet}$, and that the only value we store in $\text{GUTI}^{\text{ID}}_{\text{N}}$ are UnSet or GUTI^i for some $i \in \mathbb{N}$. Therefore it is easy to show that for every $\tau_n \prec \tau$:

$$\sigma^{\mathsf{in}}_{\tau_n}(\text{GUTI}^{\text{ID}}_{\text{N}}) \neq \mathsf{UnSet} \rightarrow \bigvee_{i \in \mathbb{N}} \sigma^{\mathsf{in}}_{\tau_n}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \text{GUTI}^i$$

Moreover, we can only store GUTI^i in $\text{GUTI}^{\text{ID}}_{\text{N}}$ at $\text{PN}(i, 1)$ or $\text{TN}(i, 1)$, and by validity τ cannot contain both $\text{PN}(i, 1)$ and $\text{TN}(i, 1)$. We conclude observing that we cannot have $\mathsf{accept}^{\text{ID}_0}_{\tau_n}$ and $\mathsf{accept}^{\text{ID}_1}_{\tau_n}$ if $\tau_n = \_, \text{PN}(i, 1)$ or $\_, \text{TN}(i, 1)$ using **(A5)** and **(A7)**. The result follows.

- **(A6)** is a consequence of **(A4)**.
- **(A8)** follows from the fact that whenever a new session of the protocol is started, we reset both $\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}$ and $\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}$. Then $\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}$ is either set to fail or to $\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}$. ■

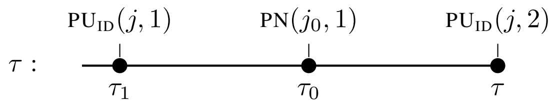
We can now state and prove our first acceptance necessary conditions.

Lemma 6. *Let* $\tau = \_, \mathsf{ai}$ *be a valid symbolic trace, then:*

1) *(Acc1) If* $\mathsf{ai} = \text{PN}(j, 1)$*, then for every* ID *we have:*

$$\mathsf{accept}^{\text{ID}}_{\tau} \rightarrow \bigvee_{\tau_0 = \_, \text{PU}_{\text{ID}}(j_0, 1) \prec \tau} \left(\pi_1(g(\phi^{in}_{\tau})) = \{\langle \text{ID}\,,\, \sigma^{in}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}_e^{j_0}}_{\mathsf{pk}_{\text{N}}} \wedge g(\phi^{in}_{\tau_0}) = \mathsf{n}^j\right)$$

2) *(Acc2) If* $\mathsf{ai} = \text{PU}_{\text{ID}}(j, 2)$*. Let* $\tau_1 = \_, \text{PU}_{\text{ID}}(j, 1) \prec \tau$*. Then:*



$$\mathsf{accept}^{\text{ID}}_{\tau} \;\rightarrow\; \bigvee_{\substack{\tau_0 = \_, \text{PN}(j_0, 1) \\ \tau_1 \prec_\tau \tau_0}} \mathsf{accept}^{\text{ID}}_{\tau_0} \;\wedge\; g(\phi^{in}_{\tau_1}) = \mathsf{n}^{j_0} \;\wedge\; \pi_1(g(\phi^{in}_{\tau_0})) = \{\langle \text{ID}\,,\, \sigma^{in}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}_e^j}_{\mathsf{pk}_{\text{N}}}$$

3) *(Acc3) If* $\mathsf{ai} = \text{TU}_{\text{ID}}(j, 1)$ *then:*

$$\mathsf{accept}^{\text{ID}}_{\tau} \;\rightarrow\; \bigvee_{\substack{\tau_0 = \_, \text{TN}(j_0, 0) \\ \tau_0 \prec \tau}} \begin{pmatrix} \mathsf{accept}^{\text{ID}}_{\tau_0} \wedge \pi_1(g(\phi^{in}_{\tau})) = \mathsf{n}^{j_0} \wedge \pi_2(g(\phi^{in}_{\tau})) = \sigma^{in}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{N}}) \oplus \mathsf{f}_k(\mathsf{n}^{j_0}) \\ \wedge\, \sigma^{in}_{\tau}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{in}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}}) \end{pmatrix}$$

4) *(Acc4) If* $\mathsf{ai} = \text{TN}(j, 1)$ *then:*

$$\mathsf{accept}^{\text{ID}}_{\tau} \;\rightarrow\; \bigvee_{\tau_0 = \_, \text{TU}_{\text{ID}}(\_, 1) \prec \tau} \mathsf{accept}^{\text{ID}}_{\tau_0} \wedge \pi_1(g(\phi^{in}_{\tau_0})) = \mathsf{n}^j$$

D. Proof of Lemma 6

*Proof of **(Acc1)**:* Let $\mathsf{ai} = \textsc{pn}(j, 1)$ and $\mathsf{k_m} \equiv \mathsf{k}^i_\mathsf{m}$. Recall that:

$$\mathsf{accept}^{\textsc{id}}_\tau \;\equiv\; \begin{pmatrix} & \mathsf{eq}(\pi_1(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_\tau)), \mathsf{sk}_\textsc{n})), \textsc{id}) \\ \wedge & \mathsf{eq}(\pi_2(g(\phi^{\mathsf{in}}_\tau)), \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_\tau)) \,,\, \mathsf{n}^j \rangle)) \end{pmatrix}$$

We apply the $\textsc{euf-mac}^1$ axiom (invariant (INV-KEY) guarantees that the syntactic side-conditions hold):

$$\begin{aligned} \mathsf{accept}^{\textsc{id}}_\tau \;&\rightarrow\; \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_\tau)) \,,\, \mathsf{n}^j \rangle) \\ &\rightarrow \left(\begin{array}{l} \displaystyle\bigvee_{\tau_0 = \_, \textsc{pu}_\textsc{id}(j_0,1) \prec \tau} \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \{\langle \textsc{id} \,,\, \sigma^{\mathsf{in}}_{\tau_0}(\textsc{sqn}^\textsc{id}_\textsc{u}) \rangle\}^{\mathsf{n}_\mathsf{e}^{j_0}}_{\mathsf{pk}_\textsc{n}} \,,\, g(\phi^{\mathsf{in}}_{\tau_0}) \rangle) \\ \vee \displaystyle\bigvee_{\tau_0 = \_, \textsc{pn}(j_0,1) \prec \tau} \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) \,,\, \mathsf{n}^{j_0} \rangle) \end{array} \right) \end{aligned}$$

From the validity of τ we know that $j_0 \neq j$. Hence using the axiom Fresh, we get that $\mathsf{n}^{j_0} \neq \mathsf{n}^j$. Using the right injectivity of the pair (axiom $\mathsf{EQInj}(\langle \_ \,,\, \cdot \rangle)$), we know that:

$$\langle \pi_1(g(\phi^{\mathsf{in}}_\tau)) \,,\, \mathsf{n}^j \rangle \neq \langle \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) \,,\, \mathsf{n}^{j_0} \rangle$$

From the collision-resistance of Mac (axiom $\textsc{cr}^1$), we have:

$$\mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_\tau)) \,,\, \mathsf{n}^j \rangle) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) \,,\, \mathsf{n}^{j_0} \rangle) \rightarrow \langle \pi_1(g(\phi^{\mathsf{in}}_\tau)) \,,\, \mathsf{n}^j \rangle = \langle \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) \,,\, \mathsf{n}^{j_0} \rangle$$

Therefore:

$$\pi_2(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_\tau)) \,,\, \mathsf{n}^j \rangle) \;\;\rightarrow\;\; \neg \left(\bigvee_{\tau_0 = \_, \textsc{pn}(j_0,1) \prec \tau} \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) \,,\, \mathsf{n}^{j_0} \rangle) \right) \tag{7}$$

From which it follows that:

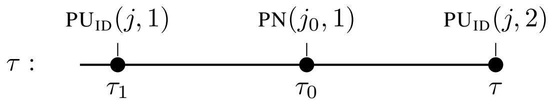
$$\mathsf{accept}^{\textsc{id}}_\tau \;\rightarrow\; \bigvee_{\tau_0 = \_\ \textsc{pu}_\textsc{id}(j_0,1) \prec \tau} \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \{\langle \textsc{id} \,,\, \sigma^{\mathsf{in}}_{\tau_0}(\textsc{sqn}^\textsc{id}_\textsc{u}) \rangle\}^{\mathsf{n}_\mathsf{e}^{j_0}}_{\mathsf{pk}_\textsc{n}} \,,\, g(\phi^{\mathsf{in}}_{\tau_0}) \rangle)$$

To conclude, we use $\textsc{cr}^1$, $\mathsf{EQInj}(\langle \_ \,,\, \cdot \rangle)$ and $\mathsf{EQInj}(\langle \cdot \,,\, \_ \rangle)$ to show that for all $\tau_0 = \_, \textsc{pu}_\textsc{id}(j_0, 1) \prec \tau$:

$$\begin{pmatrix} \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_\tau)) \,,\, \mathsf{n}^j \rangle) \\ \wedge\ \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^1_{\mathsf{k_m}}(\langle \{\langle \textsc{id} \,,\, \sigma^{\mathsf{in}}_{\tau_0}(\textsc{sqn}^\textsc{id}_\textsc{u}) \rangle\}^{\mathsf{n}_\mathsf{e}^{j_0}}_{\mathsf{pk}_\textsc{n}} \,,\, g(\phi^{\mathsf{in}}_{\tau_0}) \rangle) \end{pmatrix} \rightarrow \begin{pmatrix} \pi_1(g(\phi^{\mathsf{in}}_\tau)) = \{\langle \textsc{id} \,,\, \sigma^{\mathsf{in}}_{\tau_0}(\textsc{sqn}^\textsc{id}_\textsc{u}) \rangle\}^{\mathsf{n}_\mathsf{e}^{j_0}}_{\mathsf{pk}_\textsc{n}} \\ \wedge\ \mathsf{n}^j = g(\phi^{\mathsf{in}}_{\tau_0}) \end{pmatrix}$$

This, together with 7, concludes the proof.

*Proof of **(Acc2)**:*



If $\mathsf{ai} = \textsc{pu}_\textsc{id}(j, 2)$. Let $\mathsf{k_m}$ be the Mac key corresponding to $\textsc{id}$, i.e. $\mathsf{k_m} \equiv \mathsf{k}^\textsc{id}_\mathsf{m}$. Recall that:

$$\mathsf{accept}^{\textsc{id}}_\tau \;\equiv\; g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \sigma^{\mathsf{in}}_\tau(\mathsf{b\text{-}auth}^\textsc{id}_\textsc{u}) \,,\, \sigma^{\mathsf{in}}_\tau(\textsc{sqn}^\textsc{id}_\textsc{u}) \rangle)$$

a) Part 1: We are going to apply the $\textsc{p-euf-mac}^2$ axiom. We let:

$$S = \{\tau_0 \mid \tau_0 = \_, \textsc{pn}(j_0, 1) \prec \tau\}$$

and for all $S_0 \subseteq S$ we let:

$$b_{S_0} = \Big(\bigwedge_{\tau_0 \in S_0} \mathsf{accept}^{\textsc{id}}_{\tau_0} \Big) \wedge \Big(\bigwedge_{\tau_0 \in \overline{S_0}} \neg \mathsf{accept}^{\textsc{id}}_{\tau_0} \Big)$$

Then $(b_{S_0})_{S_0 \subseteq S}$ is a valid CS partition. It is straightforward to check that for every $S_0 \subseteq S$, for every $\tau_0 = \_, \textsc{pn}(j_0, 1) \prec \tau$, if $\tau_0 \in S_0$ then we can rewrite $[b_{S_0}]t_{\tau_0}$ into a term $[b_{S_0}]t^{S_0}_{\tau_0}$ by removing the branch corresponding to $\mathsf{accept}^{\textsc{id}}_{\tau_0}$. Therefore:

$$\mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0} \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})), \mathsf{sk}_\textsc{n}))) \rangle) \in \mathsf{set\text{-}mac}^2_{\mathsf{k_m}}(t^{S_0}_{\tau_0}) \text{ if and only if } \tau_0 \in S_0$$

Hence by applying the P-EUF-MAC^2 axiom we get that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \rightarrow \bigvee_{S_0 \subseteq S} \left(b_{S_0} \wedge \begin{array}{c} \bigvee_{\tau_0 \in S_0} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0} \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})), \mathsf{sk_N})))\rangle) \\ \vee \bigvee_{\tau_0 = \_, \text{PU}_{\text{ID}}(j_0,2) \prec \tau} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \sigma^{\mathsf{in}}_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) \,,\, \sigma^{\mathsf{in}}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle) \end{array} \right)$$

We have:

$$\begin{aligned}
\left(\begin{array}{r} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \sigma^{\mathsf{in}}_{\tau}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) \,,\, \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle) \\ \wedge\, g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \sigma^{\mathsf{in}}_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) \,,\, \sigma^{\mathsf{in}}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle) \end{array} \right) &\rightarrow \langle \sigma^{\mathsf{in}}_{\tau}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) \,,\, \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle = \langle \sigma^{\mathsf{in}}_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) \,,\, \sigma^{\mathsf{in}}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle && (\text{CR}^2) \\
&\rightarrow \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) && (\mathsf{EQInj}(\langle _ \,,\, \cdot \rangle)) \\
&\rightarrow \mathsf{false} && \textbf{(P9)}
\end{aligned}$$

Moreover, remark that for $S_0 = \emptyset$, we have:

$$\left(\bigvee_{\tau_0 \in S_0} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^{j} \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})), \mathsf{sk_N})))\rangle) \right) = \mathsf{false}$$

Putting everything together, we get that:

$$\begin{aligned}
\mathsf{accept}^{\text{ID}}_{\tau} &\rightarrow \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} \left(b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^{j} \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})), \mathsf{sk_N})))\rangle) \right) \\
&\rightarrow \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} \bigvee_{\tau_0 \in S_0} \mathsf{accept}^{\text{ID}}_{\tau_0} \wedge g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^{j} \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})), \mathsf{sk_N})))\rangle) \\
&\rightarrow \bigvee_{\substack{\tau_0 = _, \text{PN}(j_0,1) \\ \tau_0 \prec \tau}} \mathsf{accept}^{\text{ID}}_{\tau_0} \wedge g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k_m}}(\langle \mathsf{n}^{j} \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})), \mathsf{sk_N})))\rangle) \\
&\rightarrow \bigvee_{\substack{\tau_0 = _, \text{PN}(j_0,1) \\ \tau_0 \prec \tau}} \mathsf{accept}^{\text{ID}}_{\tau_0} \wedge \langle \sigma^{\mathsf{in}}_{\tau}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) \,,\, \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle = \langle \mathsf{n}^{j} \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})), \mathsf{sk_N})))\rangle && (\text{CR}^2) \\
&\rightarrow \bigvee_{\substack{\tau_0 = _, \text{PN}(j_0,1) \\ \tau_0 \prec \tau}} \begin{array}{l} \mathsf{accept}^{\text{ID}}_{\tau_0} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j} \\ \wedge\ \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) = \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})), \mathsf{sk_N}))) \end{array} && (\mathsf{EQInj}(\langle _ \,,\, \cdot \rangle) \text{ and } \mathsf{EQInj}(\langle \cdot \,,\, _ \rangle))
\end{aligned}$$

b) Part 2: It only remains to show that we can restrict ourselves to the τ_0 such that $\tau_1 \prec_{\tau} \tau_0$. Using **(Acc1)** we know that:

$$\mathsf{accept}^{\text{ID}}_{\tau_0} \rightarrow \bigvee_{\substack{\tau' = \_, \text{PU}_{\text{ID}}(j',1) \\ \tau' \prec_{\tau} \tau_0}} \left(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \{\langle \text{ID} \,,\, \sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle\}^{\mathsf{n}_{\mathsf{e}}^{j'}}_{\mathsf{pk_N}} \wedge g(\phi^{\mathsf{in}}_{\tau'}) = \mathsf{n}^{j_0} \right)$$

Let $\tau' = \_, \text{PU}_{\text{ID}}(j',1)$ such that $\tau' \prec_{\tau} \tau_0$. We now show that if $j' \neq j$ then the tests fail, which proves the impossibility of replaying an old message here. Assume $j' \neq j$, then:

$$\begin{aligned}
&\sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) = \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0})), \mathsf{sk_N}))) \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \{\langle \text{ID} \,,\, \sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle\}^{\mathsf{n}_{\mathsf{e}}^{j'}}_{\mathsf{pk_N}} \\
\rightarrow\ &\sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) = \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}})) \\
\rightarrow\ &\mathsf{false} && \textbf{(P9b)}
\end{aligned}$$

We deduce that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \rightarrow \bigvee_{\substack{\tau_0 = \_, \text{PN}(j_0,1) \\ \tau_1 \prec_{\tau} \tau_0}} \mathsf{accept}^{\text{ID}}_{\tau_0} \wedge g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^{j_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \{\langle \text{ID} \,,\, \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle\}^{\mathsf{n}_{\mathsf{e}}^{j}}_{\mathsf{pk_N}}$$

*Proof of **(Acc3)**:* Let $\mathsf{ai} = \text{TU}_{\text{ID}}(j, 1)$ and k be the f key corresponding to ID. We know that:

$$\mathsf{accept}_\tau^{\text{ID}} \;\rightarrow\; \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}}))\,, \pi_2(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f_k}(\pi_1(g(\phi_\tau^{\mathsf{in}})))\,,\, \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})\rangle)$$

We are going to apply the P-EUF-MAC^3 axiom. We let $S = S_{\text{N}} \cup S_{\text{U}}$, where:

$$S_{\text{N}} = \{\tau_0 \mid \tau_0 = \_, \text{TN}(j_0, 1) \prec \tau\} \qquad\qquad S_{\text{U}} = \{\tau_0 \mid \tau_0 = \_, \text{TU}_{\text{ID}}(j_0, 1) \prec \tau\}$$

and for all $S_0 \subseteq S$ we let:

$$b_{S_0} = \Big(\bigwedge_{\tau_0 \in S_0} \mathsf{accept}_{\tau_0}^{\text{ID}}\Big) \wedge \Big(\bigwedge_{\tau_0 \in \overline{S_0}} \neg\mathsf{accept}_{\tau_0}^{\text{ID}}\Big)$$

Then $(b_{S_0})_{S_0 \subseteq S}$ is a valid CS partition. It is straightforward to check that for every $S_0 \subseteq S$, for every $\tau_0 = \_, \text{TN}(j_0, 1) \prec \tau$, if $\tau_0 \in S$ then we can rewrite $[b_{S_0}]t_{\tau_0}$ into a term $[b_{S_0}]t_{\tau_0}^{S_0}$ by removing the branch corresponding to $\mathsf{accept}_{\tau_0}^{\text{ID}}$. Therefore:

$$\mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\,, \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}})\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}})\rangle) \in \mathsf{set\text{-}mac}^3_{\mathsf{k_m}}(t_{\tau_0}^{S_0}) \text{ if and only if } \tau_0 \in S_0$$

Similarly for every $\tau_0 = \_, \text{TU}_{\text{ID}}(j_0, 1) \prec \tau$, if $\tau_0 \in S$ then we can rewrite $[b_{S_0}]t_{\tau_0}$ as follows:

$$[b_{S_0}]t_{\tau_0} = \begin{cases} [b_{S_0}]\mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi_{\tau_0}^{\mathsf{in}}))) & \text{if } \tau_0 \in S_0 \\ [b_{S_0}]\mathsf{error} & \text{if } \tau_0 \in \overline{S_0} \end{cases}$$

Hence by applying the P-EUF-MAC^4 axiom we get that:

$$\mathsf{accept}_\tau^{\text{ID}} \rightarrow \bigvee_{S_0 \subseteq S} \left(b_{S_0} \wedge \bigvee_{\tau_0 \in S_0 \cap S_{\text{N}}} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\,, \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}})\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}})\rangle)\right)$$

By CR^3, $\mathsf{EQInj}(\langle \_\,,\,\cdot\rangle)$ and $\mathsf{EQInj}(\langle \cdot\,,\,\_\rangle)$ we have:

$$\begin{pmatrix} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}}))\,, \pi_2(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f_k}(\pi_1(g(\phi_\tau^{\mathsf{in}})))\,,\, \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})\rangle) \\ \wedge\, \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\,, \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}})\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}})\rangle) \end{pmatrix} \rightarrow$$
$$\pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \wedge \pi_2(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f_k}(\pi_1(g(\phi_\tau^{\mathsf{in}}))) = \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) \wedge \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \sigma_{\tau_0}^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}})$$

Using the idempotence of the $\oplus$ we know that:

$$\big(\pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \;\wedge\; \pi_2(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f_k}(\pi_1(g(\phi_\tau^{\mathsf{in}}))) = \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}})\big) \;\rightarrow\; \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0})$$

Moreover, remark that if $S_0 \cap S_{\text{N}} = \emptyset$, we have:

$$\bigvee_{S_0 \subseteq S} \left(b_{S_0} \wedge \bigvee_{\tau_0 \in S_0 \cap S_{\text{N}}} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\,, \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}})\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}})\rangle)\right) = \mathsf{false}$$

Putting everything together, we get that:

$$\begin{aligned}
\mathsf{accept}_\tau^{\text{ID}} \;&\rightarrow\; \bigvee_{\substack{S_0 \subseteq S \\ S_0 \cap S_{\text{N}} \neq \emptyset}} \left(b_{S_0} \wedge \bigvee_{\tau_0 \in S_0 \cap S_{\text{N}}} \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\,, \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}})\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}})\rangle)\right) \\
&\rightarrow\; \bigvee_{\substack{S_0 \subseteq S \\ S_0 \cap S_{\text{N}} \neq \emptyset}} \bigvee_{\tau_0 \in S_0 \cap S_{\text{N}}} \mathsf{accept}_{\tau_0}^{\text{ID}} \wedge \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\,, \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}})\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}})\rangle) \\
&\rightarrow\; \bigvee_{\tau_0 = _, \text{TN}(j_0, 0) \prec \tau} \mathsf{accept}_{\tau_0}^{\text{ID}} \wedge \pi_3(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}\,, \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}})\,,\, \sigma_{\tau_0}^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}})\rangle) \\
&\rightarrow\; \bigvee_{\tau_0 = _, \text{TN}(j_0, 0) \prec \tau} \mathsf{accept}_{\tau_0}^{\text{ID}} \wedge \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathsf{n}^{j_0} \begin{array}{r} \wedge\, \pi_2(g(\phi_\tau^{\mathsf{in}})) = \sigma_{\tau_0}^{\mathsf{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \\ \wedge\, \sigma_\tau^{\mathsf{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \sigma_{\tau_0}^{\mathsf{in}}(\text{GUTI}_{\text{N}}^{\text{ID}}) \end{array}
\end{aligned}$$

Proof of (Acc4): We are going to apply the P-EUF-MAC^4 axiom. We let $S = \{\tau_0 \mid \tau_0 = \_, \text{TU}_{\text{ID}}(j_0, 1) \prec \tau\}$, and for all $S_0 \subseteq S$ we let :

$$b_{S_0} = \Big(\bigwedge_{\tau_0 \in S_0} \mathsf{accept}^{\text{ID}}_{\tau_0} \Big) \wedge \Big(\bigwedge_{\tau_0 \in \overline{S_0}} \neg \mathsf{accept}^{\text{ID}}_{\tau_0} \Big)$$

Then $(b_{S_0})_{S_0 \subseteq S}$ is a valid CS partition. It is straightforward to check that for every $S_0 \subseteq S$, for every $\tau_0 = \_, \text{TU}_{\text{ID}}(j_0, 1) \prec \tau$:

$$[b_{S_0}] t_{\tau_0} = \begin{cases} [b_{S_0}] \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0}))) & \text{if } \tau_0 \in S_0 \\ [b_{S_0}] \mathsf{error} & \text{if } \tau_0 \in \overline{S_0} \end{cases}$$

Hence by applying the P-EUF-MAC^4 axiom we get that:

$$g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) \rightarrow \bigvee_{S_0 \subseteq S} b_{S_0} \wedge \left(\begin{array}{l} \displaystyle\bigvee_{\tau_0 \in S_0} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0}))) \\ \vee \displaystyle\bigvee_{\tau_0 = \_, \text{TN}(j_0, 1) \prec \tau} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^{j_0}) \end{array} \right)$$

Applying the CR^4 axiom we get that:

$$\begin{aligned} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^{j_0}) \ \wedge \ g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) \rightarrow \ & \mathsf{n}^{j_0} = \mathsf{n}^j && (\text{CR}^4) \\ \rightarrow \ & \mathsf{false} && (\mathsf{EQIndep}) \end{aligned}$$

Moreover, remark that for $S_0 = \emptyset$, we have:

$$\neg \Big(b_{S_0} \wedge \bigvee\nolimits_{\tau_0 \in S_0} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0}))) \Big)$$

Putting everything together, we get that:

$$g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) \rightarrow \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} \Big(b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0}))) \Big)$$

Let $S_0 \subseteq S$ with $S_0 \neq \emptyset$, and let $\tau_0 \in S_0$. Using the CR^4 axiom we know that:

$$g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) \ \wedge \ g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0}))) \ \rightarrow \ \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \mathsf{n}^j$$

Therefore:

$$\begin{aligned} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) \rightarrow \ & \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} \Big(b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_0}))) \Big) \\ \rightarrow \ & \bigvee_{\substack{S_0 \subseteq S \\ S_0 \neq \emptyset}} \Big(b_{S_0} \wedge \bigvee_{\tau_0 \in S_0} \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \mathsf{n}^j \Big) \end{aligned}$$

And using the fact that $b_{S_0} \rightarrow \mathsf{accept}^{\text{ID}}_{\tau_0}$:

$$g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j) \rightarrow \bigvee_{\tau_0 = \_, \text{TU}_{\text{ID}}(\_, 1) \prec \tau} \mathsf{accept}_{\tau_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \mathsf{n}^j$$

We conclude by observing that $\mathsf{accept}^{\text{ID}}_\tau \rightarrow g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k_m}}(\mathsf{n}^j)$.

E. Authentication of the User by the Network

We now prove that the AKA$^+$ protocol provides authentication of the user the network. Remark that the lemma below subsumes Lemma 1.

Lemma 7. *For all valid symbolic trace τ, ϕ^{in}_τ guarantees authentication of the user by the network:*

$$\forall \text{ID} \in \mathcal{S}_{id}, j \in \mathbb{N}, \ \ \sigma^{in}_\tau(\textit{e-auth}^j_{\text{N}}) = \text{ID} \ \rightarrow \ \bigvee_{\tau' \preceq \tau} \sigma^{in}_{\tau'}(\textit{b-auth}^{\text{ID}}_{\text{U}}) = n^j$$

Moreover, if $\tau = \_, \text{TN}(j, 1)$ then:

$$\mathsf{accept}^{\text{ID}}_\tau \ \rightarrow \bigvee_{\tau_0 = \_, \text{TU}_{\text{ID}}(\_, 1) \prec \tau} \sigma_{\tau_0}(\textit{b-auth}^{\text{ID}}_{\text{U}}) = n^j$$

Proof. We prove this by induction on τ. First, for $\tau = \epsilon$ we have that for every ID $\sigma^{\mathsf{in}}_{\tau}(\mathsf{e\text{-}auth}^{j}_{\mathrm{N}}) = \bot \neq \text{ID}$. Therefore the property holds.

Let $\tau = \tau_0, \mathsf{ai}$. Observe that for all j_0, if $\sigma^{\mathsf{up}}_{\tau}(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) = \bot$ and if the authentication property holds for $\phi^{\mathsf{in}}_{\tau_0}$:

$$\forall \text{ID} \in \mathcal{S}_{\mathsf{id}},\ \ \sigma^{\mathsf{in}}_{\tau_0}(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) = \text{ID} \ \rightarrow \bigvee_{\tau' \preceq \tau_0} \sigma^{\mathsf{in}}_{\tau'}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = \mathsf{n}^{j_0}$$

then it holds for τ. Therefore we only need to show that authentication holds for $\mathsf{ai} = \text{PN}(j,1)$ with $j_0 = j$, and for $\mathsf{ai} = \text{TN}(j,1)$ with $j_0 = j$.

- **Case $\mathsf{ai} = \text{PN}(j,1)$:** Let $\text{ID} \in \mathcal{S}_{\mathsf{id}}$. Using $\mathsf{EQConst}$, we know that $\sigma^{\mathsf{in}}_{\tau}(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) = \text{ID} \rightarrow \mathsf{accept}^{\text{ID}}_{\tau}$ is true. Using **(Acc1)** of Proposition 24, we deduce that:

$$\sigma^{\mathsf{in}}_{\tau}(\mathsf{e\text{-}auth}^{j}_{\mathrm{N}}) = \text{ID} \rightarrow \bigvee_{\tau_0 = \_, \text{PU}_{\text{ID}}(j_0,1) \prec \tau} g(\phi^{\mathsf{in}}_{\tau_0}) = \mathsf{n}^{j} \tag{8}$$

By validity of τ, we know there exists τ_2 such that $\tau_2 = \_, \text{PN}(j,0) \prec \tau$. Let $\tau_0 \prec_\tau \tau_2$. We have $\neg\mathsf{session\text{-}started}_j(\mathsf{ai}_0)$, therefore using invariant **(A1)** we get that $n^j \notin \mathsf{st}(\phi^{\mathsf{in}}_{\tau_0})$. It follows from axiom $\mathsf{EQIndep}$ that $\neg g(\phi^{\mathsf{in}}_{\tau_0}) = \mathsf{n}^j$. Hence:

$$\bigvee_{\tau_0 = \_, \text{PU}_{\text{ID}}(j_0,1) \prec \tau} g(\phi^{\mathsf{in}}_{\tau_0}) = \mathsf{n}^{j} \ \leftrightarrow \bigvee_{\substack{\tau_0 = \_, \text{PU}_{\text{ID}}(j_0,1) \\ \tau_2 \prec_\tau \tau_0 \prec \tau}} g(\phi^{\mathsf{in}}_{\tau_0}) = \mathsf{n}^{j} \tag{9}$$

Let τ_0 be such that $\tau_2 \prec_\tau \tau_0 \prec \tau$ and $\tau_0 = \_, \text{PU}_{\text{ID}}(j_0,1)$. Since $\sigma^{\mathsf{up}}_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = g(\phi^{\mathsf{in}}_{\tau_0})$, we know that $\sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = g(\phi^{\mathsf{in}}_{\tau_0})$. Hence:

$$g(\phi^{\mathsf{in}}_{\tau_0}) = \mathsf{n}^j \rightarrow \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = \mathsf{n}^j$$

Which shows that:

$$\bigvee_{\substack{\tau_0 = \_, \text{PU}_{\text{ID}}(j_0,1) \\ \tau_2 \prec_\tau \tau_0 \prec \tau}} g(\phi^{\mathsf{in}}_{\tau_0}) = \mathsf{n}^{j} \rightarrow \bigvee_{\substack{\tau_0 = \_, \text{PU}_{\text{ID}}(j_0,1) \\ \tau_2 \prec_\tau \tau_0 \prec \tau}} \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = \mathsf{n}^j \tag{10}$$

Since $\{\tau_0 \mid \tau_0 = \_, \text{PU}_{\text{ID}}(j_0,1) \wedge \tau_2 \prec_\tau \tau_0 \prec \tau\}$ is a subset of $\{\tau_1 \mid \tau_1 \prec \tau\}$, we have:

$$\begin{aligned} \bigvee_{\substack{\tau_0 = \_, \text{PU}_{\text{ID}}(j_0,1) \\ \tau_2 \prec_\tau \tau_0 \prec \tau}} \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = \mathsf{n}^j \ &\rightarrow \bigvee_{\tau_0 \prec \tau} \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = \mathsf{n}^j \\ &\rightarrow \bigvee_{\tau_0 \preceq \tau} \sigma^{\mathsf{in}}_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = \mathsf{n}^j \end{aligned} \tag{11}$$

We conclude the proof using 8, 9, 10 and 11.

- **Case $\mathsf{ai} = \text{TN}(j,1)$:** Using **(Acc4)**, we know that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \ \rightarrow \bigvee_{\tau_0 = \_, \text{TU}_{\text{ID}}(\_,1) \prec \tau} \mathsf{accept}_{\tau_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \mathsf{n}^j$$

Moreover, for every $\tau_0 = \_, \text{TU}_{\text{ID}}(\_,1) \prec \tau$, we have:

$$\mathsf{accept}^{\text{ID}}_{\tau_0} \ \wedge \ \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \mathsf{n}^j \ \rightarrow \ \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = \mathsf{n}^j$$

Hence:

$$\begin{aligned} \mathsf{accept}^{\text{ID}}_{\tau} &\rightarrow \bigvee_{\tau_0 = \_, \text{TU}_{\text{ID}}(\_,1) \prec \tau} \mathsf{accept}_{\tau_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \mathsf{n}^j \\ &\rightarrow \bigvee_{\tau_0 = \_, \text{TU}_{\text{ID}}(\_,1) \prec \tau} \sigma_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = \mathsf{n}^j \\ &\rightarrow \bigvee_{\tau_0 \preceq \tau} \sigma^{\mathsf{in}}_{\tau_0}(\mathsf{b\text{-}auth}^{\text{ID}}_{\mathrm{U}}) = \mathsf{n}^j \end{aligned}$$

■

F. Authentication of the Network by the User

We now prove that the AKA$^+$ protocols provides authentication of the network by the user. We actually prove the stronger result that for any valid symbolic trace τ, if the authentication of UE_{ID} succeeded at instant τ (i.e. $\sigma_\tau^{\text{in}}(\text{e-auth}_{\text{U}}^{\text{ID}})$ is not fail or $\perp$), then there exists some $j \in \mathbb{N}$ such that UE_{ID} authenticated the session $HN(j0$.

Lemma 8. *For all valid symbolic trace τ, ϕ_τ^{in} guarantees authentication of the network by the user. For all $\text{ID} \in \mathcal{S}_{id}$ and $j \in \mathbb{N}$, we define the formulas:*

$$\begin{aligned} \textit{suc-auth}_\tau(\text{ID}) &\equiv \sigma_\tau^{in}(\textit{e-auth}_{\text{U}}^{\text{ID}}) \neq \textit{fail} \wedge \sigma_\tau^{in}(\textit{e-auth}_{\text{U}}^{\text{ID}}) \neq \perp \\ \textit{auth}_\tau(\text{ID}, j) &\equiv \sigma_\tau^{in}(\textit{b-auth}_{\text{N}}^{j}) = \text{ID} \wedge \textit{n}^j = \sigma_\tau^{in}(\textit{e-auth}_{\text{U}}^{\text{ID}}) \end{aligned}$$

Then we have:

$$\forall \text{ID} \in \mathcal{S}_{id},\ \ \textit{suc-auth}_\tau(\text{ID}) \ \rightarrow\ \textstyle\bigvee_{j\in\mathbb{N}} \textit{auth}_\tau(\text{ID}, j)$$

Proof. We prove this by induction on τ. First, for $\tau = \epsilon$ we have that for every j, $\sigma_\tau^{\text{in}}(\text{e-auth}_{\text{N}}^{j}) = \perp$. Therefore the property holds. Let $\tau = \tau_0, \text{ai}$, assume that:

$$\forall \text{ID} \in \mathcal{S}_{\text{id}},\ \ \text{suc-auth}_{\tau_0}(\text{ID}) \ \rightarrow\ \textstyle\bigvee_{j\in\mathbb{N}} \text{auth}_{\tau_0}(\text{ID}, j)$$

If for every j_0 we have:

$$\sigma_\tau^{\text{up}}(\text{b-auth}_{\text{N}}^{j_0}) = \perp \qquad\qquad \forall \text{ID} \in \mathcal{S}_{\text{id}},\ \sigma_\tau^{\text{up}}(\text{e-auth}_{\text{U}}^{\text{ID}}) = \perp \tag{12}$$

then we have authentication of the network by the user at τ. Therefore we only need to show that authentication holds for τ in the cases where ai is equal to $\text{PN}(j,0)$, $\text{PN}(j,1)$, $\text{PU}_{\text{ID}}(j,2)$, $\text{TN}(j,0)$ or $\text{TU}_{\text{ID}}(j,1)$.

- **Case $\text{ai} = \text{PN}(j, 0)$.** we are going to show that for all $\text{ID} \in \mathcal{S}_{\text{id}}, j_0 \in \mathbb{N}$, we have:

$$(\text{suc-auth}_\tau(\text{ID}) \ \wedge\ \text{auth}_\tau(\text{ID}, j_0)) \ \leftrightarrow\ (\text{suc-auth}_{\tau_0}(\text{ID}) \ \wedge\ \text{auth}_{\tau_0}(\text{ID}, j_0)) \tag{13}$$

  which implies the wanted result. Let $\text{ID} \in \mathcal{S}_{\text{id}}, j_0 \in \mathbb{N}$.
  - In the case $j_0 \neq j$, using the validity of τ, we know that $\text{PN}(j,1) \not\preceq \tau$. This implies that $\sigma_\tau^{\text{in}}(\text{b-auth}_{\text{N}}^{j}) = \perp \neq \text{ID}$, which in turn implies that $\neg\text{auth}_\tau(\text{ID}, j)$. By a similar reasoning, we get that $\text{PN}(j,1) \notin \tau_0$, therefore $\sigma_{\tau_0}^{\text{in}}(\text{b-auth}_{\text{N}}^{j}) \neq \text{ID}$, and by consequence $\neg\text{auth}_{\tau_0}(\text{ID}, j)$. This concludes the proof of the validity of (13).
  - In the case $j_0 = j$, since $\sigma_\tau^{\text{in}}(\text{b-auth}_{\text{N}}^{j}) = \perp \neq \text{ID}$ we know that $\text{auth}_\tau(\text{ID}, j) = \text{false}$. Similarly $\text{auth}_{\tau_0}(\text{ID}, j) = \text{false}$. Therefore (13) holds for $j_0 = j$.
- **Case $\text{ai} = \text{PN}(j, 1)$.** Here also we are going to show that (13) holds for all j_0. Let $\text{ID} \in \mathcal{S}_{\text{id}}, j_0 \in \mathbb{N}$.
  - If $j_0 \neq j$, we have $\sigma_\tau^{\text{up}}(\text{b-auth}_{\text{N}}^{j_0}) = \perp$ and $\sigma_\tau^{\text{up}}(\text{e-auth}_{\text{U}}^{\text{ID}}) = \perp$. It follows that (13) holds.
  - If $j_0 = j$, using the validity of τ we know that $\sigma_{\tau_0}^{\text{in}}(\text{b-auth}_{\text{N}}^{j}) \equiv \perp$. From EQConst it follows that $\sigma_{\tau_0}^{\text{in}}(\text{b-auth}_{\text{N}}^{j}) \neq \text{ID}$, and therefore $\text{auth}_{\tau_0}(\text{ID}, j) = \text{false}$.
    To conclude this case, we only need to show that $(\text{suc-auth}_\tau(\text{ID}) \wedge \text{auth}_\tau(\text{ID}, j)) = \text{false}$.
    First, assume that there never was a call to $\text{PU}_{\text{ID}}(\_, 2)$, i.e. $\text{PU}_{\text{ID}}(\_, 2) \not\preceq \tau_1$. Then $\sigma_\tau^{\text{in}}(\text{e-auth}_{\text{U}}^{\text{ID}}) \equiv \perp$, and therefore $\text{suc-auth}_\tau(\text{ID}) = \text{false}$.
    Otherwise, let $\tau_0 = \_, \text{PU}_{\text{ID}}(j_0, 2)$ be the latest call to $\text{PU}_{\text{ID}}(\_, 2)$, i.e. $\tau_0 \not\prec_\tau \text{PU}_{\text{ID}}(\_, 2)$. By validity of τ, we know that there exists τ_2 such that $\tau_2 = \_, \text{PU}_{\text{ID}}(j_0, 1)$. We know that $\sigma_\tau^{\text{in}}(\text{e-auth}_{\text{U}}^{\text{ID}}) \equiv \sigma_{\tau_0}^{\text{up}}(\text{e-auth}_{\text{U}}^{\text{ID}})$. Hence:

$$\begin{aligned} \text{suc-auth}_\tau(\text{ID}) &\rightarrow \sigma_{\tau_0}^{\text{up}}(\text{e-auth}_{\text{U}}^{\text{ID}}) \neq \text{fail} && \text{(by definition of } \text{suc-auth}_\tau(\text{ID})) \\ &\rightarrow \text{accept}_{\tau_0}^{\text{ID}} && \text{(by definition of } \sigma_{\tau_0}^{\text{up}}(\text{e-auth}_{\text{U}}^{\text{ID}})) \\ &\rightarrow \text{accept}_{\tau_0}^{\text{ID}} \wedge \bigvee_{\substack{\tau_1 = \_, \text{PN}(j_1, 1) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} (g(\phi_{\tau_2}^{\text{in}}) = \text{n}^{j_1}) && \text{(by } \textbf{(Acc2)}) \\ &\rightarrow \bigvee_{\substack{\tau_1 = \_, \text{PN}(j_1, 1) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} \big(\sigma_{\tau_0}^{\text{up}}(\text{e-auth}_{\text{U}}^{\text{ID}}) = \text{n}^{j_1}\big) \\ &\rightarrow \bigvee_{\substack{\tau_1 = \_, \text{PN}(j_1, 1) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} \big(\sigma_\tau^{\text{in}}(\text{e-auth}_{\text{U}}^{\text{ID}}) = \text{n}^{j_1}\big) && \text{(since } \sigma_\tau^{\text{in}}(\text{e-auth}_{\text{U}}^{\text{ID}}) \equiv \sigma_{\tau_0}^{\text{up}}(\text{e-auth}_{\text{U}}^{\text{ID}})) \end{aligned}$$

    Since $\tau_0 \prec \tau$ we know that for every $\tau_1 = \_, \text{PN}(j_1, 1) \in \{\tau_1 \mid \tau_2 \prec \tau_1 \prec_\tau \tau_0\}$, $j_1 \neq j$, and therefore using EQIndep we know that $(\text{n}^{j_1} = \text{n}^j) \leftrightarrow \text{false}$. Therefore:

$$\text{suc-auth}_\tau(\text{ID}) \wedge \text{auth}_\tau(\text{ID}, j) \ \rightarrow \bigvee_{\substack{\tau_1 = \_, \text{PN}(j_1, 1) \\ \tau_2 \prec_\tau \tau_1 \prec \tau_0}} \big(\sigma_\tau^{\text{in}}(\text{e-auth}_{\text{U}}^{\text{ID}}) = \text{n}^{j_1} \wedge \text{n}^{j_1} \neq \text{n}^j \wedge \text{auth}_\tau(\text{ID}, j)\big)$$

And by definition of $\mathsf{auth}_\tau(\text{ID}, j)$:

$$\rightarrow \bigvee_{\substack{\tau_1 = \_,\text{PN}(j_1,1) \\ \tau_2 \prec_\tau \tau_1 \prec \tau_0}} \left(\sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_1} \wedge \mathsf{n}^{j_1} \neq \mathsf{n}^{j} \wedge \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j}\right)$$
$$\rightarrow \mathsf{false}$$

- **Case $\mathsf{ai} = \text{PU}_{\text{ID}}(j, 2)$.** For all $\text{ID}_0 \neq \text{ID}$ and for all $j_0 \in \mathbb{N}$, it is trivial that:

$$(\mathsf{suc\text{-}auth}_\tau(\text{ID}_0) \ \wedge\ \mathsf{auth}_\tau(\text{ID}_0, j_0)) \ \leftrightarrow\ (\mathsf{suc\text{-}auth}_{\tau_0}(\text{ID}_0) \ \wedge\ \mathsf{auth}_{\tau_0}(\text{ID}_0, j_0))$$

Therefore we only need to show that:

$$\mathsf{suc\text{-}auth}_\tau(\text{ID}) \ \rightarrow\ \bigvee_{j \in \mathbb{N}} \mathsf{auth}_\tau(\text{ID}, j)$$

First, we observe that:

$$\begin{aligned} \mathsf{suc\text{-}auth}_\tau(\text{ID}) \ &\rightarrow\ \mathsf{accept}^{\text{ID}}_\tau \\ &\rightarrow \bigvee_{\substack{\tau_0 = \_,\text{PN}(j_0,1) \\ \tau_1 = \_,\text{PU}_{\text{ID}}(j,1) \\ \tau_1 \prec_\tau \tau_0}} \begin{pmatrix} \mathsf{accept}^{\text{ID}}_{\tau_0} \ \wedge\ g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^{j_0} \ \wedge \\ \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \{\langle \text{ID}\ ,\ \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}} \end{pmatrix} \qquad \text{(by } \textbf{(Acc2)}\text{)} \end{aligned}$$

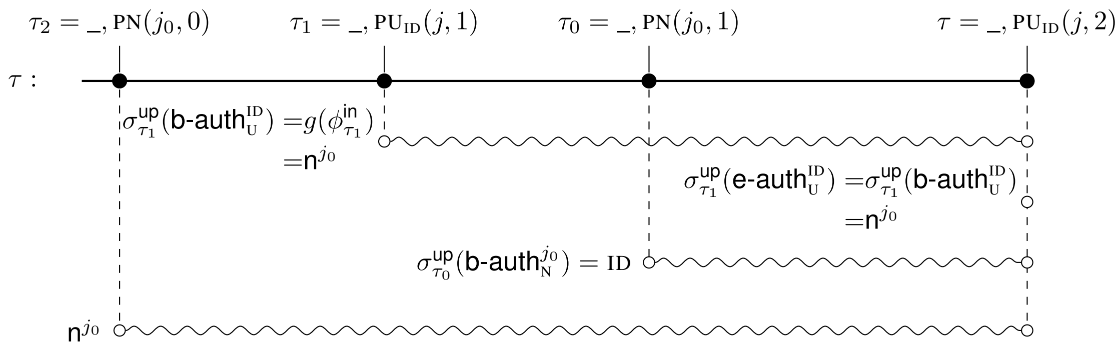
Let $\tau_0 = \_, \text{PN}(j_0, 1)$, $\tau_1 = \_, \text{PU}_{\text{ID}}(j, 1)$ such that $\tau_1 \prec_\tau \tau_0$. Let $\tau_2 = \_, \text{PN}(j_0, 1)$, by validity of τ we know that $\tau_2 \prec_\tau \tau_0$. Moreover, if $\tau_1 \prec_\tau \tau_2$ then by **(A1)** we have $\mathsf{n}^{j_0} \notin \mathsf{st}(\phi^{\mathsf{in}}_{\tau_1})$, and therefore using $\mathsf{EQIndep}$ we obtain that $g(\phi^{\mathsf{in}}_{\tau_1}) \neq \mathsf{n}^{j_0}$. Hence:

$$\mathsf{suc\text{-}auth}_\tau(\text{ID}) \ \rightarrow \bigvee_{\substack{\tau_0 = \_,\text{PN}(j_0,1) \\ \tau_1 = \_,\text{PU}_{\text{ID}}(j,1) \\ \tau_2 = \_,\text{PN}(j_0,0) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} \begin{pmatrix} \mathsf{accept}^{\text{ID}}_\tau \ \wedge\ \mathsf{accept}^{\text{ID}}_{\tau_0} \ \wedge\ g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^{j_0} \ \wedge \\ \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \{\langle \text{ID}\ ,\ \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}} \end{pmatrix}$$

Moreover, we know that:

$$\mathsf{accept}^{\text{ID}}_{\tau_0} \ \rightarrow\ \sigma^{\mathsf{up}}_{\tau_0}(\mathsf{b\text{-}auth}^{j_0}_{\text{N}}) = \text{ID} \qquad\qquad \mathsf{accept}^{\text{ID}}_\tau \ \rightarrow\ \sigma_{\tau_1}(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{up}}_{\tau_1}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}})$$

We represent graphically all the information we have below:



It follows that:

$$\begin{pmatrix} \mathsf{accept}^{\text{ID}}_\tau \ \wedge\ \mathsf{accept}^{\text{ID}}_{\tau_0} \ \wedge\ g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^{j_0} \ \wedge \\ \pi_1(g(\phi^{\mathsf{in}}_{\tau_0})) = \{\langle \text{ID}\ ,\ \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}} \end{pmatrix} \ \rightarrow\ \mathsf{auth}_\tau(\text{ID}, j_0)$$

Hence:

$$\mathsf{suc\text{-}auth}_\tau(\text{ID}) \ \rightarrow \bigvee_{\substack{\tau_0 = \_,\text{PN}(j_0,1) \\ \tau_1 = \_,\text{PU}_{\text{ID}}(j,1) \\ \tau_2 = \_,\text{PN}(j_0,0) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_0}} \mathsf{auth}_\tau(\text{ID}, j_0) \ \rightarrow\ \bigvee_{j_0 \in \mathbb{N}} \mathsf{auth}_\tau(\text{ID}, j_0)$$

- **Case $\mathsf{ai} = \text{TN}(j, 0)$.** For all $\text{ID} \in \mathcal{S}_{\mathsf{id}}$ and for all $j_0 \in \mathbb{N}$ such that $j_0 \neq j$ we have:

$$\mathsf{suc\text{-}auth}_\tau(\text{ID}) \equiv \mathsf{suc\text{-}auth}_{\tau_0}(\text{ID}) \qquad\qquad \mathsf{auth}_\tau(\text{ID}, j_0) \equiv \mathsf{auth}_{\tau_0}(\text{ID}, j_0)$$

Hence:

$$(\mathsf{suc\text{-}auth}_\tau(\text{ID}) \ \wedge\ \mathsf{auth}_\tau(\text{ID}, j_0)) \ \leftrightarrow\ (\mathsf{suc\text{-}auth}_{\tau_0}(\text{ID}) \ \wedge\ \mathsf{auth}_{\tau_0}(\text{ID}, j_0))$$

It only remains the case $j_0 = j$. We know that $\sigma^{\mathsf{in}}_{\tau_0}(\text{b-auth}^j_{\mathrm{N}}) \equiv \bot$, therefore $\text{suc-auth}_{\tau_0}(\mathrm{ID}, j) = \mathsf{false}$, which in turn implies that:

$$(\text{suc-auth}_{\tau_0}(\mathrm{ID}) \ \wedge\ \text{auth}_{\tau_0}(\mathrm{ID}, j)) = \mathsf{false}$$

Moreover:

$$\text{auth}_{\tau}(\mathrm{ID}, j) \ \rightarrow\ \mathsf{n}^j = \sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) \ \rightarrow\ \mathsf{n}^j = \sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}})$$

Using **(A1)** it is easy to show that $\mathsf{n}^j \notin \mathsf{st}(\sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}))$, therefore we have $\neg\text{auth}_{\tau}(\mathrm{ID}, j)$. This concludes this case.

- **Case $\mathsf{ai} = \mathbf{TU_{ID}}(j, 1)$.** For all $\mathrm{ID}_0 \neq \mathrm{ID}$ and for all $j_0 \in \mathbb{N}$, it is trivial that:

$$(\text{suc-auth}_{\tau}(\mathrm{ID}_0) \ \wedge\ \text{auth}_{\tau}(\mathrm{ID}_0, j_0)) \ \leftrightarrow\ (\text{suc-auth}_{\tau_0}(\mathrm{ID}_0) \ \wedge\ \text{auth}_{\tau_0}(\mathrm{ID}_0, j_0))$$

Therefore we only need to show that:

$$\text{suc-auth}_{\tau}(\mathrm{ID}) \ \rightarrow\ \bigvee\nolimits_{i\in\mathbb{N}} \text{auth}_{\tau}(\mathrm{ID}, i)$$

Let $\mathsf{k} \equiv \mathsf{k}^{\mathrm{ID}}$. We observe that:

$$\begin{aligned}
\text{suc-auth}_{\tau}(\mathrm{ID}) \ &\rightarrow\ \sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{fail} \\
&\rightarrow\ \text{accept}^{\mathrm{ID}}_{\tau} \\
&\rightarrow \bigvee_{\tau_0 = _,\mathrm{TN}(j_0,0)\prec\tau} \begin{array}{l} \text{accept}^{\mathrm{ID}}_{\tau_0} \ \wedge\ \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0} \ \wedge \\ \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_0}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \end{array} && \text{(by \textbf{(Acc3)})}
\end{aligned}$$

Let $\tau_0 = \mathrm{TN}(j_0, 0)$ such that $\tau_0 \prec_{\tau} \tau$. Then:

$$\left(\pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0} \wedge \text{accept}^{\mathrm{ID}}_{\tau}\right) \ \rightarrow\ \sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j_0}$$

Moreover using **(A7)** we know that $\text{accept}^{\mathrm{ID}}_{\tau_0} \rightarrow \sigma^{\mathsf{in}}_{\tau_0}(\text{b-auth}^j_{\mathrm{N}}) = \mathrm{ID}$. Using the validity of τ, we can easily show that for all $\tau_0 \prec_{\tau} \tau'$ we have $\sigma^{\mathsf{up}}_{\tau'}(\text{b-auth}^j_{\mathrm{N}}) \equiv \bot$. We deduce that $\text{accept}^{\mathrm{ID}}_{\tau_0} \rightarrow \sigma^{\mathsf{in}}_{\tau_0}(\text{b-auth}^j_{\mathrm{N}}) = \mathrm{ID}$. Hence:

$$\text{suc-auth}_{\tau}(\mathrm{ID}) \quad\rightarrow\quad \bigvee_{\tau_0 = \_,\mathrm{TN}(j_0,0)\prec\tau} \text{auth}_{\tau}(\mathrm{ID}, j_0) \quad\rightarrow\quad \bigvee_{\tau_0\prec\tau} \text{auth}_{\tau}(\mathrm{ID}, j_0)$$

■

G. Proof of Lemma 3

We give the proof of Lemma 3, which relies on Lemma 8.

Proof. Let τ be a valid symbolic trace. First, observe that $\sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^j$ implies that $\sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{fail}$ and that $\sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) \neq \bot$. Using the remark above and Lemma 8 we get that:

$$\begin{aligned}
\sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^j \ &\rightarrow\ \sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{fail} \wedge \sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) \neq \bot \\
&\rightarrow\ \text{suc-auth}_{\tau}(\mathrm{ID}) \\
&\rightarrow\ \bigvee_{j\in\mathbb{N}} \text{auth}_{\tau}(\mathrm{ID}, j) && \text{(By Lemma 8)} \\
&\rightarrow\ \sigma^{\mathsf{in}}_{\tau}(\text{b-auth}^j_{\mathrm{N}}) = \mathrm{ID} && \text{(Since } (\mathsf{n}^j = \sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{n}^{j'} = \sigma^{\mathsf{in}}_{\tau}(\text{e-auth}^{\mathrm{ID}}_{\mathrm{U}})) = \mathsf{false} \text{ if } j \neq j'.) \\
&\rightarrow\ \bigvee_{\tau'\preceq\tau} \sigma^{\mathsf{in}}_{\tau'}(\text{b-auth}^j_{\mathrm{N}}) = \mathrm{ID}
\end{aligned}$$

■

H. Injective Authentication of the Network by the User

We actually can show that the authentication of the network by the user is *injective*.

Lemma 9. *For all valid symbolic trace τ, ϕ^{in}_{τ} guarantees* injective *authentication of the network by the user. For all $\mathrm{ID} \in \mathcal{S}_{id}$ and $j \in \mathbb{N}$, we define the formula:*

$$\textit{inj-auth}_{\tau}(\mathrm{ID}, j) \ \ \equiv\ \ \textit{auth}_{\tau}(\mathrm{ID}, j) \ \wedge\ \bigwedge\nolimits_{i\neq j} \neg\textit{auth}_{\tau}(\mathrm{ID}, i)$$

Then we have:

$$\forall \mathrm{ID} \in \mathcal{S}_{id},\ \ \textit{suc-auth}_{\tau}(\mathrm{ID}) \ \rightarrow\ \bigvee\nolimits_{j\in\mathbb{N}} \textit{inj-auth}_{\tau}(\mathrm{ID}, j)$$

Proof. First, we show that for $\text{ID} \in \mathcal{S}_{\mathsf{id}}$ and $i_0, i_1 \in \mathbb{N}$ with $i_0 \neq i_1$:

$$\mathsf{suc\text{-}auth}_\tau(\text{ID}) \rightarrow (\neg\mathsf{auth}_\tau(\text{ID}, i_0) \vee \neg\mathsf{auth}_\tau(\text{ID}, i_1)) \tag{14}$$

Indeed:

$$\begin{aligned}
&\mathsf{suc\text{-}auth}_\tau(\text{ID}) \wedge \mathsf{auth}_\tau(\text{ID}, i_0) \wedge \mathsf{auth}_\tau(\text{ID}, i_1) \\
\rightarrow\ &\mathsf{suc\text{-}auth}_\tau(\text{ID}) \wedge \sigma^{\mathsf{in}}_\tau(\mathsf{n}^{i_0}_{\text{N}}) = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\mathsf{in}}_\tau(\mathsf{n}^{i_1}_{\text{N}}) = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \\
\rightarrow\ &\mathsf{suc\text{-}auth}_\tau(\text{ID}) \wedge \begin{cases}
\mathsf{n}^{i_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \wedge \mathsf{n}^{i_1} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) & \text{if } \text{PN}(i_0, 0) \in \tau \text{ and } \text{PN}(i_1, 0) \in \tau \\
\mathsf{n}^{i_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \wedge \bot = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) & \text{if } \text{PN}(i_0, 0) \in \tau \text{ and } \text{PN}(i_1, 0) \notin \tau \\
\bot = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \wedge \mathsf{n}^{i_1} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) & \text{if } \text{PN}(i_0, 0) \notin \tau \text{ and } \text{PN}(i_1, 0) \in \tau \\
\bot = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \wedge \bot = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) & \text{if } \text{PN}(i_0, 0) \notin \tau \text{ and } \text{PN}(i_1, 0) \notin \tau
\end{cases}
\end{aligned}$$

Using $\mathsf{EQIndep}$, we know that $\mathsf{n}^{i_1} \neq \mathsf{n}^{i_0}$. Therefore:

$$\big(\mathsf{suc\text{-}auth}_\tau(\text{ID}) \wedge \mathsf{n}^{i_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \wedge \mathsf{n}^{i_1} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) \rightarrow \mathsf{false}$$

Since $\mathsf{suc\text{-}auth}_\tau(\text{ID}) \rightarrow \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \neq \bot$, we know that:

$$\big(\mathsf{suc\text{-}auth}_\tau(\text{ID}) \wedge \bot = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) \rightarrow \mathsf{false}$$

And therefore:

$$\begin{gathered}
\big(\mathsf{suc\text{-}auth}_\tau(\text{ID}) \wedge \mathsf{n}^{i_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \wedge \bot = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) \rightarrow \mathsf{false} \\
\big(\mathsf{suc\text{-}auth}_\tau(\text{ID}) \wedge \bot = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \wedge \mathsf{n}^{i_1} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) \rightarrow \mathsf{false} \\
\big(\mathsf{suc\text{-}auth}_\tau(\text{ID}) \wedge \bot = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \wedge \bot = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) \rightarrow \mathsf{false}
\end{gathered}$$

This concludes the proof of (14). From Lemma 8 we know that:

$$\forall \text{ID} \in \mathcal{S}_{\mathsf{id}}, \ \ \mathsf{suc\text{-}auth}_\tau(\text{ID}) \ \rightarrow \ \textstyle\bigvee_{j \in \mathbb{N}} \mathsf{auth}_\tau(\text{ID}, j)$$

Moreover, using (14) we have that for every $\text{ID} \in \mathcal{S}_{\mathsf{id}}, j \in \mathbb{N}$:

$$\mathsf{suc\text{-}auth}_\tau(\text{ID}) \wedge \mathsf{auth}_\tau(\text{ID}, j) \ \rightarrow \ \textstyle\bigvee_{i \neq j} \neg\mathsf{auth}_\tau(\text{ID}, i)$$

We deduce that:

$$\forall \text{ID} \in \mathcal{S}_{\mathsf{id}}, \ \ \mathsf{suc\text{-}auth}_\tau(\text{ID}) \ \rightarrow \ \textstyle\bigvee_{j \in \mathbb{N}} \mathsf{inj\text{-}auth}_\tau(\text{ID}, j)$$

∎

Proposition 25. *For every valid symbolic trace τ, for every $j_o \in \mathbb{N}$:*

$$\mathsf{inj\text{-}auth}_\tau(\text{ID}, j_0) \ \leftrightarrow \ \mathsf{n}^{j_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})$$

Proof. To do this we show both directions. The first direction is trivial:

$$\mathsf{inj\text{-}auth}_\tau(\text{ID}, j_0) \ \rightarrow \ \mathsf{auth}_\tau(\text{ID}, j_0) \ \rightarrow \ \big(\mathsf{n}^{j_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big)$$

We now prove the converse direction:

$$\begin{aligned}
\big(\mathsf{n}^{j_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) &\rightarrow \mathsf{suc\text{-}auth}_\tau(\text{ID}) && \text{(Using } \mathsf{EQIndep}\text{)} \\
&\rightarrow \bigvee_{j_1 \in \mathbb{N}} \mathsf{inj\text{-}auth}_\tau(\text{ID}, j_1) && \text{(Lemma 9)}
\end{aligned}$$

We conclude by observing that for every $j_1 \neq j_0$,

$$\begin{aligned}
\big(\mathsf{n}^{j_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) \wedge \mathsf{inj\text{-}auth}_\tau(\text{ID}, j_1) \ &\rightarrow \ \big(\mathsf{n}^{j_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) \wedge \mathsf{auth}_\tau(\text{ID}, j_1) \\
&\rightarrow \ \big(\mathsf{n}^{j_0} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) \wedge \big(\mathsf{n}^{j_1} = \sigma^{\mathsf{in}}_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\big) \\
&\rightarrow \mathsf{false} && \text{(Using } \mathsf{EQIndep}\text{)}
\end{aligned}$$

∎

APPENDIX III
ACCEPTANCE CHARACTERIZATIONS

In this section, we prove necessary and sufficient conditions for a message to be accepted by the user or the network. This section is organized as follow: we start by showing some properties of the AKA$^+$ protocol, which we then use to show a first set of acceptance characterizations; then, using these, we show that the temporary identity $\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}$ is concealed until the subscriber starts of session of the GUTI sub-protocol; finally, using the GUTI concealment property, we show stronger acceptance characterizations.

A. First Characterizations

Proposition 26. *For every valid symbolic trace $\tau = \_, \mathsf{ai}$ and identity* ID *we have:*

- ***(B1)*** *For every $\tau_0 \preceq \tau_1 \preceq \tau$, $\sigma_{\tau_0}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{X}}) \leq \sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{X}})$.*
- ***(B2)*** *If $\mathsf{ai} = \mathrm{FU}_{\mathrm{ID}}(j)$ then for every and $j_0 \in \mathbb{N}$, if $\mathrm{FN}(j_0) \prec_\tau \mathrm{NS}_{\mathrm{ID}}(\_)$ then:*

$$\sigma_\tau(\textsf{e-auth}^{j_0}_{\mathrm{N}}) \neq \textsf{UnknownId} \rightarrow \neg \textsf{inj-auth}_\tau(\mathrm{ID}, j_0)$$

Proof. Let $\tau = \_, \mathsf{ai}$ be valid symbolic trace and $\mathrm{ID} \in \mathcal{S}_{\mathsf{id}}$. We prove **(B1)** and **(B2)**:

- **(B1)**. This is straightforward by induction over τ_1.
- **(B2)**. Let $\tau_x = \_, \mathrm{FN}(j_0) \prec \tau$. We do a case disjunction on the protocol used by the user for authentication:
  - If there exists $\tau_1 = \_, \mathrm{TU}_{\mathrm{ID}}(j, 1) \prec \tau$. We know that there exists $\tau_n \prec \tau_x$ with $\tau_n = \_, \mathrm{PN}(j_0, 1)$ or $\_, \mathrm{TN}(j_0, 1)$. Assume that $\tau_n = \_, \mathrm{PN}(j_0, 1)$. We know that $\textsf{inj-auth}_\tau(\mathrm{ID}, j_0) \rightarrow \textsf{accept}^{\mathrm{ID}}_{\tau_1}$, and by applying **(Acc3)**:

$$\begin{aligned} \textsf{inj-auth}_\tau(\mathrm{ID}, j_0) &\rightarrow \bigvee_{\substack{\tau_2 = \_, \mathrm{TN}(j_2, 0) \\ \tau_2 \prec \tau_1}} \sigma_{\tau_1}(\textsf{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^{j_2} \\ &\rightarrow \sigma_{\tau_1}(\textsf{e-auth}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{n}^{j_0} \qquad \text{(Since for every } \tau_2 = \_, \mathrm{TN}(j_2, 0) \prec \tau_1,\ j_2 \neq j_0) \\ &\rightarrow \mathsf{false} \end{aligned}$$

  Which is what we wanted.
  Now, assume that $\tau_n = \_, \mathrm{TN}(j_0, 1)$. Observe that $\sigma_{\tau_n}(\textsf{e-auth}^{j_0}_{\mathrm{N}}) \neq \mathsf{fail}$ and that $\sigma_\tau(\textsf{e-auth}^{j_0}_{\mathrm{N}}) = \sigma_{\tau_n}(\textsf{e-auth}^{j_0}_{\mathrm{N}})$. Moreover, it is straightforward to check that for every valid symbolic trace τ':

$$\Big(\textsf{inj-auth}_{\tau'}(\mathrm{ID}, j_0) \wedge \sigma_{\tau'}(\textsf{e-auth}^{j_0}_{\mathrm{N}}) \neq \textsf{UnknownId} \wedge \sigma_{\tau'}(\textsf{e-auth}^{j_0}_{\mathrm{N}}) \neq \mathsf{fail}\Big) \rightarrow \sigma_{\tau'}(\textsf{e-auth}^{j_0}_{\mathrm{N}}) = \sigma_{\tau'}(\textsf{b-auth}^{j_0}_{\mathrm{N}})$$

  Hence we deduce that:

$$\Big(\textsf{inj-auth}_\tau(\mathrm{ID}, j_0) \wedge \sigma_\tau(\textsf{e-auth}^{j_0}_{\mathrm{N}}) \neq \textsf{UnknownId}\Big) \rightarrow \sigma_\tau(\textsf{e-auth}^{j_0}_{\mathrm{N}}) = \sigma_\tau(\textsf{b-auth}^{j_0}_{\mathrm{N}})$$

  Since $\textsf{inj-auth}_\tau(\mathrm{ID}, j_0) \rightarrow \sigma_\tau(\textsf{b-auth}^{j_0}_{\mathrm{N}}) = \mathrm{ID}$, we get that:

$$\Big(\textsf{inj-auth}_\tau(\mathrm{ID}, j_0) \wedge \sigma_\tau(\textsf{e-auth}^{j_0}_{\mathrm{N}}) \neq \textsf{UnknownId}\Big) \rightarrow \sigma_\tau(\textsf{e-auth}^{j_0}_{\mathrm{N}}) = \mathrm{ID}$$

  Moreover, $\sigma_\tau(\textsf{e-auth}^{j_0}_{\mathrm{N}}) = \mathrm{ID} \rightarrow \textsf{accept}^{\mathrm{ID}}_{\tau_n}$. Using **(Acc4)** on τ_n:

$$\textsf{accept}^{\mathrm{ID}}_{\tau_n} \rightarrow \bigvee_{\tau_i = \_, \mathrm{TU}_{\mathrm{ID}}(j_i, 1) \prec \tau_n} \textsf{accept}^{\mathrm{ID}}_{\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^{j_0}$$

  Let $\tau_0 = \mathrm{TN}(j_0, 0)$ and $\tau_i = \_, \mathrm{TU}_{\mathrm{ID}}(j_i, 1) \prec \tau_n$. Observe that $\tau_i \neq \tau_1$. Using **(Acc3)**, we can check that:

$$\textsf{accept}^{\mathrm{ID}}_{\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^{j_0} \rightarrow \textsf{range}(\sigma^{\mathsf{in}}_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\tau_0}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}))$$

  Recall that $\textsf{inj-auth}_\tau(\mathrm{ID}, j_0) \rightarrow \textsf{accept}^{\mathrm{ID}}_{\tau_1}$. Moreover, $\textsf{inj-auth}_\tau(\mathrm{ID}, j_0) \rightarrow \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \mathsf{n}^{j_0}$. Hence using **(Acc3)** again we get:

$$\textsf{accept}^{\mathrm{ID}}_{\tau_1} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \mathsf{n}^{j_0} \rightarrow \textsf{range}(\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\tau_0}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}))$$

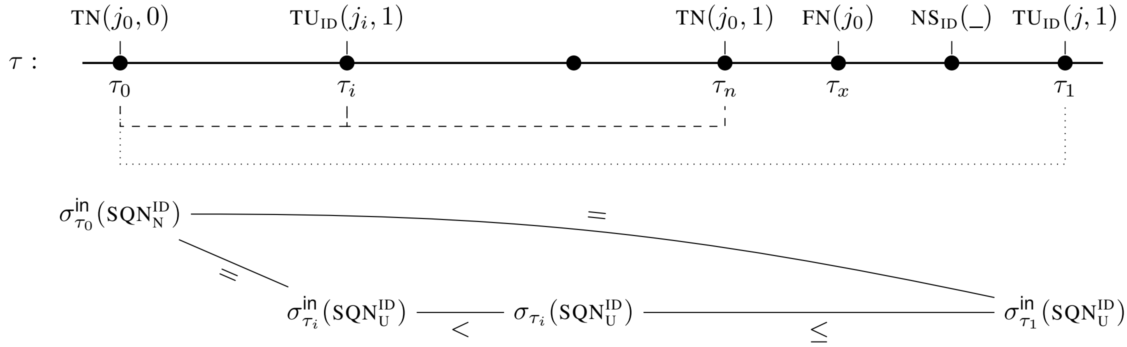
  Putting everything together:

$$\begin{aligned} \Big(\textsf{inj-auth}_\tau(\mathrm{ID}, j_0) \wedge \sigma_\tau(\textsf{e-auth}^{j_0}_{\mathrm{N}}) \neq \textsf{UnknownId}\Big) &\rightarrow \begin{pmatrix} \sigma^{\mathsf{in}}_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_0}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \\ \wedge\ \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_0}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \end{pmatrix} \\ &\rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \end{aligned}$$

Finally, $\mathsf{accept}^{\text{ID}}_{\tau_i} \rightarrow \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}})$, and using **(B1)** we know that $\sigma_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}}) \leq \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})$. We deduce that:

$$\begin{aligned}\left(\mathsf{inj\text{-}auth}_{\tau}(\text{ID}, j_0) \wedge \sigma_{\tau}(\mathsf{e\text{-}auth}^{j_0}_{\text{N}}) \neq \mathsf{UnknownId}\right) &\rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\\ &\rightarrow \mathsf{false}\end{aligned}$$

This concludes this case. We summarize graphically this proof below:



– If there exists $\tau_1 = \_, \text{PU}_{\text{ID}}(j, 2) \prec \tau$. Let $\tau_3 = \_, \text{PU}_{\text{ID}}(j, 1) \prec \tau_1$, we know that $\tau_x \prec \tau_3$. Remark that $\mathsf{inj\text{-}auth}_{\tau}(\text{ID}, j_0) \rightarrow \mathsf{accept}^{\text{ID}}_{\tau_1}$, and using **(Acc2)** we easily get that:

$$\mathsf{accept}^{\text{ID}}_{\tau_1} \rightarrow \bigvee_{\substack{\tau_2 = \_, \text{PN}(j_2, 1)\\ \tau_3 \prec \tau_2 \prec \tau_1}} \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_2}$$

Since no ID action occurred between τ_1 and τ, we have $\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) = \sigma_{\tau}(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})$. Moreover, $\mathsf{inj\text{-}auth}_{\tau}(\text{ID}, j_0) \rightarrow \sigma_{\tau}(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_0}$. Finally, for every $\tau_2 = \_, \text{PN}(j_2, 1)$ such that $\tau_3 \prec \tau_2 \prec \tau_1$, since $\tau_x \prec \tau_3$ we know that $j_2 \neq j_0$. It follows that:

$$\mathsf{inj\text{-}auth}_{\tau}(\text{ID}, j_0) \rightarrow \left(\bigvee_{\substack{\tau_2 = \_, \text{PN}(j_2, 1)\\ \tau_3 \prec \tau_2 \prec \tau_1}} \mathsf{n}^{j_0} = \mathsf{n}^{j_2}\right) \rightarrow \mathsf{false}$$

This concludes this case.

■

We now prove a first acceptance characterization:

Lemma 10. *For every valid symbolic trace $\tau = \_, ai$ and identity ID we have:*

- ***(Equ1)*** *If $ai = \text{FU}_{\text{ID}}(j)$. For every $\tau_1 = \_, \text{FN}(j_0) \prec \tau$, we let:*

$$\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \equiv \begin{pmatrix} \mathsf{inj\text{-}auth}_{\tau}(\text{ID}, j_0) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{e\text{-}auth}^{j_0}_{\text{N}}) \neq \mathsf{UnknownId}\\ \wedge\, \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \text{GUTI}^{j_0} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^{5}_{\mathsf{k_m}}(\langle \text{GUTI}^{j_0}, \mathsf{n}^{j_0}\rangle)\end{pmatrix}$$

Then:

$$\mathsf{accept}^{\text{ID}}_{\tau} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{FN}(j_0) \prec \tau\\ \tau_1 \not\prec_{\tau} \text{NS}_{\text{ID}}(\_)}} \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$$

Proof. Using Lemma 9 we know that:

$$\mathsf{suc\text{-}auth}_{\tau}(\text{ID}) \rightarrow \bigvee_{j_0 \in \mathbb{N}} \mathsf{inj\text{-}auth}_{\tau}(\text{ID}, j_0)$$

Let $\mathsf{k} \equiv \mathsf{k}_{\text{ID}}$ and $\mathsf{k_m} \equiv \mathsf{k}^{\text{ID}}_{\mathsf{m}}$. Since:

$$\mathsf{accept}^{\text{ID}}_{\tau} \equiv \mathsf{suc\text{-}auth}_{\tau}(\text{ID}) \wedge \underbrace{\pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^{5}_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\sigma^{\mathsf{in}}_{\tau}(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}))\,,\, \sigma^{\mathsf{in}}_{\tau}(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}})\rangle)}_{\mathsf{EQMac}}$$

And since $\mathsf{inj\text{-}auth}_{\tau}(\text{ID}, j_0) \rightarrow \mathsf{suc\text{-}auth}_{\tau}(\text{ID})$ we have:

$$\begin{aligned}\mathsf{accept}^{\text{ID}}_{\tau} &\leftrightarrow \bigvee_{j_0 \in \mathbb{N}} \mathsf{inj\text{-}auth}_{\tau}(\text{ID}, j_0) \wedge \mathsf{EQMac}\\ &\leftrightarrow \bigvee_{j_0 \in \mathbb{N}} \mathsf{inj\text{-}auth}_{\tau}(\text{ID}, j_0) \wedge \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^{5}_{\mathsf{k_m}}(\langle \pi_1(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0})\,,\, \mathsf{n}^{j_0}\rangle)\end{aligned}$$

Using the P-EUF-MAC^5 and CR^5 axioms, it is easy to show that for every $j_0 \in \mathbb{N}$:

$$\pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^5_{\mathsf{k_m}}(\langle \pi_1(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) \,,\, \mathsf{n}^{j_0} \rangle) \;\rightarrow\; \begin{cases} \begin{pmatrix} \pi_1(g(\phi_\tau^{\mathsf{in}})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) = \mathrm{GUTI}^{j_0} \\ \wedge\, \sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\mathrm{N}}^{j_0}) \neq \mathsf{UnknownId} \end{pmatrix} & \text{if } \mathrm{FN}(j_0) \in \tau \\ \mathsf{false} & \text{otherwise} \end{cases}$$

Hence:

$$\mathsf{accept}_\tau^{\mathrm{ID}} \;\leftrightarrow\; \bigvee_{\tau_0 = \_,\mathrm{FN}(j_0) \prec \tau} \begin{pmatrix} \mathsf{inj\text{-}auth}_\tau(\mathrm{ID}, j_0) \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\mathrm{N}}^{j_0}) \neq \mathsf{UnknownId} \\ \wedge\, \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathrm{GUTI}^{j_0} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge \pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^5_{\mathsf{k_m}}(\langle \mathrm{GUTI}^{j_0} \,,\, \mathsf{n}^{j_0} \rangle) \end{pmatrix}$$

By **(B2)**:

$$\mathsf{accept}_\tau^{\mathrm{ID}} \;\leftrightarrow\; \bigvee_{\substack{\tau_0 = \_,\mathrm{FN}(j_0) \prec \tau \\ \tau_0 \not\prec_\tau \mathrm{NS_{ID}}(\_)}} \begin{pmatrix} \mathsf{inj\text{-}auth}_\tau(\mathrm{ID}, j_0) \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\mathrm{N}}^{j_0}) \neq \mathsf{UnknownId} \\ \wedge\, \pi_1(g(\phi_\tau^{\mathsf{in}})) = \mathrm{GUTI}^{j_0} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge \pi_2(g(\phi_\tau^{\mathsf{in}})) = \mathsf{Mac}^5_{\mathsf{k_m}}(\langle \mathrm{GUTI}^{j_0} \,,\, \mathsf{n}^{j_0} \rangle) \end{pmatrix}$$

Which concludes this proof. ∎

We show the following additional properties:

Proposition 27. *For every valid symbolic trace $\tau = \_, \mathsf{ai}$ and identity* ID *we have:*

- ***(B3)*** $\sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \;\rightarrow\; \sigma_\tau(\mathrm{GUTI}_{\mathrm{U}}^{\mathrm{ID}}) \neq \mathit{UnSet}$.
- ***(B4)*** *For every $\tau_2 \prec_\tau \tau_1$:*

$$\sigma_{\tau_2}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathit{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \;\rightarrow\; \bigvee_{\substack{\tau_2 \prec_\tau \tau_x \prec_\tau \tau_1 \\ \tau_x = \_,\mathrm{TN}(j_x,0),\_,\mathrm{TN}(j_x,1) \text{ or } \_,\mathrm{PN}(j_x,1)}} \sigma_{\tau_1}^{\mathit{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathit{n}^{j_x}$$

- ***(B5)*** $\sigma_\tau(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$.
- ***(B6)*** *For every $\tau_0 \prec_\tau \tau_1$ such that $\tau_0 = \_, \mathrm{NS_{ID}}(\_)$ or ϵ, and such that $\tau_0 \not\prec_\tau \mathrm{NS_{ID}}(\_)$, we have:*

$$\sigma_{\tau_1}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \;\rightarrow\; \sigma_{\tau_1}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) > \sigma_{\tau_0}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$$

- ***(B7)*** *If for all $\tau' \preceq \tau$ such that $\tau' \not\prec_\tau \mathrm{NS_{ID}}(\_)$ we have $\tau' \neq \_, \mathrm{FU_{ID}}(\_)$, then:*

$$\sigma(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \;\rightarrow\; \mathit{false}$$

Proof. We give the proof of the properties **(B3)** to **(B7)**.

- **(B3)**. We show this by induction over τ. If $\tau = \epsilon$, we know from Definition 43 that $\sigma_\epsilon(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \mathsf{false}$ and $\sigma_\epsilon(\mathrm{GUTI}_{\mathrm{X}}^{\mathrm{ID}}) \equiv \mathsf{UnSet}$. Therefore the property holds. Let $\tau = \tau_0, \mathsf{ai}$, assume by induction that the property holds for τ_0. If ai is different from $\mathrm{TU_{ID}}(j,0), \mathrm{PU_{ID}}(j,1)$ and $\mathrm{FU}(j)$ then $\sigma_\tau^{\mathsf{up}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \sigma_\tau^{\mathsf{up}}(\mathrm{GUTI}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \bot$, in which case we conclude immediately by induction hypothesis. We have three cases remaining:
  - If $\mathsf{ai} = \mathrm{TU_{ID}}(j,0)$ or $\mathsf{ai} = \mathrm{PU_{ID}}(j,1)$ then $\sigma_\tau^{\mathsf{up}}(\mathrm{GUTI}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \mathsf{false}$. Therefore the property holds.
  - If $\mathsf{ai} = \mathrm{FU}(j)$, using **(Equ1)** we can check that:

$$\mathsf{accept}_\tau^{\mathrm{ID}} \;\rightarrow\; \bigvee_{\substack{\tau_1 = \_,\mathrm{FN}(j_0) \prec \tau \\ \tau_1 \not\prec_\tau \mathrm{NS_{ID}}(\_)}} \left(\sigma_\tau(\mathrm{GUTI}_{\mathrm{U}}^{\mathrm{ID}}) = \mathrm{GUTI}^{j_0}\right) \;\rightarrow\; \sigma_\tau(\mathrm{GUTI}_{\mathrm{U}}^{\mathrm{ID}}) \neq \mathsf{UnSet}$$

  We conclude by observing that $\sigma_\epsilon(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \mathsf{accept}_\tau^{\mathrm{ID}}$.
- **(B4)**. We prove this directly. Intuitively, this holds because if $\sigma_{\tau_2}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})$ then we know that $\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}$ was updated between τ_2 and τ_1. Moreover, if such an update occurs at $\tau_x = \_, \mathrm{PN}(j_x, 1)$ or $\mathrm{TN}(j_x, 1)$ then $\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}$ has to be equal to n^{j_x} after the update. Finally, the fact that $\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}$ is equal to n^{j_x} for some τ_x between τ_2 and τ_1 with $\tau_x = \_, \mathrm{TN}(j_x, 0)$, $\_, \mathrm{TN}(j_x, 1)$ or $\_, \mathrm{PN}(j_x, 1)$ is an invariant of the protocol. Now we give the formal proof.
  First, we remark that $\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}$ is updated only at $\mathrm{PN}(\_, 1)$ and $\mathrm{TN}(\_, 1)$. Moreover, each update either left $\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}$ unchanged or increments it by one. Finally, it is updated at $\tau_x \prec \tau$ if and only if $\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}}$ holds. If follows that:

$$\sigma_{\tau_2}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \;\rightarrow\; \bigvee_{\substack{\tau_2 \prec_\tau \tau_x \prec_\tau \tau_1 \\ \tau_x =,\_,\mathrm{TN}(j_x,1) \text{ or } \_,\mathrm{PN}(j_x,1)}} \mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}}$$

  We know that for every $\tau_2 \prec_\tau \tau_x \prec_\tau \tau_1$, if:
  - $\tau_x =, \_, \mathrm{TN}(j_x, 1)$ then $\mathsf{inc\text{-}accept}_{\tau_x}^{\mathrm{ID}} \leftrightarrow \sigma_{\tau_x}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j_x}$.

– $\tau_x = \_, \text{PN}(j_x, 1)$ then since $\text{inc-accept}^{\text{ID}}_{\tau_x} \equiv \text{inc-accept}^{\text{ID}}_{\tau_x} \wedge \sigma^{\text{in}}_{\tau_x}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_x}$, we know that $\text{inc-accept}^{\text{ID}}_{\tau_x} \rightarrow \sigma^{\text{in}}_{\tau_x}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_x}$. Besides, since $\text{session}^{\text{ID}}_{\text{N}}$ is not updated at $\text{PN}(j_x, 1)$ we deduce that $\text{inc-accept}^{\text{ID}}_{\tau_x} \rightarrow \sigma_{\tau_x}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_x}$.

Hence:

$$\sigma_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{N}}) < \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \;\rightarrow\; \bigvee_{\substack{\tau_2 \prec_\tau \tau_x \preceq \tau_1 \\ \tau_x = , \_, \text{TN}(j_x,1) \text{ or } \_, \text{PN}(j_x,1)}} \sigma_{\tau_x}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_x} \tag{15}$$

Let $\tau_2 \prec_\tau \tau_x \prec_\tau \tau_1$ such that $\tau_x =, \_, \text{TN}(j_x, 1)$ or $\_, \text{PN}(j_x, 1)$. Now, we prove by induction over τ' such that $\tau_x \preceq \tau' \prec \tau_1$ that:

$$\sigma_{\tau_x}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_x} \;\rightarrow\; \bigvee_{\substack{\tau_x \preceq \tau_n \preceq \tau' \\ \tau_n = \_, \text{TN}(j_n,0), \_, \text{TN}(j_n,1) \text{ or } \_, \text{PN}(j_n,1)}} \sigma_{\tau'}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_n}$$

For $\tau' = \tau_x$ this is obvious. For the inductive case, we do a disjunction over the final action of τ'. If $\text{session}^{\text{ID}}_{\text{N}}$ is not updated then we conclude by induction, otherwise we are in one of the following case:

– If $\tau' = \_, \text{TN}(j', 0)$ then we do a case disjunction on $\text{accept}^{\text{ID}}_{\tau'}$:

$$\neg\text{accept}^{\text{ID}}_{\tau'} \rightarrow \sigma_{\tau'}(\text{session}^{\text{ID}}_{\text{N}}) = \sigma^{\text{in}}_{\tau'}(\text{session}^{\text{ID}}_{\text{N}}) \tag{16}$$

Hence:

$$\begin{aligned}
\neg\text{accept}^{\text{ID}}_{\tau'} \wedge \sigma_{\tau_x}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_x} \;&\rightarrow \bigvee_{\substack{\tau_x \preceq \tau_n \prec \tau' \\ \tau_n = _, \text{TN}(j_n,0), _, \text{TN}(j_n,1) \text{ or } _, \text{PN}(j_n,1)}} \sigma^{\text{in}}_{\tau'}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_n} && \text{(by induction hypothesis)} \\
&\rightarrow \bigvee_{\substack{\tau_x \preceq \tau_n \prec \tau' \\ \tau_n = _, \text{TN}(j_n,0), _, \text{TN}(j_n,1) \text{ or } _, \text{PN}(j_n,1)}} \sigma_{\tau'}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_n} && \text{(Using (16))} \\
&\rightarrow \bigvee_{\substack{\tau_x \preceq \tau_n \preceq \tau' \\ \tau_n = _, \text{TN}(j_n,0), _, \text{TN}(j_n,1) \text{ or } _, \text{PN}(j_n,1)}} \sigma_{\tau'}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_n} && \text{(Relaxing the condition } \tau_n \prec \tau')
\end{aligned}$$

Moreover,

$$\text{accept}^{\text{ID}}_{\tau'} \rightarrow \left(\sigma_{\tau'}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j'}\right) \;\rightarrow\; \bigvee_{\substack{\tau_x \preceq \tau_n \preceq \tau' \\ \tau_n = \_, \text{TN}(j_n,0), \_, \text{TN}(j_n,1) \text{ or } \_, \text{PN}(j_n,1)}} \sigma_{\tau'}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_n}$$

This concludes this case.

– If $\tau_n = \_, \text{PN}(j_n, 1)$ then the proof is the same than in the previous case, but doing a case disjunction over $\text{inc-accept}^{\text{ID}}_{\tau'}$.

Let $\tau_0{}'$ be such that $\tau_1 = \tau_0{}', \_$. By applying the induction hypothesis to $\tau_0{}'$, we get:

$$\sigma_{\tau_x}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_x} \;\rightarrow\; \bigvee_{\substack{\tau_x \preceq \tau_n \preceq \tau_0{}' \\ \tau_n = \_, \text{TN}(j_n,0), \_, \text{TN}(j_n,1) \text{ or } \_, \text{PN}(j_n,1)}} \sigma_{\tau_0{}'}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_n} \;\rightarrow\; \bigvee_{\substack{\tau_x \preceq \tau_n \prec \tau_1 \\ \tau_n = \_, \text{TN}(j_n,0), \_, \text{TN}(j_n,1) \text{ or } \_, \text{PN}(j_n,1)}} \sigma^{\text{in}}_{\tau_1}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^{j_n}$$

We conclude using (15) and the property above.

- **(B5)**. We prove this by induction over τ. For $\tau = \epsilon$, from Definition 43 we know that $\sigma_\epsilon(\text{SQN}^{\text{ID}}_{\text{U}}) \equiv \text{sqn-init}^{\text{ID}}_{\text{U}}$ and $\sigma_\epsilon(\text{SQN}^{\text{ID}}_{\text{N}}) \equiv \text{sqn-init}^{\text{ID}}_{\text{N}}$. Using the axiom SQN-ini, we know that $\text{sqn-init}^{\text{ID}}_{\text{N}} \leq \text{sqn-init}^{\text{ID}}_{\text{U}}$.
For the inductive case, we let $\tau = \tau_0, \text{ai}$ and assume that the property holds for τ_0. We have three cases:
  – If when executing the action ai the value $\text{SQN}^{\text{ID}}_{\text{N}}$ is not updated. Using **(B1)** we know that $\sigma_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) \geq \sigma_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}})$, and we conclude by applying the induction hypothesis.
  – If $\text{ai} = \text{PN}(j, 1)$, then we do a case disjunction on $\text{inc-accept}^{\text{ID}}_{\tau}$. If it is true then:

$$\begin{aligned}
\text{inc-accept}^{\text{ID}}_{\tau} \;&\rightarrow \bigvee_{\tau_0 = _, \text{PU}_{\text{ID}}(j_0,1) \prec \tau} \sigma_\tau(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\text{in}}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) && \text{(Using } \textbf{(Acc1)}) \\
&\rightarrow \bigvee_{\tau_0 = _, \text{PU}_{\text{ID}}(j_0,1) \prec \tau} \sigma_\tau(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\text{in}}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) \leq \sigma_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) && \text{(Using } \textbf{(B1)}) \\
&\rightarrow \sigma_\tau(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma_\tau(\text{SQN}^{\text{ID}}_{\text{U}})
\end{aligned}$$

  If $\text{inc-accept}^{\text{ID}}_{\tau}$ is false then $\neg\text{inc-accept}^{\text{ID}}_{\tau} \rightarrow \sigma_\tau(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\text{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}})$, and we conclude by applying the induction hypothesis.

– If $\mathsf{ai} = \text{TN}(j, 1)$, then we do a case disjunction on $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau}$. First we handle the case where it is true. Let $\tau_2 = \_, \text{TN}(j, 0) \prec \tau$. We know that $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau} \to \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j}$. Moreover:

$$\begin{aligned}
\sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j} \;&\to \bigwedge_{\substack{\tau_2 \prec \tau_1 \prec \tau \\ \tau_1 = _, \text{TN}(j_x, 0), _, \text{TN}(j_x, 1) \text{ or } _, \text{PN}(j_x, 1)}} \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\text{ID}}_{\text{N}}) \neq \mathsf{n}^{j_x} \\
&\to \sigma_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) && \text{(Using the contrapositive of } \textbf{(B4)}) \\
&\to \sigma_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) && \text{(Using } \textbf{(B1)})
\end{aligned}$$

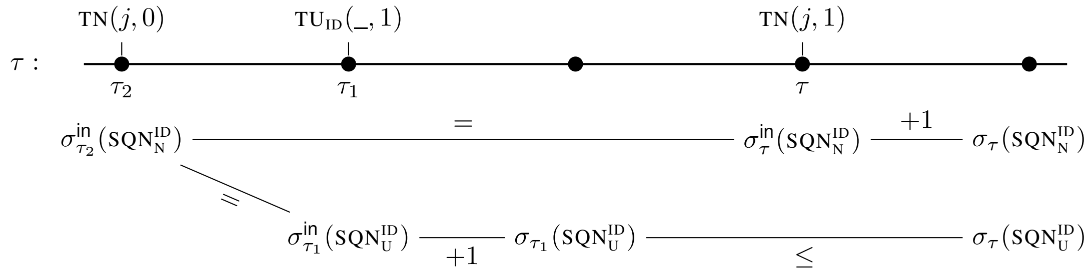
We know that $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau} \to \mathsf{accept}^{\text{ID}}_{\tau}$. Moreover, using **(Acc3)** and **(Acc4)**, we can check that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \;\to \bigvee_{\substack{\tau_1 = \_, \text{TU}_{\text{ID}}(\_, 1) \\ \tau_2 \prec \tau_1 \prec \tau}} \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{N}})$$

Moreover, $\mathsf{accept}^{\text{ID}}_{\tau} \to \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})$, and using **(B1)** we know that $\sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) \leq \sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}})$. Finally, $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau} \to \sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) + 1$. Putting everything together:

$$\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau} \to \sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}})$$

Which is what we wanted. We summarize graphically this proof below:



If $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau}$ is false then $\neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau} \to \sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}})$, and we conclude by applying the induction hypothesis.

- **(B6)**. First, observe that:

$$\sigma_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \to \bigvee_{\substack{\tau_n = \_, \text{PU}_{\text{ID}}(j, 2) \\ \tau_0 \prec \tau_n \prec \tau_1}} \mathsf{accept}^{\text{ID}}_{\tau_n} \tag{17}$$

Let $\tau_n = \_, \text{PU}_{\text{ID}}(j, 2)$ such that $\tau_0 \prec \tau_n \prec \tau_1$. Let $\tau_i = \_, \text{PU}_{\text{ID}}(j, 1)$ such that $\tau_i \prec \tau_n$. We know that $\tau_i \prec \tau_0$. We apply **(Acc2)**:

$$\mathsf{accept}^{\text{ID}}_{\tau_n} \;\to \bigvee_{\substack{\tau_x = \_, \text{PN}(j_x, 1) \\ \tau_i \prec \tau_x \prec \tau_n}} \mathsf{accept}^{\text{ID}}_{\tau_x} \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_i}) = \mathsf{n}^{j_x} \;\wedge\; \pi_1(g(\phi^{\mathsf{in}}_{\tau_x})) = \{\langle \text{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle\}^{\mathsf{n}^{j}_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}} \tag{18}$$

Let $\tau_x = \_, \text{PN}(j_x, 1)$ such that $\tau_i \prec \tau_x \prec \tau_n$. Using **(B1)**, we get that $\sigma_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) \leq \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}})$ and that $\sigma_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}})$. There are two cases, depending on whether we have $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_x}$.

– We know that $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_x} \to \sigma_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}}) + 1 > \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}})$. Putting everything together, we get that:

$$\mathsf{accept}^{\text{ID}}_{\tau_n} \wedge \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_x} \to \sigma_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \tag{19}$$

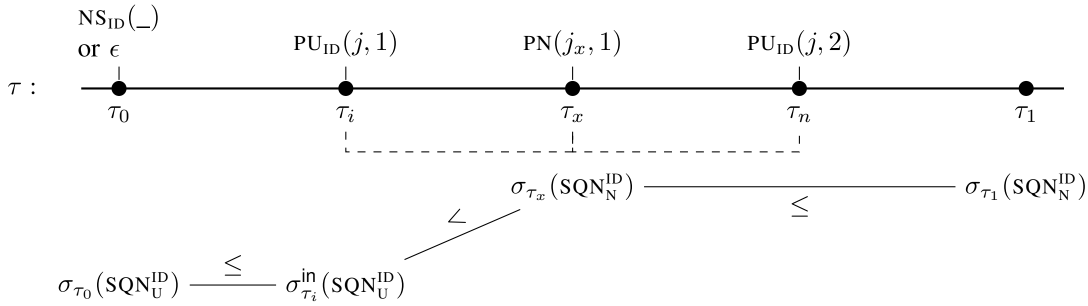
– We know that:

$$\mathsf{accept}^{\text{ID}}_{\tau_x} \wedge \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_x} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_x})) = \{\langle \text{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle\}^{\mathsf{n}^{j}_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}} \to \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{N}})$$

Moreover, $\neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_x} \to \sigma^{\mathsf{in}}_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{N}})$. We recall that $\sigma_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) \leq \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}})$ and that $\sigma_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}})$. Therefore:

$$\mathsf{accept}^{\text{ID}}_{\tau_x} \wedge \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_x} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_x})) = \{\langle \text{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_i}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle\}^{\mathsf{n}^{j}_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}} \to \sigma_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \tag{20}$$

Using (18), (19) and (20) we get that $\mathsf{accept}^{\text{ID}}_{\tau_n} \to \sigma_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}})$. We summarize this graphically below:



Since this is true for all $\tau_n = \_, \text{PU}_{\text{ID}}(j,2)$ such that $\tau_0 \prec \tau_n \prec \tau_1$, we deduce from (17) that

$$\sigma_{\tau_1}(\mathsf{sync}_{\text{U}}^{\text{ID}}) \rightarrow \sigma_{\tau_0}(\text{SQN}_{\text{U}}^{\text{ID}}) < \sigma_{\tau_1}(\text{SQN}_{\text{N}}^{\text{ID}})$$

Which concludes this proof.

- **(B7)**. Let $\tau_{\text{NS}} = \epsilon$ or $\text{NS}_{\text{ID}}(\_)$ be such that $\tau_{\text{NS}} \preceq \tau$ and $\tau_{\text{NS}} \not\prec_\tau \text{NS}_{\text{ID}}(\_)$. We show by induction over τ' with $\tau_{\text{NS}} \preceq \tau' \preceq \tau$ that $\sigma_{\tau'}(\mathsf{valid\text{-}guti}_{\text{U}}^{\text{ID}}) \equiv \mathsf{false}$.
  For $\tau' = \tau_{\text{NS}}$, this is true using from Definition 43 if if $\tau_{\text{NS}} = \epsilon$, and from the protocol term definitions if $\tau_{\text{NS}} = \text{NS}_{\text{ID}}(\_)$. The inductive case is straightforward. ■

We can now state the following acceptance characterization properties.

Lemma 11. *For every valid symbolic trace $\tau = \_, ai$ and identity ID we have:*

- ***(Equ2)*** *If $ai = \text{PU}_{\text{ID}}(j,2)$. Let $\tau_2 = \_\text{PU}_{\text{ID}}(j,1)$ such that $\tau_2 \prec \tau$. Also let:*

$$\mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \equiv \begin{pmatrix} g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}_{\mathsf{k_m^{ID}}}^2(\langle \mathsf{n}^{j_1}, \mathsf{suc}(\sigma_{\tau_2}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}}))\rangle) \wedge g(\phi_{\tau_2}^{\mathsf{in}}) = \mathsf{n}^{j_1} \\ \wedge\, \pi_1(g(\phi_{\tau_1}^{\mathsf{in}})) = \{\langle \text{ID}, \sigma_{\tau_2}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e}^j} \end{pmatrix}$$

Then:

$$\mathsf{accept}_\tau^{\text{ID}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{PN}(j_1,1) \\ \tau_2 \prec_\tau \tau_1}} \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1}$$

- ***(Equ3)*** *If $ai = \text{PN}(j,1)$. Then:*

$$\begin{aligned} \mathsf{accept}_\tau^{\text{ID}} &\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{PU}_{\text{ID}}(j_1,1) \\ \tau_1 \prec \tau}} \begin{pmatrix} g(\phi_{\tau_1}^{in}) = n^j \wedge \pi_1(g(\phi_\tau^{in})) = \{\langle \text{ID}, \sigma_{\tau_1}^{in}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{pk_{\text{N}}}^{n_e^{j_1}} \\ \wedge\, \pi_2(g(\phi_\tau^{in})) = Mac_{k_m^{\text{ID}}}^1(\langle \{\langle \text{ID}, \sigma_{\tau_1}^{in}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{pk_{\text{N}}}^{n_e^{j_1}}, g(\phi_{\tau_1}^{in})\rangle) \end{pmatrix} \\ &\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{PU}_{\text{ID}}(j_1,1) \\ \tau_1 \prec \tau}} \left(g(\phi_{\tau_1}^{in}) = n^j \wedge g(\phi_\tau^{in}) = t_{\tau_1}\right) \end{aligned}$$

- ***(Equ4)*** *If $ai = \text{TU}_{\text{ID}}(j,1)$. For every $\tau_1 = \_, \text{TN}(j_0,0)$ such that $\tau_1 \prec \tau$, we let:*

$$\mathsf{c\text{-}tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \equiv \begin{pmatrix} \pi_3(g(\phi_\tau^{in})) = Mac_{k_m}^3(\langle n^{j_0}, \sigma_{\tau_1}^{in}(\text{SQN}_{\text{N}}^{\text{ID}}), \sigma_\tau^{in}(\text{GUTI}_{\text{U}}^{\text{ID}})\rangle) \wedge \sigma_\tau^{in}(\mathsf{s\text{-}valid\text{-}guti}_{\text{U}}^{\text{ID}}) \\ \wedge\, range(\sigma_\tau^{in}(\text{SQN}_{\text{U}}^{\text{ID}}), \sigma_{\tau_1}^{in}(\text{SQN}_{\text{N}}^{\text{ID}})) \wedge g(\phi_{\tau_1}^{in}) = \sigma_{\tau_1}^{in}(\text{GUTI}_{\text{N}}^{\text{ID}}) \wedge \pi_1(g(\phi_\tau^{in})) = n^{j_0} \\ \wedge\, \pi_2(g(\phi_\tau^{in})) = \sigma_{\tau_1}^{in}(\text{SQN}_{\text{N}}^{\text{ID}}) \oplus f_k(n^{j_0}) \wedge \sigma_\tau^{in}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \sigma_{\tau_1}^{in}(\text{GUTI}_{\text{N}}^{\text{ID}}) \end{pmatrix}$$

Then:

$$\left(\mathsf{c\text{-}tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1} \rightarrow \mathsf{accept}_{\tau_1}^{\text{ID}}\right)_{\substack{\tau_1 = \_, \text{TN}(j_0,0) \\ \tau_1 \prec \tau}} \qquad \mathsf{accept}_\tau^{\text{ID}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{TN}(j_0,0) \\ \tau_1 \prec \tau}} \mathsf{c\text{-}tr}_{\mathsf{u}:\tau}^{\mathsf{n}:\tau_1}$$

- ***(Equ5)*** *If $ai = \text{TN}(j,1)$. Let $\tau_1 = \_, \text{TN}(j,0)$ such that $\tau_1 \prec \tau$, and let $\text{ID} \in \mathcal{S}_{id}$. Then:*

$$\mathsf{accept}_\tau^{\text{ID}} \leftrightarrow \bigvee_{\substack{\tau_i = \_, \text{TU}_{\text{ID}}(j_i,1) \\ \tau_1 \prec_\tau \tau_i}} \mathsf{c\text{-}tr}_{\mathsf{u}:\tau_i}^{\mathsf{n}:\tau_1} \wedge g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}_{\mathsf{k_m^{ID}}}^4(\mathsf{n}^j)$$

B. Proof of Lemma 11

*Proof of (**Equ2**):* Using **(Acc2)** we know that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau} \;\leftrightarrow\; \bigvee_{\substack{\tau_1=\_,\mathrm{PN}(j_1,1)\\ \tau_2\prec_\tau\tau_1}} \mathsf{accept}^{\mathrm{ID}}_{\tau} \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1} \;\wedge\; \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}$$

$$\leftrightarrow\; \bigvee_{\substack{\tau_1=\_,\mathrm{PN}(j_1,1)\\ \tau_2\prec_\tau\tau_1}} \begin{pmatrix} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}\,,\, \sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1} \\ \wedge\, \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}} \end{pmatrix}$$

Since $\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \;\equiv\; \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}))$:

$$\leftrightarrow\; \bigvee_{\substack{\tau_1=\_,\mathrm{PN}(j_1,1)\\ \tau_2\prec_\tau\tau_1}} \begin{pmatrix} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}\,,\, \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}))\rangle) \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1} \\ \wedge\, \pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}} \end{pmatrix}$$

$$\leftrightarrow\; \bigvee_{\substack{\tau_1=\_,\mathrm{PN}(j_1,1)\\ \tau_2\prec_\tau\tau_1}} \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$$

*Proof of (**Equ3**):* Using **(Acc1)** it is easy to check that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau} \;\leftrightarrow\; \bigvee_{\tau_1=\_,\mathrm{PU}_{\mathrm{ID}}(j_1,1)\prec\tau} \begin{pmatrix} \underset{\cdots}{g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^j} \wedge \underset{\sim\sim}{\pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^1_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \underset{\sim\sim}{\pi_1(g(\phi^{\mathsf{in}}_{\tau}))}\,,\, \underset{\cdots}{\mathsf{n}^j}\rangle) \end{pmatrix}$$

Which can be rewritten as follows (we identify above, using waves and dots, which equalities are used, and which terms are rewritten):

$$\leftrightarrow\; \bigvee_{\tau_1=\_,\mathrm{PU}_{\mathrm{ID}}(j_1,1)\prec\tau} \begin{pmatrix} g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^j \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^1_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}\,,\, g(\phi^{\mathsf{in}}_{\tau_1})\rangle) \end{pmatrix}$$

First, observe that:

$$\{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}} = \pi_1(t_{\tau_1}) \qquad\qquad \mathsf{Mac}^1_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}\,,\, g(\phi^{\mathsf{in}}_{\tau_1})\rangle) == \pi_2(t_{\tau_1})$$

We conclude easily using the injectivity of the pair.

*Proof of (**Equ4**):* Using **(Acc3)** we know that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau} \leftrightarrow \bigvee_{\substack{\tau_1=\_,\mathrm{TN}(j_0,0)\\ \tau_1\prec\tau}} \begin{pmatrix} \mathsf{accept}^{\mathrm{ID}}_{\tau} \wedge \mathsf{accept}^{\mathrm{ID}}_{\tau_1} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{pmatrix}$$

Inlining the definition of $\mathsf{accept}^{\mathrm{ID}}_{\tau_1}$:

$$\leftrightarrow \bigvee_{\substack{\tau_1=\_,\mathrm{TN}(j_0,0)\\ \tau_1\prec\tau}} \begin{pmatrix} \mathsf{accept}^{\mathrm{ID}}_{\tau} \wedge g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{pmatrix}$$

Inlining the definition of $\mathsf{accept}^{\mathrm{ID}}_{\tau}$:

$$\leftrightarrow \bigvee_{\substack{\tau_1=\_,\mathrm{TN}(j_0,0)\\ \tau_1\prec\tau}} \begin{pmatrix} \pi_3(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^3_{\mathsf{k}_{\mathsf{m}}}(\langle \underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau}))}\,, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f}_{\mathsf{k}}(\underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau}))})\,,\, \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \\ \wedge\, \sigma^{\mathsf{in}}_{\tau}(\mathsf{s\text{-}valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{range}(\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \pi_2(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f}_{\mathsf{k}}(\underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau}))})) \\ g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet} \wedge \underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0}} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f}_{\mathsf{k}}(\mathsf{n}^{j_0}) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{pmatrix}$$

We rewrite $\pi_1(g(\phi^{\mathsf{in}}_{\tau}))$ into n^{j_0}:

$$\leftrightarrow \bigvee_{\substack{\tau_1=\_,\mathrm{TN}(j_0,0)\\ \tau_1\prec\tau}} \begin{pmatrix} \pi_3(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{Mac}^3_{\mathsf{k}_{\mathsf{m}}}(\langle \underline{\mathsf{n}^{j_0}}\,, \underline{\pi_2(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f}_{\mathsf{k}}(\underline{\mathsf{n}^{j_0}})}\,,\, \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \\ \wedge\, \sigma^{\mathsf{in}}_{\tau}(\mathsf{s\text{-}valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{range}(\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \underline{\pi_2(g(\phi^{\mathsf{in}}_{\tau})) \oplus \mathsf{f}_{\mathsf{k}}(\underline{\mathsf{n}^{j_0}})}) \\ g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet} \wedge \underline{\pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0}} \\ \wedge\, \underline{\pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f}_{\mathsf{k}}(\mathsf{n}^{j_0})} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{pmatrix}$$

We rewrite $\pi_2(g(\phi^{\mathsf{in}}_\tau)) \oplus \mathsf{f_k}(\mathsf{n}^{j_0})$ into $\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$:

$$\leftrightarrow \bigvee_{\substack{\tau_1 = \_,\mathrm{TN}(j_0,0)\\ \tau_1 \prec \tau}} \begin{pmatrix} \pi_3(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})}, \sigma^{\mathsf{in}}_\tau(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \\ \wedge\, \sigma^{\mathsf{in}}_\tau(\mathsf{s\text{-}valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{range}(\sigma^{\mathsf{in}}_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})}) \\ \wedge\, g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet} \wedge \pi_1(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{n}^{j_0} \\ \wedge\, \underline{\pi_2(g(\phi^{\mathsf{in}}_\tau)) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0})} \wedge \sigma^{\mathsf{in}}_\tau(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{pmatrix} \tag{21}$$

Let $\tau_2 = \_, \mathrm{TU_{ID}}(j_0, 0) \prec \tau$. By validity of τ, there are no user ID actions between τ_2 and τ, and therefore it is easy to check that $\sigma^{\mathsf{in}}_\tau(\mathsf{s\text{-}valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\mathsf{valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}})$, and that $\sigma^{\mathsf{in}}_\tau(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})$. Moreover, using **(B3)** we know that $\sigma^{\mathsf{in}}_{\tau_2}(\mathsf{valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{UnSet}$. Therefore $\sigma^{\mathsf{in}}_\tau(\mathsf{s\text{-}valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\mathsf{in}}_\tau(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) \neq \mathsf{UnSet}$. It follows that:

$$\left(\sigma^{\mathsf{in}}_\tau(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma^{\mathsf{in}}_\tau(\mathsf{s\text{-}valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}})\right) \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet}$$

Hence we can simplify (21) by removing $\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \neq \mathsf{UnSet}$. This yields:

$$\begin{aligned} \mathsf{accept}^{\mathrm{ID}}_\tau &\leftrightarrow \bigvee_{\substack{\tau_1 = \_,\mathrm{TN}(j_0,0)\\ \tau_1 \prec \tau}} \begin{pmatrix} \pi_3(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^3_{\mathsf{k_m}}(\langle \mathsf{n}^{j_0}, \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}), \sigma^{\mathsf{in}}_\tau(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\rangle) \wedge \sigma^{\mathsf{in}}_\tau(\mathsf{s\text{-}valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}}) \\ \wedge\, \mathsf{range}(\sigma^{\mathsf{in}}_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})) \wedge g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \pi_1(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{n}^{j_0} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \wedge \sigma^{\mathsf{in}}_\tau(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}}) \end{pmatrix} \\ &\leftrightarrow \bigvee_{\substack{\tau_1 = \_,\mathrm{TN}(j_0,0)\\ \tau_1 \prec \tau}} \mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \end{aligned}$$

Finally, it is easy to check that for every $\tau_1 = \_, \mathrm{TN}(j_0, 0)$ such that $\tau_1 \prec \tau$, we have $\mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \mathsf{accept}^{\mathrm{ID}}_{\tau_1}$.

*Proof of **(Equ5)**:* Using **(Acc4)** we know that:

$$\mathsf{accept}^{\mathrm{ID}}_\tau \leftrightarrow \bigvee_{\tau_i = \_,\mathrm{TU_{ID}}(j_i,1) \prec \tau} \mathsf{accept}^{\mathrm{ID}}_\tau \wedge \mathsf{accept}_{\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j$$

Moreover, using **(Equ4)** we know that:

$$\mathsf{accept}^{\mathrm{ID}}_\tau \leftrightarrow \bigvee_{\substack{\tau_i = \_,\mathrm{TU_{ID}}(j_i,1) \prec \tau\\ \tau_2 = \_,\mathrm{TN}(j_2,0) \prec \tau_i}} \mathsf{accept}^{\mathrm{ID}}_\tau \wedge \mathsf{c\text{-}tr}^{\mathsf{n}:\tau_2}_{\mathsf{u}:\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j$$

Let $\tau_2 = \_, \mathrm{TN}(j_2, 0) \prec \tau_i$. Then we know that $\mathsf{c\text{-}tr}^{\mathsf{n}:\tau_2}_{\mathsf{u}:\tau_i} \rightarrow \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^{j_2}$. Therefore using $\mathsf{EQIndep}$ we know that if $j_2 \neq j$:

$$\left(\mathsf{c\text{-}tr}^{\mathsf{n}:\tau_2}_{\mathsf{u}:\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j\right) \rightarrow \left(\pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^{j_2} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j\right) \rightarrow \mathsf{false}$$

Hence:

$$\mathsf{accept}^{\mathrm{ID}}_\tau \leftrightarrow \bigvee_{\substack{\tau_i = \_,\mathrm{TU_{ID}}(j_i,1)\\ \tau_1 \prec_\tau \tau_i}} \mathsf{accept}^{\mathrm{ID}}_\tau \wedge \mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j$$

Since $\mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i} \rightarrow \pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \mathsf{n}^j$:

$$\leftrightarrow \bigvee_{\substack{\tau_i = \_,\mathrm{TU_{ID}}(j_i,1)\\ \tau_1 \prec_\tau \tau_i}} \mathsf{accept}^{\mathrm{ID}}_\tau \wedge \mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i}$$

We inline the definition of $\mathsf{accept}^{\mathrm{ID}}_\tau$:

$$\leftrightarrow \bigvee_{\substack{\tau_i = \_,\mathrm{TU_{ID}}(j_i,1)\\ \tau_1 \prec_\tau \tau_i}} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k^{ID}_m}}(\mathsf{n}^j) \wedge \sigma^{\mathsf{in}}_\tau(\mathsf{b\text{-}auth}^j_{\mathrm{N}}) = \mathrm{ID} \wedge \mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i}$$

Using **(Equ4)**, we know that for every $\tau_1 = \_, \mathrm{TN}(j_0, 0)$ such that $\tau_1 \prec \tau$, $\mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \mathsf{accept}^{\mathrm{ID}}_{\tau_1}$. Moreover, using **(A6)** we know that $\mathsf{accept}^{\mathrm{ID}}_{\tau_1} \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{b\text{-}auth}^j_{\mathrm{N}}) = \mathrm{ID}$. Besides, $\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{b\text{-}auth}^j_{\mathrm{N}}) = \mathrm{ID} \rightarrow \sigma^{\mathsf{in}}_\tau(\mathsf{b\text{-}auth}^j_{\mathrm{N}}) = \mathrm{ID}$. Hence $\mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \sigma^{\mathsf{in}}_\tau(\mathsf{b\text{-}auth}^j_{\mathrm{N}}) = \mathrm{ID}$. By consequence:

$$\mathsf{accept}^{\mathrm{ID}}_\tau \leftrightarrow \bigvee_{\substack{\tau_i = \_,\mathrm{TU_{ID}}(j_i,1)\\ \tau_1 \prec_\tau \tau_i}} g(\phi^{\mathsf{in}}_\tau) = \mathsf{Mac}^4_{\mathsf{k^{ID}_m}}(\mathsf{n}^j) \wedge \mathsf{c\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_i}$$

C. $\text{GUTI}^{\text{ID}}_{\text{U}}$ *Concealment*

Lemma 12. *Let τ be a valid symbolic trace and $\text{ID}_x \in \mathcal{S}_{id}$. For every $\tau_a = \_, \text{TN}(j_a, 1)$ or $\tau_a = \_, \text{PN}(j_a, 1)$ such that $\tau_a \preceq \tau$, and for every $\tau_b = \text{PU}_{\text{ID}_x}(j_i, 1)$ or $\tau_b = \text{TU}_{\text{ID}_x}(j_i, 1)$ such that $\tau_b \prec \tau_a$, if:*

$$\{\tau_1 \mid \tau_b \prec_\tau \tau_1\} \cap \{\text{PU}_{\text{ID}_x}(j, \_), \text{TU}_{\text{ID}_x}(j, \_), \text{FU}_{\text{ID}_x}(j) \mid j \in \mathbb{N}\} \subseteq \{\text{PU}_{\text{ID}_x}(j_i, 2), \text{FU}_{\text{ID}_x}(j_i)\}$$

Then there exists a derivation of:

$$\text{inc-accept}^{\text{ID}_x}_{\tau_a} \wedge \sigma_{\tau_b}(\textit{b-auth}^{\text{ID}_x}_{\text{U}}) = \textit{n}^{j_a} \wedge \text{accept}^{\text{ID}_x}_{\tau_b} \rightarrow g(\phi^{\textit{in}}_{\tau}) \neq \text{GUTI}^{j_a}$$

Proof of Lemma 12: Let $\mathsf{leak}^{\mathsf{in}}_{\tau}$ be the vector of terms containing:

- $\mathsf{leak}^{\mathsf{in}}_{\tau_0}$ if $\tau = \tau_0, \mathsf{ai}_0$ and $\tau \prec \tau_a$.
- The term β.
- All the keys except k^{ID_x}, $\mathsf{k}^{\text{ID}_x}_{\mathsf{m}}$ and the asymmetric secret key sk_{N}.
- All elements of $\sigma^{\mathsf{in}}_{\tau}$ (in an arbitrary order) except:
  - All the user ID_x values, i.e. for every X we have $\sigma^{\mathsf{in}}_{\tau}(\text{X}^{\text{ID}_x}_{\text{U}}) \notin \mathsf{leak}^{\mathsf{in}}_{\tau}$.
  - The network's GUTI value of user ID_x, i.e. $\sigma^{\mathsf{in}}_{\tau}(\text{GUTI}^{\text{ID}_x}_{\text{N}}) \notin \mathsf{leak}^{\mathsf{in}}_{\tau}$.

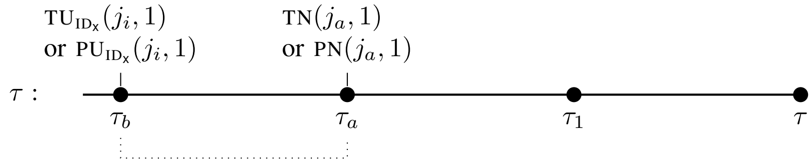
Let:

$$\beta \equiv \text{inc-accept}^{\text{ID}_x}_{\tau_a} \wedge \sigma_{\tau_b}(\text{b-auth}^{\text{ID}_x}_{\text{U}}) = \text{n}^{j_a} \wedge \text{accept}^{\text{ID}_x}_{\tau_b}$$

Let GUTI be a fresh name. We show by induction on τ_1 in $\tau_a \preceq \tau_1 \prec \tau$ that there are derivations of:

$$[\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \text{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \text{GUTI}\right)$$
$$\beta \rightarrow \sigma_{\tau_1}(\text{GUTI}^{\text{ID}_x}_{\text{N}}) = \text{GUTI}^{j_a} \quad (22)$$

We depict the situation below:



a) Case $\tau_1 = \tau_a$: First, $\beta \rightarrow \text{inc-accept}^{\text{ID}_x}_{\tau_a}$, and $\text{inc-accept}^{\text{ID}_x}_{\tau_a} \rightarrow \sigma_{\tau_a}(\text{GUTI}^{\text{ID}_x}_{\text{N}}) = \text{GUTI}^{j_a}$. Therefore we know that:

$$\beta \rightarrow \sigma_{\tau_a}(\text{GUTI}^{\text{ID}_x}_{\text{N}}) = \text{GUTI}^{j_a}$$

Then, we observe from the definition of leak_{τ_a} that $\text{GUTI}^{j_a} \notin \mathsf{st}(\mathsf{leak}_{\tau_a})$ (since $\sigma_{\tau_a}(\text{GUTI}^{\text{ID}_x}_{\text{N}})$ is *not* in leak_{τ_a}). Moreover GUTI^{j_a} does not appear in $\phi^{\mathsf{in}}_{\tau_a}$ and t_{τ_a}. Besides, GUTI is a fresh name. By consequence we can apply the Fresh axiom, and then conclude using Refl:

$$\dfrac{\dfrac{}{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}\right) \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}\right)}\ \mathsf{Refl}}{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \text{GUTI}^{j_a}\right) \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \text{GUTI}\right)}\ \mathsf{Fresh}$$

b) Case $\tau_a \prec \tau_1$: Let ai be such that $\tau_1 = \_, \mathsf{ai}$. Assume by induction that:

$$[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \text{GUTI}^{j_a}\right) \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \text{GUTI}\right) \quad (23)$$
$$\beta \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}_x}_{\text{N}}) = \text{GUTI}^{j_a} \quad (24)$$

c) Part 1: First, we show that:

$$\beta \rightarrow \sigma_{\tau_1}(\text{GUTI}^{\text{ID}_x}_{\text{N}}) = \text{GUTI}^{j_a}$$

Since we know that (22) holds, we just need to look at the case ai that updates $\text{GUTI}^{\text{ID}_x}_{\text{N}}$ to conclude:

- If $\mathsf{ai} = \text{TN}(j, 0)$. Using (23), we know that $g(\phi^{\mathsf{in}}_{\tau_1}) \neq \text{GUTI}^{j_a}$. Hence using (24) we know that:

$$\beta \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}_x}_{\text{N}}) \neq g(\phi^{\mathsf{in}}_{\tau_1})$$

  Which shows that $\beta \rightarrow \neg\text{accept}^{\text{ID}_x}_{\tau_1}$. This concludes this case.

- If $\mathsf{ai} = \textsc{pn}(j, 1)$. Since $\tau_a = \textsc{tn}(j_1, 1)$ or $\textsc{pn}(j_1, 1)$, we know by validity of τ that $j_a \neq j$. Using **(Equ3)** we know that:

$$\mathsf{accept}_{\tau_1}^{\mathrm{ID_x}} \rightarrow \bigvee_{\substack{\tau_n = \_, \textsc{pu}_{\mathrm{ID}}(j_n, 1) \\ \tau_n \prec \tau_1}} g(\phi_{\tau_n}^{\mathsf{in}}) = \mathsf{n}^j \tag{25}$$

Since $j_a \neq j$ we know that $\mathsf{n}^j \neq \mathsf{n}^{j_a}$. Moreover:

$$\sigma_{\tau_b}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID_x}}) = \mathsf{n}^{j_a} \wedge \mathsf{accept}_{\tau_b}^{\mathrm{ID_x}} \rightarrow g(\phi_{\tau_b}^{\mathsf{in}}) = \mathsf{n}^{j_a}$$

Hence $\beta \rightarrow g(\phi_{\tau_b}^{\mathsf{in}}) \neq \mathsf{n}^j$. Moreover, for every τ' between τ_b and τ_1, we know that $\tau' \neq \textsc{pu}_{\mathrm{ID_x}}(\_, 1)$. Therefore we know that:

$$\beta \wedge \mathsf{accept}_{\tau_1}^{\mathrm{ID_x}} \rightarrow \bigvee_{\substack{\tau_n = \_, \textsc{pu}_{\mathrm{ID}}(j_n, 1) \\ \tau_n \prec \tau_b}} g(\phi_{\tau_n}^{\mathsf{in}}) = \mathsf{n}^j \wedge \pi_1(g(\phi_{\tau_1}^{\mathsf{in}})) = \{\langle \mathrm{ID}_{\mathsf{x}} \,,\, \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID_x}})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e}^{j_n}}$$

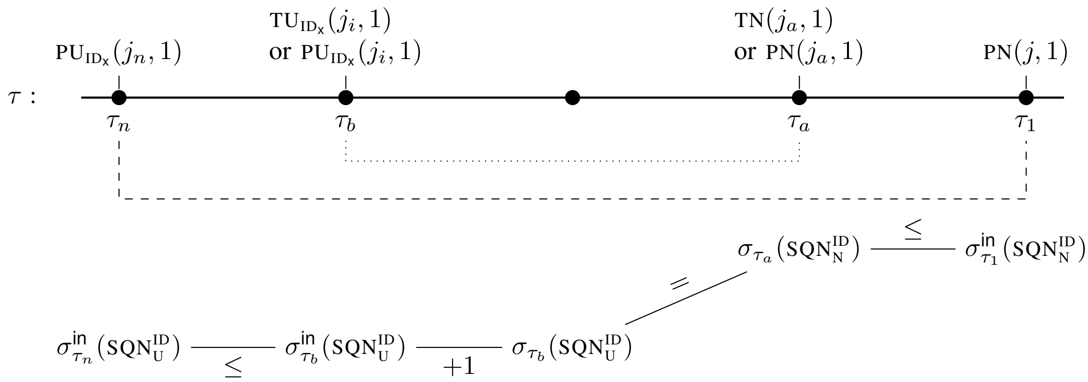
Let $\tau_n = \_, \textsc{pu}_{\mathrm{ID}}(j_n, 1)$ such that $\tau_n \prec \tau_b$. We know that:

$$\beta \rightarrow \sigma_{\tau_a}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID_x}}) = \sigma_{\tau_b}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID_x}}) = \mathsf{suc}(\sigma_{\tau_b}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID_x}}))$$

And that:

$$\sigma_{\tau_a}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID_x}}) \leq \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID_x}}) \qquad\qquad \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID_x}}) \leq \sigma_{\tau_b}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID_x}})$$

Graphically:



We deduce that:

$$\beta \wedge \mathsf{accept}_{\tau_1}^{\mathrm{ID_x}} \wedge g(\phi_{\tau_n}^{\mathsf{in}}) = \mathsf{n}^j \rightarrow \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID_x}}) > \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID_x}})$$

Moreover:

$$\left(\beta \wedge \mathsf{inc\text{-}accept}_{\tau_1}^{\mathrm{ID_x}} \wedge g(\phi_{\tau_n}^{\mathsf{in}}) = \mathsf{n}^j \wedge \pi_1(g(\phi_{\tau_1}^{\mathsf{in}})) = \{\langle \mathrm{ID}_{\mathsf{x}} \,,\, \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID_x}})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e}^{j_n}}\right) \rightarrow \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID_x}}) \leq \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID_x}})$$

Hence:

$$\left(\beta \wedge \mathsf{accept}_{\tau_1}^{\mathrm{ID_x}} \wedge g(\phi_{\tau_n}^{\mathsf{in}}) = \mathsf{n}^j \wedge \wedge \pi_1(g(\phi_{\tau_1}^{\mathsf{in}})) = \{\langle \mathrm{ID}_{\mathsf{x}} \,,\, \sigma_{\tau_n}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID_x}})\rangle\}_{\mathsf{pk_N}}^{\mathsf{n_e}^{j_n}}\right) \rightarrow \neg\mathsf{inc\text{-}accept}_{\tau_1}^{\mathrm{ID_x}}$$

Using (25), this shows that:

$$\beta \wedge \mathsf{accept}_{\tau_1}^{\mathrm{ID_x}} \rightarrow \neg\mathsf{inc\text{-}accept}_{\tau_1}^{\mathrm{ID_x}}$$

This concludes this proof.

- If $\mathsf{ai} = \textsc{tn}(j, 1)$. Since $\tau_a = \textsc{tn}(j_1, 1)$ or $\textsc{pn}(j_1, 1)$, we know by validity of τ that $j_a \neq j$. From the induction hypothesis we know that:

$$\beta \rightarrow \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID_x}}) = \mathrm{GUTI}^{j_a}$$

It is easy to check that:

$$\sigma_{\tau_1}^{\mathsf{in}}(\mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID_x}}) = \mathrm{GUTI}^{j_a} \rightarrow \sigma_{\tau_1}^{\mathsf{in}}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID_x}}) = \mathsf{n}^{j_a}$$

Hence:

$$\begin{aligned}
\beta \to\ & \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{session}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathsf{n}^{j_a} \\
\to\ & \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{session}^{\mathrm{ID_x}}_{\mathrm{N}}) \neq \mathsf{n}^{j} && \text{(Since } j \neq j_a\text{)} \\
\to\ & \neg\mathsf{inc\text{-}accept}^{\mathrm{ID_x}}_{\tau_1} \\
\to\ & \sigma_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID_x}}_{\mathrm{N}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathrm{GUTI}^{j_a}
\end{aligned}$$

Which concludes this case.

d) Part 2: We now show that:

$$[\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta_{\tau_1}]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)$$

We do a case disjunction on ai. We only details the case where ai is a symbolic action of user ID, with $\mathrm{ID} \neq \mathrm{ID_x}$, and the case where $\mathsf{ai} = \mathrm{FN}(j_a)$. All the other cases are similar to these two cases, and their proof will only be sketched.

- If ai is a symbolic action of user ID, with $\mathrm{ID} \neq \mathrm{ID_x}$, then for every $u \in \mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1}$ (resp. $u \equiv t_{\tau_1}$) we show that there exists a many-hole context C_u such that $u \equiv C_u[\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}]$ and C_u does not contain any n.
  We only detail the case $\mathsf{ai} = \mathrm{FU_{ID}}(j)$. First, observe that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau_1} \equiv \left(\begin{array}{l} \quad \mathsf{eq}(\pi_2(g(\underline{\phi^{\mathsf{in}}_{\tau_1}})), \mathsf{Mac}^5_{\underline{\mathsf{k_m}}}(\langle \pi_1(g(\underline{\phi^{\mathsf{in}}_{\tau_1}})) \oplus \mathsf{f}^{\mathsf{r}}_{\underline{\mathsf{k}}}(\underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}})}), \underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}})}\rangle)) \\ \wedge \ \ \neg\mathsf{eq}(\underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}})}, \mathsf{fail}) \ \wedge \ \neg\mathsf{eq}(\underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}})}, \bot) \end{array}\right)$$

  All the underlined subterms are in $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, therefore there exists a context C_{accept} such that $\mathsf{accept}^{\mathrm{ID}}_{\tau_1} \equiv C_{\mathsf{accept}}[\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}]$. Remark that $\mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1} = \{\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})\}$. Moreover:

$$t_{\tau_1} \equiv \text{ if } \mathsf{accept}^{\mathrm{ID}}_{\tau_1} \text{ then ok else error} \qquad\qquad \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}}) \equiv \mathsf{accept}^{\mathrm{ID}}_{\tau_1}$$

$$\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) \equiv \text{ if } \mathsf{accept}^{\mathrm{ID}}_{\tau_1} \text{ then } \pi_1(g(\underline{\phi^{\mathsf{in}}_{\tau_1}})) \oplus \mathsf{f}^{\mathsf{r}}_{\underline{\mathsf{k}}}(\underline{\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}})}) \text{ else UnSet}$$

  Using the fact that all the underlined subterms are in $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, and using C_{accept} it is easy to build the wanted contexts. We then conclude using the FA rule under context, the Dup rule and the induction hypothesis:

$$\dfrac{\dfrac{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right)}{\begin{array}{c}[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}, (C_u[\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}])_{u \in \{t_{\tau_1}, \mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1}\}}\right) \\ \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}, (C_u[\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}])_{u \in \{t_{\tau_1}, \mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1}\}}\right)\end{array}}\,(\mathsf{FA_c} + \mathsf{Dup})^*}{[\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\,R$$

- If $\mathsf{ai} = \mathrm{FN}(j_a)$. It is easy to check that:

$$\sigma^{\mathsf{in}}_{\tau_a}(\mathsf{e\text{-}auth}^{\mathrm{ID_x}}_{\mathrm{N}}) \neq \mathrm{ID_x} \to \sigma^{\mathsf{in}}_{\tau_a}(\mathrm{GUTI}^{\mathrm{ID_x}}_{\mathrm{N}}) \neq \mathrm{GUTI}^{j_a} \to \sigma^{\mathsf{in}}_{\tau}(\mathrm{GUTI}^{\mathrm{ID_x}}_{\mathrm{N}}) \neq \mathrm{GUTI}^{j_a}$$

  Therefore using the induction property (24) we deduce that $\beta \to \sigma^{\mathsf{in}}_{\tau_a}(\mathsf{e\text{-}auth}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathrm{ID_x}$. Moreover by validity of τ, there are no session j_a network actions between τ_a and τ_1. It follows that $\sigma^{\mathsf{in}}_{\tau_a}(\mathsf{e\text{-}auth}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathrm{ID_x} \to \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID_x}}_{\mathrm{N}}) = \mathrm{ID_x}$. Hence:

$$t_{\tau_1} = \left\langle \mathrm{GUTI}^{j_a} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\mathrm{ID_x}}}(\mathsf{n}^{j_a}), \mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_a}, \mathsf{n}^{j_a}\rangle)\right\rangle$$

  Observe that:

$$[\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) = [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \left\langle \mathrm{GUTI}^{j_a} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\mathrm{ID_x}}}(\mathsf{n}^{j_a}), \mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_a}, \mathsf{n}^{j_a}\rangle)\right\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right)$$

  We are now going to apply the PRF-f axiom on the left to replace $\mathrm{GUTI}^{j_a} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\mathrm{ID_x}}}(\mathsf{n}^{j_a})$ with $\mathrm{GUTI}^{j_a} \oplus \mathsf{n_f}$ where $\mathsf{n_f}$ is a fresh nonce. For every $\tau_2 = \_, \mathrm{FU_{ID}}(\_) \prec \tau_1$, we use **(Equ1)** to replace every occurrences of accept_{τ_2} in $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \beta$ with:

$$\gamma_{\tau_2} \equiv \bigvee_{\substack{\tau_3 = \_, \mathrm{FN}(\_) \prec \tau_2 \\ \tau_3 \not\prec_{\tau_2} \mathrm{NS_{ID}}(\_)}} \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_3}_{\mathsf{u}:\tau_2}$$

  which yields the terms $\phi'^{\mathsf{in}}_{\tau_1}, \mathsf{leak}'^{\mathsf{in}}_{\tau_1}, \beta'$. We can check that:

$$\mathsf{set\text{-}prf}^{\mathsf{f}^{\mathsf{r}}}_{\mathsf{k}^{\mathrm{ID_x}}}(\gamma_{\tau_2}) \subseteq \{\mathsf{n}^p \mid \exists \tau' = \_, \mathrm{FN}(p) \prec \tau_1\}$$

And that:

$$\text{set-prf}^{\mathsf{f}^{\mathsf{r}}}_{\mathsf{k}^{\mathrm{ID_x}}}(\phi'^{\mathsf{in}}_{\tau_1}, \mathsf{leak}'^{\mathsf{in}}_{\tau_1}) = \{\mathsf{n}^p \mid \exists \tau' = \_, \mathrm{FN}(p) \prec \tau_1\}$$

Therefore we can apply the PRF-faxiom as wanted: first we replace $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \beta$ by $\phi'^{\mathsf{in}}_{\tau_1}, \mathsf{leak}'^{\mathsf{in}}_{\tau_1}, \beta'$ using rule R; then we apply the PRF-faxiom; and finally we rewrite all γ_{τ_2} back into $\mathsf{accept}^{\mathrm{ID_x}}_{\tau_2}$. Then, we use the $\oplus$-indep axiom to replace $\mathrm{GUTI}^{j_a} \oplus \mathsf{n_f}$ with a fresh nonce n'_f. This yield the derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \left\langle \mathsf{n}'_\mathsf{f}\,,\, \mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_\mathsf{m}}(\langle \mathrm{GUTI}^{j_a}\,,\, \mathsf{n}^{j_a}\rangle)\right\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \left\langle \mathrm{GUTI}^{j_a} \oplus \mathsf{n_f}\,,\, \mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_\mathsf{m}}(\langle \mathrm{GUTI}^{j_a}\,,\, \mathsf{n}^{j_a}\rangle)\right\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ \oplus\text{-indep}}{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \left\langle \mathrm{GUTI}^{j_a} \oplus \mathsf{n_f}\,,\, \mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_\mathsf{m}}(\langle \mathrm{GUTI}^{j_a}\,,\, \mathsf{n}^{j_a}\rangle)\right\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ R}{[\beta']\left(\phi'^{\mathsf{in}}_{\tau_1}, \left\langle \mathrm{GUTI}^{j_a} \oplus \mathsf{n_f}\,,\, \mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_\mathsf{m}}(\langle \mathrm{GUTI}^{j_a}\,,\, \mathsf{n}^{j_a}\rangle)\right\rangle, \mathsf{leak}'^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ R}{[\beta']\left(\phi'^{\mathsf{in}}_{\tau_1}, \left\langle \mathrm{GUTI}^{j_a} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\mathrm{ID_x}}}(\mathsf{n}^{j_a})\,,\, \mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_\mathsf{m}}(\langle \mathrm{GUTI}^{j_a}\,,\, \mathsf{n}^{j_a}\rangle)\right\rangle, \mathsf{leak}'^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ \text{PRF-f}}{[\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ R$$

We do a similar reasoning to replace $\mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_\mathsf{m}}(\langle \mathrm{GUTI}^{j_a}\,,\, \mathsf{n}^{j_a}\rangle)$ with a fresh nonce n''_f using PRF-MAC^5 axiom (we omit the details):

$$\dfrac{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \langle \mathsf{n}'_\mathsf{f}\,,\, \mathsf{n}''_\mathsf{f}\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \left\langle \mathsf{n}'_\mathsf{f}\,,\, \mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_\mathsf{m}}(\langle \mathrm{GUTI}^{j_a}\,,\, \mathsf{n}^{j_a}\rangle)\right\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ (R + \text{PRF-MAC}^5)^*$$

We then do the same thing on the right side, and use the FA axiom under context

$$\dfrac{\dfrac{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{n}'_\mathsf{f}, \mathsf{n}''_\mathsf{f}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{n}'_\mathsf{f}, \mathsf{n}''_\mathsf{f}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right)}{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \langle \mathsf{n}'_\mathsf{f}\,,\, \mathsf{n}''_\mathsf{f}\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \langle \mathsf{n}'_\mathsf{f}\,,\, \mathsf{n}''_\mathsf{f}\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right)}\ \mathsf{FA_c}}{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \langle \mathsf{n}'_\mathsf{f}\,,\, \mathsf{n}''_\mathsf{f}\rangle, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi_{\tau_1}, \mathsf{leak}_{\tau_1}, \mathrm{GUTI}\right)}\ (R + \text{PRF-MAC}^5 + \text{PRF-f} + \oplus\text{-indep})^*$$

Using the fact that $\beta \in \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, we have:

$$\dfrac{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right), \mathsf{n}'_\mathsf{f}, \mathsf{n}''_\mathsf{f}, \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right), \mathsf{n}'_\mathsf{f}, \mathsf{n}''_\mathsf{f},}{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{n}'_\mathsf{f}, \mathsf{n}''_\mathsf{f}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{n}'_\mathsf{f}, \mathsf{n}''_\mathsf{f}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right)}\ \mathsf{Simp}$$

We then conclude using Fresh:

$$\dfrac{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right) \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right)}{[\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}^{j_a}\right), \mathsf{n}'_\mathsf{f}, \mathsf{n}''_\mathsf{f} \sim [\beta]\left(\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}, \mathrm{GUTI}\right), \mathsf{n}'_\mathsf{f}, \mathsf{n}''_\mathsf{f}}\ \mathsf{Fresh}^2$$

We now sketch the proof of the induction property for the remaining cases:

- If $\mathsf{ai} = \mathrm{FN}(j)$ with $j \neq j_a$. First, we can decompose t_{τ_1} into terms of $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, except for the term:

$$\left\langle \mathrm{GUTI}^{j} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\mathrm{ID_x}}}(\mathsf{n}^{j})\,,\, \mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_\mathsf{m}}(\langle \mathrm{GUTI}^{j}\,,\, \mathsf{n}^{j}\rangle)\right\rangle$$

  The rest of the proof goes as in case $\mathsf{ai} = \mathrm{FN}(j_a)$. On both side, we do the following:
  - We apply the PRF-faxiom to replace $\mathrm{GUTI}^{j} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\mathrm{ID_x}}}(\mathsf{n}^{j})$ with $\mathrm{GUTI}^{j} \oplus \mathsf{n_f}$ where $\mathsf{n_f}$ is a fresh nonce.
  - We use the $\oplus$-indep axiom to replace $\mathrm{GUTI}^{j} \oplus \mathsf{n_f}$ with a fresh nonce n'_f
  - We apply the PRF-MAC^5 axiom to replace $\mathsf{Mac}^5_{\mathsf{k}^{\mathrm{ID_x}}_\mathsf{m}}(\langle \mathrm{GUTI}^{j}\,,\, \mathsf{n}^{j}\rangle)$ with a fresh nonce n''_f.

  Finally we use Fresh to get rid of the introduced nonces n'_f and n''_f.
- If $\mathsf{ai} = \mathrm{TN}(j, 0)$. Using the induction hypothesis we know that $\beta \to \neg\mathsf{accept}^{\mathrm{ID_x}}_{\tau_1}$. We can therefore rewrite all occurrences of $\mathsf{accept}^{\mathrm{ID_x}}_{\tau_1}$ into false under the condition β. This removes all occurrences of $\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID_x}}_{\mathrm{N}})$ in $\mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1}$ and t_{τ_1}. We can then decompose the resulting terms into terms of $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$.

- If $\mathsf{ai} = \text{TN}(j,1)$. We can decompose $\mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1}$ and t_{τ_1} into terms of $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, except for the term $\mathsf{Mac}^4_{\mathsf{k}^{\text{ID}_\mathsf{x}}_\mathsf{m}}(\mathsf{n}^j)$. We get rid of this term using the PRF-MAC^4 axiom.
- If $\mathsf{ai} = \text{PN}(j,0)$. This is trivial using Fresh.
- If $\mathsf{ai} = \text{PN}(j,1)$. We use **(Equ3)** to rewrite all occurrences of $\mathsf{accept}^{\text{ID}_\mathsf{x}}_{\tau_1}$ in $\mathsf{leak}_{\tau_1} \backslash \mathsf{leak}^{\mathsf{in}}_{\tau_1}$ and t_{τ_1}. We can then decompose the resulting terms into terms of $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$, except for the term:

$$\mathsf{Mac}^2_{\mathsf{k}^{\text{ID}_\mathsf{x}}_\mathsf{m}}(\langle \mathsf{n}^j \,,\, \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_1})), \mathsf{sk}_\text{N})))\rangle)$$

  We get rid of this term using the PRF-MAC^2 axiom.
- If ai is a symbolic action of user ID, with $\text{ID} = \text{ID}_\mathsf{x}$, then either $\mathsf{ai} = \text{PU}_{\text{ID}_\mathsf{x}}(j_i, 2)$ or $\mathsf{ai} = \text{FU}_{\text{ID}_\mathsf{x}}(j_i)$.
  - If $\mathsf{ai} = \text{PU}_{\text{ID}_\mathsf{x}}(j_i, 2)$, then we show using **(Equ2)** that:

$$\beta \rightarrow \left(\mathsf{accept}^{\text{ID}_\mathsf{x}}_{\tau_1} \leftrightarrow g(\phi^{\mathsf{in}}_{\tau_1}) = t_{\tau_a}\right)$$

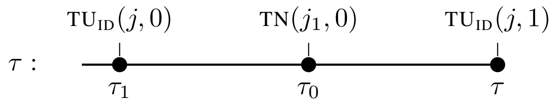
    Therefore we can rewrite $\mathsf{accept}^{\text{ID}_\mathsf{x}}_{\tau_1}$ into $g(\phi^{\mathsf{in}}_{\tau_1}) = t_{\tau_a}$ under β in t_{τ_1}. The resulting term can be easily decomposed into terms of $\phi^{\mathsf{in}}_{\tau_1}, \mathsf{leak}^{\mathsf{in}}_{\tau_1}$.
  - $\mathsf{ai} = \text{FU}_{\text{ID}_\mathsf{x}}(j_i)$. We do a similar reasoning, but using **(Equ1)** instead of **(Equ2)**. We omit the details.

D. Stronger Characterizations

Using the GUTI concealment lemma, we can show the following stronger version of **(Acc3)**:

Lemma 13. *For every valid symbolic trace $\tau = \_, \mathsf{ai}$ and identity* ID *we have:*

- ***(StrAcc1)*** *If $\mathsf{ai} = \text{TU}_\text{ID}(j,1)$. Let $\tau_1 = \_, \text{TU}_\text{ID}(j,0)$ such that $\tau_1 \prec \tau$, and let $\mathsf{k} \equiv \mathsf{k}^\text{ID}$. Then:*



$$\mathsf{accept}^\text{ID}_\tau \;\rightarrow\; \bigvee_{\substack{\tau_0 = \_, \text{TN}(j_0,0) \\ \tau_1 \prec_\tau \tau_0}} \begin{pmatrix} \mathsf{accept}^\text{ID}_{\tau_0} \;\wedge\; g(\phi^{in}_{\tau_0}) = \sigma^{in}_{\tau_1}(\text{GUTI}^\text{ID}_\text{U}) \;\wedge\; \pi_1(g(\phi^{in}_\tau)) = \mathsf{n}^{j_0} \\ \wedge\; \pi_2(g(\phi^{in}_\tau)) = \sigma^{in}_{\tau_0}(\text{SQN}^\text{ID}_\text{N}) \oplus \mathsf{f}_\mathsf{k}(\mathsf{n}^{j_0}) \wedge \sigma^{in}_\tau(\text{GUTI}^\text{ID}_\text{U}) = \sigma^{in}_{\tau_0}(\text{GUTI}^\text{ID}_\text{N}) \end{pmatrix}$$

Proof. First, by applying **(Acc3)** we get that:

$$\mathsf{accept}^\text{ID}_\tau \;\rightarrow\; \bigvee_{\substack{\tau_0 = \_, \text{TN}(j_0,0) \\ \tau_0 \prec \tau}} \begin{pmatrix} \mathsf{accept}^\text{ID}_{\tau_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{n}^{j_0} \wedge \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \sigma^{\mathsf{in}}_{\tau_0}(\text{SQN}^\text{ID}_\text{N}) \oplus \mathsf{f}_\mathsf{k}(\mathsf{n}^{j_0}) \\ \wedge\, \sigma^{\mathsf{in}}_\tau(\text{GUTI}^\text{ID}_\text{U}) = \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^\text{ID}_\text{N}) \end{pmatrix} \tag{26}$$

We have $\mathsf{accept}^\text{ID}_\tau \rightarrow \sigma^{\mathsf{in}}_\tau(\mathsf{s\text{-}valid\text{-}guti}^\text{ID}_\text{U})$, and $\sigma^{\mathsf{in}}_\tau(\mathsf{s\text{-}valid\text{-}guti}^\text{ID}_\text{U}) \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{valid\text{-}guti}^\text{ID}_\text{U})$. Let $\tau_0 = \_, \text{TN}(j_0, 0)$, we know that $\mathsf{accept}^\text{ID}_{\tau_0} \rightarrow \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^\text{ID}_\text{N}) \neq \mathsf{UnSet}$. Therefore:

$$\mathsf{accept}^\text{ID}_\tau \;\rightarrow\; \bigvee_{\substack{\tau_0 = \_, \text{TN}(j_0,0) \\ \tau_0 \prec \tau}} \begin{pmatrix} \mathsf{accept}^\text{ID}_{\tau_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{n}^{j_0} \wedge \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \sigma^{\mathsf{in}}_{\tau_0}(\text{SQN}^\text{ID}_\text{N}) \oplus \mathsf{f}_\mathsf{k}(\mathsf{n}^{j_0}) \\ \wedge\, \sigma^{\mathsf{in}}_\tau(\text{GUTI}^\text{ID}_\text{U}) = \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^\text{ID}_\text{N}) \wedge \sigma^{\mathsf{in}}_\tau(\text{GUTI}^\text{ID}_\text{U}) \neq \mathsf{UnSet} \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{valid\text{-}guti}^\text{ID}_\text{U}) \end{pmatrix}$$

To conclude, we need to get a contradiction if $\tau_0 \prec \tau_1$. Therefore, we assume that $\tau_0 \prec \tau_1$. If there does not exists any τ_2 such that $\tau_2 = \_, \text{FU}_\text{ID}(j_i) \prec \tau_1$, then it is easy to show that $\sigma^{\mathsf{in}}_\tau(\text{GUTI}^\text{ID}_\text{U}) = \mathsf{UnSet}$. In that case, from the equation above we get that $\neg\mathsf{accept}^\text{ID}_\tau$, which concludes this case.

Therefore, let τ_2 be maximal w.r.t $\prec$ such that $\tau_2 = \_, \text{FU}_\text{ID}(j_i) \prec \tau_1$. We have $\tau_2 \not\prec_\tau \text{FU}_\text{ID}(\_)$. Assume that there exists a user ID action between τ_2 and τ_1. It is easy to show by induction (over τ' in $\tau_2 \prec \tau' \preceq \tau_1$ that, since there are no $\text{FU}_\text{ID}(\_)$ action between τ_2 and τ_1, we have $\neg\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{valid\text{-}guti}^\text{ID}_\text{U})$. This implies $\neg\mathsf{accept}^\text{ID}_\tau$, which concludes this case.

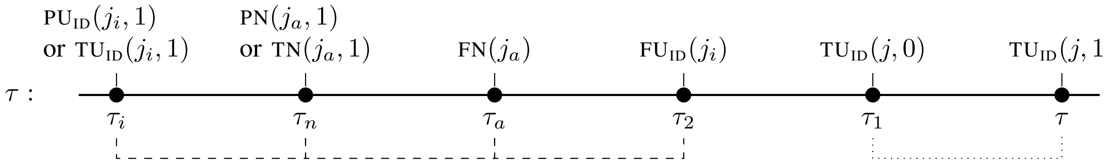
Therefore we can safely assume that there are no user ID actions between τ_2 and τ_1. We deduce that $\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{valid\text{-}guti}^\text{ID}_\text{U}) \rightarrow \mathsf{accept}^\text{ID}_{\tau_2}$. Hence $\mathsf{accept}^\text{ID}_\tau \rightarrow \mathsf{accept}^\text{ID}_{\tau_2}$. By applying **(Equ1)** to τ_2, we know that:

$$\mathsf{accept}^\text{ID}_\tau \;\rightarrow\; \bigvee_{\substack{\tau_a = \_, \text{FN}(j_a) \prec \tau_2 \\ \tau_a \not\prec_\tau \text{NS}_\text{ID}(\_)}} \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \tag{27}$$

We recall that:

$$\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \;\equiv\; \begin{pmatrix} \mathsf{inj\text{-}auth}_{\tau_2}(\text{ID}, j_a) \wedge \sigma^{\mathsf{in}}_{\tau_2}(\mathsf{e\text{-}auth}^{j_a}_\text{N}) \neq \mathsf{UnknownId} \\ \wedge\, \pi_1(g(\phi^{\mathsf{in}}_{\tau_2})) = \text{GUTI}^{j_a} \oplus \mathsf{f}^\mathsf{r}_\mathsf{k}(\mathsf{n}^{j_a}) \wedge\; \pi_2(g(\phi^{\mathsf{in}}_{\tau_2})) = \mathsf{Mac}^5_{\mathsf{k}_\mathsf{m}}(\langle \text{GUTI}^{j_a} \,,\, \mathsf{n}^{j_a}\rangle) \end{pmatrix}$$

Let $\tau_a = \_, \text{FN}(j_a) \prec \tau_2$ such that $\tau_a \not\prec_\tau \text{NS}_{\text{ID}}(\_)$. We know that there exists $\tau_n = \_, \text{PN}(j_a, 1)$ and $\tau_n = \_, \text{TN}(j_a, 1)$ such that $\tau_n \prec \tau_a$, and that $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \rightarrow \mathsf{accept}^{\text{ID}}_{\tau_n}$. Let $\tau_i = \_, \text{PU}_{\text{ID}}(j_i, 1)$ or $\_, \text{TU}_{\text{ID}}(j_i, 1)$ such that $\tau_i \prec \tau_2$. If $\tau_n \prec \tau_i$, we can show using **(Acc1)** if $\tau_n = \_, \text{PN}(j_a, 1)$ or **(Acc4)** if $\tau_n = \_, \text{PN}(j_a, 1)$ that we have $\neg\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2}$. Therefore, we assume that $\tau_i \prec \tau_n$. We depict the situation below:



We can check that $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \rightarrow \sigma_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \text{GUTI}^{j_a}$. Moreover, since there are no user ID actions between τ_2 and τ_1 or between τ_1 and τ, $\sigma_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau}(\text{GUTI}^{\text{ID}}_{\text{U}})$. From (26), we know that $\mathsf{accept}^{\text{ID}}_{\tau} \rightarrow \sigma^{\mathsf{in}}_{\tau}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}})$. It follows that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \rightarrow \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \text{GUTI}^{j_a} \tag{28}$$

If $\tau_0 \prec \tau_n$, then it is easy to check that $\sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}}) \neq \text{GUTI}^{j_a}$. Therefore we have $\neg(\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2})$.

Now, we assume that $\tau_n \prec \tau_0$. Recall that we assumed $\tau_0 \prec \tau_1$. Our goal is to apply the GUTI concealment lemma (Lemma 12) to τ_0 get a contradiction. We can check that the following hypothesis of Lemma 12 is true:

$$\{\tau' \mid \tau_i \prec_{\tau_0} \tau_b\} \cap \{\text{PU}_{\text{ID}}(j, \_), \text{TU}_{\text{ID}}(j, \_), \text{FU}_{\text{ID}}(j) \mid j \in \mathbb{N}\} \subseteq \{\text{PU}_{\text{ID}}(j_i, 2), \text{FU}_{\text{ID}}(j_i)\}$$

We deduce that:

$$\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_n} \wedge \sigma_{\tau_i}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_a} \wedge \mathsf{accept}^{\text{ID}_{\mathsf{x}}}_{\tau_i} \rightarrow g(\phi^{\mathsf{in}}_{\tau_0}) \neq \text{GUTI}^{j_a} \tag{29}$$

We know that:

$$\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \rightarrow \mathsf{accept}^{\text{ID}}_{\tau_i} \wedge \sigma_{\tau_i}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_a} \tag{30}$$

Moreover, $\neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_n} \rightarrow \sigma_{\tau_n}(\text{GUTI}^{\text{ID}}_{\text{N}}) \neq \text{GUTI}^{j_a}$. It is then straightforward to check that $\neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_n} \rightarrow \sigma_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}}) \neq \text{GUTI}^{j_a}$. Therefore, using (28) we get that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \wedge \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_n} \rightarrow \left(\sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \text{GUTI}^{j_a} \wedge \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}}) \neq \text{GUTI}^{j_a}\right) \rightarrow \mathsf{false}$$

Hence $\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \rightarrow \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_n}$. Therefore using (29) and (30), we get:

$$\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \rightarrow g(\phi^{\mathsf{in}}_{\tau_0}) \neq \text{GUTI}^{j_a} \tag{31}$$

We have $\mathsf{accept}^{\text{ID}}_{\tau_0} \rightarrow g(\phi^{\mathsf{in}}_{\tau_0}) = \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}})$. We get from this, (28) and (31) that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \wedge \mathsf{accept}^{\text{ID}}_{\tau_0} \rightarrow \mathsf{false}$$

We showed that this holds for every $\tau_a = \_, \text{FN}(j_a) \prec \tau_2$. We deduce from (27) that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{accept}^{\text{ID}}_{\tau_0} \rightarrow \mathsf{false}$$

Since we have this for every $\tau_0 \prec \tau_1$, we can rewrite (26) to get:

$$\mathsf{accept}^{\text{ID}}_{\tau} \;\rightarrow\; \bigvee_{\substack{\tau_0 = \_, \text{TN}(j_0, 0) \\ \tau_1 \prec \tau_0 \prec \tau}} \begin{pmatrix} \mathsf{accept}^{\text{ID}}_{\tau_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0} \wedge \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \\ \wedge\, \sigma^{\mathsf{in}}_{\tau}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}}) \end{pmatrix} \tag{32}$$

To conclude, we observe that $\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \text{GUTI}^{j_a}$. We recall that $\mathsf{accept}^{\text{ID}}_{\tau_0} \rightarrow g(\phi^{\mathsf{in}}_{\tau_0}) = \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}})$. We conclude using (28) that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_2} \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{U}}) = g(\phi^{\mathsf{in}}_{\tau_0})$$

Since this holds for every $\tau_a = \_, \text{FN}(j_a) \prec \tau_2$, we deduce from (27) that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{accept}^{\text{ID}}_{\tau_0} \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{U}}) = g(\phi^{\mathsf{in}}_{\tau_0})$$

Hence using (32) we get:

$$\mathsf{accept}^{\text{ID}}_{\tau} \;\rightarrow\; \bigvee_{\substack{\tau_0 = \_, \text{TN}(j_0, 0) \\ \tau_1 \prec \tau_0 \prec \tau}} \begin{pmatrix} \mathsf{accept}^{\text{ID}}_{\tau_0} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau})) = \mathsf{n}^{j_0} \wedge \pi_2(g(\phi^{\mathsf{in}}_{\tau})) = \sigma^{\mathsf{in}}_{\tau_0}(\text{SQN}^{\text{ID}}_{\text{N}}) \oplus \mathsf{f_k}(\mathsf{n}^{j_0}) \\ \wedge\, \sigma^{\mathsf{in}}_{\tau}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_0}(\text{GUTI}^{\text{ID}}_{\text{N}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{U}}) = g(\phi^{\mathsf{in}}_{\tau_0}) \end{pmatrix}$$

This concludes this proof. ■

We can now prove the following strong acceptance characterization properties:

Lemma 14. *For every valid symbolic trace $\tau = \_, ai$ and identity* ID *we have:*

- ***(StrEqu1)*** *If $ai = \text{FU}_{\text{ID}}(j)$. For every $\tau_1 = \_, \text{FN}(j_0) \prec \tau$, if we let $\tau_2 = \_, \text{TU}_{\text{ID}}(j, 0)$ or $\_, \text{PU}_{\text{ID}}(j, 1)$ then:*

$$\mathsf{accept}^{\text{ID}}_{\tau} \;\leftrightarrow\; \bigvee_{\tau_2 \prec_\tau \tau_1 = \_, \text{FN}(j_0)} \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$$

- ***(StrEqu2)*** *If $ai = \text{TU}_{\text{ID}}(j, 1)$. Let $\tau_2 = \_, \text{TU}_{\text{ID}}(j, 0)$ such that $\tau_2 \prec \tau$. Then for every τ_1 such that $\tau_1 = \_, \text{TN}(j_1, 0)$ and $\tau_2 \prec_\tau \tau_1$, we let:*

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\equiv\; \begin{pmatrix} \quad \pi_1(g(\phi^{\mathit{in}}_{\tau})) = \mathit{n}^{j_1} \;\wedge\; \pi_2(g(\phi^{\mathit{in}}_{\tau})) = \sigma^{\mathit{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \oplus \mathit{f}_{\mathit{k}^{\text{ID}}}(\mathit{n}^{j_1}) \\ \wedge\; \pi_3(g(\phi^{\mathit{in}}_{\tau})) = \mathit{Mac}^3_{\mathit{k}^{\text{ID}}_{\mathit{m}}}(\langle \mathit{n}^{j_1}, \sigma^{\mathit{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}), \sigma^{\mathit{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}})\rangle) \\ \wedge\; g(\phi^{\mathit{in}}_{\tau_1}) = \sigma^{\mathit{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) \;\wedge\; \sigma^{\mathit{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathit{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) \;\wedge\; \sigma^{\mathit{in}}_{\tau_2}(\mathsf{valid\text{-}guti}^{\text{ID}}_{\text{U}}) \\ \wedge\; \mathit{range}(\sigma^{\mathit{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}), \sigma^{\mathit{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}})) \end{pmatrix}$$

Then we have:

$$\left(\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\rightarrow\; \mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{accept}^{\text{ID}}_{\tau_1}\right)_{\substack{\tau_1 = \_, \text{TN}(j_1, 0) \\ \tau_2 \prec_\tau \tau_1}} \qquad \mathsf{accept}^{\text{ID}}_{\tau} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{TN}(j_1, 0) \\ \tau_2 \prec_\tau \tau_1}} \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$$

- ***(StrEqu3)*** *If $ai = \text{TN}(j, 1)$. Let $\tau_1 = \_, \text{TN}(j, 0)$ such that $\tau_1 \prec \tau$. Let $\text{ID} \in \mathcal{S}_{\mathit{id}}$ and τ_i, τ_2 be such that $\tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1)$, $\tau_2 = \_, \text{TU}_{\text{ID}}(j_i, 0)$ and $\tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i$. Let:*

$$\mathsf{full\text{-}tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i} \;\equiv\; \left(\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau_i} \wedge g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^4_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{n}^j)\right)$$

Then we have:

$$\left(\mathsf{full\text{-}tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i} \;\rightarrow\; \mathsf{accept}^{\text{ID}}_{\tau} \wedge \mathsf{accept}^{\text{ID}}_{\tau_i} \wedge \mathsf{accept}^{\text{ID}}_{\tau_1}\right)_{\substack{\tau_2 = \_, \text{TU}_{\text{ID}}(j_i, 0) \\ \tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \qquad \mathsf{accept}^{\text{ID}}_{\tau} \;\leftrightarrow\; \bigvee_{\substack{\tau_2 = \_, \text{TU}_{\text{ID}}(j_i, 0) \\ \tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1) \\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \mathsf{full\text{-}tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i}$$

- ***(StrEqu4)*** *If $ai = \text{PU}_{\text{ID}}(j, 2)$ then for every $\tau_1 = \_, \text{PN}(j_1, 1)$ such that $\tau_2 \prec_\tau \tau_1$, we have:*

$$\left(\neg\sigma^{\mathit{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1} \wedge \sigma^{\mathit{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) = \mathbf{0}$$

Moreover:

$$\left(\neg\sigma^{\mathit{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{accept}^{\text{ID}}_{\tau}\right) \;\rightarrow\; \sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) - \sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) = \mathbf{0}$$

E. Proof of Lemma 14

*Proof of **(StrEqu1)**:* First, we apply **(Equ1)**:

$$\mathsf{accept}^{\text{ID}}_{\tau} \;\leftrightarrow\; \bigvee_{\substack{\tau_1 = \_, \text{FN}(j_0) \prec \tau \\ \tau_1 \not\prec_\tau \text{NS}_{\text{ID}}(\_)}} \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$$

Let $\tau_1 = \_, \text{FN}(j_0) \prec \tau$. Remark that if $\tau_2 \prec \tau_1$ then $\tau_1 \not\prec_\tau \text{NS}_{\text{ID}}(\_)$. Hence to conclude we just need to show that if $\tau_1 \prec \tau_2$ then $\neg\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$.

Let $\tau_i = \_, \text{PU}_{\text{ID}}(j, 2)$ or $\_, \text{TU}_{\text{ID}}(j, 1)$ such that $\tau_i \prec \tau$. We do a case disjunction on τ_i:

- If $\tau_i = \_, \text{PU}_{\text{ID}}(j, 2)$. We know that $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow \mathsf{accept}^{\text{ID}}_{\tau_i}$, hence by applying **(Acc2)** to τ_i:

$$\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \;\rightarrow\; \bigvee_{\substack{\tau_x = \_, \text{PN}(j_x, 1) \\ \tau_2 \prec \tau_x \prec \tau_i}} \mathsf{accept}^{\text{ID}}_{\tau_x} \;\wedge\; g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_x} \;\wedge\; \pi_1(g(\phi^{\mathsf{in}}_{\tau_x})) = \{\langle \text{ID}, \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}}$$

  We know that $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \rightarrow g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_0}$. We deduce that the main term of the disjunction above is false whenever $j_x \neq j_0$. Hence we have $\neg\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$ if there does not exist any τ_0 such that $\tau_2 \prec \tau_0 \prec \tau_i$ and $\tau_0 = \_, \text{PN}(j_0, 1)$.
  If $\tau_1 \prec \tau_2$ then we know that for every τ_0, if $\tau_0 = \_, \text{PN}(j_0, 1) \prec \tau$ then $\tau_0 \prec \tau_1$, and by transitivity $\tau_0 \prec \tau_2$. Hence there does not exist any τ_0 such that $\tau_2 \prec \tau_0 \prec \tau_i$ and $\tau_0 = \_, \text{PN}(j_0, 1)$. We deduce that if $\tau_1 \prec \tau_2$ then $\neg\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}$ holds, which is what we wanted.

- If $\tau_i = \_, \text{TU}_{\text{ID}}(j, 1)$. We know that $\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_1} \to \text{accept}_{\tau_i}^{\text{ID}}$, hence by applying **(StrAcc1)** to τ_i:

$$\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_1} \;\to \bigvee_{\substack{\tau_x = \_, \text{TN}(j_x, 0)\\ \tau_2 \prec \tau_x \prec \tau_i}} \begin{pmatrix} \text{accept}_{\tau_x}^{\text{ID}} \;\wedge\; g(\phi_{\tau_x}^{\text{in}}) = \sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) \;\wedge\; \pi_1(g(\phi_{\tau_i}^{\text{in}})) = \text{n}^{j_x} \\ \wedge\; \pi_2(g(\phi_{\tau_i}^{\text{in}})) = \sigma_{\tau_x}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) \oplus \text{f}_{\text{k}}(\text{n}^{j_x}) \wedge \sigma_{\tau_i}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \sigma_{\tau_x}^{\text{in}}(\text{GUTI}_{\text{N}}^{\text{ID}}) \end{pmatrix}$$

  Similarly to what we did for $\tau_i = \_, \text{PU}_{\text{ID}}(j_i, 2)$, the main term above if false if $j_x \neq j_0$. Hence we have $\neg\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_1}$ if there does not exist any τ_0 such that $\tau_2 \prec \tau_0 \prec \tau_i$ and $\tau_0 = \_, \text{TN}(j_0, 0)$. Since this is the case whenever $\tau_1 \prec \tau_2$, we deduce that if $\tau_1 \prec \tau_2$ then $\neg\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_1}$ holds. This concludes this case, and this proof.

*Proof of **(StrEqu2)**:* We start by repeating the proof of **(Equ4)**, but using **(StrAcc1)** instead of **(Acc3)**. All the reasonings we did apply, only the set of τ_1 the disjunction quantifies upon changes. We quantify over τ_1 in $\{\tau_1 \mid \tau_1 = \_, \text{TN}(j_0, 0) \wedge \tau_2 \prec_\tau \tau_1\}$ instead of $\{\tau_1 \mid \tau_1 = \_, \text{TN}(j_0, 0) \wedge \tau_1 \prec \tau\}$. We get that:

$$\text{accept}_{\tau}^{\text{ID}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{TN}(j_0, 0)\\ \tau_2 \prec_\tau \tau_1}} \begin{pmatrix} \pi_3(g(\phi_{\tau}^{\text{in}})) = \text{Mac}_{\text{k}_\text{m}}^3(\langle \text{n}^{j_0}, \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}), \sigma_{\tau}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})\rangle) \wedge \sigma_{\tau}^{\text{in}}(\text{s-valid-guti}_{\text{U}}^{\text{ID}}) \\ \wedge\, \text{range}(\sigma_{\tau}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}), \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}})) \wedge g(\phi_{\tau_1}^{\text{in}}) = \sigma_{\tau_1}^{\text{in}}(\text{GUTI}_{\text{N}}^{\text{ID}}) \wedge \pi_1(g(\phi_{\tau}^{\text{in}})) = \text{n}^{j_0} \\ \wedge\, \pi_2(g(\phi_{\tau}^{\text{in}})) = \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) \oplus \text{f}_{\text{k}}(\text{n}^{j_0}) \wedge \sigma_{\tau}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \sigma_{\tau_1}^{\text{in}}(\text{GUTI}_{\text{N}}^{\text{ID}}) \end{pmatrix} \tag{33}$$

Since no user ID action occurs between τ_2 and τ, we know that:

$$\sigma_{\tau}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) \qquad\qquad \sigma_{\tau}^{\text{in}}(\text{s-valid-guti}_{\text{U}}^{\text{ID}}) \leftrightarrow \sigma_{\tau_2}^{\text{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}})$$

Using this, we can rewrite (33) as follows (we underline the subterms where rewriting occurred):

$$\text{accept}_{\tau}^{\text{ID}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{TN}(j_0, 0)\\ \tau_2 \prec_\tau \tau_1}} \begin{pmatrix} \pi_3(g(\phi_{\tau}^{\text{in}})) = \text{Mac}_{\text{k}_\text{m}}^3(\langle \text{n}^{j_0}, \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}), \underline{\sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})}\rangle) \wedge \underline{\sigma_{\tau_2}^{\text{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}})} \\ \wedge\, \text{range}(\sigma_{\tau}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}), \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}})) \wedge g(\phi_{\tau_1}^{\text{in}}) = \sigma_{\tau_1}^{\text{in}}(\text{GUTI}_{\text{N}}^{\text{ID}}) \\ \wedge\, \pi_1(g(\phi_{\tau}^{\text{in}})) = \text{n}^{j_0} \wedge \pi_2(g(\phi_{\tau}^{\text{in}})) = \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) \oplus \text{f}_{\text{k}}(\text{n}^{j_0}) \wedge \underline{\sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})} = \sigma_{\tau_1}^{\text{in}}(\text{GUTI}_{\text{N}}^{\text{ID}}) \end{pmatrix}$$

We rewrite $\sigma_{\tau_1}^{\text{in}}(\text{GUTI}_{\text{N}}^{\text{ID}})$ into $\sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})$:

$$\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{TN}(j_0, 0)\\ \tau_2 \prec_\tau \tau_1}} \begin{pmatrix} \pi_3(g(\phi_{\tau}^{\text{in}})) = \text{Mac}_{\text{k}_\text{m}}^3(\langle \text{n}^{j_0}, \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}), \sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})\rangle) \wedge \sigma_{\tau_2}^{\text{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}}) \\ \wedge\, \text{range}(\sigma_{\tau}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}), \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}})) \wedge g(\phi_{\tau_1}^{\text{in}}) = \underline{\sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})} \\ \wedge\, \pi_1(g(\phi_{\tau}^{\text{in}})) = \text{n}^{j_0} \wedge \pi_2(g(\phi_{\tau}^{\text{in}})) = \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) \oplus \text{f}_{\text{k}}(\text{n}^{j_0}) \wedge \sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \sigma_{\tau_1}^{\text{in}}(\text{GUTI}_{\text{N}}^{\text{ID}}) \end{pmatrix}$$

Finally we re-order the conjuncts:

$$\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{TN}(j_0, 0)\\ \tau_2 \prec_\tau \tau_1}} \begin{pmatrix} \pi_1(g(\phi_{\tau}^{\text{in}})) = \text{n}^{j_1} \;\wedge\; \pi_2(g(\phi_{\tau}^{\text{in}})) = \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) \oplus \text{f}_{\text{k}^{\text{ID}}}(\text{n}^{j_1}) \\ \wedge\; \pi_3(g(\phi_{\tau}^{\text{in}})) = \text{Mac}_{\text{k}_\text{m}^{\text{ID}}}^3(\langle \text{n}^{j_1}, \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}), \sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}})\rangle) \\ \wedge\; g(\phi_{\tau_1}^{\text{in}}) = \sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) \;\wedge\; \sigma_{\tau_2}^{\text{in}}(\text{GUTI}_{\text{U}}^{\text{ID}}) = \sigma_{\tau_1}^{\text{in}}(\text{GUTI}_{\text{N}}^{\text{ID}}) \;\wedge\; \sigma_{\tau_2}^{\text{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}}) \\ \wedge\; \text{range}(\sigma_{\tau}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}), \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}})) \end{pmatrix}$$

$$\leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{TN}(j_0, 0)\\ \tau_2 \prec_\tau \tau_1}} \text{part-tr}_{\text{u}:\tau_2, \tau}^{\text{n}:\tau_1}$$

Checking that for every $\tau_1 = \_, \text{TN}(j_1, 0) \tau_2 \prec_\tau \tau_1$:

$$\left(\text{part-tr}_{\text{u}:\tau_2, \tau}^{\text{n}:\tau_1} \;\to\; \text{accept}_{\tau}^{\text{ID}} \wedge \text{accept}_{\tau_1}^{\text{ID}}\right)$$

is straightforward.

*Proof of **(StrEqu3)**:* The proof that:

$$\text{accept}_{\tau}^{\text{ID}} \;\leftrightarrow \bigvee_{\substack{\tau_2 = \_, \text{TU}_{\text{ID}}(j_i, 0)\\ \tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1)\\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \text{full-tr}_{\text{u}:\tau_2, \tau_i}^{\text{n}:\tau_1, \tau}$$

is exactly the same than the proof of **(Equ5)**, but using **(StrEqu2)** instead of **(Equ4)**.

Finally, it is straightforward to check that for every $\tau_2 = \_, \text{TU}_{\text{ID}}(j_i, 0)$, $\tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1)$ such that $\tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i$ we have:

$$\left(\text{full-tr}_{\text{u}:\tau_2, \tau_i}^{\text{n}:\tau_1, \tau} \;\to\; \text{accept}_{\tau}^{\text{ID}} \wedge \text{accept}_{\tau_i}^{\text{ID}} \wedge \text{accept}_{\tau_1}^{\text{ID}}\right)$$

Proof of (StrEqu4): Let $\tau_2 = \_\text{PU}_{\text{ID}}(j, 1)$ such that $\tau_2 \prec \tau$. Using **(Equ2)**, we know that:

$$\mathsf{accept}^{\text{ID}}_{\tau} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{PN}(j_1, 1) \\ \tau_2 \prec_\tau \tau_1}} \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$$

Therefore to prove **(StrEqu4)** it is sufficient to show that for every τ_1 such that $\tau_1 = \_, \text{PN}(j_1, 1)$ and $\tau_2 \prec_\tau \tau_1$ we have:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \rightarrow \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) = \mathbf{0} \wedge \sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) - \sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}}) = \mathbf{0}$$

Hence let τ_1 with $\tau_1 = \_, \text{PN}(j_1, 1)$ and $\tau_2 \prec_\tau \tau_1$.

a) Part 1: First, we are going to show that:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}) \tag{34}$$

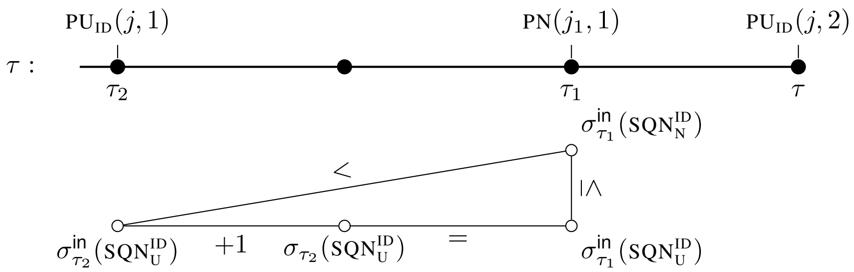
We know that $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1} \rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})$, which is what we wanted. Hence it only remains to show (34) when $\neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1}$. Using **(B5)** we know that $\sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})$. By validity of τ there are no user action between τ_2 and τ, hence $\sigma_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})$. Observe that:

$$\left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1}\right) \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) > \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})$$

And:

$$\left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1}\right) \rightarrow \sigma_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}) + 1$$

Graphically:



We deduce that:

$$\begin{aligned}\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1}\right) &\rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}) + 1 \\ &\rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}) + 1 \\ &\rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})\end{aligned} \tag{35}$$

Which is what we wanted to show.

b) Part 2: We now show that:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) > \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{N}}) \tag{36}$$

First, notice that:

$$\begin{aligned}\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1} &\rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) + 1 \\ &\rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) > \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \\ &\rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) > \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{N}}) && \text{(By } \textbf{(B1)}\text{)}\end{aligned}$$

Therefore we only need to prove:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1}\right) \rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) > \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{N}})$$

Which is straightforward:

$$\begin{aligned}\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1}\right) &\rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}) + 1 && \text{(By (35))} \\ &\rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) > \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}) \\ &\rightarrow \sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) > \sigma_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{N}}) && \text{(By } \textbf{(B5)}\text{)}\end{aligned}$$

Which concludes the proof of (36).

c) Part 3: We give the proof of:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \wedge \sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) - \sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \mathbf{0} \tag{37}$$

By validity of τ we know that $\sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$, therefore using (34) we know that:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

To conclude, we need to show that $\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}$ was kept unchanged since τ_1, i.e. that $\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$ implies that $\sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$. This requires that no SUPI or GUTI network session incremented $\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}$. Therefore we need to show the two following properties:

- **SUPI:** For every $\tau_1 \prec_\tau \tau_i$ such that $\tau_i = \_, \mathrm{PN}(j_i, 1)$:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \neg\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_i} \tag{38}$$

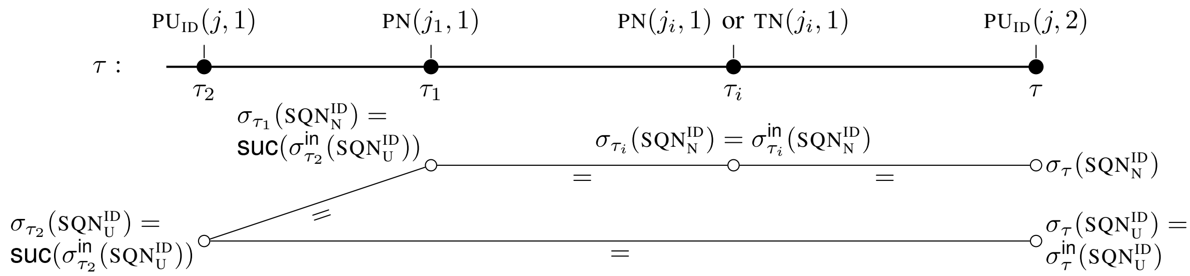
- **GUTI:** For every $\tau_1 \prec_\tau \tau_i$ such that $\tau_i = \_, \mathrm{TN}(j_i, 1)$:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \neg\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_i} \tag{39}$$

Assuming the two properties above, showing that (37) holds is easy. First, using (38) and (39) we know that:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$$

We know that $\sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$. We deduce that $\sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma_\tau(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$, which concludes this case. We summarize graphically this proof below:



d) Part 4 (Proof of (38)*):* Let $\tau_1 \prec_\tau \tau_i$ such that $\tau_i = \_, \mathrm{PN}(j_i, 1)$. Using **(Acc1)** we know that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau_i} \;\rightarrow\; \bigvee_{\tau' = \_, \mathrm{PU}_{\mathrm{ID}}(j', 1) \prec_\tau \tau_i} \left(\pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j'}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}} \wedge g(\phi^{\mathsf{in}}_{\tau'}) = \mathsf{n}^{j_i}\right)$$

We know that $\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1} \neq \mathsf{n}^{j_i}$. Moreover from the validity of τ we know that for every τ'' such that:

$$\tau_2 = \_, \mathrm{PU}_{\mathrm{ID}}(j, 1) \prec_\tau \tau'' = \_, \mathsf{ai}'' \prec_\tau \tau = \_, \mathrm{PU}_{\mathrm{ID}}(j, 2)$$

We have $\mathsf{ai}'' \neq \mathrm{PU}_{\mathrm{ID}}(\_, \_)$. Hence:

$$\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \mathsf{accept}^{\mathrm{ID}}_{\tau_i} \;\rightarrow\; \bigvee_{\tau' = \_, \mathrm{PU}_{\mathrm{ID}}(j', 1) \prec_\tau \tau_2} \left(\pi_1(g(\phi^{\mathsf{in}}_{\tau_i})) = \{\langle \mathrm{ID}\,,\, \sigma^{\mathsf{in}}_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^{j'}_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}} \wedge g(\phi^{\mathsf{in}}_{\tau'}) = \mathsf{n}^{j_i}\right)$$

Which implies that:

$$\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_i} \;\rightarrow\; \bigvee_{\tau' = \_, \mathrm{PU}_{\mathrm{ID}}(j', 1) \prec_\tau \tau_2} \left(\sigma_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}))\right)$$

We recall (34):

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \left(\sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\right)$$

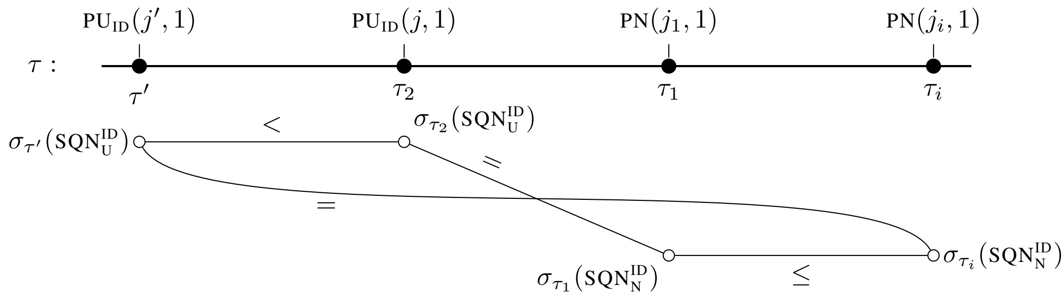
Let $\tau' = \_, \mathrm{PU}_{\mathrm{ID}}(j', 1) \prec_\tau \tau_2$. We know using **(B1)** that:

$$\sigma_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \qquad\qquad \sigma_{\tau'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \leq \sigma_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

Moreover using **(A2)** we know that $\sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \neq \sigma_{\tau_2}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$, hence $\sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau_2}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$. This implies that:

$$\begin{aligned}
&\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \wedge \mathsf{inc\text{-}accept}_{\tau_i}^{\mathrm{ID}} \\
\rightarrow\ & \bigvee_{\tau'=_,\mathrm{PU}_{\mathrm{ID}}(j',1)\prec_\tau \tau_2} \begin{pmatrix} \sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau_2}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \sigma_{\tau_2}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) = \sigma_{\tau_1}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \\ \wedge \sigma_{\tau_1}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \leq \sigma_{\tau_i}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \wedge \sigma_{\tau_i}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) = \sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \end{pmatrix} \\
\rightarrow\ & \bigvee_{\tau'=_,\mathrm{PU}_{\mathrm{ID}}(j',1)\prec_\tau \tau_2} (\sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) < \sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})) \\
\rightarrow\ & \mathsf{false}
\end{aligned}$$

Which concludes this proof. We summarize graphically below:



e) Part 5 (Proof of (39)*):* Let $\tau_1 \prec_\tau \tau_i$ such that $\tau_i = \_,\mathrm{TN}(j_i,1)$. Using Lemma 7, we know that:

$$\mathsf{accept}_{\tau_i}^{\mathrm{ID}} \rightarrow \left(\sigma_{\tau_i}^{\mathsf{in}}(\mathsf{e\text{-}auth}_{\mathrm{N}}^{j}) = \mathrm{ID}\right) \rightarrow \bigvee_{\substack{\tau'=\_,\mathrm{TU}_{\mathrm{ID}}(\_,1) \\ \tau'\prec_\tau \tau_i}} \sigma_{\tau'}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j_i}$$

Since $\mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \rightarrow g(\phi_{\tau_2}^{\mathsf{in}}) = \mathsf{n}^{j_1}$, we know that $\mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \rightarrow \sigma_{\tau_2}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j_1}$. As we know that $\mathsf{n}^{j_1} \neq \mathsf{n}^{j_i}$, we deduce that $\mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \rightarrow \sigma_{\tau_2}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) \neq \mathsf{n}^{j_i}$. Moreover using the validity of τ we know that $\sigma_{\tau_i}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \sigma_{\tau_2}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}})$. Therefore:

$$\left(\mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \wedge \mathsf{accept}_{\tau_i}^{\mathrm{ID}}\right) \rightarrow \bigvee_{\substack{\tau'=\_,\mathrm{TU}_{\mathrm{ID}}(\_,1) \\ \tau'\prec_\tau \tau_2}} \sigma_{\tau'}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j_i}$$

Let $\tau' = \_,\mathrm{TU}_{\mathrm{ID}}(\_,1)$ with $\tau' \prec_\tau \tau_2$. We know that $\sigma_{\tau'}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j_i}$ implies that $\sigma_{\tau'}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) \neq \mathsf{fail}$, and therefore $\mathsf{accept}_{\tau'}$ holds:

$$\left(\sigma_{\tau'}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j_i}\right) \rightarrow \left(\sigma_{\tau'}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) \neq \mathsf{fail}\right) \rightarrow \mathsf{accept}_{\tau'}$$

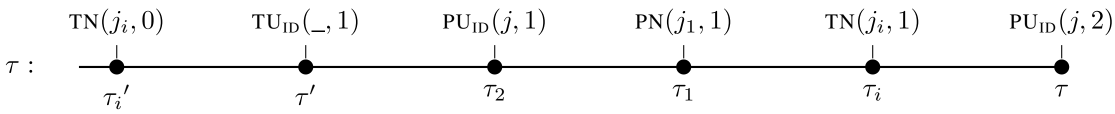
By applying **(Acc3)** we know that:

$$\mathsf{accept}_{\tau'} \rightarrow \bigvee_{\tau_i'=\_,\mathrm{TN}(j_i',0)\prec_\tau \tau'} \pi_1(g(\phi_{\tau'}^{\mathsf{in}})) = \mathsf{n}^{j_i'}$$

Since $[\mathsf{accept}_{\tau'}]\sigma_{\tau'}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = [\mathsf{accept}_{\tau'}]\pi_1(g(\phi_{\tau'}^{\mathsf{in}}))$ we deduce:

$$\left(\sigma_{\tau'}(\mathsf{b\text{-}auth}_{\mathrm{U}}^{\mathrm{ID}}) = \mathsf{n}^{j_i}\right) \rightarrow \mathsf{false} \text{ if } \tau' \prec_\tau \mathrm{TN}(j_i,0)$$

Hence if $\tau' \prec_\tau \mathrm{TN}(j_i,0)$ we know that $\neg\left(\mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \wedge \mathsf{accept}_{\tau_i}^{\mathrm{ID}}\right)$, which is what we wanted to show. Therefore let $\tau_i' = \_,\mathrm{TN}(j_i,0)$, and assume $\tau_i' \prec_\tau \tau'$. We summarize graphically this below:



We recall (36):

$$\left(\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1}\right) \rightarrow \left(\sigma_{\tau_2}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})\right)$$

Hence, using **(B4)** we know that:

$$\left(\neg\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1}\right) \rightarrow \bigvee_{\substack{\tau_2 \preceq \tau_x \preceq \tau_1 \\ \tau_x=\_,\mathrm{TN}(j_x,0) \text{ or } \_,\mathrm{TN}(j_x,1) \text{ or } \_,\mathrm{PN}(j_x,1)}} \sigma_{\tau_1}(\mathsf{session}_{\mathrm{N}}^{\mathrm{ID}}) = \mathsf{n}^{j_x}$$

Since $\text{TN}(j_i, 0) \prec_\tau \tau_2$ and $\tau_1 \prec_\tau \text{TN}(j_i, 1)$:

$$\left(\neg\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \rightarrow \sigma_{\tau_1}(\mathsf{session}^{\text{ID}}_{\text{N}}) \neq \mathsf{n}^{j_i}$$

For every $\tau_1 \preceq \tau''$ we have:

$$\sigma_{\tau''}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \begin{cases} \text{if inc-accept}^{\text{ID}}_{\tau''} \text{ then } \mathsf{n}^{j''} \text{ else } \sigma^{\mathsf{in}}_{\tau''}(\mathsf{session}^{\text{ID}}_{\text{N}}) & \text{if } \tau'' = \_, \text{PN}(j'', 1) \\ \text{if accept}^{\text{ID}}_{\tau''} \text{ then } \mathsf{n}^{j''} \text{ else } \sigma^{\mathsf{in}}_{\tau''}(\mathsf{session}^{\text{ID}}_{\text{N}}) & \text{if } \tau'' = \_, \text{TN}(j'', 0) \\ \sigma^{\mathsf{in}}_{\tau''}(\mathsf{session}^{\text{ID}}_{\text{N}}) & \text{otherwise} \end{cases}$$

Since $\tau' \not\prec_\tau \text{TN}(j_i, 0)$, we know that after having set $\sigma_{\tau''}(\mathsf{session}^{\text{ID}}_{\text{N}})$ to n^{j_1} at τ_1, it can never be set to n^{j_i}. Formally, we show by induction that:

$$\sigma_{\tau_1}(\mathsf{session}^{\text{ID}}_{\text{N}}) \neq \mathsf{n}^{j_i} \;\rightarrow\; \sigma_{\tau''}(\mathsf{session}^{\text{ID}}_{\text{N}}) \neq \mathsf{n}^{j_i}$$

We conclude by observing that $\sigma^{\mathsf{in}}_{\tau_i}(\mathsf{session}^{\text{ID}}_{\text{N}}) \neq \mathsf{n}^{j_i} \rightarrow \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_i}$.

f) Part 6: To conclude the proof of **(StrEqu4)**, it only remains to show that:

$$\left(\neg\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1} \tag{40}$$

Since $\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \mathsf{accept}^{\text{ID}}_{\tau_1}$, and since:

$$\left(\mathsf{accept}^{\text{ID}}_{\tau_1} \wedge \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_1}\right) \;\leftrightarrow\; \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) > \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})$$

To show that (40) holds, it is sufficient to show that:

$$\left(\neg\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})$$

We generalize this, and show by induction that for every τ_n such that $\tau_2 \preceq \tau_n \prec_\tau \tau_1$, we have:

$$\left(\neg\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})$$

- If $\tau_n = \tau_2$, this is immediate using **(B5)** and the fact that $\sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}})$.
- Let $\tau_n >_\tau \tau_2$. By induction, assume that:

$$\left(\neg\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})$$

  We then have three cases:
  - If $\tau_n \neq \_, \text{PN}(\_, 1)$ and $\tau_n \neq \_, \text{TN}(\_, 1)$, we know that $\sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}})$, and we conclude directly using the induction hypothesis.
  - If $\tau_n = \_, \text{PN}(j_n, 1)$. Using **(Equ3)** we know that:

$$\begin{aligned} \sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) \neq \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) &\rightarrow \mathsf{accept}^{\text{ID}}_{\tau_n} \\ &\rightarrow \bigvee_{\substack{\tau_x = \_, \text{PU}_{\text{ID}}(j_x, 1) \\ \tau_x \prec_\tau \tau_n}} \underbrace{\begin{pmatrix} g(\phi^{\mathsf{in}}_{\tau_x}) = \mathsf{n}^{j_n} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau_n})) = \{\langle \text{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}^{j_n}_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}} \\ \wedge\; \pi_2(g(\phi^{\mathsf{in}}_{\tau_n})) = \mathsf{Mac}^1_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle\{\langle \text{ID}\,,\, \sigma^{\mathsf{in}}_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}^{j_n}_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}}\,,\, g(\phi^{\mathsf{in}}_{\tau_x})\rangle) \end{pmatrix}}_{\theta_{\tau_x}} \end{aligned}$$

    Since $\tau_n \prec_\tau \tau_1$, we know that $j_n \neq j_1$. Moreover, $\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1}$. By consequence:

$$\left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_n}\right) \rightarrow \mathsf{false}$$

    Which shows that $\left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \theta_{\tau_2}\right) \rightarrow \mathsf{false}$. Hence:

$$\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) \neq \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) \rightarrow \bigvee_{\substack{\tau_x = \_, \text{PU}_{\text{ID}}(j_x, 1) \\ \tau_x \prec_\tau \tau_2}} \theta_{\tau_x}$$

    Observe that for every $\tau_x = \_, \text{PU}_{\text{ID}}(j_x, 1)$ such that $\tau_x \prec_\tau \tau_2$:

$$\theta_{\tau_x} \rightarrow \sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) = \text{if } \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{U}}) \text{ then } \sigma^{\mathsf{in}}_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{U}}) \text{ else } \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}})$$

    Using **(B1)**, we know that $\sigma^{\mathsf{in}}_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{U}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})$. Therefore:

$$\theta_{\tau_x} \;\rightarrow\; \sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) \;\leq\; \text{if } \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau_x}(\text{SQN}^{\text{ID}}_{\text{U}}) \text{ then } \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}) \text{ else } \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}})$$

And using the induction hypothesis, we get that:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \theta_{\tau_x}\right) \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

Hence:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \neq \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})\right) \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

From which we deduce, using the induction hypothesis, that:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

– If $\tau_n = \_, \mathrm{TN}(j_n, 1)$. Using **(StrEqu2)**, we know that:

$$\begin{aligned}\sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \neq \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) &\rightarrow\; \mathsf{accept}^{\mathrm{ID}}_{\tau_n} \\ &\rightarrow \bigvee_{\substack{\tau_x{}' = \_,\mathrm{TU_{ID}}(j_x,0)\\ \tau_n{}' = \_,\mathrm{TN}(j_n,0)\\ \tau_x = \_,\mathrm{TU_{ID}}(j_x,1)\\ \tau_x{}' \prec_\tau \tau_n{}' \prec_\tau \tau_x \prec_\tau \tau_n}} \mathsf{full\text{-}tr}^{\mathsf{n}:\tau_n{}',\tau_n}_{\mathsf{u}:\tau_x{}',\tau_x}\end{aligned}$$

Let $\tau_x = \_, \mathrm{TU_{ID}}(j_x, 1)$, $\tau_n{}' = \_, \mathrm{TN}(j_n, 0)$, $\tau_x{}' = \_, \mathrm{TU_{ID}}(j_x, 0)$ be such that $\tau_x{}' \prec_\tau \tau_n{}' \prec_\tau \tau_x \prec_\tau \tau_n$. One can check that:

$$\begin{aligned}\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_n} &\rightarrow \bigwedge_{\tau_x \prec_\tau \tau_i \prec_\tau \tau_n} \neg\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_i} \\ &\rightarrow\; \sigma_{\tau_n{}'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})\end{aligned}$$

Moreover, since:

$$\mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_n} \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau_x}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \;=\; \sigma_{\tau_n{}'}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$$

We deduce that:

$$\mathsf{full\text{-}tr}^{\mathsf{n}:\tau_n{}',\tau_n}_{\mathsf{u}:\tau_x{}',\tau_x} \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{if}\ \mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_n}\ \mathsf{then}\ \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_x}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}))\ \mathsf{else}\ \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$$

By validity of τ, we know that $j_x \neq j$ and that $\tau_x \prec_\tau \tau_2$. Therefore using **(B1)** we know that $\sigma_{\tau_x}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$. Moreover $\sigma_{\tau_x}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{suc}(instate_{\tau_x}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}))$. Hence:

$$\mathsf{full\text{-}tr}^{\mathsf{n}:\tau_n{}',\tau_n}_{\mathsf{u}:\tau_x{}',\tau_x} \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \mathsf{if}\ \mathsf{inc\text{-}accept}^{\mathrm{ID}}_{\tau_n}\ \mathsf{then}\ \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\ \mathsf{else}\ \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})$$

And using the induction hypothesis, we get that:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \mathsf{full\text{-}tr}^{\mathsf{n}:\tau_n{}',\tau_n}_{\mathsf{u}:\tau_x{}',\tau_x}\right) \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

Hence:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \wedge \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \neq \sigma^{\mathsf{in}}_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})\right) \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

From which we deduce, using the induction hypothesis, that:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \sigma_{\tau_n}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) \leq \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$$

Appendix IV
Unlinkability

The goal of this section is to prove unlinkability of the AKA^+ protocol. To do this, we need, for every valid basic symbolic trace τ, to show that there exists a derivation of $\phi_\tau \sim \phi_{\underline{\tau}}$. We show this by induction on τ.

A. *Resistance against de-synchronization attacks*

To show that the GUTI protocol guarantees unlinkability, we need the protocol the be resilient to de-synchronization attacks: for every agent ID, the adversary should not be able to keep ID synchronized in the left protocol, while de-synchronizing $\nu_\tau(\text{ID})$ in the right protocol.

Therefore, we need the range check on the sequence number to hold on the left iff the range check hold on the right. More precisely, for every identity ID and the matching identity $\nu_\tau(\text{ID})$ on the right, the range checks on the sequence numbers should be indistinguishable:

$$\mathsf{range}(\sigma_\tau(\text{SQN}_\text{U}^\text{ID}), \sigma_\tau(\text{SQN}_\text{N}^\text{ID})) \;\sim\; \mathsf{range}(\sigma_{\underline{\tau}}(\text{SQN}_\text{U}^{\nu_\tau(\text{ID})}), \sigma_{\underline{\tau}}(\text{SQN}_\text{N}^{\nu_\tau(\text{ID})})) \tag{41}$$

But the property above is not a invariant of the AKA^+ protocol for two reasons:

- First, knowing that the range checks are indistinguishable after a symbolic execution τ is not enough to show that they are indistinguishable after $\tau_1 = \tau, \mathsf{ai}$ (for some ai). For example, take a model where $\mathsf{range}(u, v)$ is implemented as a check that the difference between u and v lies in some interval:

  $$[\![\mathsf{range}(u, v)]\!] \text{ if and only if } [\![u]\!] - [\![v]\!] \in \{0, \dots, D\}$$

  for some constant $D > 0$, and suc is implemented as an increment by one. Then, a priori, we may have:

  $$[\![\sigma_\tau(\text{SQN}_\text{U}^\text{ID})]\!] - [\![\sigma_\tau(\text{SQN}_\text{N}^\text{ID})]\!] = 0 \in \{0, \dots, D\}$$
  $$[\![\sigma_{\underline{\tau}}(\text{SQN}_\text{U}^{\nu_\tau(\text{ID})})]\!] - [\![\sigma_{\underline{\tau}}(\text{SQN}_\text{N}^{\nu_\tau(\text{ID})})]\!] = D \in \{0, \dots, D\}$$

  While (41) holds for τ, it does not hold for $\tau_1 = \tau, \text{PU}_\text{ID}(j, 1)$. Indeed, after executing $\text{PU}_\text{ID}(j, 1)$ we have:

  $$[\![\sigma_{\tau_1}(\text{SQN}_\text{U}^\text{ID})]\!] - [\![\sigma_{\tau_1}(\text{SQN}_\text{N}^\text{ID})]\!] = 1 \in \{0, \dots, D\}$$
  $$[\![\sigma_{\underline{\tau_1}}(\text{SQN}_\text{U}^{\nu_{\tau_1}(\text{ID})})]\!] - [\![\sigma_{\underline{\tau_1}}(\text{SQN}_\text{N}^{\nu_{\tau_1}(\text{ID})})]\!] = D + 1 \notin \{0, \dots, D\}$$

  To avoid this, we require that $\mathsf{range}(\_,\_)$ and $\mathsf{suc}(\_)$ are implemented as, respectively, an equality check and an integer by-one increment.
  Moreover, we strengthen the induction property to show that the difference between the sequence numbers are indistinguishable, i.e.:

  $$\sigma_\tau(\text{SQN}_\text{U}^\text{ID}) - \sigma_\tau(\text{SQN}_\text{N}^\text{ID}) \;\sim\; \sigma_{\underline{\tau}}(\text{SQN}_\text{U}^{\nu_\tau(\text{ID})}) - \sigma_{\underline{\tau}}(\text{SQN}_\text{N}^{\nu_\tau(\text{ID})}) \tag{42}$$

- Second, the property in (42) actually does not always hold: after a $\text{NS}_\text{ID}(\_)$ action, the agent ID and the network may be synchronized on the left (if, e.g., the SUPI protocol has just been successfully executed), but $\nu_\tau(\text{ID})$ is not synchronized with the network.
  Even though the property does not hold, there is no attack on unlinkability. Indeed a desynchronization attack would need the GUTI protocol to succeed on the left and fail on the right. But the GUTI protocol requires that a fresh GUTI has been established between ID (resp. $\nu_\tau(\text{ID})$) and the network. This can only be achieved through a honest execution of the SUPI protocol. As such a execution will re-synchronized the agent and the network sequence numbers *on both side*, there is no attack.
  To model this, we extend the symbolic state with a new boolean variable, $\mathsf{sync}_\text{U}^\text{ID}$, that records whether there was a successful execution of the SUPI protocol with agent ID since the last $\text{NS}_\text{ID}(\_)$. This variable is only here for proof purposes, and is never used in the actual protocol. We can then state the synchronization invariant:

$$\underbrace{\begin{array}{c}\mathsf{if}\ \sigma_\tau(\mathsf{sync}_\text{U}^\text{ID})\ \mathsf{then}\ \sigma_\tau(\text{SQN}_\text{U}^\text{ID}) - \sigma_\tau(\text{SQN}_\text{N}^\text{ID})\\ \mathsf{else}\ \bot\end{array}}_{\mathsf{sync\text{-}diff}_\tau^\text{ID}} \sim \underbrace{\begin{array}{c}\mathsf{if}\ \sigma_{\underline{\tau}}(\mathsf{sync}_\text{U}^{\nu_\tau(\text{ID})})\ \mathsf{then}\ \sigma_{\underline{\tau}}(\text{SQN}_\text{U}^{\nu_\tau(\text{ID})}) - \sigma_{\underline{\tau}}(\text{SQN}_\text{N}^{\nu_\tau(\text{ID})})\\ \mathsf{else}\ \bot\end{array}}_{\mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\text{ID})}}$$

B. Strengthened induction hypothesis

Definition 44. *Let $L = (i_1, \dots, i_l)$ be a list of indexes, and $(b_i)_{i\in L}$, $(t_i)_{i\in L}$ two list of terms. Then:*

$$\underset{i\in L}{\textsf{case}}((b_i)_{i\in L} : (m_i)_{i\in L}) \equiv \begin{cases} \textsf{if } b_{i_1} \textsf{ then } m_{i_1} \textsf{ else } \underset{i\in L_0}{\textsf{case}}((b_i)_{i\in L_0} : (m_i)_{i\in L_0}) & \text{when } L \neq \emptyset \text{ and } L_0 = (i_2, \dots, i_l) \\ \perp & \text{otherwise} \end{cases}$$

We will often abuse notation, and write $\underset{i\in L}{\textsf{case}}(b_i : m_i)$ instead of $\underset{i\in L}{\textsf{case}}((b_i)_{i\in L} : (m_i)_{i\in L})$.

Proposition 28. *Let $L = (i_1, \dots, i_l)$ be a list of indexes, and $(b_i)_{i\in L}$, $(t_i)_{i\in L}$ two list of terms. If $(b_i)_{i\in L}$ is a $\textsf{CS}$ partition, then for any permutation π of $\{1, \dots, l\}$, if we let $L_\pi = (i_{\pi(1)}, \dots, i_{\pi l})$ then:*

$$\underset{i\in L}{\textsf{case}}(b_i : m_i) = \underset{i\in L_\pi}{\textsf{case}}(b_i : m_i)$$

When that is the case, we write $\underset{i\in\{i_1,\dots,i_l\}}{\textsf{case}}(b_i : m_i)$ (i.e. we use a set notation instead of list notation).

Proof. The proof is straightforward by induction over $|L|$. ∎

If $(b_i)_{i\in L}$ is such that $(\bigvee_{i\in L} b_i) = \textsf{true}$ then the case where all tests fail and we return $\perp$ never happens. This motivates the introduction of a second definition.

Definition 45. *Let $L = (i_1, \dots, i_l)$ be a list of indexes with $l \geq 1$, and $(b_i)_{i\in L}$, $(t_i)_{i\in L}$ two list of terms. Then:*

$$\underset{i\in L}{\textsf{s-case}}((b_i)_{i\in L} : (m_i)_{i\in L}) \equiv \begin{cases} \textsf{if } b_{i_1} \textsf{ then } m_{i_1} \textsf{ else } \underset{i\in L_0}{\textsf{case}}((b_i)_{i\in L_0} : (m_i)_{i\in L_0}) & \text{when } L_0 = (i_2, \dots, i_l) \text{ and } l \geq 1 \\ m_1 & \text{if } l = 1 \end{cases}$$

Proposition 29. *For every list of terms $(b_i)_{i\in L}$ and $(t_i)_{i\in L}$, if $(\bigvee_{i\in L} b_i) = \textsf{true}$ then:*

$$\underset{i\in L}{\textsf{case}}(b_i : m_i) = \underset{i\in L}{\textsf{s-case}}(b_i : m_i)$$

Proof. We omit the proof. ∎

Definition 46. *Let $\tau = \textsf{ai}_0, \dots, \textsf{ai}_n$ be a valid basic symbolic trace. Then $\textsf{reveal}_\tau$ is a list of elements of the form $u \sim v$, where u, v are terms, representing the information that can be safely leaked to the adversary. Let $\textsf{ai} = \textsf{ai}_n$. Then $\textsf{reveal}_\tau$ contains exactly the following list of elements:*

1) *All the elements from $\textsf{reveal}_{\tau_0}$, where $\tau_0 = \textsf{ai}_0, \dots, \textsf{ai}_{n-1}$.*
2) *For every base identity ID, let:*

$$\textsf{m-suci}_\tau^{\text{ID}} \equiv [\sigma_\tau(\textsf{valid-guti}_{\text{U}}^{\text{ID}})]\sigma_\tau(\text{GUTI}_{\text{U}}^{\text{ID}})$$

We then have the following synchronization invariants.

$$\sigma_\tau(\textsf{valid-guti}_{\text{U}}^{\text{ID}}) \sim \sigma_{\underline{\tau}}(\textsf{valid-guti}_{\text{U}}^{\nu_\tau(\text{ID})}) \qquad \textsf{m-suci}_\tau^{\text{ID}} \sim \textsf{m-suci}_{\underline{\tau}}^{\nu_\tau(\text{ID})} \qquad \sigma_\tau(\textsf{sync}_{\text{U}}^{\text{ID}}) \sim \sigma_{\underline{\tau}}(\textsf{sync}_{\text{U}}^{\nu_\tau(\text{ID})})$$

$$\textsf{sync-diff}_\tau^{\text{ID}} \sim \textsf{sync-diff}_{\underline{\tau}}^{\nu_\tau(\text{ID})} \qquad \textsf{len}(\langle \text{ID}, \sigma_\tau^{\textsf{in}}(\textsf{sqn-init}_{\text{U}}^{\text{ID}})\rangle) \sim \textsf{len}(\langle \text{ID}, \sigma_\tau^{\textsf{in}}(\textsf{sqn-init}_{\text{U}}^{\text{ID}})\rangle)$$

3) *If $\textsf{ai} \neq \text{NS\_}(\_)$ then for every base identity ID:*

$$\sigma_\tau(\text{SQN}_{\text{U}}^{\text{ID}}) - \sigma_\tau^{\textsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}}) \sim \sigma_{\underline{\tau}}(\text{SQN}_{\text{U}}^{\nu_\tau(\text{ID})}) - \sigma_{\underline{\tau}}^{\textsf{in}}(\text{SQN}_{\text{U}}^{\nu_\tau(\text{ID})})$$

4) *If $\textsf{ai} = \text{TU}_{\text{ID}}(j, 0)$, then:*

$$\sigma_\tau(\textsf{s-valid-guti}_{\text{U}}^{\text{ID}}) \sim \sigma_{\underline{\tau}}(\textsf{s-valid-guti}_{\text{U}}^{\nu_\tau(\text{ID})})$$

5) *If $\textsf{ai} = \text{PU}_{\text{ID}}(j, 1)$, then:*

$$\{\langle \text{ID}, \sigma_\tau^{\textsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\textsf{pk}_{\text{N}}}^{\textsf{n}_e^j} \sim \{\langle \nu_\tau(\text{ID}), \sigma_\tau^{\textsf{in}}(\text{SQN}_{\text{U}}^{\nu_\tau(\text{ID})})\rangle\}_{\textsf{pk}_{\text{N}}}^{\textsf{n}_e^j}$$

$$\textsf{Mac}_{\textsf{k}_m^{\text{ID}}}^1(\langle\{\langle \text{ID}, \sigma_\tau^{\textsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\textsf{pk}_{\text{N}}}^{\textsf{n}_e^j}, g(\phi_\tau^{\textsf{in}})\rangle) \sim \textsf{Mac}_{\textsf{k}_m^{\nu_\tau(\text{ID})}}^1(\langle\{\langle \nu_\tau(\text{ID}), \sigma_{\underline{\tau}}^{\textsf{in}}(\text{SQN}_{\text{U}}^{\nu_\tau(\text{ID})})\rangle\}_{\textsf{pk}_{\text{N}}}^{\textsf{n}_e^j}, g(\phi_{\underline{\tau}}^{\textsf{in}})\rangle)$$

6) *If $\textsf{ai} = \text{PU}_{\text{ID}}(\_, 2)$, $\text{TU}_{\text{ID}}(\_, 1)$ or $\text{FU}_{\text{ID}}(\_)$:*

$$\sigma_\tau(\textsf{e-auth}_{\text{U}}^{\text{ID}}) \sim \sigma_{\underline{\tau}}(\textsf{e-auth}_{\text{U}}^{\nu_\tau(\text{ID})})$$

7) *If $\text{TU}_{\text{ID}}(j, 1)$ then for every $\tau_1 = \_, \text{TN}(j_0, 0)$ such that $\text{TU}_{\text{ID}}(j, 0) \prec_\tau \tau_1$:*

$$\textsf{Mac}_{\textsf{k}_m^{\text{ID}}}^4(\textsf{n}^{j_0}) \sim \textsf{Mac}_{\textsf{k}_m^{\nu_\tau(\text{ID})}}^4(\textsf{n}^{j_0})$$

8) *If* $\mathsf{ai} = \text{PN}(j,1)$ *then for every base identity* ID*, for every* $\tau_1 = \_, \text{PU}_{\text{ID}}(j_1, 1) \prec \tau$ *such that* $\tau_1 \not\prec_\tau \text{NS}_{\text{ID}}(\_)$ *we have:*

$$\mathsf{Mac}^2_{k_m^{\text{ID}}}(\langle \mathsf{n}^j\ ,\ \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}_{\text{U}}^{\text{ID}}))\rangle) \ \sim\ \mathsf{Mac}^2_{k_m^{\nu_\tau(\text{ID})}}(\langle \mathsf{n}^j\ ,\ \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}_{\text{U}}^{\nu_\tau(\text{ID})}))\rangle)$$

9) *If* $\mathsf{ai} = \text{PN}(j,1)$ *or* $\mathsf{ai} = \text{TN}(j,1)$*, for all base identity* ID*, we let:*

$$\begin{aligned}
\mathsf{net\text{-}e\text{-}auth}_\tau(\text{ID}, j) &\equiv \mathsf{eq}(\sigma_\tau(\mathsf{e\text{-}auth}^j_{\text{N}}), \text{ID}) \\
\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\text{ID}, j) &\equiv \bigvee_{\underline{\text{ID}} \in \mathsf{copies\text{-}id}(\text{ID})} \mathsf{eq}(\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^j_{\text{N}}), \underline{\text{ID}})
\end{aligned}$$

Then we ask that:

$$\mathsf{net\text{-}e\text{-}auth}_\tau(\text{ID}, j) \ \sim\ \underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\text{ID}, j)$$

10) *If* $\mathsf{ai} = \text{FN}(j)$ *for every base identity* ID *we let* $\{\underline{\text{ID}}_1, \dots, \underline{\text{ID}}_{l_{\text{ID}}}\} = \mathsf{copies\text{-}id}(\text{ID})$*. We define:*

$$\begin{aligned}
\mathsf{t\text{-}suci\text{-}}\oplus_\tau(\text{ID}, j) &\equiv \text{GUTI}^j \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\text{ID}}}(\mathsf{n}^j) \\
\underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\tau}}(\text{ID}, j) &\equiv \underset{1 \le i \le l_{\text{ID}}}{\mathsf{s\text{-}case}}(\mathsf{eq}(\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^j_{\text{N}}), \underline{\text{ID}}_i) : \text{GUTI}^j \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\text{ID}}_i}}(\mathsf{n}^j)) \\
\mathsf{t\text{-}mac}_\tau(\text{ID}, j) &\equiv \mathsf{Mac}^5_{k_m^{\text{ID}}}(\langle \text{GUTI}^j\ ,\ \mathsf{n}^j\rangle) \\
\underline{\mathsf{t\text{-}mac}_{\tau}}(\text{ID}, j) &\equiv \underset{1 \le i \le l_{\text{ID}}}{\mathsf{s\text{-}case}}(\mathsf{eq}(\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^j_{\text{N}}), \underline{\text{ID}}_i) : \mathsf{Mac}^5_{k_m^{\underline{\text{ID}}_i}}(\langle \text{GUTI}^j\ ,\ \mathsf{n}^j\rangle))
\end{aligned}$$

Then we ask that:

$$\begin{aligned}
\text{GUTI}^j &\sim \text{GUTI}^j \\
[\mathsf{net\text{-}e\text{-}auth}_\tau(\text{ID}, j)]\,(\mathsf{t\text{-}suci\text{-}}\oplus_\tau(\text{ID}, j)) &\sim [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\text{ID}, j)]\left(\underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\tau}}(\text{ID}, j)\right) \\
[\mathsf{net\text{-}e\text{-}auth}_\tau(\text{ID}, j)]\,(\mathsf{t\text{-}mac}_\tau(\text{ID}, j)) &\sim [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\text{ID}, j)]\left(\underline{\mathsf{t\text{-}mac}_{\tau}}(\text{ID}, j)\right)
\end{aligned}$$

Let $(u_i \sim v_i)_{i \in I}$ *be such that* $\mathsf{reveal}_\tau = (u_i \sim v_i)_{i\in I}$*. Then we let* $\mathsf{l\text{-}reveal}_\tau = (u_i)_{i\in I}$ *be the list of left elements of* reveal_τ*, and* $\mathsf{r\text{-}reveal}_\tau = (v_i)_{i\in I}$ *list of left elements of* reveal_τ *(in the same order).*

Proposition 30. *For every basic valid symbolic trace* $\tau = \_, \mathsf{ai}$*:*

- ***(Der1)*** *For every base identity, for every* τ_1 *such that* $\tau_1 \prec \tau$ *and* $\tau_1 \not\prec_\tau \text{NS}_{\text{ID}}(\_)$*, there exist derivations using only* FA *and* Dup *of:*

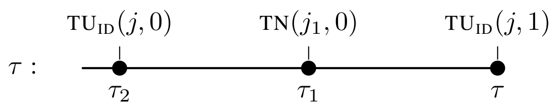
$$\frac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{l}\mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\mathsf{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{N}}) < \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) \\ \sim\ \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}}) \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{N}}) < \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{U}})\end{array}}\ \mathsf{Simp}$$

$$\frac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{l}\mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) < \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) \\ \sim\ \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}}) \wedge \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{N}}) < \sigma^{\mathsf{in}}_{\underline{\tau}}(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{U}})\end{array}}\ \mathsf{Simp}$$

- ***(Der2)*** *If* $\mathsf{ai} = \text{FU}_{\text{ID}}(j)$*. For every* $\text{ID} \in \mathcal{S}_{\mathsf{id}}$*, for every* $\tau_1 = \_, \text{FN}(j_0) \prec \tau$ *such that* $\tau_1 \not\prec_\tau \text{NS}_{\text{ID}}(\_)$*:*
  - *We have* $\underline{\tau_1} = \_, \text{FN}(j_0)$*,* $\underline{\tau} = \_, \text{FU}_{\nu_\tau(\text{ID})}(j)$*,* $\underline{\tau_1} \prec_{\underline{\tau}} \underline{\tau}$ *and* $\underline{\tau_1} \not\prec_{\underline{\tau}} \text{NS}_{\nu_\tau(\text{ID})}(\_)$*. Therefore,* $\mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}}$ *is well-defined.*
  - *There is a derivation of the form:*

$$\frac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau}\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}}}\ \mathsf{Simp}$$

- ***(Der3)*** *If* $\mathsf{ai} = \text{TU}_{\text{ID}}(j,1)$*. For every* $\tau_1 = \_, \text{TN}(j_1, 0)$*,* $\tau_2 = \_, \text{TU}_{\text{ID}}(j, 0)$ *such that* $\tau_2 \prec_\tau \tau_1$*:*

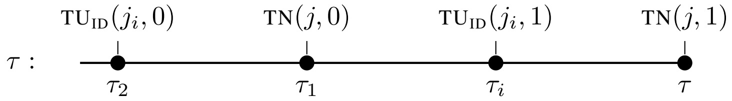


  - *We have* $\underline{\tau_2} = \_, \text{TU}_{\nu_\tau(\text{ID})}(j, 0)$*,* $\underline{\tau_1} = \_, \text{TU}_{\nu_\tau(\text{ID})}(j, 1)$ *and* $\underline{\tau_2} \prec_{\underline{\tau}} \underline{\tau_1} \prec_{\underline{\tau}} \underline{\tau}$*. Therefore,* $\mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}$ *is well-defined.*

– *There is a derivation of the form:*

$$\frac{\phi_{\tau}^{in}, \textit{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{in}, \textit{r-reveal}_{\tau_0}}{\phi_{\tau}^{in}, \textit{l-reveal}_{\tau_0}, \text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \;\sim\; \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}}}\ \textit{Simp}$$

- ***(Der4)*** *If* $\textsf{ai} = \text{TN}(j,1)$. *For every* $\text{ID} \in \mathcal{S}_{id}$, $\tau_i = \_, \text{TU}_{\text{ID}}(j_i,1)$, $\tau_1 = \_, \text{TN}(j,0)$, $\tau_2 = \_, \text{TU}_{\text{ID}}(j_i,0)$ *such that* $\tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i$*:*



  – *We have* $\underline{\tau_2} = \_, \text{TU}_{\nu_{\tau_1}(\text{ID})}(j_i,0)$, $\underline{\tau_i} = \_, \text{TU}_{\nu_{\tau_1}(\text{ID})}(j_i,1)$ *and* $\underline{\tau_2} \prec_{\underline{\tau}} \underline{\tau_1} \prec_{\underline{\tau}} \underline{\tau_i} \prec_{\underline{\tau}} \underline{\tau}$. *Therefore,* $\text{full-tr}^{\text{n}:\underline{\tau_1},\underline{\tau}}_{\text{u}:\underline{\tau_2},\underline{\tau_i}}$ *is well-defined.*
  – *There is a derivation of the form:*

$$\frac{\phi_{\tau}^{in}, \textit{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{in}, \textit{r-reveal}_{\tau_0}}{\phi_{\tau}^{in}, \textit{l-reveal}_{\tau_0}, \text{full-tr}^{\text{n}:\tau_1,\tau}_{\text{u}:\tau_2,\tau_i} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{full-tr}^{\text{n}:\underline{\tau_1},\underline{\tau}}_{\text{u}:\underline{\tau_2},\underline{\tau_i}}}\ \textit{Simp}$$

The proof is given in Section V

Lemma 15. *For all valid basic symbolic trace* τ *with at most* C *actions* NS*, there exists a derivation of:*

$$\phi_\tau, \textit{l-reveal}_\tau \sim \phi_{\underline{\tau}}, \textit{r-reveal}_\tau$$

The proof is given in Section VI.

Using this lemma, we can prove our main theorem, which we recall below:

Theorem (Theorem 1)**.** *The* 5G-AKA *protocol is* σ_{ul}*-unlinkable for an arbitrary number of agents and sessions when the asymmetric encryption* $\{\_\}^{\_}_{\_}$ *is* IND-CCA1 *secure and* $\textsf{f}$ *and* $\textsf{f}^{\textsf{r}}$ *(resp.* $\textsf{Mac}^1$*–*$\textsf{Mac}^5$*) satisfy jointly the* PRF *assumption.*

Proof. Using Proposition 19, we only need to show that for every $\tau \in \text{dom}(\mathcal{R}_{\text{ul}})$, there is a derivation of $\phi_\tau \sim \phi_{\underline{\tau}}$ using $\textsf{Ax}$. Moreover, using Assumption 1 we know that for every $\tau \in \text{dom}(\mathcal{R}_{\text{ul}})$, τ is a valid symbolic trace. Therefore, it is sufficient to prove that for every valid symbolic trace τ, we have a derivation using $\textsf{Ax}$ of $\phi_\tau \sim \phi_{\underline{\tau}}$. Using Lemma 15, we know that we have a derivation of $\phi_\tau, \text{l-reveal}_\tau \sim \phi_{\underline{\tau}}, \text{r-reveal}_\tau$. We conclude using the $\textsf{Restr}$ rule:

$$\frac{\phi_\tau, \text{l-reveal}_\tau \sim \phi_{\underline{\tau}}, \text{r-reveal}_\tau}{\phi_\tau \sim \phi_{\underline{\tau}}}\ \text{Restr}$$

■

APPENDIX V
PROOF OF PROPOSITION 30

Proof of ***(Der1)***

We have two cases:

- either there exists l such that $\mathrm{NS}_{\mathrm{ID}}(l) \prec \tau$ and $\mathrm{NS}_{\mathrm{ID}}(l) \not\prec_\tau \mathrm{NS}_{\mathrm{ID}}(\_)$. In that case we have $\mathrm{NS}_{\mathrm{ID}}(l) \prec_\tau \tau_1$.
- or for every i, $\mathrm{NS}_{\mathrm{ID}}(i) \not\prec_\tau \tau_1$.

Let $\underline{\mathrm{ID}} = \nu_\tau(\mathrm{ID})$. We summarize the situation graphically in Fig. 17. In both case, for every $\tau_1 \preceq \tau' \prec \tau$ we have:

$$\left(\sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_{\underline{\tau}'}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\right) \in \mathsf{reveal}_{\tau_0}$$
$$\left([\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\left(\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) - \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\right), [\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}})]\left(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\right)\right) \in \mathsf{reveal}_{\tau_0}$$

We know that:

$$\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \;=\; \sigma_{\tau_0}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \;=\; \sum_{\tau_1 \preceq \tau'} \sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})$$

And:

$$\begin{aligned}\left(\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\right) \;\leftrightarrow\; \\ \sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \left(\left(\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\right) + [\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\left(\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) - \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\right) < \mathbf{0}\right)\end{aligned}$$

Similarly:

$$\begin{aligned}\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) = \sigma_{\underline{\tau_0}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) &= \sum_{\underline{\tau_1} \preceq \underline{\tau}' \preceq \underline{\tau_0}} \sigma_{\underline{\tau}'}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) \\ &= \sum_{\tau_1 \preceq \tau'} \sigma_{\underline{\tau}'}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\end{aligned}$$

And:

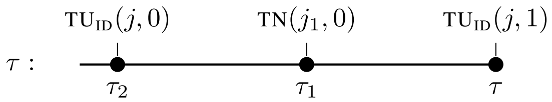
$$\begin{aligned}\left(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) \wedge \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) < \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\right) \;\leftrightarrow\; \\ \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) \wedge \left(\left(\left(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\right) + [\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}})]\left(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\right)\right) < \mathbf{0}\right)\end{aligned}$$

Putting everything together, we get the following derivation:

$$\cfrac{\cfrac{\mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{c}\mathsf{l\text{-}reveal}_{\tau_0}, \sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}), [\sigma_{\tau}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\left(\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) - \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\right), \left(\sigma_{\tau'}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_{\tau'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}),\right)_{\tau_1 \preceq \tau'} \\ \sim \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}}), [\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}})]\left(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\right), \left(\sigma_{\underline{\tau}'}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) - \sigma_{\underline{\tau}'}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}}),\right)_{\tau_1 \preceq \tau'}\end{array}}\;\mathsf{Dup}^*}{\begin{array}{c}\mathsf{l\text{-}reveal}_{\tau_0}, \sigma_{\tau_1}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}}) \wedge \sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) < \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \\ \sim\; \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\underline{\mathrm{ID}}}) \wedge \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\underline{\mathrm{ID}}}) < \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\underline{\mathrm{ID}}})\end{array}}\;\mathsf{Simp}$$

The derivation of (30) is very similar. We omit the details, and only give the graphical representation of the situation in Fig. 18.

Proof of ***(Der3)***



Recall that:

$$\mathsf{part\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1} \;\equiv\; \left(\begin{array}{l}\quad \pi_1(g(\phi_{\tau}^{\mathsf{in}})) = \mathsf{n}^{j_1} \;\wedge\; \pi_2(g(\phi_{\tau}^{\mathsf{in}})) = \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}) \oplus \mathsf{f}_{\mathsf{k}^{\mathrm{ID}}}(\mathsf{n}^{j_1}) \\ \wedge\; \pi_3(g(\phi_{\tau}^{\mathsf{in}})) = \mathsf{Mac}^3_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \mathsf{n}^{j_1}, \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}), \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{GUTI}_{\mathrm{U}}^{\mathrm{ID}})\rangle) \\ \wedge\; g(\phi_{\tau_1}^{\mathsf{in}}) = \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{GUTI}_{\mathrm{U}}^{\mathrm{ID}}) \;\wedge\; \sigma_{\tau_2}^{\mathsf{in}}(\mathrm{GUTI}_{\mathrm{U}}^{\mathrm{ID}}) = \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{GUTI}_{\mathrm{N}}^{\mathrm{ID}}) \;\wedge\; \sigma_{\tau_2}^{\mathsf{in}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \\ \wedge\; \mathsf{range}(\sigma_{\tau}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}), \sigma_{\tau_1}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}}))\end{array}\right) \tag{43}$$

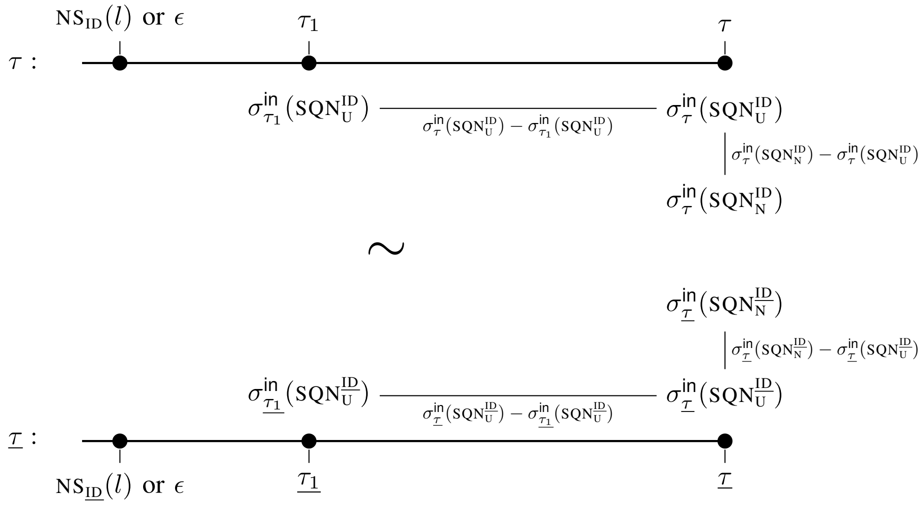


Fig. 17. First Graphical Representation for the Proof of **(Der1)**

Since τ is valid, we know that for every τ', if $\tau_2 \prec_\tau \tau'$ then $\tau' \neq \mathrm{NS_{ID}}(\_)$. It follows that $\underline{\tau_2} = \_, \mathrm{TU}_{\nu_\tau(\mathrm{ID})}(j, 0)$ and $\underline{\tau} = \_, \mathrm{TU}_{\nu_\tau(\mathrm{ID})}(j, 1)$. The fact that $\underline{\tau_2} \prec_{\underline{\tau}} \underline{\tau_1}$ is then straightforward. Letting $\underline{\mathrm{ID}} = \nu_\tau(\mathrm{ID})$, we can then check that:

$$\text{part-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \equiv \left(\begin{array}{l} \pi_1(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \mathsf{n}^{j_1} \;\wedge\; \pi_2(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN^{\underline{ID}}_N}) \oplus \mathsf{f}_{\mathsf{k}^{\underline{\mathrm{ID}}}}(\mathsf{n}^{j_1}) \\ \wedge\; \pi_3(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \mathsf{Mac}^3_{\mathsf{k}^{\underline{\mathrm{ID}}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN^{\underline{ID}}_N}), \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI^{\underline{ID}}_U})\rangle) \\ \wedge\; g(\phi^{\mathsf{in}}_{\underline{\tau_1}}) = \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI^{\underline{ID}}_U}) \;\wedge\; \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI^{\underline{ID}}_U}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{GUTI^{\underline{ID}}_N}) \;\wedge\; \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\text{valid-guti}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \\ \wedge\; \text{range}(\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathrm{SQN^{\underline{ID}}_U}), \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{SQN^{\underline{ID}}_N})) \end{array} \right) \tag{44}$$

We have two cases.

a) Case 1: Assume that for all $\tau' \prec_\tau \tau_1$ such that $\tau' \not\prec_\tau \mathrm{NS_{ID}}(\_)$ we have $\tau' \neq \_, \mathrm{FU_{ID}}(\_)$.

Then we know that for all $\underline{\tau'} <_{\underline{\tau}} \underline{\tau_1}$ such that $\underline{\tau'} \not\prec_{\underline{\tau}} \mathrm{NS}_{\nu_\tau(\mathrm{ID})}(\_)$ we have $\underline{\tau'} \neq \_, \mathrm{FU}_{\nu_\tau(\mathrm{ID})}(\_)$. Therefore using **(B7)** twice we get:

$$\text{part-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \text{false} \qquad\qquad \text{part-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \rightarrow \text{false}$$

Therefore we have a trivial derivation:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{false} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{false}}\ \mathsf{FA}}{\phi^{\mathsf{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{part-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{part-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}}\ R \tag{45}$$

b) Case 2: Assume that there exists $\tau_3 = \_, \mathrm{FU_{ID}}(j_0)$ such that $\tau_3 \prec_\tau \tau_1$, $\tau_3 \not\prec_\tau \mathrm{NS_{ID}}(\_)$ and $\tau_3 \not\prec_\tau \mathrm{FU_{ID}}(\_)$. Then $\underline{\tau_3} = \_, \mathrm{FU}_{\nu_\tau(\mathrm{ID})}(\_)$, $\underline{\tau_3} <_{\underline{\tau}} \underline{\tau_1}$, $\underline{\tau_3} \not\prec_{\underline{\tau}} \mathrm{NS}_{\nu_\tau(\mathrm{ID})}(\_)$ and $\underline{\tau_3} \not\prec_{\underline{\tau}} \mathrm{FU}_{\nu_\tau(\mathrm{ID})}(\_)$.

First, we show that $j_0 \neq j$: assume that $j_0 = j$, then we know that $\tau \prec_\tau \tau_3$, which is absurd. Therefore $j_0 \neq j$. Using the validity of τ, we know that τ_3 cannot occur between $\tau_2 = \_, \mathrm{TU_{ID}}(j, 0)$ and $\tau = \_, \mathrm{TU_{ID}}(j, 0)$. Hence $\tau_3 \prec_\tau \tau_2$.

Let τ_{NS} be the latest $\mathrm{NS_{ID}}(\_)$, if it exists, or ϵ otherwise: $\tau_{\mathrm{NS}} = \_, \mathrm{NS_{ID}}(\_)$ or ϵ and $\tau_{\mathrm{NS}} \not\prec_\tau \mathrm{NS_{ID}}(\_)$. Let τ_x be $\_, \mathrm{TU_{ID}}(j_0, 0)$ or $\_, \mathrm{PU_{ID}}(j_0, 1)$ be the beginning of the U session associated to τ_3. We know that $\tau_{\mathrm{NS}} \prec_\tau \tau_x \prec_\tau \tau_3$.

We know that $\text{part-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}})$. As $\tau_3 \not\prec_\tau \mathrm{FU_{ID}}(\_)$, we know that there are no $\mathrm{FU_{ID}}(\_)$ action between τ_3 and τ_2. If there exists a action by user ID between τ_3 and τ_2, then we have either $\tau_3 \prec_\tau \mathrm{PU_{ID}}(\_, 1) \prec_\tau \tau_2$ or $\tau_3 \prec_\tau \mathrm{TU_{ID}}(\_, 0) \prec_\tau \tau_2$. In both case, $\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}}$ is set to false, and cannot be set back to something else without a $\mathrm{FU_{ID}}(\_)$ action. It follows that if there exists a user action between τ_3 and τ_2 then $\neg\sigma^{\mathsf{in}}_{\tau_2}(\text{valid-guti}^{\mathrm{ID}}_{\mathrm{U}})$. Using the same reasoning we have $\neg\sigma^{\mathsf{in}}_{\underline{\tau_2}}(\text{valid-guti}^{\underline{\mathrm{ID}}}_{\mathrm{U}})$ if there exists a user action between τ_3 and τ_2. Hence in that case the derivation (45) works.

By consequence we now assume that:

$$\{\_, \mathrm{TU_{ID}}(\_), \_, \mathrm{PU_{ID}}(\_, \_)1, \mathrm{FU_{ID}}(\_)\} \cap \{\tau' \mid \tau_3 \prec_\tau \tau' \prec_\tau \tau_2\} = \emptyset \tag{46}$$

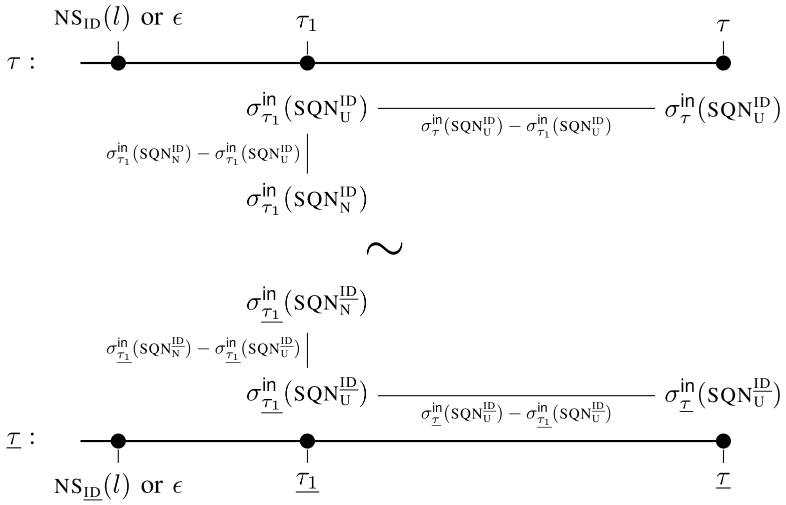


Fig. 18. Second Graphical Representation for the Proof of **(Der1)**

It follows that $\neg\mathsf{accept}^{\mathrm{ID}}_{\tau_3} \to \neg\sigma^{\mathsf{in}}_{\tau_2}(\mathsf{valid\text{-}guti}^{\mathrm{ID}}_{\mathrm{U}})$, hence $\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \to \mathsf{accept}^{\mathrm{ID}}_{\tau_3}$. We also deduce from (46) that $\sigma_{\tau_3}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) \equiv \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}})$. Applying **(StrEqu1)**, we know that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau_3} \;\leftrightarrow \bigvee_{\tau_x \prec_\tau \tau_a = \_,\mathrm{FN}(j_a) \prec_\tau \tau_3} \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3}$$

Therefore:

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\leftrightarrow \bigvee_{\tau_x \prec_\tau \tau_a = \_,\mathrm{FN}(j_a) \prec_\tau \tau_3} \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$$

Similarly, we show that $\sigma_{\underline{\tau_3}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \equiv \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}})$ and that:

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \;\leftrightarrow \bigvee_{\tau_x \prec_\tau \tau_a = \_,\mathrm{FN}(j_a) \prec_\tau \tau_3} \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}$$

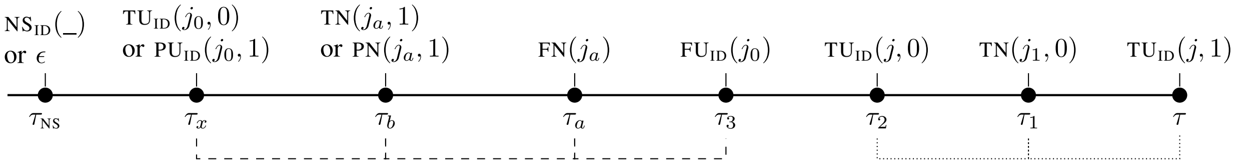
We can start building the wanted derivation:

$$\dfrac{\dfrac{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right)_{\tau_x \prec_\tau \tau_a = \_,\mathrm{FN}(j_a) \prec_\tau \tau_3} \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}\right)_{\tau_x \prec_\tau \tau_a = \_,\mathrm{FN}(j_a) \prec_\tau \tau_3}\end{array}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \displaystyle\bigvee_{\tau_x \prec_\tau \tau_a = \_,\mathrm{FN}(j_a) \prec_\tau \tau_3} \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \displaystyle\bigvee_{\tau_x \prec_\tau \tau_a = \_,\mathrm{FN}(j_a) \prec_\tau \tau_3} \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}\end{array}}\ \mathsf{FA}^*}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}}\ R$$

Let $\tau_a = \_, \mathrm{FN}(j_a)$ be such that $\tau_x \prec_\tau \tau_a \prec_\tau \tau_3$. Let τ_b be $\_, \mathrm{TN}(j_a, 1)$ or $\_, \mathrm{PN}(j_a, 1)$ such that $\tau_b \prec_\tau \tau_a$. To conclude, we just need to build a derivation of:

$$\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}$$

The proof consist in rewriting $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$ and $\mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}$ such that they can be decomposed (using FA) into corresponding parts appearing in reveal_{τ_0}. We do this piece by piece: the waved underlined part first, the dotted underlined and the dashed underlined part. We represent graphically the protocols executions below:



c) Part 1 (Waves): We are going to give a derivation of:

$$\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma^{\mathsf{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{GUTI}^{\text{ID}}_{\text{N}})$$

Recall that $\sigma_{\tau_3}(\text{GUTI}^{\text{ID}}_{\text{U}}) \equiv \sigma^{\mathsf{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}})$ and $\sigma_{\underline{\tau_3}}(\text{GUTI}^{\text{ID}}_{\text{U}}) \equiv \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\text{GUTI}^{\text{ID}}_{\text{U}})$. Therefore it is sufficient to give a derivation of:

$$\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma_{\underline{\tau_3}}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{GUTI}^{\text{ID}}_{\text{N}})$$

We know that:

$$[\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3}]\sigma_{\tau_3}(\text{GUTI}^{\text{ID}}_{\text{U}}) = [\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3}]\text{GUTI}^{j_a}$$

Hence:

$$\left(\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}})\right) \;\leftrightarrow\; \left(\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \text{GUTI}^{j_a}\right)$$

Intuitively, the only way we can have $\sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \text{GUTI}^{j_a}$ is:

- if the SUPI or GUTI network session j_a accepts with the increasing sequence number condition.
- and if $\sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}})$ was not over-written between τ_b and τ_1.

It is actually straightforward to show by induction that:

$$\sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) \neq \text{GUTI}^{j_a} \;\leftrightarrow\; \left(\neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_b} \vee \bigvee_{\substack{\tau'=\_,\text{TN}(j',1) \\ \text{or } \tau'=\_,\text{PN}(j',1) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \vee \bigvee_{\substack{\tau'=\_,\text{TN}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} \mathsf{accept}^{\text{ID}}_{\tau'}\right)$$

Hence:

$$\begin{aligned}
&\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) \\
\leftrightarrow\;& \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_b} \wedge \bigwedge_{\substack{\tau'=_,\text{TN}(j',1) \\ \text{or } \tau'=_,\text{PN}(j',1) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \wedge \bigwedge_{\substack{\tau'=_,\text{TN}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} \neg\mathsf{accept}^{\text{ID}}_{\tau'} \\
\leftrightarrow\;& \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_b} \wedge \bigwedge_{\substack{\tau'=_,\text{TN}(j',1) \\ \text{or } \tau'=_,\text{PN}(j',1) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \wedge \bigwedge_{\substack{\tau'=_,\text{TN}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\tau'}) \neq \text{GUTI}^{j_a}
\end{aligned}$$

For every $\tau_n = \_, \text{TN}(\_,1)$ or $\_, \text{PN}(\_,1)$, we know that $\text{SQN}^{\text{ID}}_{\text{N}}$ is incremented at τ_n if and only if $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_n}$ is true. Therefore:

$$\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_n} \;\leftrightarrow\; \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) < \sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}})$$

Using the fact that $\sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{U}})$, we can rewrite this as:

$$\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_n} \;\leftrightarrow\; \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma^{\mathsf{in}}_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma_{\tau_n}(\text{SQN}^{\text{ID}}_{\text{U}})$$

Using this remark we can show that:

$$\begin{aligned}
&\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) \\
\leftrightarrow\;& \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \begin{pmatrix} \sigma^{\mathsf{in}}_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma^{\mathsf{in}}_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{U}}) \\ < \; \sigma_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{U}}) \end{pmatrix} \wedge \begin{pmatrix} \sigma_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{U}}) \\ = \; \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) \end{pmatrix} \wedge \bigwedge_{\substack{\tau'=_,\text{TN}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\tau'}) \neq \text{GUTI}^{j_a}
\end{aligned} \tag{47}$$

Doing exactly the same reasoning, we show that:

$$\begin{aligned}
&\mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma_{\underline{\tau_3}}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{GUTI}^{\text{ID}}_{\text{N}}) \\
\leftrightarrow\;& \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \begin{pmatrix} \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\text{SQN}^{\text{ID}}_{\text{U}}) \\ < \; \sigma_{\underline{\tau_b}}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma_{\underline{\tau_b}}(\text{SQN}^{\text{ID}}_{\text{U}}) \end{pmatrix} \wedge \begin{pmatrix} \sigma_{\underline{\tau_b}}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma_{\underline{\tau_b}}(\text{SQN}^{\text{ID}}_{\text{U}}) \\ = \; \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\text{ID}}_{\text{U}}) \end{pmatrix} \wedge \bigwedge_{\substack{\tau'=_,\text{TN}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\underline{\tau'}}) \neq \text{GUTI}^{j_a}
\end{aligned} \tag{48}$$

We introduce some notation that will be used later: for every symbolic trace $\tau = \tau_0, \mathsf{ai}$ and identity ID, we let $\mathsf{sync\text{-}diff\text{-}in}^{\mathrm{ID}}_{\tau} \equiv \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_0}$.

We now split the proof in two, depending on whether $\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$ is true or false. Let $\psi \equiv \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}})$ and $\underline{\psi} \equiv \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{N}})$. Using the fact that:

$$\left(\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}})\right) \in \mathsf{reveal}_{\tau_0}$$

We can build the derivation:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi, \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}, \neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi, \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}, \neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}\end{array}}\;\mathsf{Dup}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \psi \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\psi}}\;\mathsf{Simp}$$

We now build a derivation of $\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi$ and one for $\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi$:

- Using the fact that we have $\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$ and (47), we know that:

$$\begin{aligned}&\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\mathrm{GUTI}^{\mathrm{ID}}_{\mathrm{N}})\\ \leftrightarrow\;& \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \begin{pmatrix} \mathsf{sync\text{-}diff\text{-}in}^{\mathrm{ID}}_{\tau_b} \\ < \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_b}\end{pmatrix} \wedge \begin{pmatrix} \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_b} \\ = \mathsf{sync\text{-}diff\text{-}in}^{\mathrm{ID}}_{\tau_1}\end{pmatrix} \wedge \bigwedge_{\substack{\tau' = \_,\mathrm{TN}(j',0)\\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\tau'}) \neq \mathrm{GUTI}^{j_a}\end{aligned}$$

  Similarly, using (48) we get:

$$\begin{aligned}&\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma_{\underline{\tau_3}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathrm{GUTI}^{\underline{\mathrm{ID}}}_{\mathrm{N}})\\ \leftrightarrow\;& \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \begin{pmatrix} \mathsf{sync\text{-}diff\text{-}in}^{\underline{\mathrm{ID}}}_{\underline{\tau_b}} \\ < \mathsf{sync\text{-}diff}^{\underline{\mathrm{ID}}}_{\underline{\tau_b}}\end{pmatrix} \wedge \begin{pmatrix} \mathsf{sync\text{-}diff}^{\underline{\mathrm{ID}}}_{\underline{\tau_b}} \\ = \mathsf{sync\text{-}diff\text{-}in}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}}\end{pmatrix} \wedge \bigwedge_{\substack{\tau' = \_,\mathrm{TN}(j',0)\\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\underline{\tau'}}) \neq \mathrm{GUTI}^{j_a}\end{aligned}$$

  Moreover, we know that:

$$\left(\left(\mathrm{GUTI}^{j_a}, \mathrm{GUTI}^{j_a}\right) \in \mathsf{reveal}_{\tau_0}\right)_{\substack{\tau' = \_,\mathrm{TN}(j',0)\\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} \qquad \left(\mathsf{sync\text{-}diff\text{-}in}^{\mathrm{ID}}_{\tau_1}, \mathsf{sync\text{-}diff\text{-}in}^{\underline{\mathrm{ID}}}_{\underline{\tau_1}}\right) \in \mathsf{reveal}_{\tau_0}$$

$$\left(\mathsf{sync\text{-}diff\text{-}in}^{\mathrm{ID}}_{\tau_b}, \mathsf{sync\text{-}diff\text{-}in}^{\underline{\mathrm{ID}}}_{\underline{\tau_b}}\right) \in \mathsf{reveal}_{\tau_0} \qquad \left(\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_b}, \mathsf{sync\text{-}diff}^{\underline{\mathrm{ID}}}_{\underline{\tau_b}}\right) \in \mathsf{reveal}_{\tau_0}$$

$$\left(\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}})\right) \in \mathsf{reveal}_{\tau_0}$$

  And using **(Der2)**, we know that we have a derivation of:

$$\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3}}\;\mathsf{Simp}$$

  Using this, we can rewrite $\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi$ and $\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}$ as two terms that decompose, using FA, into matching part of reveal_{τ_0}. By consequence we can build the following derivation:

$$\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}\psi \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}}\;\mathsf{Simp} \tag{49}$$

- We now focus on the case where we have $\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$.
  First, assume that $\tau_b = \_, \mathrm{TN}(j_a, 1)$. In that case, we know that $\mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \to \mathsf{accept}^{\mathrm{ID}}_{\tau_b}$. Since $\mathsf{accept}^{\mathrm{ID}}_{\tau_b} \to \sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$, we get that $(\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi) \leftrightarrow \mathsf{false}$. Similarly we have $(\neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}) \leftrightarrow \mathsf{false}$. By consequence, we have a trivial derivation:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{false} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{false}}\;\mathsf{FA}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \psi \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\mathrm{ID}}}_{\mathrm{U}}) \wedge \underline{\psi}}\;\mathsf{Simp}$$

Now assume that $\tau_b = \_, \text{PN}(j_a, 1)$. Since $\tau_3 = \_, \text{FU}_{\text{ID}}(j_0) \prec \tau$, we know by validity of τ there there exists $\tau' = \_, \text{PU}_{\text{ID}}(j_0, 2)$ or $\_, \text{TU}_{\text{ID}}(j_0, 1)$ such that $\tau' \prec_\tau \tau_3$. It is straightforward to check that if $\tau' = \_, \text{TU}_{\text{ID}}(j_0, 1)$ then since $\tau_b = \_, \text{PN}(j_a, 1)$ we have $\text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \leftrightarrow \text{false}$ and $\text{fu-tr}^{\text{n}:\underline{\tau_a}}_{\text{u}:\underline{\tau_3}} \leftrightarrow \text{false}$. Building the wanted derivation is then trivial. Therefore assume that $\tau' = \_, \text{PU}_{\text{ID}}(j_0, 2)$. Observe that $\text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \rightarrow \text{accept}^{\text{ID}}_{\tau'}$. We have two cases:

- Assume $\tau' \prec_\tau \tau_b$. Using **(Equ2)**, we know that:

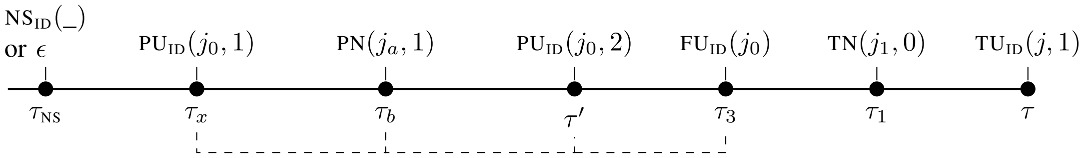
$$\begin{aligned} \text{accept}^{\text{ID}}_{\tau'} &\rightarrow \bigvee_{\substack{\tau_n = \_, \text{PN}(j_n, 1) \\ \tau_x \prec_\tau \tau_n \prec_\tau \tau'}} \text{supi-tr}^{\text{n}:\tau_n}_{\text{u}:\tau_x, \tau'} \\ &\rightarrow \bigvee_{\substack{\tau_n = \_, \text{PN}(j_n, 1) \\ \tau_x \prec_\tau \tau_n \prec_\tau \tau'}} g(\phi^{\text{in}}_{\tau_x}) = \text{n}^{j_n} \\ &\rightarrow \bigvee_{\substack{\tau_n = \_, \text{PN}(j_n, 1) \\ \tau_x \prec_\tau \tau_n \prec_\tau \tau'}} \sigma^{\text{ID}}_{\tau_x}(\text{b-auth}^{\text{ID}}_{\text{U}}) = \text{n}^{j_n} \\ &\rightarrow \sigma^{\text{ID}}_{\tau_x}(\text{b-auth}^{\text{ID}}_{\text{U}}) \neq \text{n}^{j_a} \qquad \text{(Since } \tau' \prec_\tau \tau_b\text{)} \end{aligned}$$

  Moreover:

$$\text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \rightarrow \sigma^{\text{ID}}_{\tau'}(\text{e-auth}^{\text{ID}}_{\text{U}}) = \text{n}^{j_a} \rightarrow \sigma^{\text{ID}}_{\tau_x}(\text{b-auth}^{\text{ID}}_{\text{U}}) = \text{n}^{j_a}$$

  Therefore $\text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \rightarrow \text{false}$. Similarly we can show that $\text{fu-tr}^{\text{n}:\underline{\tau_a}}_{\text{u}:\underline{\tau_3}} \rightarrow \text{false}$. It is then easy build the wanted derivation.

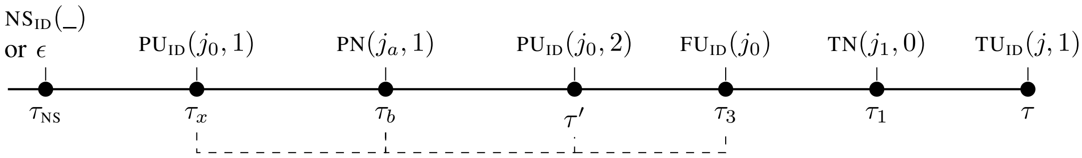
- Assume $\tau_b \prec_\tau \tau'$. We summarize graphically the situation below:



  First, since there are no ID actions between τ_b and τ', we know that $\neg\sigma^{\text{in}}_{\tau_b}(\text{sync}^{\text{ID}}_{\text{U}}) \rightarrow \neg\sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}})$. Recall that $\text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \rightarrow \text{accept}^{\text{ID}}_{\tau'}$. Using **(Equ2)**, it is simple to check that $\text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \wedge \text{accept}^{\text{ID}}_{\tau'} \rightarrow \text{supi-tr}^{\text{n}:\tau_b}_{\text{u}:\tau_x, \tau'}$. Therefore:

$$\begin{aligned} \left(\neg\sigma^{\text{in}}_{\tau_b}(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3}\right) &\rightarrow \neg\sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{accept}^{\text{ID}}_{\tau'} \\ &\rightarrow \text{inc-accept}^{\text{ID}}_{\tau_b} \wedge \sigma^{\text{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{N}}) = \mathbf{0} \qquad \text{(Using } \textbf{(StrEqu4)}\text{)} \\ &\qquad \wedge \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}}) - \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) = \mathbf{0} \end{aligned}$$

  Using again the fact that there are no ID actions between τ_b and τ', we know that $\sigma^{\text{in}}_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{U}}) \equiv \sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}})$. Moreover $\sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) \equiv \sigma_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}})$, therefore $\sigma^{\text{in}}_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}})$. Similarly, we know that $\sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) \equiv \sigma^{\text{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}})$. Summarizing:



$$\begin{array}{ccc} \sigma^{\text{in}}_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{N}}) & \overset{=}{\longrightarrow} & \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) \\ & & \Big| \, \| \\ \sigma^{\text{in}}_{\tau_b}(\text{SQN}^{\text{ID}}_{\text{U}}) & \overset{=}{\longrightarrow} & \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}}) \end{array}$$

  Using the fact that we have $\neg\sigma^{\text{in}}_{\tau_b}(\text{sync}^{\text{ID}}_{\text{U}})$ and (47), we know that:

$$\begin{aligned} &\neg\sigma^{\text{in}}_{\tau_b}(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \wedge \sigma_{\tau_3}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\text{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) \\ \leftrightarrow\ &\neg\sigma^{\text{in}}_{\tau_b}(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{fu-tr}^{\text{n}:\tau_a}_{\text{u}:\tau_3} \wedge \text{inc-accept}^{\text{ID}}_{\tau_b} \wedge \begin{pmatrix} \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}}) \\ = \ \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) - \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) \end{pmatrix} \wedge \bigwedge_{\substack{\tau' = \_, \text{TN}(j', 0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\text{in}}_{\tau'}) \neq \text{GUTI}^{j_a} \end{aligned}$$

Besides, $\mathsf{accept}^{\text{ID}}_{\tau'} \rightarrow \sigma_{\tau'}(\mathsf{sync}^{\text{ID}}_{\text{U}})$, and since $\tau' \prec_\tau \tau_1$ we know that $\sigma_{\tau'}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \rightarrow \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}})$. Hence:

$$\begin{aligned} & \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \sigma_{\tau_3}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) \\ \leftrightarrow\ & \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \wedge \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau_b} \wedge \mathsf{sync\text{-}diff}^{\text{ID}}_{\tau'} = \mathsf{sync\text{-}diff\text{-}in}^{\text{ID}}_{\tau_1} \wedge \bigwedge_{\substack{\tau'=\_,\text{TN}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\tau'}) \neq \text{GUTI}^{j_a} \end{aligned}$$

Similarly we have:

$$\begin{aligned} & \neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \sigma_{\underline{\tau_3}}(\text{GUTI}^{\underline{\text{ID}}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{GUTI}^{\underline{\text{ID}}}_{\text{N}}) \\ \leftrightarrow\ & \neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}} \wedge \mathsf{inc\text{-}accept}^{\underline{\text{ID}}}_{\underline{\tau_b}} \wedge \mathsf{sync\text{-}diff}^{\underline{\text{ID}}}_{\underline{\tau'}} = \mathsf{sync\text{-}diff\text{-}in}^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \bigwedge_{\substack{\tau'=\_,\text{TN}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} g(\phi^{\mathsf{in}}_{\underline{\tau'}}) \neq \text{GUTI}^{j_a} \end{aligned}$$

And using **(Der2)**, we know that we have a derivation of:

$$\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\tau_a}_{\mathsf{u}:\tau_3} \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{fu\text{-}tr}^{\mathsf{n}:\underline{\tau_a}}_{\mathsf{u}:\underline{\tau_3}}}\ \mathsf{Simp}$$

Moreover, we know that:

$$\left(\left(\text{GUTI}^{j_a}, \text{GUTI}^{j_a}\right) \in \mathsf{reveal}_{\tau_0}\right)_{\substack{\tau'=\_,\text{TN}(j',0) \\ \tau_b \prec_\tau \tau' \prec_\tau \tau_1}} \qquad \left(\mathsf{sync\text{-}diff\text{-}in}^{\text{ID}}_{\tau_1}, \mathsf{sync\text{-}diff\text{-}in}^{\underline{\text{ID}}}_{\underline{\tau_1}}\right) \in \mathsf{reveal}_{\tau_0}$$

$$\left(\mathsf{sync\text{-}diff}^{\text{ID}}_{\tau}, \mathsf{sync\text{-}diff}^{\underline{\text{ID}}}_{\underline{\tau'}}\right) \in \mathsf{reveal}_{\tau_0} \qquad \left(\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\text{ID}}_{\text{U}}), \sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}})\right) \in \mathsf{reveal}_{\tau_0}$$

Similarly to what we did in (49), we can rewrite $\neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \psi$ and $\neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \underline{\psi}$ as two terms that decompose, using FA, into matching part of reveal_{τ_0}. By consequence we can build the following derivation:

$$\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}\psi\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\tau_b}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \psi\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\underline{\tau_b}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \underline{\psi}}\ \mathsf{Simp}$$

d) Part 2 (Dots): Using **(StrEqu2)** we know that $\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \mathsf{accept}^{\text{ID}}_{\tau_1}$. Therefore, using **(A6)** we get that $\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \neg\mathsf{accept}^{\text{ID}'}_{\tau_1}$ for every $\text{ID}' \neq \text{ID}$. It follows that $\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow t_{\tau_1} = \mathsf{msg}^{\text{ID}}_{\tau_1}$, and therefore:

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \ \rightarrow\ \pi_2(t_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \oplus \mathsf{f}_{\mathsf{k}^{\text{ID}}}(\mathsf{n}^{j_1}) \tag{50}$$

And:

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \ \rightarrow\ \pi_3(t_{\tau_1}) = \mathsf{Mac}^3_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}, \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}), \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{U}})\rangle)$$

Moreover, since no action from agent ID occurs between τ_2 and τ_1, we know that $\sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}})$. Hence:

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \ \rightarrow\ \pi_3(t_{\tau_1}) = \mathsf{Mac}^3_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}, \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}), \sigma^{\mathsf{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}})\rangle) \tag{51}$$

Therefore using (50) and (51) we can rewrite $\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}$ as follows:

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \ =\ \left(\begin{array}{l} \quad \pi_1(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{n}^{j_1} \ \wedge\ \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \pi_2(t_{\tau_1}) \ \wedge\ \pi_3(g(\phi^{\mathsf{in}}_\tau)) = \pi_3(t_{\tau_1}) \\ \wedge\ g(\phi^{\mathsf{in}}_{\tau_1}) = \sigma^{\mathsf{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) \ \wedge\ \sigma^{\mathsf{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) \ \wedge\ \sigma^{\mathsf{in}}_{\tau_2}(\mathsf{valid\text{-}guti}^{\text{ID}}_{\text{U}}) \\ \wedge\ \mathsf{range}(\sigma^{\mathsf{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}}), \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}})) \end{array}\right)$$

By a similar reasoning we rewrite $\mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}$ as follows:

$$\mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \ \equiv\ \left(\begin{array}{l} \quad \pi_1(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \mathsf{n}^{j_1} \ \wedge\ \pi_2(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \pi_2(t_{\underline{\tau_1}}) \ \wedge\ \pi_3(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \pi_3(t_{\underline{\tau_1}}) \\ \wedge\ g(\phi^{\mathsf{in}}_{\underline{\tau_1}}) = \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\text{GUTI}^{\underline{\text{ID}}}_{\text{U}}) \ \wedge\ \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\text{GUTI}^{\underline{\text{ID}}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{GUTI}^{\underline{\text{ID}}}_{\text{N}}) \ \wedge\ \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathsf{valid\text{-}guti}^{\underline{\text{ID}}}_{\text{U}}) \\ \wedge\ \mathsf{range}(\sigma^{\mathsf{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}), \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}})) \end{array}\right)$$

e) Part 3 (Dash): Since $\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\text{ID}}_{\text{U}})$ we know that:

$$\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \;\rightarrow\; \sigma^{\text{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) \;=\; \text{m-suci}^{\;\text{ID}}_{\tau}$$

Besides, as $\sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\text{ID}}_{\text{U}}) \rightarrow \sigma^{\text{in}}_{\tau_2}(\text{sync}^{\text{ID}}_{\text{U}})$, and since $\sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\text{ID}}_{\text{U}}) \rightarrow \sigma^{\text{in}}_{\tau_1}(\text{valid-guti}^{\text{ID}}_{\text{U}})$ (because $\tau_2 \prec_\tau \tau_1$ and $\tau_2 \not\prec_\tau \text{NS}_{\text{ID}}(\_)$), we know that:

$$\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \rightarrow \big(\text{range}(\sigma^{\text{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}), \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}})) \leftrightarrow (\sigma^{\text{in}}_{\tau_1}(\text{valid-guti}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}))\big)$$

Similarly we have:

$$\text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}} \;\rightarrow\; \sigma^{\text{in}}_{\underline{\tau_2}}(\text{GUTI}^{\underline{\text{ID}}}_{\text{U}}) \;=\; \text{m-suci}^{\;\underline{\text{ID}}}_{\underline{\tau}}$$

$$\text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}} \rightarrow \Big(\text{range}(\sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}), \sigma^{\text{in}}_{\underline{\tau_1}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}})) \leftrightarrow \Big(\sigma^{\text{in}}_{\underline{\tau_1}}(\text{valid-guti}^{\underline{\text{ID}}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) = \sigma^{\text{in}}_{\underline{\tau_1}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}})\Big)\Big)$$

Moreover:

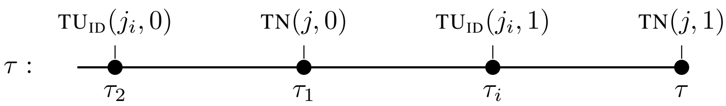
$$\Big(\text{m-suci}^{\;\text{ID}}_{\tau} \;\sim\; \text{m-suci}^{\;\underline{\text{ID}}}_{\underline{\tau}}\Big) \in \text{reveal}_{\tau_0} \qquad\qquad \Big(\sigma^{\text{in}}_{\tau_2}(\text{valid-guti}^{\text{ID}}_{\text{U}}) \;\sim\; \sigma^{\text{in}}_{\underline{\tau_2}}(\text{valid-guti}^{\underline{\text{ID}}}_{\text{U}})\Big) \in \text{reveal}_{\tau_0}$$

Finally, using **(Der1)**, we know that we have a derivation of:

$$\frac{\text{l-reveal}_{\tau_0} \;\sim\; \text{r-reveal}_{\tau_0}}{\text{l-reveal}_{\tau_0}, \sigma^{\text{in}}_{\tau_1}(\text{valid-guti}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{N}}) \;\sim\; \text{r-reveal}_{\tau_0}, \sigma^{\text{in}}_{\underline{\tau_1}}(\text{valid-guti}^{\underline{\text{ID}}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) = \sigma^{\text{in}}_{\underline{\tau_1}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}})}\ \text{FA}^*$$

f) Part 4 (conclusion): To conclude, we combine the derivations of Part 1, Part 2 and Part 3.

*Proof of **(Der4)***



Recall that:

$$\text{full-tr}^{\text{n}:\tau_1,\tau}_{\text{u}:\tau_2,\tau_i} \;\equiv\; \Big(\text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau_i} \wedge g(\phi^{\text{in}}_{\tau}) = \text{Mac}^4_{\text{k}^{\text{ID}}_{\text{m}}}(\text{n}^j)\Big)$$

The fact that $\underline{\tau_2} = \_, \text{TU}_{\nu_{\tau_1}(\text{ID})}(j_i, 0)$, $\underline{\tau_i} = \_, \text{TU}_{\nu_{\tau_1}(\text{ID})}(j_i, 1)$ and $\underline{\tau_2} <_{\underline{\tau}} \underline{\tau_1} <_{\underline{\tau}} \underline{\tau_i}$ is straightforward from **(Der3)**. It is easy to check that:

$$\text{full-tr}^{\text{n}:\underline{\tau_1},\underline{\tau}}_{\text{u}:\underline{\tau_2},\underline{\tau_i}} \;\equiv\; \Big(\text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau_i}} \wedge g(\phi^{\text{in}}_{\underline{\tau}}) = \text{Mac}^4_{\text{k}^{\nu_{\tau_1}(\text{ID})}_{\text{m}}}(\text{n}^j)\Big)$$

Moreover:

$$\Big(\text{Mac}^4_{\text{k}^{\text{ID}}_{\text{m}}}(\text{n}^j), \text{Mac}^4_{\text{k}^{\nu_{\tau_1}(\text{ID})}_{\text{m}}}(\text{n}^j)\Big) \in \text{reveal}_{\tau_0}$$

And, using **(Der3)**, we know that there exists a derivation using only FA and Dup of:

$$\phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0} \;\rightarrow\; \begin{pmatrix} \phi^{\text{in}}_{\tau}, \text{l-reveal}_{\tau_0}, \text{part-tr}^{\text{n}:\tau_1}_{\text{u}:\tau_2,\tau} \\ \sim\; \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{part-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau_2},\underline{\tau}} \end{pmatrix}$$

It is therefore easy to built the wanted derivation using only FA and Dup.

*Proof of **(Der2)***

We recall that:

$$\text{fu-tr}^{\text{n}:\tau_1}_{\text{u}:\tau} \;\equiv\; \begin{pmatrix} \text{inj-auth}_\tau(\text{ID}, j_0) \wedge \sigma^{\text{in}}_{\tau}(\text{e-auth}^{j_0}_{\text{N}}) \neq \text{UnknownId} \\ \wedge\; \pi_1(g(\phi^{\text{in}}_{\tau})) = \text{GUTI}^{j_0} \oplus \text{f}^{\text{r}}_{\text{k}}(\text{n}^{j_0}) \wedge\; \pi_2(g(\phi^{\text{in}}_{\tau})) = \text{Mac}^5_{\text{k}_{\text{m}}}(\langle \text{GUTI}^{j_0}, \text{n}^{j_0}\rangle) \end{pmatrix}$$

$$\text{fu-tr}^{\text{n}:\underline{\tau_1}}_{\text{u}:\underline{\tau}} \;\equiv\; \begin{pmatrix} \text{inj-auth}_{\underline{\tau}}(\nu_\tau(\text{ID}), j_0) \wedge \sigma^{\text{in}}_{\underline{\tau}}(\text{e-auth}^{j_0}_{\text{N}}) \neq \text{UnknownId} \\ \wedge\; \pi_1(g(\phi^{\text{in}}_{\underline{\tau}})) = \text{GUTI}^{j_0} \oplus \text{f}^{\text{r}}_{\text{k}}(\text{n}^{j_0}) \wedge\; \pi_2(g(\phi^{\text{in}}_{\underline{\tau}})) = \text{Mac}^5_{\text{k}_{\text{m}}}(\langle \text{GUTI}^{j_0}, \text{n}^{j_0}\rangle) \end{pmatrix}$$

Let $j_0 \in \mathbb{N}$. Using Proposition 25 on τ, we know that:

$$\text{inj-auth}_\tau(\text{ID}, j_0) \;\leftrightarrow\; \text{n}^{j_0} = \sigma^{\text{in}}_{\tau}(\text{e-auth}^{\text{ID}}_{\text{U}}) \tag{52}$$

Similarly, using Proposition 25 on $\underline{\tau}$ we have:

$$\text{inj-auth}_{\underline{\tau}}(\nu_\tau(\text{ID}), j_0) \;\leftrightarrow\; \mathsf{n}^{j_0} = \sigma^{\text{in}}_{\underline{\tau}}(\text{e-auth}^{\nu_\tau(\text{ID})}_{\text{U}}) \tag{53}$$

Let τ_0 be such that $\tau = \tau_0, \mathsf{ai}$. It is straightforward to check that for any $n \in \mathbb{N}$:

$$\underbrace{\left(\sigma_{\tau_0}(\text{e-auth}^{j_0}_{\text{N}}) = \text{UnknownId}\right)}_{\text{unk}} \;\leftrightarrow\; \bigwedge_{1 \leq i \leq B} \neg\text{net-e-auth}_\tau(\mathsf{A}_i, j_0)$$

$$\underbrace{\left(\sigma_{\underline{\tau_0}}(\text{e-auth}^{j_0}_{\text{N}}) = \text{UnknownId}\right)}_{\underline{\text{unk}}} \;\leftrightarrow\; \bigwedge_{1 \leq i \leq B} \neg\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j_0)$$

Since for all $1 \leq i \leq B$:

$$(\text{net-e-auth}_\tau(\mathsf{A}_i, j_0) \sim \underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j_0)) \in \text{reveal}_{\tau_0}$$

and since $\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \wedge \text{unk} \;\rightarrow\; \text{false}$ and $\text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}} \wedge \underline{\text{unk}} \;\rightarrow\; \text{false}$, we deduce that:

$$\dfrac{\dfrac{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, b_{j_i} \wedge \neg\text{unk} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}} \wedge \neg\underline{\text{unk}}}{\begin{array}{c}\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, \text{unk}, \text{false}, \text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \wedge \neg\text{unk} \\ \sim\phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \underline{\text{unk}}, \text{false}, \text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}} \wedge \neg\underline{\text{unk}}\end{array}}\,\text{Dup}^*}{\dfrac{\begin{array}{c}\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, \text{unk}, \text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \wedge \text{unk}, \text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \wedge \neg\text{unk} \\ \sim\phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \underline{\text{unk}}, \text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}} \wedge \underline{\text{unk}}, \text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}} \wedge \neg\underline{\text{unk}}\end{array}}{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, \text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}}}\,\text{FA}^*}\,R$$

From the definitions, we get that:

$$\left(\sigma^{\text{in}}_\tau(\text{b-auth}^{j_0}_{\text{N}}) = \text{ID}\right) \;\rightarrow\; \left(\sigma^{\text{in}}_\tau(\text{e-auth}^{j_0}_{\text{N}}) = \text{ID} \vee \sigma^{\text{in}}_\tau(\text{e-auth}^{j_0}_{\text{N}}) = \text{UnknownId}\right)$$

Therefore:

$$\left(\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \wedge \neg\text{unk}\right) \;\rightarrow\; \sigma^{\text{in}}_\tau(\text{e-auth}^{j_0}_{\text{N}}) = \text{ID} \;\rightarrow\; \text{net-e-auth}_\tau(\text{ID}, j_0)$$

Moreover:

$$\left(\text{net-e-auth}_\tau(\text{ID}, j_0) \;\rightarrow\; \left(\begin{array}{c}\text{GUTI}^{j_0} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\mathsf{n}^{j_0}) = [\text{net-e-auth}_\tau(\text{ID}, j_0)]\text{t-suci-}\oplus_\tau(\text{ID}, j_0) \\ \wedge\, \text{Mac}^5_{\mathsf{k_m}}(\langle \text{GUTI}^{j_0}, \mathsf{n}^{j_0}\rangle) = [\text{net-e-auth}_\tau(\text{ID}, j_0)]\text{t-mac}_\tau(\text{ID}, j_0)\end{array}\right)\right)$$

Using (52) and the observations above, we can rewrite $\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \wedge \neg\text{unk}$ as follows:

$$\text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \wedge \neg\text{unk} \;=\; \left(\begin{array}{l}\quad\mathsf{n}^{j_0} = \sigma^{\text{in}}_\tau(\text{e-auth}^{\text{ID}}_{\text{U}}) \;\wedge\; \neg\text{unk} \\ \wedge\, \pi_1(g(\phi^{\text{in}}_\tau)) = [\text{net-e-auth}_\tau(\text{ID}, j_0)]\text{t-suci-}\oplus_\tau(\text{ID}, j_0) \\ \wedge\, \pi_2(g(\phi^{\text{in}}_\tau)) = [\text{net-e-auth}_\tau(\text{ID}, j_0)]\text{t-mac}_\tau(\text{ID}, j_0)\end{array}\right)$$

Similarly, using (53), we can rewrite $\text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}} \wedge \neg\underline{\text{unk}}$ as follows:

$$\text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}} \wedge \neg\underline{\text{unk}} \;=\; \left(\begin{array}{l}\quad\mathsf{n}^{j_0} = \sigma^{\text{in}}_{\underline{\tau}}(\text{e-auth}^{\nu_\tau(\text{ID})}_{\text{U}}) \;\wedge\; \neg\underline{\text{unk}} \\ \wedge\, \pi_1(g(\phi^{\text{in}}_{\underline{\tau}})) = [\underline{\text{net-e-auth}_{\underline{\tau}}}(\text{ID}, j_0)]\underline{\text{t-suci-}\oplus_{\underline{\tau}}}(\text{ID}, j_0) \\ \wedge\, \pi_2(g(\phi^{\text{in}}_{\underline{\tau}})) = [\underline{\text{net-e-auth}_{\underline{\tau}}}(\text{ID}, j_0)]\underline{\text{t-mac}_{\underline{\tau}}}(\text{ID}, j_0)\end{array}\right)$$

We can now conclude the proof:

$$\dfrac{\dfrac{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\begin{array}{c}\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, \sigma_\tau(\text{e-auth}^{\text{ID}}_{\text{U}}), \left(\begin{array}{l}\mathsf{n}^{j_0}, \neg\text{unk}, \text{GUTI}^{j_0}, \\ {[\text{net-e-auth}_\tau(\text{ID}, j_0)]}\text{t-suci-}\oplus_\tau(\text{ID}, j_0), \\ {[\text{net-e-auth}_\tau(\text{ID}, j_0)]}\text{t-mac}_\tau(\text{ID}, j_0)\end{array}\right) \\ \sim\phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \sigma_{\underline{\tau}}(\text{e-auth}^{\nu_\tau(\text{ID})}_{\text{U}}), \left(\begin{array}{l}\mathsf{n}^{j_0}, \neg\underline{\text{unk}}, \text{GUTI}^{j_0}, \\ {[\underline{\text{net-e-auth}_{\underline{\tau}}}(\text{ID}, j_0)]}\underline{\text{t-suci-}\oplus_{\underline{\tau}}}(\text{ID}, j_0), \\ {[\underline{\text{net-e-auth}_{\underline{\tau}}}(\text{ID}, j_0)]}\underline{\text{t-mac}_{\underline{\tau}}}(\text{ID}, j_0)\end{array}\right)\end{array}}\,\text{Dup}^*}{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, \text{fu-tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau} \wedge \neg\text{unk} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \text{fu-tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau}} \wedge \neg\underline{\text{unk}}}\,R + \text{FA}^*$$

APPENDIX VI
PROOF OF LEMMA 15

The proof is by induction over τ. For $\tau = \epsilon$, we just need to check that the elements from Item 2 of Definition 46 are indistinguishable, which is obvious from the definition of σ_ϵ in Definition 43.

We now show the inductive case: let $\tau = \mathsf{ai}_0, \dots, \mathsf{ai}_n$ be a valid basic symbolic trace with at most C actions NS, and let $\underline{\mathsf{ai}_0}, \dots, \underline{\mathsf{ai}_n}$ be such that $\underline{\tau} = \underline{\mathsf{ai}_0}, \dots, \underline{\mathsf{ai}_n}$. Also let $\tau_0 = \mathsf{ai}_0, \dots, \mathsf{ai}_{n-1}$ and $\underline{\tau_0} = \underline{\mathsf{ai}_0}, \dots, \underline{\mathsf{ai}_{n-1}}$. We assume by induction that there exists a derivation of:

$$\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}$$

We do a case disjunction on the value of ai.

A. Case $\mathsf{ai} = \mathrm{NS}_{\mathrm{ID}}(j)$

We know that $\underline{\mathsf{ai}} = \mathrm{NS}_{\nu_{\underline{\tau}}(\mathrm{ID})}(j)$ and $\nu_\tau(\mathrm{ID}) = \mathsf{fresh\text{-}id}(\nu_{\tau_0}(\mathrm{ID}))$. Moreover, $\phi_\tau \equiv \phi_\tau^{\mathsf{in}}$ and $\phi_{\underline{\tau}} \equiv \phi_{\underline{\tau}}^{\mathsf{in}}$. Hence $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincide everywhere except on:

$$\sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \sim \sigma_{\underline{\tau}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \qquad \mathsf{sync\text{-}diff}_\tau^{\mathrm{ID}} \sim \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})} \qquad \mathsf{m\text{-}suci}_\tau^{\mathrm{ID}} \sim \mathsf{m\text{-}suci}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}$$

We can easily conclude with the following derivation:

$$\dfrac{\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{false}, \bot, \mathsf{false} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{false}, \bot, \mathsf{false}}\ \mathsf{Simp}}{\begin{array}{c}\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}), \mathsf{m\text{-}suci}_\tau^{\mathrm{ID}}, \mathsf{sync\text{-}diff}_\tau^{\mathrm{ID}} \\ \sim\ \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}), \mathsf{m\text{-}suci}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}, \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}\end{array}}\ R$$

B. Case $\mathsf{ai} = \mathrm{PN}(j, 0)$

We know that $\underline{\mathsf{ai}} = \mathrm{PN}(j, 0)$. Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides completely. Using invariant **(A1)** we know that $\mathsf{n}^j \not\in \mathsf{st}(\phi_\tau^{\mathsf{in}})$, and $\mathsf{n}^j \not\in \mathsf{st}(\phi_{\underline{\tau_0}})$. Therefore we conclude this case easily using the axiom Fresh:

$$\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n}^j \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{n}^j}\ \mathsf{Fresh}$$

C. Case $\mathsf{ai} = \mathrm{PU}_{\mathrm{ID}}(j, 1)$

We know that $\underline{\mathsf{ai}} = \mathrm{PU}_{\nu_\tau(\mathrm{ID})}(j, 1)$. Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on the pairs:

$$\sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \ \sim\ \sigma_{\underline{\tau}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \qquad \mathsf{m\text{-}suci}_\tau^{\mathrm{ID}} \ \sim\ \mathsf{m\text{-}suci}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})} \qquad \mathsf{sync\text{-}diff}_\tau^{\mathrm{ID}} \ \sim\ \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}$$

$$\sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) \ \sim\ \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \qquad \Big(\{\langle \mathrm{ID}\,,\, \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^j} \ \sim\ \{\langle \nu_\tau(\mathrm{ID})\,,\, \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^j}\Big)$$

$$\Big(\mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\mathrm{ID}}}(\langle \{\langle \mathrm{ID}\,,\, \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^j}\,,\, g(\phi_\tau^{\mathsf{in}})\rangle) \ \sim\ \mathsf{Mac}^1_{\mathsf{k}_{\mathsf{m}}^{\nu_\tau(\mathrm{ID})}}(\langle \{\langle \nu_\tau(\mathrm{ID})\,,\, \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})\rangle\}_{\mathsf{pk}_{\mathrm{N}}}^{\mathsf{n}_{\mathsf{e}}^j}\,,\, g(\phi_{\underline{\tau}}^{\mathsf{in}})\rangle)\Big)$$

a) Part 1: We know that $\sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}) \equiv \sigma_{\underline{\tau}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) \equiv \mathsf{false}$. We deduce that $\mathsf{m\text{-}suci}_\tau^{\mathrm{ID}} = \mathsf{m\text{-}suci}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})} = \bot$. It follows that we have the derivation:

$$\dfrac{\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{false}, \bot \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{false}, \bot}\ \mathsf{FA}^*}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma_\tau(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\mathrm{ID}}), \mathsf{m\text{-}suci}_\tau^{\mathrm{ID}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau}}(\mathsf{valid\text{-}guti}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}), \mathsf{m\text{-}suci}_{\underline{\tau}}^{\nu_\tau(\mathrm{ID})}}\ R \tag{54}$$

b) Part 2: We have:

$$\begin{array}{rcll}\sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) & = & \mathsf{suc}(\sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})) - \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) & = \mathbf{1} \\ \sigma_{\underline{\tau}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) & = & \mathsf{suc}(\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})})) - \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\nu_\tau(\mathrm{ID})}) & = \mathbf{1}\end{array}$$

And:

$$\begin{array}{rcl}\mathsf{sync\text{-}diff}_\tau^{\mathrm{ID}} & = & [\sigma_\tau(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})]\,(\sigma_\tau(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}}) - \sigma_\tau(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})) \\ & = & \big[\sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})\big]\,\big(\mathsf{suc}(\sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{U}}^{\mathrm{ID}})) - \sigma_\tau^{\mathsf{in}}(\mathrm{SQN}_{\mathrm{N}}^{\mathrm{ID}})\big) \\ & = & \big[\sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\mathrm{U}}^{\mathrm{ID}})\big]\,\big(\mathsf{suc}(\mathsf{sync\text{-}diff}_{\tau_0}^{\mathrm{ID}})\big)\end{array}$$

Similarly, $\text{sync-diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}} = \left[\sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\text{ID})}_{\text{U}})\right]\left(\text{suc}(\text{sync-diff}^{\nu_\tau(\text{ID})}_{\underline{\tau_0}})\right)$. Hence we have the derivation:

$$\dfrac{\dfrac{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, \sigma^{\text{in}}_\tau(\text{sync}^{\text{ID}}_{\text{U}}), \text{sync-diff}^{\text{ID}}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \sigma^{\text{in}}_{\underline{\tau}}(\text{sync}^{\nu_\tau(\text{ID})}_{\text{U}}), \text{sync-diff}^{\nu_\tau(\text{ID})}_{\underline{\tau_0}}}\ \text{Dup}^*}{\begin{array}{c}\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0},\ \text{sync-diff}^{\text{ID}}_\tau, \quad \sigma_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) - \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) \\ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},\ \text{sync-diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}, \sigma_{\underline{\tau}}(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{U}}) - \sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{U}})\end{array}}\ \text{Simp} \tag{55}$$

c) Part 3: Let $s_l \equiv \text{len}(\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})\rangle)$. Using the CCA1 axiom we directly have that:

$$\dfrac{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, s_l \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, s_l \qquad \dfrac{\overline{\text{len}(\text{ID}) = \text{len}(\nu_\tau(\text{ID}))} \qquad \text{len}(\sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})) = \text{len}(\sigma^{\text{in}}_\tau(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{U}}))}{\text{len}(\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})\rangle) = \text{len}(\langle \nu_\tau(\text{ID})\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{U}})\rangle)}}{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, \{\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^j_{\text{e}}}_{\text{pk}_{\text{N}}} \ \sim\ \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, \{\langle \nu_\tau(\text{ID})\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{U}})\rangle\}^{\text{n}^j_{\text{e}}}_{\text{pk}_{\text{N}}}}\ \text{CCA1} \tag{56}$$

Moreover, using Proposition 21, we know that:

$$\overline{\text{len}(\sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})) = \text{len}(\sigma^{\text{in}}_\tau(\text{SQN}^{\nu_\tau(\text{ID})}_{\text{U}}))}$$

Similarly, we can show that $s_l = \text{len}(\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{sqn-init}^{\text{ID}}_{\text{U}})\rangle)$. Since:

$$\big(\text{len}(\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{sqn-init}^{\text{ID}}_{\text{U}})\rangle), \text{len}(\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{sqn-init}^{\text{ID}}_{\text{U}})\rangle)\big) \in \text{reveal}_{\tau_0}$$

we know that:

$$\dfrac{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0} \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}}{\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}, s_l \sim \phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0}, s_l}\ R + \text{Dup}$$

This completes the derivation in 56.

d) Part 4: To conclude, it only remains to deal with the Mac^1 terms. We start by computing $\text{set-mac}^1_{\text{k}^{\text{ID}}_{\text{m}}}$:

$$\begin{aligned}\text{set-mac}^1_{\text{k}^{\text{ID}}_{\text{m}}}(\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}) \ = \ & \left\{\langle \{\langle \text{ID}\,,\, \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^{j_1}_{\text{e}}}_{\text{pk}_{\text{N}}}\,,\, g(\phi^{\text{in}}_{\tau_1})\rangle \mid \tau_1 = \_, \text{PU}_{\text{ID}}(j_1, 1) \prec \tau\right\} \\ \cup\ & \left\{\langle \pi_1(g(\phi^{\text{in}}_{\tau_1}))\,,\, \text{n}^{j_1}\rangle \mid \tau_1 = \_, \text{PN}(j_1, 1) \prec \tau\right\}\end{aligned}$$

We want to get rid of the second set above: using **(Equ3)**, we know that for every $\tau_1 = \_, \text{PN}(j_1, 1) \prec \tau$:

$$\text{accept}^{\text{ID}}_\tau \ \leftrightarrow \bigvee_{\substack{\tau_2 = \_, \text{PU}_{\text{ID}}(j_2, 1) \\ \tau_2 \prec_\tau \tau_1}} \begin{pmatrix} g(\phi^{\text{in}}_{\tau_2}) = \text{n}^j \wedge \pi_1(g(\phi^{\text{in}}_{\tau_1})) = \{\langle \text{ID}\,,\, \sigma^{\text{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^{j_2}_{\text{e}}}_{\text{pk}_{\text{N}}} \\ \wedge\ \pi_2(g(\phi^{\text{in}}_{\tau_1})) = \text{Mac}^1_{\text{k}^{\text{ID}}_{\text{m}}}(\langle \{\langle \text{ID}\,,\, \sigma^{\text{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^{j_2}_{\text{e}}}_{\text{pk}_{\text{N}}}\,,\, g(\phi^{\text{in}}_{\tau_2})\rangle)\end{pmatrix} \tag{57}$$

We let Ψ' be the vector of terms $\phi^{\text{in}}_\tau, \text{l-reveal}_{\tau_0}$ where we replaced every occurrence of $\text{accept}^{\text{ID}}_{\tau_1}$ (where $\tau_1 = \_, \text{PN}(j_1, 1) \prec \tau$) by the equivalent term from (57). We can check that we have:

$$\text{set-mac}^1_{\text{k}^{\text{ID}}_{\text{m}}}(\Psi') \ = \ \left\{\langle \{\langle \text{ID}\,,\, \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^{j_1}_{\text{e}}}_{\text{pk}_{\text{N}}}\,,\, g(\phi^{\text{in}}_{\tau_1})\rangle \mid \tau_1 = \_, \text{PU}_{\text{ID}}(j_1, 1) \prec \tau\right\}$$

For every $\tau_1 = \_, \text{PU}_{\text{ID}}(j_1, 1) \prec \tau$ it is easy to show using Proposition 21 that :

$$\text{len}(\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})\rangle) = \text{len}(\langle \text{ID}\,,\, \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle)$$

Moreover, using the axioms in Ax_{len} we know that $\text{len}(\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})\rangle) \neq 0$. Therefore, using Proposition 18 we get that we have:

$$\{\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^j_{\text{e}}}_{\text{pk}_{\text{N}}} \neq \{\langle \text{ID}\,,\, \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^{j_1}_{\text{e}}}_{\text{pk}_{\text{N}}}$$

Hence by left injectivity of $\langle \cdot\,,\, \_\rangle$:

$$\langle \{\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^j_{\text{e}}}_{\text{pk}_{\text{N}}}\,,\, g(\phi^{\text{in}}_\tau)\rangle \neq \langle \{\langle \text{ID}\,,\, \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^{j_1}_{\text{e}}}_{\text{pk}_{\text{N}}}\,,\, g(\phi^{\text{in}}_{\tau_1})\rangle$$

It follows that we can apply the PRF-MAC[1] axiom to replace the following term by a fresh nonce n:

$$\text{Mac}^1_{\text{k}^{\text{ID}}_{\text{m}}}(\langle \{\langle \text{ID}\,,\, \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\text{n}^j_{\text{e}}}_{\text{pk}_{\text{N}}}\,,\, g(\phi^{\text{in}}_\tau)\rangle)$$

We then rewrite every occurrence of the right-hand side of (57) into $\mathsf{accept}^{\text{ID}}_{\tau_1}$ (where $\tau_1 = \_, \text{PN}(j_1, 1) \prec \tau$). This yields the derivation:

$$\frac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0} \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\nu_\tau(\text{ID})}}(\langle\{\langle \nu_\tau(\text{ID}) \,,\, \sigma^{\mathsf{in}}_{\underline{\tau}}(\text{SQN}_\text{U}^{\nu_\tau(\text{ID})})\rangle\}^{\mathsf{n}_\mathsf{e}^j}_{\mathsf{pk}_\text{N}} \,,\, g(\phi^{\mathsf{in}}_{\underline{\tau}})\rangle)}{\begin{array}{c}\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0},\, \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\text{ID}}}(\langle\{\langle \text{ID} \,,\, \sigma^{\mathsf{in}}_\tau(\text{SQN}_\text{U}^{\text{ID}})\rangle\}^{\mathsf{n}_\mathsf{e}^j}_{\mathsf{pk}_\text{N}} \,,\, g(\phi^{\mathsf{in}}_\tau)\rangle) \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\, \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\nu_\tau(\text{ID})}}(\langle\{\langle \nu_\tau(\text{ID}) \,,\, \sigma^{\mathsf{in}}_{\underline{\tau}}(\text{SQN}_\text{U}^{\nu_\tau(\text{ID})})\rangle\}^{\mathsf{n}_\mathsf{e}^j}_{\mathsf{pk}_\text{N}} \,,\, g(\phi^{\mathsf{in}}_{\underline{\tau}})\rangle)\end{array}} \;\text{PRF-MAC}^1$$

We then do the same on the right side (we omit the details), and conclude using Fresh:

$$\frac{\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{n}}\;\mathsf{Fresh}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0} \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\nu_\tau(\text{ID})}}(\langle\{\langle \nu_\tau(\text{ID}) \,,\, \sigma^{\mathsf{in}}_{\underline{\tau}}(\text{SQN}_\text{U}^{\nu_\tau(\text{ID})})\rangle\}^{\mathsf{n}_\mathsf{e}^j}_{\mathsf{pk}_\text{N}} \,,\, g(\phi^{\mathsf{in}}_{\underline{\tau}})\rangle)} \;\text{PRF-MAC}^1$$

We conclude the proof by combining the derivation above with the derivations in (54), (55) and (56), and by using the induction hypothesis.

D. Case $\mathsf{ai} = \text{PN}(j, 1)$

We know that $\underline{\mathsf{ai}} = \text{PN}(j, 1)$. For every base identity ID, let M_ID be the set:

$$M_\text{ID} \;=\; \{\tau_2 \mid \tau_2 = \_, \text{PU}_\text{ID}(j_1, 1) \prec \tau \wedge \forall \tau_1 \text{ s.t. } \tau_1 \prec_\tau \tau_1\, \tau_1 \neq \_, \text{NS}_\text{ID}(\_)\}$$

Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on the following pairs:

$$\left(\mathsf{sync\text{-}diff}^{\text{ID}}_\tau \;\sim\; \mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}\right)_{\text{ID}\in\mathcal{S}_\mathsf{bid}} \qquad \left(\mathsf{net\text{-}e\text{-}auth}_\tau(\text{ID}, j) \;\sim\; \underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\text{ID}, j)\right)_{\text{ID}\in\mathcal{S}_\mathsf{bid}}$$

$$\left(\mathsf{Mac}^2_{\mathsf{k}_\mathsf{m}^{\text{ID}}}(\langle \mathsf{n}^j \,,\, \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}_\text{U}^{\text{ID}}))\rangle) \;\sim\; \mathsf{Mac}^2_{\mathsf{k}_\mathsf{m}^{\nu_\tau(\text{ID})}}(\langle \mathsf{n}^j \,,\, \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_2}}(\text{SQN}_\text{U}^{\nu_\tau(\text{ID})}))\rangle)\right)_{\tau_2\in M_\text{ID},\text{ID}\in\mathcal{S}_\mathsf{bid}}$$

a) Part 1: Let ID be a base identity. We consider all the new sessions started with identity ID in τ:

$$\{\text{NS}_\text{ID}(0), \dots, \text{NS}_\text{ID}(l_\text{ID})\} = \{\text{NS}_\text{ID}(i) \mid \text{NS}_\text{ID}(i) \in \tau\}$$

This induce a partition of symbolic actions in τ for identity ID. Indeed, let k be such that $\text{ID} = \mathsf{A}_{k,0}$, and for every $-1 \leq i \leq l_\text{ID}$, let $\underline{\text{ID}}_i = \mathsf{A}_{k,i+1}$. Then we define, for every $-1 \leq i \leq l_\text{ID}$:

$$T^i_\text{ID} \;=\; \left\{\tau_1 \mid \tau_1 = \_, \text{PU}_\text{ID}(j_1, 1) \wedge \begin{cases} \text{NS}_\text{ID}(i) \prec_\tau \tau_1 \prec_\tau \text{NS}_\text{ID}(i+1) & \text{if } 1 \leq i < l_\text{ID} \\ \tau_1 \prec_\tau \text{NS}_\text{ID}(0) & \text{if } i = -1 \\ \text{NS}_\text{ID}(l) \prec_\tau \tau_1 \prec \tau & \text{if } i = l \end{cases}\right\}$$

And $T_\text{ID} = \{\tau_1 \mid \tau_1 = \_, \text{PU}_\text{ID}(j_1, 1) \wedge \tau_1 \prec \tau\}$. We have $T_\text{ID} = \biguplus_{-1\leq i\leq l_\text{ID}} T^i_\text{ID}$, and for every $-1 \leq i \leq l_\text{ID}$:

$$\forall \tau_1 \in T^i_\text{ID},\, \nu_{\tau_1}(\text{ID}) = \underline{\text{ID}}_i \quad \text{ and } \quad T^i_\text{ID} \;=\; \left\{\tau_1 \mid \underline{\tau_1} = \_, \text{PU}_{\underline{\text{ID}}_i}(j_1, 1) \wedge \underline{\tau_1} \prec \underline{\tau_1}\right\}$$

b) Part 2: Using **(Equ3)** we know that:

$$\mathsf{accept}^{\text{ID}}_\tau \;\leftrightarrow\; \bigvee_{\tau_1 = \_, \text{PU}_\text{ID}(j_1,1)\in T_\text{ID}} \underbrace{\begin{pmatrix} g(\phi^{\mathsf{in}}_{\tau_1}) = \mathsf{n}^j \wedge \pi_1(g(\phi^{\mathsf{in}}_\tau)) = \{\langle \text{ID} \,,\, \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}_\text{U}^{\text{ID}})\rangle\}^{\mathsf{n}_\mathsf{e}^{j_1}}_{\mathsf{pk}_\text{N}} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_\tau)) = \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\text{ID}}}(\langle\{\langle \text{ID} \,,\, \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}_\text{U}^{\text{ID}})\rangle\}^{\mathsf{n}_\mathsf{e}^{j_1}}_{\mathsf{pk}_\text{N}} \,,\, g(\phi^{\mathsf{in}}_{\tau_1})\rangle) \end{pmatrix}}_{b^{\text{ID}}_{\tau_1}} \tag{58}$$

For all $\tau_1 \in T_\text{ID}$, we let $b^{\text{ID}}_{\tau_1}$ be the main term of the disjunction above.

Similarly, using **(Equ3)** on $\underline{\tau}$, which is a valid symbolic frame, we have that for every $-1 \leq i \leq l_\text{ID}$:

$$\mathsf{accept}^{\underline{\text{ID}}_i}_{\underline{\tau}} \;\leftrightarrow\; \bigvee_{\tau_1 = \_, \text{PU}_\text{ID}(j_1,1)\in T^i_\text{ID}} \underbrace{\begin{pmatrix} g(\phi^{\mathsf{in}}_{\underline{\tau_1}}) = \mathsf{n}^j \wedge \pi_1(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \{\langle \underline{\text{ID}}_i \,,\, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}_\text{U}^{\underline{\text{ID}}_i})\rangle\}^{\mathsf{n}_\mathsf{e}^{j_1}}_{\mathsf{pk}_\text{N}} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\underline{\tau}})) = \mathsf{Mac}^1_{\mathsf{k}_\mathsf{m}^{\underline{\text{ID}}_i}}(\langle\{\langle \underline{\text{ID}}_i \,,\, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}_\text{U}^{\underline{\text{ID}}_i})\rangle\}^{\mathsf{n}_\mathsf{e}^{j_1}}_{\mathsf{pk}_\text{N}} \,,\, g(\phi^{\mathsf{in}}_{\underline{\tau_1}})\rangle) \end{pmatrix}}_{\underline{b^{\underline{\text{ID}}_i}_{\tau_1}}} \tag{59}$$

Moreover, if we let $\{\underline{\text{ID}}_{l_\text{ID}+1}, \dots, \underline{\text{ID}}_m\}$ be such that:

$$\mathsf{copies\text{-}id}(\text{ID}) = \{\underline{\text{ID}}_0, \dots, \underline{\text{ID}}_{l_\text{ID}}\} \uplus \{\underline{\text{ID}}_{l_\text{ID}+1}, \dots, \underline{\text{ID}}_m\}$$

Then, for all $i > l_{\text{ID}}$, we have $\mathsf{accept}_{\underline{\tau}}^{\text{ID}_i} \leftrightarrow \mathsf{false}$. Therefore, using **(A5)**, we can show that:

$$\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}^{\text{ID}}} \leftrightarrow \bigvee_{-1 \leq i \leq l} \mathsf{accept}_{\underline{\tau}}^{\text{ID}_i} \tag{60}$$

c) Part 3: For every $\tau_1, \tau_2 \in T_{\text{ID}}$ such that $\tau_1 \neq \tau_2$, $\tau_1 = \_, \text{PU}_{\text{ID}}(j_1, 1)$ and $\tau_2 = \_, \text{PU}_{\text{ID}}(j_2, 1)$, using Proposition 18 and 21 we can show that:

$$\begin{aligned} b_{\tau_1}^{\text{ID}} \wedge b_{\tau_2}^{\text{ID}} &\rightarrow \{\langle \text{ID}\,,\, \sigma_{\tau_1}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}} = \{\langle \text{ID}\,,\, \sigma_{\tau_2}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_2}} \\ &\rightarrow \mathsf{false} \end{aligned} \tag{61}$$

Similarly, for every $\tau_1, \tau_2 \in T_{\text{ID}}^{\text{ID}_i}$ such that $\tau_1 \neq \tau_2$, $\tau_1 = \_, \text{PU}_{\text{ID}}(j_1, 1)$ and $\tau_2 = \_, \text{PU}_{\text{ID}}(j_2, 1)$, using Proposition 18 and 21 we have that:

$$\begin{aligned} \underline{b_{\underline{\tau_1}}^{\text{ID}_i}} \wedge \underline{b_{\underline{\tau_2}}^{\text{ID}_i}} &\rightarrow \{\langle \underline{\text{ID}}_i\,,\, \sigma_{\underline{\tau_1}}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}_i})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_1}} = \{\langle \underline{\text{ID}}_i\,,\, \sigma_{\underline{\tau_2}}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}_i})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_2}} \\ &\rightarrow \mathsf{false} \end{aligned} \tag{62}$$

Moreover, since for all identities $\text{ID}_1 \neq \text{ID}_2$, we have $\mathsf{eq}(\text{ID}_1, \text{ID}_2) = \mathsf{false}$ we know that:

$$(\mathsf{accept}_{\tau}^{\text{ID}_1} \wedge \mathsf{accept}_{\tau}^{\text{ID}_2}) = \mathsf{false} \qquad \left(\mathsf{accept}_{\underline{\tau}}^{\text{ID}_1} \wedge \mathsf{accept}_{\underline{\tau}}^{\text{ID}_2}\right) = \mathsf{false}$$

And for all non base identity ID, using **(Acc1)** we know that $\mathsf{accept}_{\tau}^{\text{ID}} \leftrightarrow \mathsf{false}$. We deduce that:

$$\left(\left((b_{\tau_1}^{\text{ID}})_{\tau_1 \in T_{\text{ID}}}\right)_{\text{ID} \in \mathcal{S}_{\mathsf{bid}}}, \underbrace{\textstyle\bigwedge_{\text{ID} \in \mathcal{S}_{\mathsf{bid}}} \neg \mathsf{accept}_{\tau}^{\text{ID}}}_{b_{\mathsf{unk}}}\right) \qquad \text{and} \qquad \left(\left((\underline{b_{\underline{\tau_1}}^{\text{ID}_i}})_{\substack{\tau_1 \in T_{\text{ID}}^{\text{ID}_i} \\ -1 \leq i \leq l_{\text{ID}}}}\right)_{\text{ID} \in \mathcal{S}_{\mathsf{bid}}}, \underbrace{\textstyle\bigwedge_{\text{ID} \in \mathcal{S}_{\mathsf{id}}} \neg \mathsf{accept}_{\tau}^{\text{ID}}}_{\underline{b_{\mathsf{unk}}}}\right)$$

are CS partitions. Besides, for all $\tau_1 \in T_{\text{ID}}$ we have:

$$\left[b_{\tau_1}^{\text{ID}}\right]\left(t_\tau = \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\tau_1}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}}))\rangle)\right) \qquad \text{and} \qquad [b_{\mathsf{unk}}]\,(t_\tau = \mathsf{UnknownId})$$

From Proposition 28 we deduce:

$$\begin{aligned} t_\tau = \ &\mathsf{if}\ \neg b_{\mathsf{unk}}\ \mathsf{then}\ \underset{\substack{\tau_1 \in T_{\text{ID}} \\ \text{ID} \in \mathcal{S}_{\mathsf{bid}}}}{\mathsf{case}}\,(b_{\tau_1}^{\text{ID}} : \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\tau_1}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}}))\rangle)) \\ &\mathsf{else}\ \mathsf{UnknownId} \end{aligned} \tag{63}$$

Similarly, for every $-1 \leq i \leq l$, for every $\tau_1 \in T_i^{\text{ID}}$:

$$\left[\underline{b_{\underline{\tau_1}}^{\text{ID}_i}}\right]\left(t_{\underline{\tau}} = \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}_i}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\underline{\tau_1}}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}_i}))\rangle)\right) \qquad \text{and} \qquad \left[\underline{b_{\mathsf{unk}}}\right]\left(t_{\underline{\tau}} = \mathsf{UnknownId}\right)$$

Again, from Proposition 28 we deduce:

$$\begin{aligned} t_{\underline{\tau}} = \ &\mathsf{if}\ \neg \underline{b_{\mathsf{unk}}}\ \mathsf{then}\ \underset{\substack{\tau_1 \in T_{\text{ID}}^{i} \\ -1 \leq i \leq l_{\text{ID}} \\ \text{ID} \in \mathcal{S}_{\mathsf{bid}}}}{\mathsf{case}}\,(\underline{b_{\underline{\tau_1}}^{\text{ID}_i}} : \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}_i}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\underline{\tau_1}}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}_i}))\rangle)) \\ &\mathsf{else}\ \mathsf{UnknownId} \end{aligned}$$

Since $T_{\text{ID}} = \biguplus_{-1 \leq i \leq l_{\text{ID}}} T_{\text{ID}}^{i}$, and since $\forall \tau_1 \in T_{\text{ID}}^{i}$, $\underline{\text{ID}}_i = \nu_{\tau_1}(\text{ID})$, we know that:

$$\begin{aligned} t_{\underline{\tau}} = \ &\mathsf{if}\ \neg \underline{b_{\mathsf{unk}}}\ \mathsf{then}\ \underset{\substack{\tau_1 \in T_{\text{ID}} \\ \text{ID} \in \mathcal{S}_{\mathsf{bid}}}}{\mathsf{case}}\,(\underline{b_{\underline{\tau_1}}^{\nu_{\tau_1}(\text{ID})}} : \mathsf{Mac}_{\mathsf{k}_{\mathsf{m}}^{\nu_{\tau_1}(\text{ID})}}^{2}(\langle \mathsf{n}^j\,,\, \mathsf{suc}(\sigma_{\underline{\tau_1}}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\nu_{\tau_1}(\text{ID})}))\rangle)) \\ &\mathsf{else}\ \mathsf{UnknownId} \end{aligned} \tag{64}$$

d) Part 4: We are going to show that for every $\text{ID} \in \mathcal{S}_{\mathsf{bid}}$, for every $\tau_1 = \text{PU}_{\text{ID}}(j_1, 1) \in T_{\text{ID}}$, there is a derivation of:

$$\Phi_{\tau_1} \quad \equiv \quad \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, b^{\text{ID}}_{\tau_1} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b^{\text{ID}_i}_{\underline{\tau_1}}}$$

For this, we rewrite $b^{\text{ID}}_{\tau_1}$ and $\underline{b^{\text{ID}_i}_{\underline{\tau_1}}}$ using, respectively, (58) and (59). First, remark that:

$$\frac{\phi^{\mathsf{in}}_{\tau} \sim \phi^{\mathsf{in}}_{\underline{\tau}}}{\phi^{\mathsf{in}}_{\tau}, \phi^{\mathsf{in}}_{\tau_1} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \phi^{\mathsf{in}}_{\underline{\tau_1}}} \ \mathsf{Dup}^*$$

And that the following pairs of terms are in reveal_{τ_0}:

$$(\mathsf{n}^j, \mathsf{n}^j) \qquad \Big(\{\langle \text{ID} , \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}}, \{\langle \nu_{\tau_1}(\text{ID}) , \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}}\Big)$$

$$\Big(\mathsf{Mac}^1_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle\{\langle \text{ID} , \sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}} , g(\phi^{\mathsf{in}}_{\tau_1})\rangle), \mathsf{Mac}^1_{\mathsf{k}^{\nu_{\tau_1}(\text{ID})}_{\mathsf{m}}}(\langle\{\langle \nu_{\tau_1}(\text{ID}) , \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}})\rangle\}^{\mathsf{n}^{j_1}_{\mathsf{e}}}_{\mathsf{pk}_{\text{N}}} , g(\phi^{\mathsf{in}}_{\underline{\tau_1}})\rangle)\Big)$$

Therefore:

$$\frac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, b^{\text{ID}}_{\tau_1} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b^{\text{ID}_i}_{\underline{\tau_1}}}} \ \mathsf{Simp} \tag{65}$$

Combining this with (58), (59) and (60), we have:

$$\cfrac{\cfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \Big(b^{\text{ID}}_{\underline{\tau_1}}\Big)_{\tau_1 \in T_{\text{ID}}} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \Big(\underline{b^{\text{ID}_i}_{\underline{\tau_1}}}\Big)_{\tau_1 \in T_{\text{ID}}}} \ \mathsf{Simp}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{net\text{-}e\text{-}auth}^{\text{ID}}_{\tau} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\mathsf{net\text{-}e\text{-}auth}^{\text{ID}}_{\underline{\tau}}}} \ \mathsf{Simp} \tag{66}$$

And:

$$\cfrac{\cfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \Big(b^{\text{ID}}_{\underline{\tau_1}}\Big)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \Big(\underline{b^{\text{ID}_i}_{\underline{\tau_1}}}\Big)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}}} \ \mathsf{Simp}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, b_{\mathsf{unk}} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b_{\mathsf{unk}}}} \ \mathsf{Simp} \tag{67}$$

We can now prove that $t_{\tau} \sim t_{\underline{\tau}}$. First we rewrite t_{τ} and $t_{\underline{\tau}}$ using, respectively, (63) and (64). Then we split the proof with FA, and combine it with (65) and (67). This yields:

$$\cfrac{\cfrac{\begin{array}{l}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \Big(\mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle)\Big)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}} \\ \sim \ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \Big(\mathsf{Mac}^2_{\mathsf{k}^{\nu_{\tau_1}(\text{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}}))\rangle)\Big)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}}\end{array}}{\begin{array}{l}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, b_{\mathsf{unk}}, \Big(b^{\text{ID}}_{\tau_1}, \mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle)\Big)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}} \\ \sim \ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{b_{\mathsf{unk}}}, \Big(\underline{b^{\nu_{\tau_1}(\text{ID})}_{\underline{\tau_1}}}, \mathsf{Mac}^2_{\mathsf{k}^{\nu_{\tau_1}(\text{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}}))\rangle)\Big)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}}\end{array}}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_{\tau} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}} \ \mathsf{Simp} \tag{68}$$

Notice that for every $\text{ID} \in \mathcal{S}_{\mathsf{bid}}$, $M_{\text{ID}} = T^{l_{\text{ID}}}_{\text{ID}}$. Therefore the Mac part in $\mathsf{reveal}_{\tau} \backslash \mathsf{reveal}_{\tau_0}$ appears in the derivation above, i.e.:

$$\begin{array}{ll} & \Big(\mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle), \mathsf{Mac}^2_{\mathsf{k}^{\nu_{\tau}(\text{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_2}}(\text{SQN}^{\nu_{\tau}(\text{ID})}_{\text{U}}))\rangle)\Big)_{\tau_2 \in M_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}} \\ \subseteq & \Big(\mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle), \mathsf{Mac}^2_{\mathsf{k}^{\nu_{\tau_1}(\text{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}}))\rangle)\Big)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}} \end{array} \tag{69}$$

e) Part 5: Let $\text{ID} \in \mathcal{S}_{\mathsf{bid}}$. Our goal is to apply the PRF-MAC^2 hypothesis to $\mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle)$ simultaneously for every $\tau_1 \in T_{\text{ID}}$ in:

$$\Psi \ \equiv \ \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \Big(\mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle)\Big)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}}$$

Using **(Equ2)** we know that for every $\text{NS}_{\text{ID}}(l_{\text{ID}}) \prec_{\tau} \tau_i = \_, \text{PU}_{\text{ID}}(j_i, 2)$:

$$\mathsf{accept}^{\text{ID}}_{\tau_i} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{PN}(j_1, 1) \\ \tau_2 = \_, \text{PU}_{\text{ID}}(j_i, 1) \\ \tau_2 \prec_{\tau} \tau_1 \prec \tau}} g(\phi^{\mathsf{in}}_{\tau}) = \mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1} , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle) \ \wedge \ g(\phi^{\mathsf{in}}_{\tau_2}) = \mathsf{n}^{j_1} \tag{70}$$

Let Ψ' be the formula obtained from Ψ by rewriting every $\mathsf{accept}^{\text{ID}}_{\tau_i}$ s.t. $\text{NS}_{\text{ID}}(l_{\text{ID}}) \prec_\tau \tau_i = \_, \text{PU}_{\text{ID}}(j_i, 2)$ using the equation above. Then we can check that for every $\tau_1 \in T_{\text{ID}}$, there is only one occurrence of $\mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle)$ in Ψ'. Moreover:

$$\begin{aligned}\mathsf{set\text{-}mac}^2_{\text{ID}}(\Psi') \setminus \{\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle\} \;\; = \;\; & \big\{\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle \mid \tau_2 \in T_{\text{ID}} \wedge \tau_1 \neq \tau_2\big\} \\ \cup \; & \big\{\langle \mathsf{n}^{j_0} , \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_i})), \mathsf{sk}_{\text{N}})))\rangle \mid \tau_i = \_, \text{PN}(j_0, 1) \prec \tau\big\}\end{aligned}$$

To apply the PRF-MAC^2 axioms, it is sufficient to show that for every element u in the set above, we have $(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle \neq u$:

- Using **(A2)** we know that for every $\tau_1, \tau_2 \in T_{\text{ID}}$, if $\tau_1 \neq \tau_2$ then $\sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}})) \neq \sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}))$. Therefore:
$$\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle \;\neq\; \langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle$$
- for every $\tau_i = \_, \text{PN}(j_0, 1) \prec \tau$, we have $j_0 < j$, hence $\mathsf{n}^{j_0} \neq \mathsf{n}^j$ and by consequence:
$$\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle \;\neq\; \langle \mathsf{n}^{j_0} , \mathsf{suc}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau_i})), \mathsf{sk}_{\text{N}})))\rangle$$

We can conclude: we rewrite Ψ into Ψ'; we apply PRF-MAC^2 for every $\tau_1 \in T_{\text{ID}}$, replacing $\mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle)$ by a fresh nonce n^{j,τ_1}; and we rewrite any term of the form (70) back into $\mathsf{accept}^{\text{ID}}_{\tau_i}$. Doing this for every base identity $\text{ID} \in \mathcal{S}_{\mathsf{bid}}$, this yields:

$$\dfrac{\begin{array}{l}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{n}^{j,\tau_1}\right)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}} \\ \sim \; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}^{\nu_{\tau_1}(\text{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}}))\rangle)\right)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}}\end{array}}{\begin{array}{l}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}))\rangle)\right)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}} \\ \sim \; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}^{\nu_{\tau_1}(\text{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}}))\rangle)\right)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}}\end{array}} \; (\text{PRF-MAC}^2)^*$$

We then do the same thing to replace, for every base identity ID and $\tau_1 \in T_{\text{ID}}$, the mac $\mathsf{Mac}^2_{\mathsf{k}^{\nu_{\tau_1}(\text{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}}))\rangle)$ by the nonce n^{j,τ_1} in the formula:

$$\underline{\Psi} \;\equiv\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}^{\nu_{\tau_1}(\text{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}}))\rangle)\right)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}}$$

The proof is similar, we omit to check the details. This yields:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{n}^{j,\tau_1}\right)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{n}^{j,\tau_1}\right)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}}}\;\mathsf{Fresh}^*}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{n}^{j,\tau_1}\right)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^2_{\mathsf{k}^{\nu_{\tau_1}(\text{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^j , \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\text{SQN}^{\nu_{\tau_1}(\text{ID})}_{\text{U}}))\rangle)\right)_{\tau_1 \in T_{\text{ID}}, \text{ID} \in \mathcal{S}_{\mathsf{bid}}}} \; (\text{PRF-MAC}^2)^*$$

Combining this with (68), we get:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\vdots}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}} \; \mathsf{Simp}^* \tag{71}$$

f) Part 6: We now handle the $\mathsf{sync\text{-}diff}^{\text{ID}}_\tau \sim \mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}$ part. We first handle the case where $\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})$ is false. Observe that $\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) = \sigma^{\mathsf{in}}_{\tau_0}(\mathsf{sync}^{\text{ID}}_{\text{U}})$, $\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}}) = \sigma^{\mathsf{in}}_{\underline{\tau_0}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}})$ and that $(\sigma^{\mathsf{in}}_{\tau_0}(\mathsf{sync}^{\text{ID}}_{\text{U}}), \sigma^{\mathsf{in}}_{\underline{\tau_0}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}})) \in \mathsf{reveal}_{\tau_0}$. Moreover:

$$[\neg\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_\tau \;=\; \bot \qquad\qquad [\neg\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}} \;=\; \bot$$

Hence:

$$\dfrac{\dfrac{\mathsf{l\text{-}reveal}_{\tau_0}, [\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_\tau \;\sim\; \mathsf{r\text{-}reveal}_{\tau_0}, [\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}}{\begin{array}{l}\mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}), \quad [\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_\tau, \quad [\neg\sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_\tau \\ \sim\; \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}}), [\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}, [\neg\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}\end{array}}\;\mathsf{Simp}}{\mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}^{\text{ID}}_\tau \;\sim\; \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}} \; \mathsf{FA}^* \tag{72}$$

Therefore we can focus on the case where $\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})$ is true. For all $\mathrm{ID} \in \mathcal{S}_{\mathsf{bid}}$, we let:

$$\mathsf{inc}\text{-}\mathrm{SQN}^{\mathrm{ID}}_{\tau} \;\equiv\; \mathsf{geq}(\pi_2(\mathsf{dec}(\pi_1(g(\phi^{\mathsf{in}}_{\tau})), \mathsf{sk}^{\mathrm{ID}}_{\mathrm{N}})), \sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}))$$

Then:

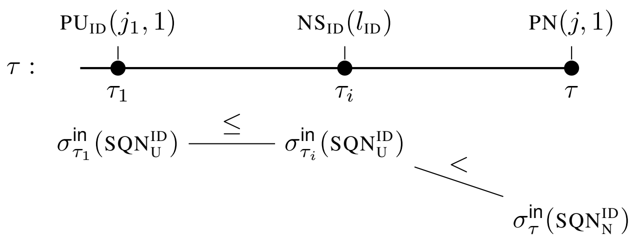
$$[\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\mathrm{ID}}_{\tau} \;=\; \underset{\tau_1 \in T_{\mathrm{ID}}}{\mathsf{case}} \left(b^{\mathrm{ID}}_{\tau_1} : \begin{array}{r} \mathsf{if} \begin{pmatrix} \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \\ \wedge\, \mathsf{inc}\text{-}\mathrm{SQN}^{\mathrm{ID}}_{\tau} \end{pmatrix} \mathsf{then}\ \sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) - \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}})) \\ \mathsf{else}\ [\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\mathrm{ID}}_{\tau_0} \end{array} \right) \tag{73}$$

And:

$$[\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} \;=$$
$$\underset{\tau_1 \in T^{\mathrm{ID}}_{\mathrm{ID}} l_{\mathrm{ID}}}{\mathsf{case}} \left(\underline{b^{\nu_\tau(\mathrm{ID})}_{\tau_1}} : \begin{array}{r} \mathsf{if} \begin{pmatrix} \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \\ \wedge\, \mathsf{inc}\text{-}\mathrm{SQN}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} \end{pmatrix} \mathsf{then}\ \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathrm{SQN}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) - \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathrm{SQN}^{\nu_\tau(\mathrm{ID})}_{\mathrm{N}})) \\ \mathsf{else}\ [\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}} \end{array} \right) \tag{74}$$

Take $\tau_1 \in T_{\mathrm{ID}}$, and let τ_i be such that $\tau_i = \_, \mathrm{NS}_{\mathrm{ID}}(l_{\mathrm{ID}})$ and $\tau_i \prec \tau$. We have two cases:

- If $\tau_1 \prec_\tau \mathrm{NS}_{\mathrm{ID}}(l_{\mathrm{ID}})$, then using **(B1)** and **(B6)**, we know that $\sigma^{\mathsf{in}}_{\tau_1}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}) \leq \sigma^{\mathsf{in}}_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$ and that $\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \rightarrow \sigma^{\mathsf{in}}_{\tau}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{N}}) > \sigma^{\mathsf{in}}_{\tau_i}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})$. We summarize this below:



  Hence $\neg(b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{inc}\text{-}\mathrm{SQN}^{\mathrm{ID}}_{\tau})$.
  Now we look at the right protocol: since $\tau_1 \prec_\tau \mathrm{NS}_{\mathrm{ID}}(l_{\mathrm{ID}})$, we know that $\nu_{\tau_1}(\mathrm{ID}) = \underline{\mathrm{ID}}_{l_{\mathrm{ID}}-p}$ for some $p > 0$. Hence $\nu_{\tau_1}(\mathrm{ID}) \neq \underline{\mathrm{ID}}_{l_{\mathrm{ID}}} = \nu_\tau(\mathrm{ID})$, which implies that:

$$\underline{b^{\nu_{\tau_1}(\mathrm{ID})}_{\tau_1}} \;\rightarrow\; \mathsf{accept}^{\nu_{\tau_1}(\mathrm{ID})}_{\underline{\tau}} \;\rightarrow\; \neg\mathsf{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} \;\rightarrow\; \bigwedge_{\tau_2 \in T^{l_{\mathrm{ID}}}_{\mathrm{ID}}} \neg\underline{b^{\nu_\tau(\mathrm{ID})}_{\tau_2}}$$

  We deduce that:

$$[b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\mathrm{ID}}_{\tau} \;=\; [b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\mathrm{ID}}_{\tau_0}$$
$$[\underline{b^{\nu_{\tau_1}(\mathrm{ID})}_{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} \;=\; [\underline{b^{\nu_{\tau_1}(\mathrm{ID})}_{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}}$$

  Since $(\mathsf{sync}\text{-}\mathsf{diff}^{\mathrm{ID}}_{\tau_0}, \mathsf{sync}\text{-}\mathsf{diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}}) \in \mathsf{reveal}_{\tau_0}$, we have:

$$\dfrac{\dfrac{\mathsf{l}\text{-}\mathsf{reveal}_{\tau_0}, b^{\mathrm{ID}}_{\tau_1} \;\sim\; \mathsf{r}\text{-}\mathsf{reveal}_{\tau_0}, \underline{b^{\nu_{\tau_1}(\mathrm{ID})}_{\tau_1}}}{\mathsf{l}\text{-}\mathsf{reveal}_{\tau_0}, b^{\mathrm{ID}}_{\tau_1}, \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}), \mathsf{sync}\text{-}\mathsf{diff}^{\mathrm{ID}}_{\tau_0} \;\sim\; \mathsf{r}\text{-}\mathsf{reveal}_{\tau_0}, \underline{b^{\nu_{\tau_1}(\mathrm{ID})}_{\tau_1}}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}), \mathsf{sync}\text{-}\mathsf{diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}}}\ \mathsf{Dup}^*}{\mathsf{l}\text{-}\mathsf{reveal}_{\tau_0}, [b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\mathrm{ID}}_{\tau} \;\sim\; \mathsf{r}\text{-}\mathsf{reveal}_{\tau_0}, [\underline{b^{\nu_{\tau_1}(\mathrm{ID})}_{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}\ \mathsf{FA}^*$$

  Combining this with (65), we can get rid of $b^{\mathrm{ID}}_{\tau_1} \sim \underline{b^{\nu_{\tau_1}(\mathrm{ID})}_{\tau_1}}$:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l}\text{-}\mathsf{reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r}\text{-}\mathsf{reveal}_{\tau_0}}{\vdots}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l}\text{-}\mathsf{reveal}_{\tau_0}, [b^{\mathrm{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\mathrm{ID}}_{\tau} \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r}\text{-}\mathsf{reveal}_{\tau_0}, [\underline{b^{\nu_{\tau_1}(\mathrm{ID})}_{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync}\text{-}\mathsf{diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}\end{array}}\ \mathsf{FA}^* \tag{75}$$

- If $\tau_1 \not\preceq_\tau \text{NS}_{\text{ID}}(l_{\text{ID}})$, then $\nu_{\tau_1}(\text{ID}) = \nu_\tau(\text{ID})$. Let $\underline{\text{ID}} = \nu_\tau(\text{ID})$, and using (73) and (74) we get that:

$$\begin{aligned}
[b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_\tau = \quad & [b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})]\left(\sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) - \mathsf{suc}(\sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{N}}))\right)\\
& + \text{if } b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\text{ID}}_\tau \text{ then } \mathbf{-1} \text{ else } \mathbf{0}\\
[b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\underline{\text{ID}}}_{\underline{\tau}} = \quad & \left[b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}})\right]\left(\sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) - \mathsf{suc}(\sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}}))\right)\\
& + \text{if } b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\underline{\text{ID}}}_{\underline{\tau}} \text{ then } \mathbf{-1} \text{ else } \mathbf{0}
\end{aligned}$$

Hence using (65) we get:

$$\dfrac{\dfrac{\phi^{\text{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\text{ID}}_\tau \;\sim\; \phi^{\text{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\underline{\text{ID}}}_{\underline{\tau}}}{\begin{array}{c}\phi^{\text{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, b^{\text{ID}}_{\tau_1}, \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}), \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) - \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{N}}), b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\text{ID}}_\tau\\ \sim\; \phi^{\text{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, b^{\underline{\text{ID}}}_{\underline{\tau_1}}, \sigma^{\text{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}), \sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) - \sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}}), b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\underline{\text{ID}}}_{\underline{\tau}}\end{array}}\,\textsf{Dup}}{\phi^{\text{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, [b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_\tau \;\sim\; \phi^{\text{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, [b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\underline{\text{ID}}}_{\underline{\tau}}}\,\textsf{FA}^* \tag{76}$$

We split the proof in two, depending on whether $\sigma^{\text{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}})$ is true or not.

  – If it is true, this is simple:

$$\begin{gathered}
\left(\sigma^{\text{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\text{ID}}_\tau\right) \leftrightarrow \left(b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{N}})\right)\\
\left(\sigma^{\text{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\underline{\text{ID}}}_{\underline{\tau}}\right) \leftrightarrow \left(b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\underline{\tau_1}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) < \sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}})\right)
\end{gathered}$$

  Hence using (65) we get:

$$\dfrac{\dfrac{\begin{array}{c}\phi^{\text{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\text{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{N}})\\ \sim\; \phi^{\text{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\text{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\underline{\tau_1}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) < \sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}})\end{array}}{\begin{array}{c}\phi^{\text{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{N}})\\ \sim\; \phi^{\text{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\underline{\tau_1}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) < \sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}})\end{array}}\,\textsf{Simp}}{\begin{array}{c}\phi^{\text{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\text{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge b^{\text{ID}}_{\tau_1} \wedge \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\text{ID}}_\tau\\ \sim\; \phi^{\text{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\text{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge b^{\underline{\text{ID}}}_{\underline{\tau_1}} \wedge \sigma^{\text{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \mathsf{inc\text{-}SQN}^{\underline{\text{ID}}}_{\underline{\tau}}\end{array}}\,R$$

  We conclude the case $\sigma^{\text{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}})$ using **(Der1)**:

$$\dfrac{\mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{c}\phi^{\text{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\text{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{N}})\\ \sim\; \phi^{\text{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\text{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\underline{\tau_1}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) < \sigma^{\text{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{N}})\end{array}}\,\textsf{Simp} \tag{77}$$

  – If $\mathsf{sync}^{\text{ID}}_{\text{U}}$ is false at τ_1 and true at τ, then we know that there is an instant $\tau_1 \preceq \tau_a$ such that $\neg\sigma^{\text{in}}_{\tau_a}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\text{in}}_{\tau_a}(\mathsf{sync}^{\text{ID}}_{\text{U}})$. Since $\mathsf{sync}^{\text{ID}}_{\text{U}}$ is only updated at instant $\text{PU}_{\text{ID}}(\_,\_)$ and $\text{NS}_{\text{ID}}(\_)$, and since $\tau_1 \not\preceq_\tau \text{NS}_{\text{ID}}(\_)$, the only possibilities are τ_a of the form $\_, \text{PU}_{\text{ID}}(j_a, 2)$. In that case, we must have $\mathsf{accept}^{\text{ID}}_{\tau_a}$. Formally, it is straightforward to show by induction that:

$$\left(b^{\text{ID}}_{\tau_1} \wedge \neg\sigma^{\text{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\text{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})\right) \;\rightarrow \bigvee_{\substack{\tau_a = \_, \text{PU}_{\text{ID}}(j_a, 2)\\ \tau_1 \prec_\tau \tau_a}} \neg\sigma^{\text{in}}_{\tau_a}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{accept}^{\text{ID}}_{\tau_a} \tag{78}$$

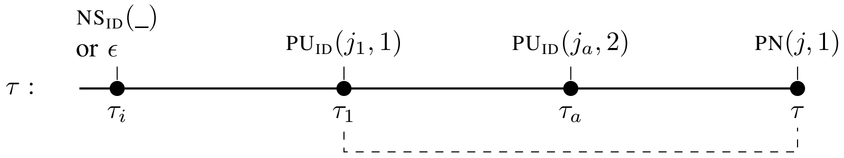
  Using **(StrEqu4)**, we know that:

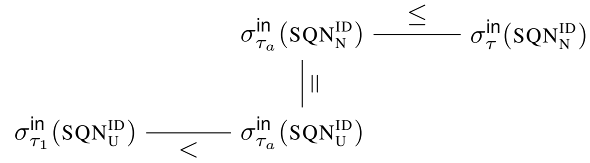
$$\mathsf{accept}^{\text{ID}}_{\tau_a} \wedge \neg\sigma^{\text{in}}_{\tau_a}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \;\rightarrow\; \sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{N}})$$

  We know that $\sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma^{\text{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}})$ and $\sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\text{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{N}})$. Moreover using **(B1)** we have:

$$\sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) \leq \sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) \qquad\qquad \sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\text{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{N}})$$

  Finally, we know that $\sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) = \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) + 1$, and therefore $\sigma_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}}) > \sigma^{\text{in}}_{\tau_1}(\text{SQN}^{\text{ID}}_{\text{U}})$. We summarize this graphically:





Therefore:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau_a}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{accept}^{\text{ID}}_{\tau_a}\right) \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau_a}(\mathsf{sync}^{\text{ID}}_{\text{N}})$$

Hence we deduce from (78) that:

$$\left(b^{\text{ID}}_{\tau_1} \wedge \neg\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}})\right) \;\rightarrow\; \mathsf{inc}\text{-}\text{SQN}^{\text{ID}}_{\tau}$$

Similarly, we show that:

$$\left(\underline{b^{\text{ID}}_{\tau_1}} \wedge \neg\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}})\right) \;\rightarrow\; \mathsf{inc}\text{-}\text{SQN}^{\underline{\text{ID}}}_{\underline{\tau}}$$

Hence using (65) we get:

$$\dfrac{\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}), b^{\text{ID}}_{\tau_1}, \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}), \underline{b^{\text{ID}}_{\tau_1}}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}})}\;\mathsf{Dup}^*}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge b^{\text{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \underline{b^{\text{ID}}_{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}})\end{array}}\;\mathsf{Simp}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge b^{\text{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge \mathsf{inc}\text{-}\text{SQN}^{\text{ID}}_{\tau} \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \neg\sigma^{\mathsf{in}}_{\underline{\tau_1}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \underline{b^{\text{ID}}_{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \mathsf{inc}\text{-}\text{SQN}^{\underline{\text{ID}}}_{\underline{\tau}}\end{array}}\;R \tag{79}$$

Combining (77), (79) with (65) and (76), it is easy to build a derivation of the form:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\vdots}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, [b^{\text{ID}}_{\tau_1} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_{\tau} \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, [\underline{b^{\nu_{\tau_1}(\text{ID})}_{\tau_1}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\underline{\text{ID}}}_{\underline{\tau}}\end{array}}\;\mathsf{FA}^* \tag{80}$$

g) Part 7: Now it only remains to put everything together. First combining (65), (75) and (80), we get:

$$\dfrac{\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\vdots}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(b^{\text{ID}}_{\tau_1}, [\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}) \wedge b^{\text{ID}}_{\tau_1}]\mathsf{sync\text{-}diff}^{\text{ID}}_{\tau}\right)_{\tau_1 \in T_{\text{ID}}} \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\underline{b^{\nu_{\tau_1}(\text{ID})}_{\tau_1}}, [\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}}) \wedge \underline{b^{\nu_{\tau_1}(\text{ID})}_{\tau_1}}]\mathsf{sync\text{-}diff}^{\underline{\text{ID}}}_{\underline{\tau}}\right)_{\tau_1 \in T_{\text{ID}}}\end{array}}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, [\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_{\tau} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, [\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\underline{\text{ID}}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\underline{\text{ID}}}_{\underline{\tau}}}\;\mathsf{FA}^*$$

Combine with (72), this yields:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\vdots}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}^{\text{ID}}_{\tau} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}^{\underline{\text{ID}}}_{\underline{\tau}}}\;\mathsf{FA}^* \tag{81}$$

We conclude the proof of this case by combining (66), (71), and (81) (recall that the Mac in $\mathsf{reveal}_{\tau} \backslash \mathsf{reveal}_{\tau_0}$ where handled in (69)).

E. Case $\mathsf{ai} = \text{PU}_{\text{ID}}(j, 2)$

We know that $\underline{\mathsf{ai}} = \text{PU}_{\nu_\tau(\text{ID})}(j, 2)$. Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on the pairs:

$$\mathsf{sync\text{-}diff}_\tau^{\text{ID}} \sim \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\text{ID})} \qquad \sigma_\tau(\mathsf{e\text{-}auth}_{\text{U}}^{\text{ID}}) \sim \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}_{\text{U}}^{\nu_\tau(\text{ID})}) \qquad \sigma_\tau(\mathsf{sync}_{\text{U}}^{\text{ID}}) \sim \sigma_{\underline{\tau}}(\mathsf{sync}_{\text{U}}^{\nu_\tau(\text{ID})})$$

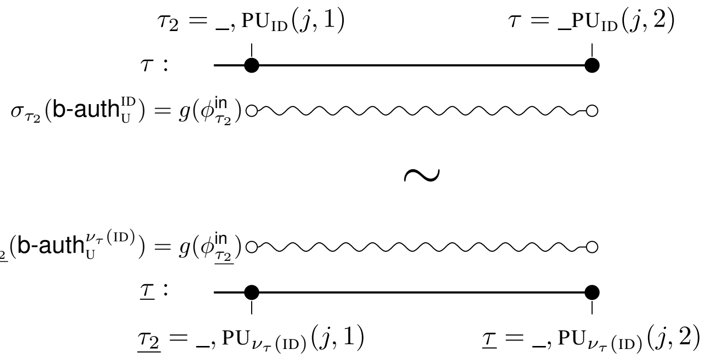
Therefore we are looking for a derivation of:

$$\Phi \equiv \begin{array}{c} \phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_\tau^{\text{ID}}, \sigma_\tau(\mathsf{e\text{-}auth}_{\text{U}}^{\text{ID}}), \sigma_\tau(\mathsf{sync}_{\text{U}}^{\text{ID}}), \mathsf{accept}_\tau^{\text{ID}} \\ \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\text{ID})}, \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}_{\text{U}}^{\nu_\tau(\text{ID})}), \sigma_{\underline{\tau}}(\mathsf{sync}_{\text{U}}^{\nu_\tau(\text{ID})}), \mathsf{accept}_{\underline{\tau}}^{\nu_\tau(\text{ID})} \end{array} \tag{82}$$

Let $\tau_2 = \_, \text{PU}_{\text{ID}}(j, 1) \prec \tau$. We know that $\tau_2 \not\prec_\tau \text{NS}_{\text{ID}}(\_)$, and therefore $\underline{\tau_2} = \_, \text{PU}_{\nu_\tau(\text{ID})}(j, 1)$. We also know that:

$$\sigma_\tau^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}}) \equiv \sigma_{\tau_2}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}}) \equiv g(\phi_{\tau_2}^{\mathsf{in}}) \qquad \sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{b\text{-}auth}_{\text{U}}^{\nu_\tau(\text{ID})}) \equiv \sigma_{\underline{\tau_2}}(\mathsf{b\text{-}auth}_{\text{U}}^{\nu_\tau(\text{ID})}) \equiv g(\phi_{\underline{\tau_2}}^{\mathsf{in}})$$

We summarize this graphically:



Hence we can start deconstructing the terms using FA and simplifying with Dup:

$$\dfrac{\dfrac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_\tau^{\text{ID}}, \mathsf{accept}_\tau^{\text{ID}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\text{ID})}, \mathsf{accept}_{\underline{\tau}}^{\nu_\tau(\text{ID})}}{\begin{array}{c}\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\text{ID}}, \mathsf{accept}_\tau^{\text{ID}}, g(\phi_{\tau_2}) \\ \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\text{ID})}, \mathsf{accept}_{\underline{\tau}}^{\nu_\tau(\text{ID})}, g(\phi_{\underline{\tau_2}})\end{array}} \text{ Simp}}{\Phi} \text{ Simp}$$

a) Part 1: We now focus on $\mathsf{accept}_\tau^{\text{ID}}$. Let:

$$T = \{\tau_1 \mid \tau_1 = \_, \text{PN}(j_1, 1) \wedge \tau_2 \prec_\tau \tau_1 \prec \tau\}$$

Using **(Equ2)** we know that:

$$\mathsf{accept}_\tau^{\text{ID}} \leftrightarrow \bigvee_{\tau_1 = \_, \text{PN}(j_1,1) \in T} \underbrace{\begin{pmatrix} g(\phi_\tau^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}(\langle \mathsf{n}^{j_1}, \mathsf{suc}(\sigma_{\tau_2}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}}))\rangle) \wedge g(\phi_{\tau_2}^{\mathsf{in}}) = \mathsf{n}^{j_1} \\ \wedge\ \pi_1(g(\phi_{\tau_1}^{\mathsf{in}})) = \{\langle \text{ID}, \sigma_{\tau_2}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}} \end{pmatrix}}_{\mathsf{supi\text{-}tr}_{\mathsf{u}:\tau_2,\tau}^{\mathsf{n}:\tau_1}} \tag{83}$$

Using again **(Equ2)** on $\underline{\tau}$ (which is a valid symbolic trace) we also have:

$$\mathsf{accept}_{\underline{\tau}}^{\nu_\tau(\text{ID})} \leftrightarrow \bigvee_{\tau_1 = \_, \text{PN}(j_1,1) \in T} \underbrace{\begin{pmatrix} g(\phi_{\underline{\tau}}^{\mathsf{in}}) = \mathsf{Mac}^2_{\mathsf{k}_{\mathsf{m}}^{\nu_\tau(\text{ID})}}(\langle \mathsf{n}^{j_1}, \mathsf{suc}(\sigma_{\underline{\tau_2}}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\nu_\tau(\text{ID})}))\rangle) \wedge g(\phi_{\underline{\tau_2}}^{\mathsf{in}}) = \mathsf{n}^{j_1} \\ \wedge\ \pi_1(g(\phi_{\underline{\tau_1}}^{\mathsf{in}})) = \{\langle \text{ID}^{\nu_\tau(\text{ID})}, \sigma_{\underline{\tau_2}}^{\mathsf{in}}(\text{SQN}_{\text{U}}^{\nu_\tau(\text{ID})})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j}} \end{pmatrix}}_{\mathsf{supi\text{-}tr}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}^{\mathsf{n}:\underline{\tau_1}}}$$

b) Part 2: We focus on $\mathsf{sync\text{-}diff}_\tau^{\text{ID}}$. First we get rid of the case where $\sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\text{U}}^{\text{ID}})$ is true. Indeed, we have:

$$[\sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\text{U}}^{\text{ID}})]\mathsf{sync\text{-}diff}_\tau^{\text{ID}} = [\sigma_\tau^{\mathsf{in}}(\mathsf{sync}_{\text{U}}^{\text{ID}})]\mathsf{suc}(\mathsf{sync\text{-}diff}_{\tau_0}^{\text{ID}})$$

$$[\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\text{U}}^{\nu_\tau(\text{ID})})]\mathsf{sync\text{-}diff}_{\underline{\tau}}^{\nu_\tau(\text{ID})} = [\sigma_{\underline{\tau}}^{\mathsf{in}}(\mathsf{sync}_{\text{U}}^{\nu_\tau(\text{ID})})]\mathsf{suc}(\mathsf{sync\text{-}diff}_{\underline{\tau_0}}^{\nu_\tau(\text{ID})})$$

And:

$$\left(\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_0}, \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}}\right) \in \mathsf{reveal}_{\tau_0} \qquad \left(\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})\right) \in \mathsf{reveal}_{\tau_0}$$

Therefore:

$$\frac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, [\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, [\neg\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}} \;\mathsf{Simp}$$

Similarly:

$$[\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \neg\mathsf{accept}^{\mathrm{ID}}_{\tau}]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} \;=\; \bot \qquad [\neg\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \wedge \neg\mathsf{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} \;=\; \bot$$

Hence we can go one step further:

$$\frac{\dfrac{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}, [\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge b_{\tau_1}]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau}\right)_{\tau_1\in T}\\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}, [\neg\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \wedge \underline{b}_{\underline{\tau_1}},]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}\right)_{\tau_1\in T}\end{array}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\mathrm{ID}}_{\tau}, \quad [\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{accept}^{\mathrm{ID}}_{\tau}]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau}\\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}, [\neg\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \wedge \mathsf{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}\end{array}} \;\mathsf{Simp}^*}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\mathrm{ID}}_{\tau}, \quad \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau}\\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}, \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}\end{array}} \;\mathsf{Simp} \tag{84}$$

c) Part 3: Using **(StrEqu4)** twice, we know that for every $\tau_1 \in T$:

$$\left(\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right) \;\rightarrow\; \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} = \mathbf{0} \tag{85}$$

And that:

$$\left(\neg\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}\right) \;\rightarrow\; \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} = \mathbf{0} \tag{86}$$

Using (85) and (86), we can extend the derivation in (84):

$$\frac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right)_{\tau_1\in T} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}\right)_{\tau_1\in T}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}, [\neg\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}]\mathbf{0}\right)_{\tau_1\in T}\\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{supi\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}, [\neg\sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \wedge \mathsf{supi\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}]\mathbf{0}\right)_{\tau_1\in T}\end{array}} \;\mathsf{Simp}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\mathrm{ID}}_{\tau}, \quad \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau}\\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}, \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}\end{array}} \;\mathsf{Simp} \tag{87}$$

We can check that for all $\tau_1 = \_, \mathrm{PN}(j_1, 1) \in T$, since $\tau_2 \prec_\tau \tau_1$ and $\tau_2 \not\prec_\tau \mathrm{NS_{ID}}(\_)$ we have that:

$$\left(\mathsf{Mac}^2_{\mathsf{k}^{\mathrm{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}, \mathsf{suc}(\sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}}))\rangle), \mathsf{Mac}^2_{\mathsf{k}^{\nu_\tau(\mathrm{ID})}_{\mathsf{m}}}(\langle \mathsf{n}^{j_1}, \mathsf{suc}(\sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{SQN}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}))\rangle)\right) \in \mathsf{reveal}_{\tau_0} \qquad \left(\mathsf{n}^{j_1}, \mathsf{n}^{j_1}\right) \in \mathsf{reveal}_{\tau_0}$$

$$\left(\{\langle \mathrm{ID}, \sigma^{\mathsf{in}}_{\tau_2}(\mathrm{SQN}^{\mathrm{ID}}_{\mathrm{U}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}, \{\langle \mathrm{ID}^{\nu_\tau(\mathrm{ID})}, \sigma^{\mathsf{in}}_{\underline{\tau_2}}(\mathrm{SQN}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})\rangle\}^{\mathsf{n}^j_{\mathsf{e}}}_{\mathsf{pk}_{\mathrm{N}}}\right) \in \mathsf{reveal}_{\tau_0}$$

We can complete the derivation in (87): first, for every $\tau_1 \in T$, we deconstruct $b_{\tau_1} \sim \underline{b}_{\underline{\tau_1}}$ with FA; and then, we absorb the subterms into reveal_{τ_0} using rule Dup (which is sound using the remark above). This yields:

$$\frac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\mathrm{ID}}_{\tau}, \quad \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau}\\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}, \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}\end{array}} \;\mathsf{Simp}$$

Finally we conclude using the induction hypothesis.

F. Case $\mathsf{ai} = \text{FN}(j)$

We know that $\mathsf{ai} = \text{FN}(j)$. Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on the following pairs: for every base identity ID:

$$\begin{aligned} \text{GUTI}^j &\sim \text{GUTI}^j \\ [\mathsf{net\text{-}e\text{-}auth}_\tau(\text{ID}, j)]\,(\mathsf{t\text{-}suci\text{-}}\oplus_\tau(\text{ID}, j)) &\sim [\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\text{ID}, j)]\left(\underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\underline{\tau}}}(\text{ID}, j)\right) \\ [\mathsf{net\text{-}e\text{-}auth}_\tau(\text{ID}, j)]\,(\mathsf{t\text{-}mac}_\tau(\text{ID}, j)) &\sim [\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\text{ID}, j)]\left(\underline{\mathsf{t\text{-}mac}_{\underline{\tau}}}(\text{ID}, j)\right) \end{aligned}$$

a) Part 1: Let $\text{ID} \in \mathcal{S}_{\mathsf{id}}$. Using Lemma 7, we know that:

$$\sigma_\tau(\mathsf{e\text{-}auth}_{\text{N}}^j) = \text{ID} \;\rightarrow\; \bigvee_{\tau' \preceq \tau} \sigma_{\tau'}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}}) = \mathsf{n}^j$$

Let $\tau' \preceq \tau$. If ID is not a base identity we know that $\sigma_{\tau'}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}}) \equiv \bot$, and therefore:

$$\neg\left(\sigma_{\tau'}(\mathsf{b\text{-}auth}_{\text{U}}^{\text{ID}}) = \mathsf{n}^j\right)$$

It follows that $\mathsf{eq}(\sigma_\tau(\mathsf{e\text{-}auth}_{\text{N}}^j), \text{ID}) = \mathsf{false}$. We can then check that:

$$t_\tau = \begin{array}{l} \text{if } \mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_1, j) \text{ then} \\ \quad \langle \mathsf{t\text{-}suci\text{-}}\oplus_\tau(\mathsf{A}_1, j)\,,\, \mathsf{t\text{-}mac}_\tau(\mathsf{A}_1, j)\rangle \\ \text{else if } \mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_2, j) \text{ then} \\ \quad \langle \mathsf{t\text{-}suci\text{-}}\oplus_\tau(\mathsf{A}_2, j)\,,\, \mathsf{t\text{-}mac}_\tau(\mathsf{A}_2, j)\rangle \\ \qquad \dots \\ \text{else UnknownId} \end{array} \qquad t_{\underline{\tau}} = \begin{array}{l} \text{if } \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_1, j) \text{ then} \\ \quad \langle \underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\underline{\tau}}}(\mathsf{A}_1, j)\,,\, \underline{\mathsf{t\text{-}mac}_{\underline{\tau}}}(\mathsf{A}_1, j)\rangle \\ \text{else if } \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_2, j) \text{ then} \\ \quad \langle \underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\underline{\tau}}}(\mathsf{A}_2, j)\,,\, \underline{\mathsf{t\text{-}mac}_{\underline{\tau}}}(\mathsf{A}_2, j)\rangle \\ \qquad \dots \\ \text{else UnknownId} \end{array}$$

Using the FA axiom, we can split t_τ and $t_{\underline{\tau}}$ as follows:

$$\frac{\begin{array}{c} \big(\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j),\, [\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}suci\text{-}}\oplus_\tau(\mathsf{A}_i, j),\, [\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}mac}_\tau(\mathsf{A}_i, j)\big)_{i \le B} \\ \sim \big(\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_i, j),\, [\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\underline{\tau}}}(\mathsf{A}_i, j),\, [\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\underline{\tau}}}(\mathsf{A}_i, j)\big)_{i \le B} \end{array}}{t_\tau \sim t_{\underline{\tau}}}\ \mathsf{FA}^*$$

Since:

$$\left(\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j), \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_i, j)\right) \in \mathsf{reveal}_{\tau_0}$$

We just need to prove that there is a derivation of:

$$\begin{aligned} &\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0},\, \big([\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}suci\text{-}}\oplus_\tau(\mathsf{A}_i, j),\, [\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}mac}_\tau(\mathsf{A}_i, j)\big)_{i \le B} \\ \sim\, &\phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0},\, \big([\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\underline{\tau}}}(\mathsf{A}_i, j),\, [\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\underline{\tau}}}(\mathsf{A}_i, j)\big)_{i \le B} \end{aligned}$$

Assume that we have a proof of

$$\begin{aligned} &\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0},\; \big([\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}suci\text{-}}\oplus_\tau(\mathsf{A}_i, j),\; [\mathsf{net\text{-}e\text{-}auth}_\tau(\mathsf{A}_i, j)]\mathsf{t\text{-}mac}_\tau(\mathsf{A}_i, j)\big)_{i \le B} \\ \sim\, &\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0},\; \big(\mathsf{n}_{i,j},\; \mathsf{n}'_{i,j}\big)_{i \le B} \end{aligned} \tag{88}$$

And:

$$\begin{aligned} &\phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0},\; \big(\mathsf{n}_{i,j},\; \mathsf{n}'_{i,j}\big)_{i \le B} \\ \sim\, &\phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0},\; \big([\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}}\oplus_{\underline{\tau}}}(\mathsf{A}_i, j),\; [\underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\underline{\tau}}}(\mathsf{A}_i, j)\big)_{i \le B} \end{aligned} \tag{89}$$

Where for all $\{\mathsf{n}_{i,j}, \mathsf{n}'_{i,j} \mid 1 \le i \le B\}$ are fresh distinct nonces. Since:

$$\frac{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_\tau^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0},\; \big(\mathsf{n}_{i,j},\; \mathsf{n}'_{i,j}\big)_{i \le B} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0},\; \big(\mathsf{n}_{i,j},\; \mathsf{n}'_{i,j}\big)_{i \le B}}\ \mathsf{Fresh}$$

We can conclude by induction.

b) Part 2: It only remains to give derivations of the formulas in Eq. (88) and Eq. (89). We only give the proof for Eq. (89), and we omit the derivation of Eq. (88) (as it is similar, and simpler).

Instead of doing the proof simultaneously for all i in $\{1, \dots, B\}$, we give the proof for a single i. We let the reader check that the syntactic side-conditions necessary for the derivations for i and i', with $i \neq i'$, are compatible. Therefore the derivations can be sequentially composed, which yield the full proof.

Let $1 \leq i \leq B$. By transitivity, we only have to show that:

$$\begin{aligned} &\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ \mathsf{n}'_{i,j} \\ \sim\ &\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\tau}}(\mathsf{A}_i, j)\end{aligned} \tag{90}$$

And:

$$\begin{aligned} &\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\tau}}(\mathsf{A}_i, j) \\ \sim\ &\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}\oplus}_{\tau}}(\mathsf{A}_i, j),\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\tau}}(\mathsf{A}_i, j)\end{aligned} \tag{91}$$

c) Derivation of Formula (91)*:* Let $\{\underline{\mathrm{ID}}_1, \dots, \underline{\mathrm{ID}}_l\} = \mathsf{copies\text{-}id}(\mathrm{ID}_i)$. We define, for every $0 \leq y \leq l$, the partially randomized terms $\underline{\mathsf{t\text{-}suci\text{-}\oplus}^y_{\tau}}(\mathrm{ID}_i, j)$:

$$\begin{aligned} \underline{\mathsf{t\text{-}suci\text{-}\oplus}^y_{\underline{\tau}}}(\mathrm{ID}_i, j) \ \equiv\ & \text{if } \mathsf{eq}(\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^j_{\mathrm{N}}), \underline{\mathrm{ID}}_1) \text{ then } \mathsf{n}^1_{i,j} \\ & \dots \\ & \text{else if } \mathsf{eq}(\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^j_{\mathrm{N}}), \underline{\mathrm{ID}}_{y-1}) \text{ then } \mathsf{n}^{y-1}_{i,j} \\ & \text{else if } \mathsf{eq}(\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^j_{\mathrm{N}}), \underline{\mathrm{ID}}_y) \text{ then } \mathrm{GUTI}^j \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^j) \\ & \dots \\ & \text{else } \mathrm{GUTI}^j \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_l}}(\mathsf{n}^j)\end{aligned}$$

Remark that:

$$[\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}\oplus}^0_{\tau}}(\mathrm{ID}_i, j) \ =\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}\oplus}_{\tau}}(\mathsf{A}_i, j)$$

And that:

$$\frac{}{\begin{aligned} &\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ \mathsf{n}_{i,j}, \qquad\qquad [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\tau}}(\mathsf{A}_i, j) \\ \sim\ &\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}\oplus}^l_{\tau}}(\mathrm{ID}_i, j),\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\tau}}(\mathsf{A}_i, j)\end{aligned}}\ \textsf{indep-branch}$$

Hence by transitivity, to prove that there exists a derivation of Formula (91) it is sufficient to prove that, for every $0 < y \leq l$, that we have a derivation of $\phi_{y-1} \sim \phi_y$, where:

$$\begin{aligned} \phi_{y-1} \ &\equiv\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}\oplus}^{y-1}_{\tau}}(\mathrm{ID}_i, j),\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\tau}}(\mathsf{A}_i, j) \\ \phi_y \ &\equiv\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}suci\text{-}\oplus}^{y}_{\tau}}(\mathrm{ID}_i, j),\ [\underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathsf{A}_i, j)]\underline{\mathsf{t\text{-}mac}_{\tau}}(\mathsf{A}_i, j)\end{aligned}$$

Let $1 \leq y \leq B$, we are going to give a derivation of $\phi_{y-1} \sim \phi_y$. This is done in two times:

- First, we are going to use the PRF-f^{r} axiom applied to f^{r}, with key $\mathsf{k}^{\underline{\mathrm{ID}}_y}$, to replace $\mathrm{GUTI}^j \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^j)$ with $\mathrm{GUTI}^j \oplus \mathsf{n}''^y_{i,j}$ (where $\mathsf{n}''^y_{i,j}$ is a fresh nonce).

  First, observe that there is only one occurrence of $\mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^j)$ in ϕ_{y-1} (and none in ϕ_y). Moreover:

$$\begin{aligned} \mathsf{set\text{-}prf}^{\mathsf{f}^{\mathsf{r}}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\phi_{y-1}, \phi_y) \setminus \{\mathsf{n}^j\} \ =\ & \left\{\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) \mid \tau_1 = \_, \mathrm{FU}_{\underline{\mathrm{ID}}_y}(p) \prec \tau\right\} \\ & \cup\ \{\mathsf{n}^p \mid \tau_1 = \_, \mathrm{FN}(p) \prec \tau\}\end{aligned}$$

  Let $\tau_1 = \_, \mathrm{FN}(p) \prec \tau$. We know that $p \neq j$, and therefore that $(\mathsf{n}^p = \mathsf{n}^j) = \mathsf{false}$. We deduce that:

$$\mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^j) \ =\ \left[\bigwedge_{\tau_1 = \_, \mathrm{FN}(p) \prec \tau} \mathsf{n}^p \neq \mathsf{n}^j\right] \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^j)$$

  But we still need guards for $\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^j$, for every $\tau_1 = \_, \mathrm{FU}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(p) \prec \tau$. The problem is that it is not true that $(\sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{\mathrm{ID}}_{\mathrm{U}}) = \mathsf{n}^j) = \mathsf{false}$. We solve this problem by rewriting ϕ_{y-1} (resp. ϕ_y) into the vector of terms ϕ'_{y-1} (resp. ϕ'_y) obtained by replacing (recursively) any occurrence of $\mathsf{accept}^{\mathsf{k}^{\underline{\mathrm{ID}}_y}}_{\tau_1}$ with:

$$\bigvee_{\substack{\tau_0 = \_\mathrm{FN}(j_0) \prec \tau_1 \\ \tau_0 \not\prec \tau_1\, \mathrm{NS}_{\underline{\mathrm{ID}}_y}(\_)}} \left(\begin{aligned} &\mathsf{inj\text{-}auth}_{\tau_1}(\underline{\mathrm{ID}}_y, j_0) \wedge \sigma^{\mathsf{in}}_{\tau_1}(\mathsf{e\text{-}auth}^{j_0}_{\mathrm{N}}) \neq \mathsf{UnknownId} \\ \wedge\ &\pi_1(g(\phi^{\mathsf{in}}_{\tau_1})) = \mathrm{GUTI}^{j_0} \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}^{\underline{\mathrm{ID}}_y}}(\mathsf{n}^{j_0}) \wedge\ \pi_2(g(\phi^{\mathsf{in}}_{\tau_1})) = \mathsf{Mac}^5_{\mathsf{k}^{\underline{\mathrm{ID}}_y}_{\mathsf{m}}}(\langle \mathrm{GUTI}^{j_0}\ , \mathsf{n}^{j_0}\rangle)\end{aligned}\right) \tag{92}$$

Which is sound using **(Equ1)**. We then have:

$$\text{set-prf}^{\mathsf{f}^{\mathsf{r}}}_{\mathsf{k}^{\text{ID}_y}}(\phi') \quad = \quad \{\mathsf{n}^p \mid \tau_1 = \_, \text{FN}(p) \prec \tau\}$$

Therefore we can apply the PRF-f^{r} axioms as wanted: first we replace ϕ_{y-1} and ϕ_y by ϕ'_{y-1} and ϕ'_y using rule R; then we apply the PRF-f^{r} axiom; and finally we rewrite any term of the form (92) back into $\text{accept}^{\mathsf{k}^{\text{ID}_y}}_{\tau_1}$.

- Then, we use the $\oplus$-indep axiom to replace $\text{GUTI}^j \oplus \mathsf{n}''^{y}_{i,j}$ with $\mathsf{n}^y_{i,j}$.

d) Derivation of Formula (90)*:* We use the same proof technique. We define, for every $0 \leq y \leq l$, the partially randomized terms $\underline{\text{t-mac}^y_\tau}(\text{ID}_i, j)$:

$$\begin{aligned} \underline{\text{t-mac}^y_{\underline{\tau}}}(\text{ID}_i, j) \quad \equiv \quad & \text{if eq}(\sigma_{\underline{\tau}}(\text{e-auth}^j_{\text{N}}), \underline{\text{ID}}_1) \text{ then } \mathsf{n}'^1_{i,j} \\ & \quad \ldots \\ & \text{else if eq}(\sigma_{\underline{\tau}}(\text{e-auth}^j_{\text{N}}), \underline{\text{ID}}_{y-1}) \text{ then } \mathsf{n}'^{y-1}_{i,j} \\ & \text{else if eq}(\sigma_{\underline{\tau}}(\text{e-auth}^j_{\text{N}}), \underline{\text{ID}}_y) \text{ then } \text{Mac}^5_{\mathsf{k}_\mathsf{m}^{\text{ID}_y}}(\langle \text{GUTI}^j, \mathsf{n}^j \rangle) \\ & \quad \ldots \\ & \text{else } \text{Mac}^5_{\mathsf{k}_\mathsf{m}^{\text{ID}_l}}(\langle \text{GUTI}^j, \mathsf{n}^j \rangle) \end{aligned}$$

Remark that:

$$[\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}^0_{\underline{\tau}}}(\text{ID}_i, j) \quad = \quad [\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}_{\underline{\tau}}}(\mathsf{A}_i, j)$$

And that:

$$\frac{}{\begin{aligned} &\phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ \mathsf{n}'_{i,j} \\ \sim\ &\phi^{\text{in}}_{\underline{\tau}}, \text{r-reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}^l_{\underline{\tau}}}(\mathsf{A}_i, j)\end{aligned}} \text{ indep-branch}$$

Hence by transitivity, to prove that there exists a derivation of Formula (90) it is sufficient to prove that, for every $0 < y \leq l$, that we have a derivation of $\psi_{y-1} \sim \psi_y$, where:

$$\begin{aligned} \psi_{y-1} \quad &\equiv \quad \psi_{\underline{\tau_0}}, \text{r-reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}^{y-1}_{\underline{\tau}}}(\text{ID}_i, j) \\ \psi_y \quad &\equiv \quad \psi_{\underline{\tau_0}}, \text{r-reveal}_{\tau_0},\ \mathsf{n}_{i,j},\ [\underline{\text{net-e-auth}_{\underline{\tau}}}(\mathsf{A}_i, j)]\underline{\text{t-mac}^{y}_{\underline{\tau}}}(\text{ID}_i, j) \end{aligned}$$

Let $1 \leq y \leq B$, we are going to give a derivation of $\psi_{y-1} \sim \psi_y$. For this, we are going to use the PRF-MAC^5 axiom with key $\mathsf{k}_\mathsf{m}^{\text{ID}_y}$, to replace $\text{Mac}^5_{\mathsf{k}_\mathsf{m}^{\text{ID}_y}}(\langle \text{GUTI}^j, \mathsf{n}^j \rangle)$ with a fresh nonce $\tilde{\mathsf{n}}^y_{i,j}$.

First, observe that there is only one occurrence of $\text{Mac}^5_{\mathsf{k}_\mathsf{m}^{\text{ID}_y}}(\langle \text{GUTI}^j, \mathsf{n}^j \rangle)$ in ψ_{y-1} (and none in ψ_y). Moreover:

$$\begin{aligned} \text{set-mac}^5_{\mathsf{k}^{\text{ID}_y}}(\psi_{y-1}, \psi_y) \setminus \{\langle \text{GUTI}^j, \mathsf{n}^j \rangle\} \quad = \quad & \\ & \{\langle \text{GUTI}^p, \mathsf{n}^p \rangle \mid \tau_1 = \_, \text{FN}(p) \prec \tau\} \\ & \cup \left\{\langle \pi_1(g(\phi^{\text{in}}_{\tau_1})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\sigma^{\text{in}}_{\tau_1}(\text{e-auth}^{\mathsf{k}^{\text{ID}_y}}_{\text{U}})), \sigma^{\text{in}}_{\tau_1}(\text{e-auth}^{\mathsf{k}^{\text{ID}_y}}_{\text{U}}) \rangle \mid \tau_1 = \_, \text{FN}(p) \prec \tau\right\} \end{aligned}$$

Let $\tau_1 = \_, \text{FN}(p) \prec \tau$. Since GUTI^j is a fresh nonce, we know using EQIndep and the injectivity of the pair function that:

$$\big(\langle \text{GUTI}^j, \mathsf{n}^j \rangle = \langle \text{GUTI}^p, \mathsf{n}^p \rangle\big) = \text{false}$$
$$\Big(\langle \text{GUTI}^j, \mathsf{n}^j \rangle = \langle \pi_1(g(\phi^{\text{in}}_{\tau_1})) \oplus \mathsf{f}^{\mathsf{r}}_{\mathsf{k}}(\sigma^{\text{in}}_{\tau_1}(\text{e-auth}^{\mathsf{k}^{\text{ID}_y}}_{\text{U}})), \sigma^{\text{in}}_{\tau_1}(\text{e-auth}^{\mathsf{k}^{\text{ID}_y}}_{\text{U}}) \rangle\Big) = \text{false}$$

Therefore we can directly apply the PRF-MAC^5 axiom, which concludes this case.

G. Case $\mathit{ai} = \text{FU}_{\text{ID}}(j)$

We know that $\underline{\text{ai}} = \text{FU}_{\nu_\tau(\text{ID})}(j)$. Here l-reveal$_\tau$ and l-reveal$_{\tau_0}$ coincides everywhere except on the pairs:

$$\begin{aligned} \sigma_\tau(\text{valid-guti}^{\text{ID}}_{\text{U}}) \quad &\sim \quad \sigma_{\underline{\tau}}(\text{valid-guti}^{\nu_\tau(\text{ID})}_{\text{U}}) \\ \underbrace{\begin{array}{c}\text{if } \sigma_\tau(\text{valid-guti}^{\text{ID}}_{\text{U}}) \text{ then } \sigma_\tau(\text{GUTI}^{\text{ID}}_{\text{U}}) \\ \text{else } \bot\end{array}}_{\text{m-suci}^{\text{ID}}_\tau} \quad &\sim \quad \underbrace{\begin{array}{c}\text{if } \sigma_{\underline{\tau}}(\text{valid-guti}^{\nu_\tau(\text{ID})}_{\text{U}}) \text{ then } \sigma_{\underline{\tau}}(\text{GUTI}^{\nu_\tau(\text{ID})}_{\text{U}}) \\ \text{else } \bot\end{array}}_{\text{m-suci}^{\nu_\tau(\text{ID})}_{\underline{\tau}}} \end{aligned}$$

Moreover, we also need to show that:

$$\text{accept}^{\text{ID}}_\tau \sim \text{accept}^{\nu_\tau(\text{ID})}_{\underline{\tau}}$$

Recall that $\tau = \tau_0, \mathsf{ai}$ and $\underline{\tau} = \underline{\tau_0}, \underline{\mathsf{ai}}$, and that:

$$\begin{aligned}
\sigma_\tau(\text{valid-guti}_{\text{U}}^{\text{ID}}) &\equiv \text{accept}_\tau^{\text{ID}} \\
\sigma_\tau(\text{GUTI}_{\text{U}}^{\text{ID}}) &\equiv \text{ if accept}_\tau^{\text{ID}} \text{ then } \pi_1(g(\phi_\tau^{\text{in}})) \oplus \mathsf{f}_{\mathsf{k}}^{\mathsf{r}}(\sigma_{\tau_0}(\text{e-auth}_{\text{U}}^{\text{ID}})) \\
&\quad\ \text{else UnSet} \\
\sigma_{\underline{\tau}}(\text{valid-guti}_{\text{U}}^{\nu_\tau(\text{ID})}) &\equiv \text{accept}_{\underline{\tau}}^{\nu_\tau(\text{ID})} \\
\sigma_{\underline{\tau}}(\text{GUTI}_{\text{U}}^{\nu_\tau(\text{ID})}) &\equiv \text{ if accept}_{\underline{\tau}}^{\nu_\tau(\text{ID})} \text{ then } \pi_1(g(\phi_{\underline{\tau}}^{\text{in}})) \oplus \mathsf{f}_{\mathsf{k}}^{\mathsf{r}}(\sigma_{\underline{\tau_0}}(\text{e-auth}_{\text{U}}^{\nu_\tau(\text{ID})})) \\
&\quad\ \text{else UnSet}
\end{aligned}$$

Therefore we want a proof of:

$$\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{accept}_\tau^{\text{ID}}, \text{m-suci}_\tau^{\text{ID}} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{accept}_{\underline{\tau}}^{\nu_\tau(\text{ID})}, \text{m-suci}_{\underline{\tau}}^{\nu_\tau(\text{ID})} \tag{93}$$

Using **(Equ1)**, we know that:

$$\text{accept}_\tau^{\text{ID}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_,\text{FN}(j_0) \prec \tau \\ \tau_1 \not\prec_\tau \text{NS}_{\text{ID}}(\_)}} \text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_1} \tag{94}$$

We know that $\underline{\tau} = \underline{\tau_0}, \text{FU}_{\nu_\tau(\text{ID})}(j)$ is a valid symbolic trace. Using **(Equ1)** again, we know that:

$$\text{accept}_{\underline{\tau}}^{\nu_\tau(\text{ID})} \leftrightarrow \bigvee_{\substack{\tau_1 = \_,\text{FN}(j_0) \prec \tau \\ \tau_1 \not\prec_\tau \text{NS}_{\text{ID}}(\_)}} \text{fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_1}} \tag{95}$$

Let:

$$\{j_0, \dots, j_l\} = \{i \mid \tau' = \_, \text{FN}(i) \prec \tau \wedge \tau' \not\prec_\tau \text{NS}_{\text{ID}}(\_)\}$$

One can check that:

$$\{j_0, \dots, j_l\} = \{i \mid \tau' = \_, \text{FN}(i) \prec \underline{\tau} \wedge \tau' \not\prec_{\underline{\tau}} \text{NS}_{\nu_\tau(\text{ID})}(\_)\}$$

For all $0 \le i \le l$, let τ_{j_i} be such that $\tau_{j_i} = \_, \text{FN}(j_i) \prec \tau$. One can check that:

$$\begin{aligned}
\text{m-suci}_\tau^{\text{ID}} = &\text{ if fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_0}} \text{ then GUTI}^{j_0} \\
&\text{ else if fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_1}} \text{ then GUTI}^{j_1} \\
&\quad \dots \\
&\text{ else GUTI}^{j_l}
\end{aligned}
\qquad
\begin{aligned}
\text{m-suci}_{\underline{\tau}}^{\nu_\tau(\text{ID})} = &\text{ if fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_0}}} \text{ then GUTI}^{j_0} \\
&\text{ else if fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_1}}} \text{ then GUTI}^{j_1} \\
&\quad \dots \\
&\text{ else GUTI}^{j_l}
\end{aligned}$$

We can now start giving a derivation of (93):

$$\dfrac{\dfrac{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_i}}\right)_{i \le l} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_i}}}\right)_{i \le l}}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_i}}\right)_{i \le l}, \left(\text{GUTI}^{j_i}\right)_{i \le l} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_i}}}\right)_{i \le l}, \left(\text{GUTI}^{j_i}\right)_{i \le l}} \text{Dup}^*}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \text{accept}_\tau^{\text{ID}}, \text{m-suci}_\tau^{\text{ID}} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \text{accept}_{\underline{\tau}}^{\nu_\tau(\text{ID})}, \text{m-suci}_{\underline{\tau}}^{\nu_\tau(\text{ID})}} \text{FA}^*$$

Since for all $1 \le i \le l$, $(\text{GUTI}^{j_i} \sim \text{GUTI}^{j_i}) \in \text{reveal}_{\tau_0}$. Finally, we conclude using **(Der2)** for every $0 \le i \le l$:

$$\dfrac{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}}{\phi_\tau^{\text{in}}, \text{l-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\tau}^{\text{n}:\tau_{j_i}}\right)_{i \le l} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \left(\text{fu-tr}_{\text{u}:\underline{\tau}}^{\text{n}:\underline{\tau_{j_i}}}\right)_{i \le l}} \text{FA}^*$$

H. Case $\mathsf{ai} = \text{TU}_{\text{ID}}(j, 0)$

We know that $\underline{\mathsf{ai}} = \text{TU}_{\nu_\tau(\text{ID})}(j, 0)$. Let $\underline{\text{ID}} = \nu_\tau(\text{ID})$. Here l-reveal_τ and l-reveal_{τ_0} coincides everywhere except on:

$$\sigma_\tau(\text{valid-guti}_{\text{U}}^{\text{ID}}) \sim \sigma_{\underline{\tau}}(\text{valid-guti}_{\text{U}}^{\underline{\text{ID}}}) \qquad \sigma_\tau(\text{s-valid-guti}_{\text{U}}^{\text{ID}}) \sim \sigma_{\underline{\tau}}(\text{s-valid-guti}_{\text{U}}^{\underline{\text{ID}}}) \qquad \text{m-suci}_\tau^{\text{ID}} \sim \text{m-suci}_{\underline{\tau}}^{\underline{\text{ID}}}$$

Handling these is completely trivial because:

$$\sigma_\tau(\text{valid-guti}_{\text{U}}^{\text{ID}}) \equiv \text{false} \qquad \sigma_{\underline{\tau}}(\text{valid-guti}_{\text{U}}^{\underline{\text{ID}}}) \equiv \text{false} \qquad \sigma_\tau(\text{s-valid-guti}_{\text{U}}^{\text{ID}}) \equiv \sigma_\tau^{\text{in}}(\text{valid-guti}_{\text{U}}^{\text{ID}})$$

$$\sigma_{\underline{\tau}}(\text{s-valid-guti}_{\text{U}}^{\underline{\text{ID}}}) \equiv \sigma_{\underline{\tau}}^{\text{in}}(\text{valid-guti}_{\text{U}}^{\underline{\text{ID}}}) \qquad \text{m-suci}_\tau^{\text{ID}} \equiv \bot \qquad \text{m-suci}_{\underline{\tau}}^{\underline{\text{ID}}} \equiv \bot$$

And $(\sigma^{\mathsf{in}}_{\tau}(\mathsf{valid\text{-}guti}^{\text{ID}}_{\text{U}}), \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{valid\text{-}guti}^{\underline{\text{ID}}}_{\text{U}})) \in \mathsf{reveal}_{\tau_0}$. Finally, we conclude by observing that:

$$t_\tau = \text{if } \sigma^{\mathsf{in}}_{\tau}(\mathsf{valid\text{-}guti}^{\text{ID}}_{\text{U}}) \text{ then } \mathsf{m\text{-}suci}^{\,\text{ID}}_{\,\tau} \text{ else NoGuti} \qquad t_{\underline{\tau}} = \text{if } \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{valid\text{-}guti}^{\underline{\text{ID}}}_{\text{U}}) \text{ then } \mathsf{m\text{-}suci}^{\,\underline{\text{ID}}}_{\,\underline{\tau}} \text{ else NoGuti}$$

Hence:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{valid\text{-}guti}^{\underline{\text{ID}}}_{\text{U}})}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\tau}(\mathsf{valid\text{-}guti}^{\text{ID}}_{\text{U}}), \mathsf{m\text{-}suci}^{\,\text{ID}}_{\,\tau}, \text{NoGuti} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{valid\text{-}guti}^{\underline{\text{ID}}}_{\text{U}}), \mathsf{m\text{-}suci}^{\,\underline{\text{ID}}}_{\,\underline{\tau}}, \text{NoGuti}}\;\text{Dup}^*}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}}\;\text{Simp}$$

I. Case $\mathsf{ai} = \text{TN}(j,0)$

We know that $\underline{\mathsf{ai}} = \text{TN}(j,0)$. Using **(A6)**, we know that for every $\text{ID} \neq \text{ID}'$, $\neg\mathsf{accept}^{\text{ID}}_{\tau} \leftrightarrow \neg\mathsf{accept}^{\text{ID}'}_{\tau}$. Therefore the answer from the network does not depend on the order in which we make the $\mathsf{accept}^{\text{ID}}_{\tau}$ tests. Formally, the following list of conditionals is a CS partition:

$$\left((\mathsf{accept}^{\text{ID}}_{\tau})_{\text{ID} \in \mathcal{S}_{\mathsf{id}}}\,,\; \bigwedge_{\text{ID} \in \mathcal{S}_{\mathsf{id}}} \neg\mathsf{accept}^{\text{ID}}_{\tau} \right)$$

To get a uniform notation, we let $\mathsf{accept}^{\text{ID}_{\mathsf{dum}}}_{\tau} \equiv \bigwedge_{\text{ID} \in \mathcal{S}_{\mathsf{id}}} \neg\mathsf{accept}^{\text{ID}}_{\tau}$, and $\mathcal{S}_{\mathsf{ext\text{-}id}} = \mathcal{S}_{\mathsf{id}} \cup \{\text{ID}_{\mathsf{dum}}\}$. Hence using Proposition 28 we get that:

$$t_\tau \;=\; \underset{\text{ID} \in \mathcal{S}_{\mathsf{ext\text{-}id}}}{\mathsf{case}}\,(\mathsf{accept}^{\text{ID}}_{\tau} : \mathsf{msg}^{\text{ID}}_{\tau})$$

We are now going to show that for every $\text{ID} \in \mathcal{S}_{\mathsf{ext\text{-}id}}$, the term $\mathsf{msg}^{\text{ID}}_{\tau}$ can be replaced by $\langle \mathsf{n}^j\,, \mathsf{n}^{\oplus}_{\text{ID}}\,,\, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle$ (where $(\mathsf{n}^{\oplus}_{\text{ID}})_{\text{ID} \in \mathcal{S}_{\mathsf{ext\text{-}id}}}$ and $(\mathsf{n}^{\mathsf{Mac}}_{\text{ID}})_{\text{ID} \in \mathcal{S}_{\mathsf{ext\text{-}id}}}$ are fresh distinct nonces). We will then conclude easily using the fresh axiom.

Let $\text{ID}_1, \dots, \text{ID}_l$ be an arbitrary enumeration of $\mathcal{S}_{\mathsf{ext\text{-}id}}$. For every $1 \leq n \leq l$, and for every $\text{ID}_i \in \{\text{ID}_1, \dots, \text{ID}_l\}$, we let:

$$\mathsf{rnd\text{-}msg}^{\text{ID}_i}_{n} \;\equiv\; \begin{cases} \langle \mathsf{n}^j\,, \mathsf{n}^{\oplus}_{\text{ID}_i}\,,\, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}_i} \rangle & \text{if } i \leq n \\ \mathsf{rnd\text{-}msg}^{\text{ID}_i}_{\tau} & \text{if } i > n \end{cases}$$

And we let t_n be the term t_τ where the subterms $\mathsf{msg}^{\text{ID}}_{\tau}$ have been replaced by $\langle \mathsf{n}^j\,, \mathsf{n}^{\oplus}_{\text{ID}}\,,\, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle$ for the first n identities:

$$t_n \equiv \underset{\text{ID} \in \mathcal{S}_{\mathsf{ext\text{-}id}}}{\mathsf{case}}\,(\mathsf{accept}^{\text{ID}}_{\tau} : \mathsf{rnd\text{-}msg}^{\text{ID}}_{n})$$

We can check that $t_0 \equiv t_\tau$.

a) Part 1: We now show that for every $1 \leq n \leq l$, we have a derivation of:

$$\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_{n-1} \;\sim\; \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_n \tag{96}$$

Let n be in $\{1, \dots, l\}$. Let $\text{ID} = \text{ID}_n$, $\mathsf{k} = \mathsf{k}^{\text{ID}}$ and $\mathsf{k_m} = \mathsf{k}^{\text{ID}}_{\mathsf{m}}$. We are going to apply PRF-f axiom with key k to replace $\mathsf{f}_{\mathsf{n}^j}(\mathsf{k})$ by n_{ID}, where n_{ID} is a fresh nonce. Recall that:

$$\mathsf{msg}^{\text{ID}}_{\tau} \;\equiv\; \langle \mathsf{n}^j\,, \underbrace{\sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}})}_{u_{\text{SQN}}} \oplus \mathsf{f}_{\mathsf{k}^{\text{ID}}}(\mathsf{n}^j)\,,\, \underbrace{\mathsf{Mac}^3_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \mathsf{n}^j\,, \sigma^{\mathsf{in}}_{\tau}(\text{SQN}^{\text{ID}}_{\text{N}})\,,\, \sigma^{\mathsf{in}}_{\tau}(\text{GUTI}^{\text{ID}}_{\text{N}})\rangle)}_{u_{\mathsf{Mac}}} \rangle$$

We let ψ be the context with one hole (which has only one occurrence) such that:

$$\psi[\langle \mathsf{n}^j\,, u_{\text{SQN}} \oplus \mathsf{f}_{\mathsf{k}^{\text{ID}}}(\mathsf{n}^j)\,,\, u_{\mathsf{Mac}} \rangle] \equiv \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_{n-1} \qquad \psi[\langle \mathsf{n}^j\,, \mathsf{n}^{\oplus}_{\text{ID}}\,,\, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle] \equiv \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_n$$

Let $\psi_0[] \equiv \psi[\langle \mathsf{n}^j\,, u_{\text{SQN}} \oplus []\,,\, u_{\mathsf{Mac}} \rangle]$. Notice that:

$$\begin{aligned} \mathsf{set\text{-}prf}^{\mathsf{f}}_{\mathsf{k}}(\psi_0[]) \;&=\; \{\pi_1(\phi^{\mathsf{in}}_{\tau_1}) \mid \tau_1 = \_, \text{TU}_{\text{ID}}(p,1) \prec \tau\} \\ &\quad\; \cup \{\mathsf{n}^p \mid \tau_1 = \_, \text{TN}(p) \prec \tau\} \end{aligned}$$

We want to get rid of the sub-terms of the form $\mathsf{f}_{\mathsf{k}}(\pi_1(\phi^{\mathsf{in}}_{\tau_1}))$, for any τ_1 such that $\tau_1 = \_, \text{TU}_{\text{ID}}(p,1) \prec \tau$. To do this, for every $\tau_1 = \_, \text{TU}_{\text{ID}}(p,1) \prec \tau$, we let $\tau_3 = \_, \text{TU}_{\text{ID}}(j_p, 0) \prec \tau$, and we apply **(StrEqu2)** to rewrite all occurrence of $\mathsf{accept}^{\text{ID}}_{\tau_1}$ in ψ_0 using:

$$\mathsf{accept}^{\text{ID}}_{\tau_1} \leftrightarrow \bigvee_{\substack{\tau_2 = \_, \text{TN}(j_1, 0) \\ \tau_3 \prec_{\tau_1} \tau_2 \prec_{\tau_1} \tau_1}} (\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_2}_{\mathsf{u}:\tau_3,\tau_1}) \tag{97}$$

This yields a vector of terms $\psi_0'[]$ with one hole. It is easy to check that:

$$\mathsf{set\text{-}prf}^{\mathsf{f}}_{\mathsf{k}}(\psi_0'[]) \;=\; \{\mathsf{n}^p \mid \tau_1 = \_, \text{TN}(p) \prec \tau\}$$

By validity of τ, we know that for every $\tau_1 = \_, \text{TN}(p) \prec \tau$, we have $p \neq j$. Therefore using fresh we have $(\mathsf{n}^j = \mathsf{n}^P) \leftrightarrow \mathsf{false}$. It follows that we can apply the PRF-f axiom in $\psi_0'[\mathsf{f}_{\mathsf{n}^j}(\mathsf{k})]$, replacing $\mathsf{f}_{\mathsf{n}^j}(\mathsf{k})$ by n_{ID}, which yields $\psi_0'[\mathsf{n}_{\text{ID}}]$. We then rewrite any term of the form in (97) back into $\mathsf{accept}^{\text{ID}}_{\tau_1}$, obtaining $\psi_0[\mathsf{n}_{\text{ID}}] \equiv \psi[\langle \mathsf{n}^j, u_{\text{SQN}} \oplus \mathsf{n}_{\text{ID}}, u_{\mathsf{Mac}} \rangle]$. We then use $\oplus$-indep to replace $u_{\text{SQN}} \oplus \mathsf{n}_{\text{ID}}$ by $\mathsf{n}^{\oplus}_{\text{ID}}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, u_{\mathsf{Mac}} \rangle] \sim \psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle]}{\psi[\langle \mathsf{n}^j, u_{\text{SQN}} \oplus \mathsf{n}_{\text{ID}}, u_{\mathsf{Mac}} \rangle] \sim \psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle]}\ \oplus\text{-indep}}{\psi_0'[\mathsf{n}_{\text{ID}}] \sim \psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle]}\ R}{\psi_0'[\mathsf{f}_{\mathsf{n}^j}(\mathsf{k})] \sim \psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle]}\ \text{PRF-f}}{\psi[\langle \mathsf{n}^j, u_{\text{SQN}} \oplus \mathsf{f}_{\mathsf{k}^{\text{ID}}}(\mathsf{n}^j), u_{\mathsf{Mac}} \rangle] \sim \psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle]}\ R}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_{n-1} \ \sim\ \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_n}\ R$$

We now the same thing with u_{Mac}, applying PRF-MAC[3] axiom to replace u_{Mac} by $\mathsf{n}^{\mathsf{Mac}}_{\text{ID}}$. The proof is similar to the one we just did for PRF-f, and we omit the details. We then conclude using Refl. This yields:

$$\dfrac{\dfrac{}{\psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle] \sim \psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle]}\ \text{Refl} \\ \vdots}{\psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, u_{\mathsf{Mac}} \rangle] \sim \psi[\langle \mathsf{n}^j, \mathsf{n}^{\oplus}_{\text{ID}}, \mathsf{n}^{\mathsf{Mac}}_{\text{ID}} \rangle]}$$

b) Part 2: Using the fact that $t_0 \equiv t_\tau$ and (96), and using the transitivity axiom, we can build a derivation of:

$$\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \ \sim\ \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_l$$

Moreover, using the indep-branch axiom we know that:

$$\dfrac{}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_l \ \sim\ \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n}}\ \text{indep-branch}$$

where n is a fresh nonce. Using transitivity again, we get a derivation of:

$$\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \ \sim\ \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \tag{98}$$

Repeating everything we did in **Part 1**, we can show that we have a derivation of:

$$\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{n}' \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}} \tag{99}$$

where n' is a fresh nonce. We then conclude using the transitivity and Fresh:

$$\dfrac{\dfrac{(98)}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \\ \sim\ \phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n}\end{array}} \quad \dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{n} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{n}'}\ \text{Fresh} \quad \dfrac{(99)}{\begin{array}{c}\phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{n}' \\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}\end{array}}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}}\ \text{Trans}$$

J. Case $\mathsf{ai} = \text{TU}_{\text{ID}}(j, 1)$

We know that $\underline{\mathsf{ai}} = \text{TU}_{\nu_\tau(\text{ID})}(j, 1)$. Let $\underline{\text{ID}} = \nu_\tau(\text{ID})$. By validity of τ, we know that there exists $\tau_2 = \_, \text{TU}_{\text{ID}}(j, 0)$ such that $\tau_2 \prec \tau$. Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on:

$$\sigma_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) - \sigma^{\mathsf{in}}_\tau(\text{SQN}^{\text{ID}}_{\text{U}}) \ \sim\ \sigma_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) - \sigma^{\mathsf{in}}_{\underline{\tau}}(\text{SQN}^{\underline{\text{ID}}}_{\text{U}}) \qquad\qquad \sigma_\tau(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) \ \sim\ \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^{\underline{\text{ID}}}_{\text{U}})$$

$$\left(\mathsf{Mac}^4_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{n}^{j_0}) \ \sim\ \mathsf{Mac}^4_{\mathsf{k}^{\underline{\text{ID}}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \text{TN}(j_0, 0) \\ \tau_2 \prec_\tau \tau_1}}$$

First, using **(StrEqu2)** twice we know that:

$$\mathsf{accept}^{\text{ID}}_\tau \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{TN}(j_1, 0) \\ \tau_2 \prec_\tau \tau_1}} \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2, \tau} \qquad\qquad \mathsf{accept}^{\underline{\text{ID}}}_{\underline{\tau}} \leftrightarrow \bigvee_{\substack{\tau_1 = \_, \text{TN}(j_1, 0) \\ \tau_2 \prec_\tau \tau_1}} \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2}, \underline{\tau}}$$

Using **(Der3)** we know that for every $\tau_1 = \_, \text{TN}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$ we have a derivation:

$$\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2, \tau} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2}, \underline{\tau}}}\ \text{Simp} \tag{100}$$

Therefore we can build the following derivation:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}\right)_{\substack{\tau_1=\_,\textsc{tn}(j_1,0)\\ \tau_2\prec_\tau\tau_1}} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}\right)_{\substack{\tau_1=\_,\textsc{tn}(j_1,0)\\ \tau_2\prec_\tau\tau_1}}}\ \textsf{Simp}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\textsc{id}}_\tau \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\underline{\textsc{id}}}_{\underline{\tau}}}\ \textsf{Simp} \tag{101}$$

a) Part 1: We can check that for every $\tau_1 = \_, \textsc{tn}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$:

$$\begin{aligned}
&\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \sigma_\tau(\mathsf{e\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{n}^{j_1} &\qquad& \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \rightarrow \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^{\underline{\textsc{id}}}_{\textsc{u}}) = \mathsf{n}^{j_1}\\
&\neg\mathsf{accept}^{\textsc{id}}_\tau \rightarrow \sigma_\tau(\mathsf{e\text{-}auth}^{\textsc{id}}_{\textsc{u}}) = \mathsf{fail} && \neg\mathsf{accept}^{\underline{\textsc{id}}}_{\underline{\tau}} \rightarrow \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^{\underline{\textsc{id}}}_{\textsc{u}}) = \mathsf{fail}
\end{aligned}$$

And $(\mathsf{n}^{j_1}, \mathsf{n}^{j_1}) \in \mathsf{reveal}_{\tau_0}$. Therefore we can decompose $\sigma_\tau(\mathsf{e\text{-}auth}^{\textsc{id}}_{\textsc{u}})$ and $\sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^{\underline{\textsc{id}}}_{\textsc{u}})$ using FA and get rid of the resulting terms using (100) and (101):

$$\dfrac{\dfrac{\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{c}\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\textsc{id}}_\tau, \left(\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau}, \mathsf{n}^{j_1}\right)_{\substack{\tau_1=\_,\textsc{tn}(j_1,0)\\ \tau_2\prec_\tau\tau_1}}, \mathsf{fail}\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{accept}^{\underline{\textsc{id}}}_{\underline{\tau}}, \left(\mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}}, \mathsf{n}^{j_1}\right)_{\substack{\tau_1=\_,\textsc{tn}(j_1,0)\\ \tau_2\prec_\tau\tau_1}}, \mathsf{fail}\end{array}}\ \textsf{Simp}}{\begin{array}{c}\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{if}\ \mathsf{accept}^{\textsc{id}}_\tau\ \mathsf{then} \displaystyle\mathop{\mathsf{case}}_{\substack{\tau_1=\_,\textsc{tn}(j_1,0)\\ \tau_2\prec_\tau\tau_1}} (\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} : \mathsf{n}^{j_1})\ \mathsf{else\ fail}\\ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{if}\ \mathsf{accept}^{\underline{\textsc{id}}}_{\underline{\tau}}\ \mathsf{then} \displaystyle\mathop{\mathsf{case}}_{\substack{\tau_1=\_,\textsc{tn}(j_1,0)\\ \tau_2\prec_\tau\tau_1}} (\mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} : \mathsf{n}^{j_1})\ \mathsf{else\ fail}\end{array}}\ \textsf{Simp}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma_\tau(\mathsf{e\text{-}auth}^{\textsc{id}}_{\textsc{u}}) \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau}}(\mathsf{e\text{-}auth}^{\underline{\textsc{id}}}_{\textsc{u}})}\ R \tag{102}$$

b) Part 2: Observe that for every $\tau_1 = \_, \textsc{tn}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$:

$$\begin{aligned}
&\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow \sigma_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) - \sigma^{\mathsf{in}}_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = \mathbf{1} &\qquad& \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \rightarrow \sigma_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}}) - \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}}) = \mathbf{1}\\
&\neg\mathsf{accept}^{\textsc{id}}_\tau \rightarrow \sigma_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) - \sigma^{\mathsf{in}}_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) = \mathbf{0} && \neg\mathsf{accept}^{\underline{\textsc{id}}}_{\underline{\tau}} \rightarrow \sigma_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}}) - \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}}) = \mathbf{0}
\end{aligned}$$

It is then easy to adapt the derivation in (102) to get a derivation of (we omit the details):

$$\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \sigma_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) - \sigma^{\mathsf{in}}_\tau(\textsc{sqn}^{\textsc{id}}_{\textsc{u}}) \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \sigma_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}}) - \sigma^{\mathsf{in}}_{\underline{\tau}}(\textsc{sqn}^{\underline{\textsc{id}}}_{\textsc{u}})}\ \textsf{Simp} \tag{103}$$

c) Part 3: We finally take care of t_τ and the Mac^4 terms. First, we check that for every $\tau_1 = \_, \textsc{tn}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$:

$$\begin{aligned}
&\mathsf{part\text{-}tr}^{\mathsf{n}:\tau_1}_{\mathsf{u}:\tau_2,\tau} \rightarrow t_\tau = \mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{n}^{j_0}) &\qquad& \mathsf{part\text{-}tr}^{\mathsf{n}:\underline{\tau_1}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau}} \rightarrow t_{\underline{\tau}} = \mathsf{Mac}^4_{\mathsf{k}^{\underline{\textsc{id}}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\\
&\neg\mathsf{accept}^{\textsc{id}}_\tau \rightarrow t_\tau = \mathsf{error} && \neg\mathsf{accept}^{\underline{\textsc{id}}}_{\underline{\tau}} \rightarrow t_{\underline{\tau}} = \mathsf{error}
\end{aligned}$$

Similarly to what we did in (102), we decompose t_τ and $t_{\underline{\tau}}$ using (100) and (101). Omitting the detail of the derivation, this yield:

$$\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1=\_,\textsc{tn}(j_0,0)\\ \tau_2\prec_\tau\tau_1}} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^4_{\mathsf{k}^{\underline{\textsc{id}}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1=\_,\textsc{tn}(j_0,0)\\ \tau_2\prec_\tau\tau_1}}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, t_\tau \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}}\ \textsf{Simp}$$

Observe that the Mac^4 terms here are exactly the Mac^4 terms in $\mathsf{l\text{-}reveal}_\tau \backslash \mathsf{l\text{-}reveal}_{\tau_0}$. To conclude this proof, it only remains to give a derivation of:

$$\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1=\_,\textsc{tn}(j_0,0)\\ \tau_2\prec_\tau\tau_1}} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^4_{\mathsf{k}^{\underline{\textsc{id}}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1=\_,\textsc{tn}(j_0,0)\\ \tau_2\prec_\tau\tau_1}}$$

For every $\tau_1 = \_, \textsc{tn}(j_1, 0)$ such that $\tau_2 \prec_\tau \tau_1$, we are going to apply the $\textsc{prf-mac}^4$ axiom with key $\mathsf{k}^{\textsc{id}}_{\mathsf{m}}$ to replace $\mathsf{Mac}^4_{\mathsf{k}^{\textsc{id}}_{\mathsf{m}}}(\mathsf{n}^{j_0})$ by a fresh nonce n_{τ_1}. Let $\psi \equiv \phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}$, observe that:

$$\begin{aligned}
\mathsf{set\text{-}mac}^4_{\textsc{id}}(\psi) \ &=\ \left\{\pi_1(g(\phi^{\mathsf{in}}_{\tau_a})) \mid \tau_a = _, \textsc{tu}_{\textsc{id}}(j_a, 1) \prec \tau\right\}\\
&\quad \cup \left\{\mathsf{n}^{j_n} \mid \tau_n = _, \textsc{tn}(j_n, 1) \prec \tau\right\}
\end{aligned}$$

Let:

$$\mathcal{N} = \left\{ \mathsf{n}^{j_0} \mid \tau_1 = \_, \text{TN}(j_0, 0) \wedge \tau_2 \prec_\tau \tau_1 \right\}$$

Our goal is to rewrite ψ into a vector of terms ψ_1 such that $\textsf{set-mac}^4_{\text{ID}}(\psi_1) \cap \mathcal{N} = \emptyset$. This will allow us to apply the PRF-MAC^4 axiom. We are going to rewrite ψ as follows:

- Let $\tau_a = \_, \text{TU}_{\text{ID}}(j_a, 1) \prec \tau$. By validity of τ, we know that $\tau_a \prec_\tau \tau_2$, and that there exists $\tau_b = \_, \text{TU}_{\text{ID}}(j_a, 0) \prec_\tau \tau_a$. Using **(StrEqu2)**, we know that:

$$\textsf{accept}^{\text{ID}}_{\tau_a} \leftrightarrow \bigvee_{\substack{\tau_x = \_, \text{TN}(j_x, 0) \\ \tau_b \prec_\tau \tau_x \prec_\tau \tau_a}} \textsf{part-tr}^{\mathsf{n}:\tau_x}_{\mathsf{u}:\tau_b, \tau_a}$$

  We let $\alpha^{\text{ID}}_{\tau_a}$ be the right-hand side of the equation above. Using this, we can check that:

$$t_{\tau_a} \;=\; \textsf{if } \alpha^{\text{ID}}_{\tau_a} \textsf{ then } \underset{\substack{\tau_x = \_, \text{TN}(j_x, 0) \\ \tau_b \prec_\tau \tau_x \prec_\tau \tau_a}}{\textsf{case}} (\textsf{part-tr}^{\mathsf{n}:\tau_x}_{\mathsf{u}:\tau_b, \tau_a} : \textsf{Mac}^4_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{n}^{j_x})) \textsf{ else error}$$

  Let $\kappa^{\text{ID}}_{\tau_a}$ be the right-hand side of the equation above. For every $\tau_x = \_, \text{TN}(j_x, 0)$ such that $\tau_2 \prec_\tau \tau_1$, we have $\mathsf{n}^{j_x} \in \textsf{set-mac}^4_{\text{ID}}(\alpha^{\text{ID}}_{\tau_a}, \kappa^{\text{ID}}_{\tau_a})$ if and only if $\tau_b \prec_\tau \tau_x \prec_\tau \tau_a$. Therefore:

$$\begin{aligned} & \textsf{set-mac}^4_{\text{ID}} \left(\alpha^{\text{ID}}_{\tau_a}, \kappa^{\text{ID}}_{\tau_a} \right) \cap \mathcal{N} \\ = \;& \left\{ \mathsf{n}^{j_x} \mid \tau_x = \_, \text{TN}(j_x, 0) \wedge \tau_b \prec_\tau \tau_x \prec_\tau \tau_a \right\} \cap \left\{ \mathsf{n}^{j_0} \mid \tau_1 = \_, \text{TN}(j_0, 0) \wedge \tau_2 \prec_\tau \tau_1 \right\} \\ = \;& \left\{ \mathsf{n}^{j_x} \mid \tau_x = \_, \text{TN}(j_x, 0) \wedge \tau_b \prec_\tau \tau_x \prec_\tau \tau_a \wedge \tau_2 \prec_\tau \tau_x \right\} \end{aligned}$$

  By validity of τ, we know that $\tau_a \prec_\tau \tau_2$. This implies that whenever $\tau_b \prec_\tau \tau_x \prec_\tau \tau_a$ and $\tau_2 \prec_\tau \tau_x$, we have $\tau_x \prec_\tau \tau_2 \prec_\tau \tau_x$. Hence:

$$\textsf{set-mac}^4_{\text{ID}} \left(\alpha^{\text{ID}}_{\tau_a}, \kappa^{\text{ID}}_{\tau_a} \right) \cap \mathcal{N} \;=\; \emptyset \tag{104}$$

  Let ψ_0 be ψ in which we replace, for every $\tau_a = \_, \text{TU}_{\text{ID}}(j_a, 1) \prec \tau$, any occurrence of $\textsf{accept}^{\text{ID}}_{\tau_a}$ and t_{τ_a} by, respectively, $\alpha^{\text{ID}}_{\tau_a}$ and $\kappa^{\text{ID}}_{\tau_a}$. We then have:

$$\textsf{set-mac}^4_{\text{ID}}(\psi_0) \;=\; \left\{ \mathsf{n}^{j_n} \mid \tau_n = \_, \text{TN}(j_n, 1) \prec \tau \right\} \;\cup \bigcup_{\substack{\tau_a = \_, \text{TU}_{\text{ID}}(j_a, 1) \\ \tau_a \prec \tau}} \textsf{set-mac}^4_{\text{ID}} \left(\alpha^{\text{ID}}_{\tau_a}, \kappa^{\text{ID}}_{\tau_a} \right)$$

  And using (104), we know that:

$$\textsf{set-mac}^4_{\text{ID}}(\psi_0) \cap \mathcal{N} = \left\{ \mathsf{n}^{j_n} \mid \tau_n = \_, \text{TN}(j_n, 1) \prec \tau \right\} \tag{105}$$

- Let $\tau_n = \_, \text{TN}(j_n, 1)$ and $\tau_n{}' = \_, \text{TN}(j_n, 0)$ such that $\tau_n{}' \prec_\tau \tau_n$. Using **(StrEqu3)**, we know that:

$$\textsf{accept}^{\text{ID}}_{\tau_n} \;\leftrightarrow \bigvee_{\substack{\tau_i{}' = \_, \text{TU}_{\text{ID}}(j_i, 0) \\ \tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1) \\ \tau_i{}' \prec_\tau \tau_n{}' \prec_\tau \tau_i \prec_\tau \tau_n}} \textsf{full-tr}^{\mathsf{n}:\tau_n{}', \tau_n}_{\mathsf{u}:\tau_i{}', \tau_i}$$

  Let $\lambda^{\text{ID}}_{\tau_n}$ be the right-hand side of the equation above. We can check that $\mathsf{n}^{j_n} \in \textsf{set-mac}^4_{\text{ID}}(\lambda^{\text{ID}}_{\tau_n})$ if and only if there exists $\tau_i{}' = \_, \text{TU}_{\text{ID}}(j_i, 0)$ and $\tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1)$ such that $\tau_i{}' \prec_\tau \tau_n{}' \prec_\tau \tau_i \prec_\tau \tau_n$. Since $\tau_i \prec \tau$, we know that $j_i \neq j$. Therefore $\tau_i \prec_\tau \tau_2$, and we can show that:

$$\textsf{set-mac}^4_{\text{ID}} \left(\lambda^{\text{ID}}_{\tau_n} \right) \cap \mathcal{N} \;=\; \emptyset \tag{106}$$

  Let ψ_1 be ψ_0 in which we replace, for every $\tau_n = \_, \text{TN}(j_n, 1)$ and $\tau_n{}' = \_, \text{TN}(j_n, 0)$ such that $\tau_n{}' \prec_\tau \tau_n$, any occurrence of $\textsf{accept}^{\text{ID}}_{\tau_n}$ by $\lambda^{\text{ID}}_{\tau_a}$. Using (105) and (106), we can check that:

$$\textsf{set-mac}^4_{\text{ID}}(\psi_1) \cap \mathcal{N} \;=\; \emptyset$$

  Which is what we wanted to show.

d) Part 4: Let $\tau_1 = \_, \text{TN}(j_0, 0)$ be such that $\tau_2 \prec_\tau \tau_1$. For every ${\tau_1}' = \_, \text{TN}(j_0', 0)$ be such that $\tau_2 \prec_\tau {\tau_1}'$, if $j_0' \neq j_0$ then $(\mathsf{n}^{j_0'} = \mathsf{n}^{j_0}) \leftrightarrow \mathsf{false}$. Moreover, since $\mathsf{set\text{-}mac}^4_{\text{ID}}(\psi_1) \cap \mathcal{N} = \emptyset$, we know that for every $\mathsf{n} \in \mathsf{set\text{-}mac}^4_{\text{ID}}(\psi_1)$, $(\mathsf{n} = \mathsf{n}^{j_0}) \leftrightarrow \mathsf{false}$.

We can therefore apply simultaneously the PRF-MAC^4 axiom with key $\mathsf{k}^{\text{ID}}_{\mathsf{m}}$ for every $\tau_1 = \_, \text{TN}(j_0, 0)$ be such that $\tau_2 \prec_\tau \tau_1$, to replace $\mathsf{Mac}^4_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{n}^{j_0})$ by a fresh nonce n_{τ_1}. We then rewrite back ψ_1 into ψ. This yield the derivation:

$$\dfrac{\dfrac{\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, (\mathsf{n}_{\tau_1})_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \zeta}{\psi_1, (\mathsf{n}_{\tau_1})_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \zeta}\ R}{\psi_1, \left(\mathsf{Mac}^4_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \zeta}\ \text{PRF-MAC}^4}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \left(\mathsf{Mac}^4_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \zeta}\ R$$

where:

$$\zeta \equiv \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left((\mathsf{Mac}^4_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}}$$

Observe that we never used the fact that τ was a *basic* trace of actions above, but only the fact that τ is a *valid* trace of actions. Therefore the same reasoning applies to ζ, which allows us, for every $\tau_1 = \_, \text{TN}(j_0, 0)$ be such that $\tau_2 \prec_\tau \tau_1$, to replace $\mathsf{Mac}^4_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{n}^{j_0})$ by a fresh nonce n'_{τ_1}. We conclude using fresh. We get:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, (\mathsf{n}_{\tau_1})_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, (\mathsf{n}'_{\tau_1})_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}}}\ \mathsf{fresh}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, (\mathsf{n}_{\tau_1})_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \left((\mathsf{Mac}^4_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\mathsf{n}^{j_0})\right)_{\substack{\tau_1 = \_, \text{TN}(j_0,0)\\ \tau_2 \prec_\tau \tau_1}}}\ R + \text{PRF-MAC}^4$$

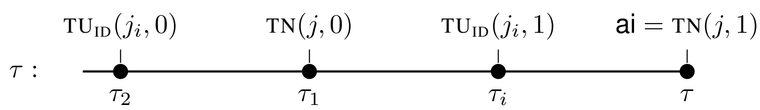
Which concludes this proof.

K. Case $\mathsf{ai} = \text{TN}(j, 1)$

We know that $\underline{\mathsf{ai}} = \text{TN}(j, 1)$. Here $\mathsf{l\text{-}reveal}_\tau$ and $\mathsf{l\text{-}reveal}_{\tau_0}$ coincides everywhere except on:

$$\mathsf{net\text{-}e\text{-}auth}_\tau(\text{ID}, j) \sim \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\text{ID}, j) \qquad\qquad \mathsf{sync\text{-}diff}^{\text{ID}}_\tau \sim \mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}$$

Let $\text{ID} \in \mathcal{S}_{\mathsf{bid}}$, $\tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1)$, $\tau_1 = \_, \text{TN}(j, 0)$, $\tau_2 = \_, \text{TU}_{\text{ID}}(j_i, 0)$ such that $\tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i$:



Let $\mathsf{f} \equiv \mathsf{full\text{-}tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i}$ and $\underline{\mathsf{f}} \equiv \mathsf{full\text{-}tr}^{\mathsf{n}:\underline{\tau_1},\underline{\tau}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau_i}}$. Using **(Der4)** we know that we have the following derivation:

$$\dfrac{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_\tau, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{f} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\mathsf{f}}}\ \mathsf{Simp} \tag{107}$$

Since $\mathsf{f} \to \mathsf{accept}^{\text{ID}}_\tau$, we have:

$$[\mathsf{f} \wedge \sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_\tau = [\mathsf{f} \wedge \sigma^{\mathsf{in}}_\tau(\mathsf{sync}^{\text{ID}}_{\text{U}})] \begin{pmatrix} \mathsf{if}\ \sigma^{\mathsf{in}}_\tau(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^j\ \mathsf{then}\ \mathsf{suc}(\mathsf{sync\text{-}diff}^{\text{ID}}_{\tau_0}) \\ \mathsf{else}\ \mathsf{sync\text{-}diff}^{\text{ID}}_{\tau_0} \end{pmatrix}$$

a) Case 1: Assume that $\tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1) \prec_\tau \text{NS}_{\text{ID}}(\_)$. Let $\tau_{\text{NS}} = \_, \text{NS}_{\text{ID}}(j_{\text{NS}})$ be the latest session reset in τ, i.e. $\tau_{\text{NS}} <_\tau \tau$ and $\tau_{\text{NS}} \not<_\tau \text{NS}_{\text{ID}}(\_)$. We show by induction that for every τ' such that $\tau_{\text{NS}} \preceq \tau'$ we have:

$$\left(f \wedge \sigma^{\mathsf{in}}_\tau(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^j\right) \to \sigma_{\tau_{\text{NS}}}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) \tag{108}$$

Let τ' be such that $\tau_{\text{NS}} \preceq \tau'$:

- If $\tau' = \tau_{\text{NS}}$ then the property trivially holds.
- If $\tau_{\text{NS}} \prec_\tau \tau'$. The only cases where $\text{SQN}^{\text{ID}}_{\text{N}}$ is updated are $\text{PN}(j', 1)$ and $\text{TN}(j', 1)$:
  - If $\tau' = \_, \text{PN}(j', 1)$: since $\tau = \text{TN}(j, 1)$ we know by validity of τ that $j' \neq j$. Therefore:

$$\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \to \left(\sigma_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j'}\right) \to \left(\sigma_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) \neq \mathsf{n}^j\right) \to \left(\sigma^{\mathsf{in}}_\tau(\mathsf{session}^{\text{ID}}_{\text{N}}) \neq \mathsf{n}^j\right)$$

It follows that:

$$\left(\sigma^{\text{in}}_{\tau}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^j\right) \ \rightarrow\ \neg\text{inc-accept}^{\text{ID}}_{\tau'} \ \rightarrow\ \left(\sigma^{\text{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}})\right)$$

And we conclude by applying the induction hypothesis.

– If $\tau' = \_, \text{TN}(j', 1)$: since $\tau = \text{TN}(j, 1)$ and $\tau' \prec \tau$, we know that $j' \neq j$ (by validity of τ). Therefore:

$$\left(\sigma^{\text{in}}_{\tau}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^j\right) \ \rightarrow\ \neg\text{inc-accept}^{\text{ID}}_{\tau'} \ \rightarrow\ \left(\sigma^{\text{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}})\right)$$

And we conclude by applying the induction hypothesis.

This concludes the proof of (108).

We then prove by induction over τ', for $\text{NS}_{\text{ID}}(j_{\text{NS}}) \preceq \tau' \preceq \tau$ we have:

$$\left(f \wedge \sigma^{\text{in}}_{\tau}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^j\right) \ \rightarrow\ \neg\sigma_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) \tag{109}$$

Let ai' be such that $\tau' = \_, \text{ai}'$.

- The case $\text{ai}' = \text{NS}_{\text{ID}}(j_{\text{NS}})$ is trivial since we then have $\sigma_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) = \text{false}$.
- If $\text{ai}' \neq \text{PU}_{\text{ID}}(\_, 2)$, then since $\text{NS}(j_{\text{NS}}) \not\prec_{\tau} \text{NS}(\_)$ we know that $\text{ai}' \neq \text{NS}(\_)$. Hence $\sigma^{\text{up}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) = \perp$, which implies $\sigma_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) \equiv \sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}})$. By induction hypothesis we know that:

$$\left(f \wedge \sigma^{\text{in}}_{\tau}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^j\right) \ \rightarrow\ \neg\sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}})$$

which concludes this case.
- If $\text{ai}' = \text{PU}_{\text{ID}}(j', 2)$. Let $\tau''' = \_, \text{PU}_{\text{ID}}(j', 1) <_{\tau}$. By validity of τ we know that $\tau_{\text{NS}} \prec_{\tau} \tau'''$. Using **(Equ2)** we know that:

$$\text{accept}^{\text{ID}}_{\tau'} \ \leftrightarrow \bigvee_{\substack{\tau''=\_,\text{PN}(j'',1)\\ \tau'''\prec_{\tau}\tau''\prec_{\tau}\tau'}} \text{supi-tr}^{\text{n}:\tau''}_{\text{u}:\tau''',\tau'}$$

And using **(StrEqu4)**:

$$\left(\neg\sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{supi-tr}^{\text{n}:\tau''}_{\text{u}:\tau''',\tau'}\right) \ \rightarrow\ \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}}) - \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) = \mathbf{0}$$

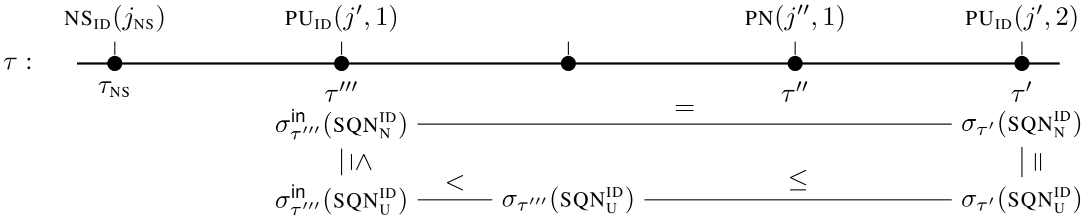
Using (108), we know that:

$$\left(f \wedge \sigma^{\text{in}}_{\tau}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^j\right) \ \rightarrow\ \left(\sigma_{\tau_{\text{NS}}}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma^{\text{in}}_{\tau'''}(\text{SQN}^{\text{ID}}_{\text{N}}) \wedge \sigma_{\tau_{\text{NS}}}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}})\right)$$

Therefore:

$$\left(f \wedge \sigma^{\text{in}}_{\tau}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^j\right) \ \rightarrow\ \left(\sigma^{\text{in}}_{\tau'''}(\text{SQN}^{\text{ID}}_{\text{N}}) = \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}})\right)$$

Using **(B5)** we know that $\sigma^{\text{in}}_{\tau'''}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\text{in}}_{\tau'''}(\text{SQN}^{\text{ID}}_{\text{U}})$, and by **(B1)** we know that $\sigma_{\tau'''}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}})$. Moreover $\sigma_{\tau'''}(\text{SQN}^{\text{ID}}_{\text{N}}) = \text{suc}(\sigma^{\text{in}}_{\tau'''}(\text{SQN}^{\text{ID}}_{\text{N}})) < \sigma^{\text{in}}_{\tau'''}(\text{SQN}^{\text{ID}}_{\text{N}})$. We summarize all of this graphically below:



Putting everything together we get that:

$$\left(\text{f} \wedge \neg\sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{supi-tr}^{\text{n}:\tau''}_{\text{u}:\tau''',\tau'}\right) \ \rightarrow\ \left(\sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma_{\tau'}(\text{SQN}^{\text{ID}}_{\text{U}})\right) \ \rightarrow\ \text{false}$$

We deduce that:

$$\left(\text{f} \wedge \neg\sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{accept}^{\text{ID}}_{\tau'}\right) \ \rightarrow \bigvee_{\substack{\tau''=\_,\text{PN}(j'',1)\\ \text{PU}_{\text{ID}}(j',1)\prec_{\tau}\tau''\prec_{\tau}\tau'}} \left(\text{f} \wedge \neg\sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}}) \wedge \text{supi-tr}^{\text{n}:\tau''}_{\text{u}:\_,\tau'}\right)$$
$$\rightarrow\ \text{false}$$

Moreover, using the induction hypothesis we know that:

$$\left(f \wedge \sigma^{\text{in}}_{\tau}(\text{session}^{\text{ID}}_{\text{N}}) = \text{n}^j\right) \ \rightarrow\ \neg\sigma^{\text{in}}_{\tau'}(\text{sync}^{\text{ID}}_{\text{U}})$$

Therefore:

$$\left(f \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j}\right) \;\rightarrow\; \neg\mathsf{accept}_{\tau'} \;\rightarrow\; \neg\sigma_{\tau'}(\mathsf{sync}^{\text{ID}}_{\text{U}})$$

This concludes the proof by induction of (109). Using (109) we get that:

$$[\mathsf{f}]\mathsf{sync\text{-}diff}^{\text{ID}}_{\tau} = [\mathsf{f} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}})]\mathsf{sync\text{-}diff}^{\text{ID}}_{\tau_0}$$

We know that $\underline{\mathsf{f}} \rightarrow \mathsf{accept}^{\nu_{\tau_2}(\text{ID})}_{\underline{\tau}}$. Moreover, $\nu_{\tau_2}(\text{ID}) \neq \nu_{\tau}(\text{ID})$, hence using **(A5)** we know that $\underline{\mathsf{f}} \rightarrow \neg\mathsf{accept}^{\nu_{\tau}(\text{ID})}_{\underline{\tau}}$. Hence:

$$[\underline{\mathsf{f}}]\mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}} = [\underline{\mathsf{f}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}})]\mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau_0}}$$

Using the derivation in (107) and the fact that:

$$\left(\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}), \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}})\right) \in \mathsf{reveal}_{\tau_0} \qquad\qquad \left(\mathsf{sync\text{-}diff}^{\text{ID}}_{\tau}, \mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau_0}}\right) \in \mathsf{reveal}_{\tau_0}$$

We can build the derivation:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\begin{array}{c}\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{f}, \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\text{ID}}_{\text{U}}), \quad \mathsf{sync\text{-}diff}^{\text{ID}}_{\tau_0} \\ \sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\mathsf{f}}, \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\text{ID})}_{\text{U}}), \mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau_0}}\end{array}}\ \mathsf{Simp}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, [\mathsf{f}]\mathsf{sync\text{-}diff}^{\text{ID}}_{\tau} \;\sim\; \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, [\underline{\mathsf{f}}]\mathsf{sync\text{-}diff}^{\nu_\tau(\text{ID})}_{\underline{\tau}}}\ \mathsf{Simp} \tag{110}$$

b) Case 2: Assume that $\tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1) \not\prec_{\tau} \text{NS}_{\text{ID}}(\_)$. We introduce the term θ_{PN} (resp. θ_{TN}) which states that no SUPI (resp. GUTI) network session has been initiated which ID between τ_1 and τ:

$$\theta_{\text{PN}} \;\equiv\; \bigwedge_{\substack{\tau'=\_,\text{PN}(\_,1)\\ \tau_1 \prec_\tau \tau'}} \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \qquad\qquad \theta_{\text{TN}} \;\equiv\; \bigwedge_{\substack{\tau'=\text{TN}(\_,0)\\ \tau_1 \prec_\tau \tau'}} \neg\mathsf{accept}^{\text{ID}}_{\tau'}$$

It is easy to show that:

$$\left(\mathsf{f} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j}\right) \;\leftrightarrow\; (\mathsf{f} \wedge \theta_{\text{PN}} \wedge \theta_{\text{TN}})$$

We are now going to show that for every $\tau_1 \preceq \tau'$, $P(\tau')$ holds where $P(\tau')$ is the term:

$$P(\tau') \;\equiv\; (\mathsf{f} \wedge \theta_{\text{PN}}) \;\rightarrow\; \left(\begin{array}{l}\sigma_{\tau'}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \mathsf{UnSet} \\ \wedge\, \sigma_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j}\end{array} \;\wedge \bigwedge_{\substack{\tau_1 \prec_\tau \tau'' \preceq \tau'\\ \tau''=\text{TN}(\_,0)}} \neg\mathsf{accept}^{\text{ID}}_{\tau''}\right) \tag{111}$$

Since $\mathsf{f} \rightarrow \mathsf{accept}_{\tau_1}$, we know that $\mathsf{f} \rightarrow \sigma_{\tau_1}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \mathsf{UnSet}$. This shows that $P(\mathsf{suc}_{\tau}(\tau_1))$ holds. Let $\tau_1 \preceq \tau'_0$, and assume $P(\tau'_0)$ holds by induction. Let $\tau' = \mathsf{suc}_{\tau}(\tau'_0)$. We have four cases:

- If $\tau' \not\in \{\text{TN}(\_,0), \text{TN}(\_,1), \text{PN}(\_,1)\}$ then $P(\tau') \equiv P(\tau'_0)$, which concludes this case.
- If $\tau' = \text{TN}(\_,0)$, then using the induction hypothesis $P(\tau'_0)$ we know that $\mathsf{f} \wedge \theta_{\text{PN}} \rightarrow \sigma^{\mathsf{in}}_{\tau'}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \mathsf{UnSet}$. Therefore $\mathsf{f} \wedge \theta_{\text{PN}} \rightarrow \neg\mathsf{accept}^{\text{ID}}_{\tau'}$. We know that $\mathsf{f} \wedge \theta_{\text{PN}} \rightarrow \sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j}$. We conclude by observing that:

$$\left(\neg\mathsf{accept}^{\text{ID}}_{\tau'} \wedge \sigma^{\mathsf{in}}_{\tau'}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \mathsf{UnSet} \wedge \sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j}\right) \rightarrow \left(\sigma_{\tau'}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \mathsf{UnSet} \wedge \sigma_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j}\right)$$

- If $\tau' = \text{TN}(j',1)$. Since $\tau' \prec \tau$, we know that $j \neq j'$. Therefore $\sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j} \rightarrow \sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) \neq \mathsf{n}^{j'}$. We deduce that $\mathsf{f} \wedge \theta_{\text{PN}} \rightarrow \neg\mathsf{accept}^{\text{ID}}_{\tau'}$. This concludes this case.
- If $\tau' = \_, \text{PN}(\_,1)$. We know that:

$$\mathsf{f} \wedge \theta_{\text{PN}} \rightarrow \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'}$$

  We then directly conclude using the facts that:

$$\neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \rightarrow \sigma_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau'}(\mathsf{session}^{\text{ID}}_{\text{N}}) \qquad\qquad \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \rightarrow \sigma_{\tau'}(\text{GUTI}^{\text{ID}}_{\text{N}}) = \sigma^{\mathsf{in}}_{\tau'}(\text{GUTI}^{\text{ID}}_{\text{N}})$$

By applying (111) at instant τ_0, we get that:

$$\left(\mathsf{f} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\text{ID}}_{\text{N}}) = \mathsf{n}^{j}\right) \;\leftrightarrow\; (\mathsf{f} \wedge \theta_{\text{PN}} \wedge \theta_{\text{TN}}) \;\leftrightarrow\; (\mathsf{f} \wedge \theta_{\text{PN}}) \tag{112}$$

c) Part 1: Let $\tau' = \_, \text{PN}(j', 1)$, with $\tau_1 \prec_\tau \tau'$. Let $\tau'_0 = \text{PN}(j', 0)$. Using **(Equ3)** we know that:

$$\mathsf{accept}^{\text{ID}}_{\tau'} \;\leftrightarrow\; \bigvee_{\substack{\tau_a = \_, \text{PU}_{\text{ID}}(j_a, 1) \\ \tau'_0 \prec_\tau \tau_a \prec_\tau \tau'}} \underbrace{\begin{pmatrix} g(\phi^{\mathsf{in}}_{\tau_a}) = \mathsf{n}^{j'} \wedge \pi_1(g(\phi^{\mathsf{in}}_{\tau'})) = \{\langle \text{ID} \,,\, \sigma^{\mathsf{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle\}^{\mathsf{n}_{\mathsf{e}}^{j_a}}_{\mathsf{pk}_{\text{N}}} \\ \wedge\, \pi_2(g(\phi^{\mathsf{in}}_{\tau'})) = \mathsf{Mac}^1_{\mathsf{k}^{\text{ID}}_{\mathsf{m}}}(\langle \{\langle \text{ID} \,,\, \sigma^{\mathsf{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) \rangle\}^{\mathsf{n}_{\mathsf{e}}^{j_a}}_{\mathsf{pk}_{\text{N}}} \,,\, g(\phi^{\mathsf{in}}_{\tau_a}) \rangle) \end{pmatrix}}_{\lambda^{\tau'}_{\tau_a}} \tag{113}$$

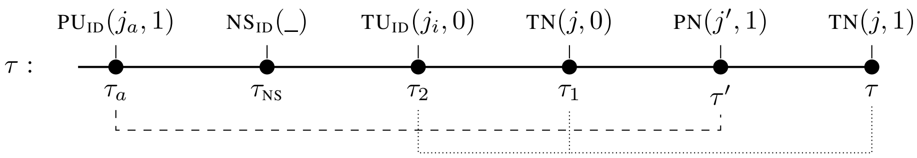
We define:

$$\tau_{\text{NS}} = \begin{cases} \text{NS}_{\text{ID}}(j_{\text{NS}}) & \text{if there exists } j_{\text{NS}} \text{ s.t. } \text{NS}_{\text{ID}}(j_{\text{NS}}) <_\tau \tau \text{ and } \text{NS}_{\text{ID}}(j_{\text{NS}}) \not\prec_\tau \text{NS}_{\text{ID}}(\_). \\ \epsilon & \text{otherwise} \end{cases}$$

Let $\tau_a = \_, \text{PU}_{\text{ID}}(j_a, 1)$ such that $\tau'_0 \prec_\tau \tau_a \prec_\tau \tau'$. Since $\tau_i = \_, \text{TU}_{\text{ID}}(j_i, 1) \not\prec_\tau \text{NS}_{\text{ID}}(\_)$, we have only three interleavings possible: $\tau_1 \prec_\tau \tau_a$, $\tau_1 \prec_\tau \tau_a$ or $\tau_{\text{NS}} \prec_\tau \tau_a \prec_\tau \tau_2$. First, we are going to show that in the first two cases we have:

$$\mathsf{f} \wedge \lambda^{\tau'}_{\tau_a} \;\rightarrow\; \neg \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'}$$

- If $\tau_a \prec_\tau \tau_{\text{NS}}$, we have the following interleaving:



By definition of $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'}$, and using the fact that $\lambda^{\tau'}_{\tau_a} \rightarrow \mathsf{accept}^{\text{ID}}_{\tau'}$ we know that:

$$\left(\lambda^{\tau'}_{\tau_a} \wedge \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'}\right) \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}})$$

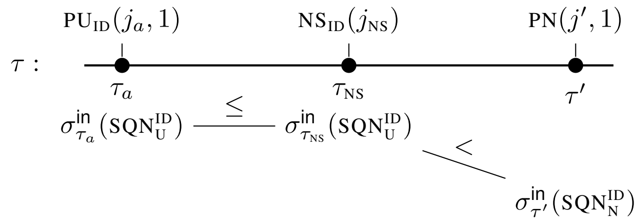
To conclude this case, we only need to show that:

$$\left(\lambda^{\tau'}_{\tau_a} \wedge \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'}\right) \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) \tag{114}$$

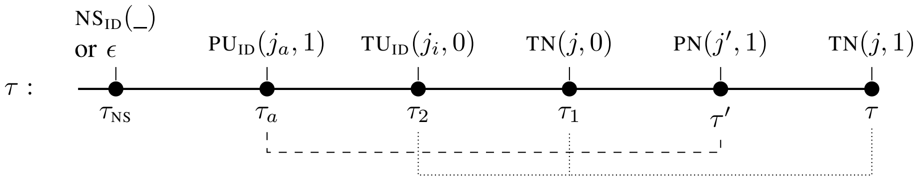
From which we obtain directly a contradiction, implies that:

$$\mathsf{f} \wedge \lambda^{\tau'}_{\tau_a} \;\rightarrow\; \neg \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \qquad\qquad \text{when } \tau_a \prec_\tau \tau_{\text{NS}} \tag{115}$$

The proof of (114) is straightforward using **(B1)** and **(B6)**, we just give the proof graphically below:



- If $\tau_{\text{NS}} \prec_\tau \tau_a \prec_\tau \tau_2$, we have the following interleaving:



We know that $\lambda^{\tau'}_{\tau_a} \rightarrow \sigma_{\tau_a}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \mathsf{UnSet}$, and that $\mathsf{f} \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\mathsf{sync}^{\text{ID}}_{\text{U}})$. By **(B3)**, we get $\mathsf{f} \rightarrow \sigma^{\mathsf{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) \neq \mathsf{UnSet}$. This means that $\text{GUTI}^{\text{ID}}_{\text{U}}$ is unset at τ_a, but set at τ_2. Therefore there was a successful run of the protocol (SUPI or GUTI) between τ_a and τ_2. More precisely, using Proposition 23 we have:

$$\begin{aligned} \mathsf{f} \wedge \lambda^{\tau'}_{\tau_a} \;&\rightarrow\; \left(\sigma_{\tau_a}(\text{GUTI}^{\text{ID}}_{\text{U}}) = \mathsf{UnSet} \wedge \sigma^{\mathsf{in}}_{\tau_2}(\text{GUTI}^{\text{ID}}_{\text{U}}) \neq \mathsf{UnSet}\right) \\ &\rightarrow \bigvee_{\substack{\tau'' = \_, \text{FU}_{\text{ID}}(j'') \\ \tau_a \prec_\tau \tau'' \prec_\tau \tau_2}} \mathsf{accept}^{\text{ID}}_{\tau''} \end{aligned} \tag{116}$$

Let $\tau'' = \_, \text{FU}_{\text{ID}}(j'')$ such that $\tau_a \prec_\tau \tau'' \prec_\tau \tau_2$. We then have two cases:

– Assume $j'' = j_a$. In order to have $\mathsf{accept}^{\text{ID}}_{\tau''}$, we need the SUPI or GUTI session j'' to have been executed before τ''. Intuitively, this cannot happen if $j'' = j_a$ because the user session j_a is interacting with the network session j', and $\tau'' \prec_\tau \tau'$. Formally, using the fact that $j'' = j_a$ we are going to show that:

$$\left(\lambda^{\tau'}_{\tau_a} \wedge \mathsf{accept}^{\text{ID}}_{\tau''}\right) \rightarrow \mathsf{false} \tag{117}$$

First, by **(Equ1)** we know that:

$$\begin{aligned}\mathsf{accept}^{\text{ID}}_{\tau''} &\rightarrow \bigvee_{\text{FN}(j_x) \not\prec_{\tau''} \text{NS}_{\text{ID}}(\_)} \mathsf{inj\text{-}auth}_{\tau''}(\text{ID}, j_x)\\ &\rightarrow \bigvee_{\text{FN}(j_x) \not\prec_{\tau''} \text{NS}_{\text{ID}}(\_)} \left(\sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{j_x}_{\text{N}}) = \text{ID} \wedge \sigma^{\mathsf{in}}_{\tau''}(\mathsf{e\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_x}\right)\end{aligned}$$

By **(A8)** we get:

$$\rightarrow \bigvee_{\text{FN}(j_x) \not\prec_{\tau''} \text{NS}_{\text{ID}}(\_)} \left(\sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{j_x}_{\text{N}}) = \text{ID} \wedge \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_x}\right) \tag{118}$$

We know that $\lambda^{\tau'}_{\tau_a} \rightarrow \sigma^{\mathsf{in}}_{\tau_a}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j'}$. Moreover, using the validity of τ we know that $\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}$ is not updated between τ_a and τ'', therefore $\lambda^{\tau'}_{\tau_a} \rightarrow \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j'}$. Putting this together with (118), and using the fact that:

$$\left(\sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j_x} \wedge \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j'}\right) \rightarrow \mathsf{false} \text{ if } j_x \neq j'$$

We get:

$$\mathsf{accept}^{\text{ID}}_{\tau''} \wedge \lambda^{\tau'}_{\tau_a} \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{j'}_{\text{N}}) = \text{ID} \wedge \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{\text{ID}}_{\text{U}}) = \mathsf{n}^{j'}$$

Since $\tau'' \prec_\tau \tau'$, we know that $\sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{j'}_{\text{N}}) = \bot$. This yields a contradiction:

$$\begin{aligned}&\rightarrow\; \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{j'}_{\text{N}}) = \text{ID} \wedge \sigma^{\mathsf{in}}_{\tau''}(\mathsf{b\text{-}auth}^{j'}_{\text{N}}) = \bot\\ &\rightarrow\; \mathsf{false}\end{aligned}$$

Which concludes the proof of (117).

– Assume $j'' \neq j_a$. Intuitively, we know that $\mathsf{accept}^{\text{ID}}_{\tau''}$ implies that $\text{SQN}^{\text{ID}}_{\text{U}}$ and $\text{SQN}^{\text{ID}}_{\text{N}}$ have been incremented and synchronized between τ_a and τ'. Therefore we know that the test $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'}$ fails. Formally, we show that:

$$\mathsf{accept}^{\text{ID}}_{\tau''} \;\rightarrow\; \sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau''}(\text{SQN}^{\text{ID}}_{\text{N}}) \tag{119}$$

We give the outline of the proof. First, we apply **(StrEqu1)** to τ''. Then, we take $\tau''_0 = \_, \text{FN}(j_e) \prec \tau''$. We let $\tau''_1 = \_, \text{PN}(j_e, 1)$ or $\_, \text{TN}(j_e, 1)$ such that $\tau''_1 \prec \tau''_0$, and we do a case disjunction on τ''_1:

* If $\tau''_1 = \_, \text{PN}(j_e, 1)$, then we use **(StrEqu4)** on it, and we show that $\sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau''}(\text{SQN}^{\text{ID}}_{\text{N}})$ by doing a case disjunction on $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau''_1}$.
* If $\tau''_1 = \_, \text{TN}(j_e, 1)$, then we use **(StrEqu2)** on it, and we show that $\sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau''}(\text{SQN}^{\text{ID}}_{\text{N}})$ using **(B4)**

We omit the details.

Using **(B1)** we know that $\sigma^{\mathsf{in}}_{\tau''}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}})$ and $\sigma^{\mathsf{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) \leq \sigma_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}})$. Hence, we deduce from (119) that:

$$\mathsf{accept}^{\text{ID}}_{\tau''} \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) \tag{120}$$

Moreover, by definition of $\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'}$, and using the fact that $\lambda^{\tau'}_{\tau_a} \rightarrow \mathsf{accept}^{\text{ID}}_{\tau'}$ we know that:

$$\left(\lambda^{\tau'}_{\tau_a} \wedge \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'}\right) \;\rightarrow\; \sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) \tag{121}$$

Putting (120) and (121) together:

$$\left(\lambda^{\tau'}_{\tau_a} \wedge \mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \wedge \mathsf{accept}^{\text{ID}}_{\tau''}\right) \;\rightarrow\; \left(\sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}}) \leq \sigma^{\mathsf{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) \wedge \sigma^{\mathsf{in}}_{\tau_a}(\text{SQN}^{\text{ID}}_{\text{U}}) < \sigma^{\mathsf{in}}_{\tau'}(\text{SQN}^{\text{ID}}_{\text{N}})\right) \;\rightarrow\; \mathsf{false}$$

Hence:

$$\left(\lambda^{\tau'}_{\tau_a} \wedge \mathsf{accept}^{\text{ID}}_{\tau''}\right) \;\rightarrow\; \neg\mathsf{inc\text{-}accept}^{\text{ID}}_{\tau'} \tag{122}$$

From (116), (117) and (122) we deduce that:

$$\begin{aligned}\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} &\rightarrow \bigvee_{\substack{\tau''=\_,\text{FU}_{\text{ID}}(j'') \\ \tau_a \prec_\tau \tau'' \prec_\tau \tau_2}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \wedge \mathsf{accept}_{\tau''}^{\text{ID}} \\ &\rightarrow \bigvee_{\substack{\tau''=\_,\text{FU}_{\text{ID}}(j'') \\ \tau_a \prec_\tau \tau'' \prec_\tau \tau_2}} \neg\mathsf{inc\text{-}accept}_{\tau'}^{\text{ID}}\end{aligned}$$

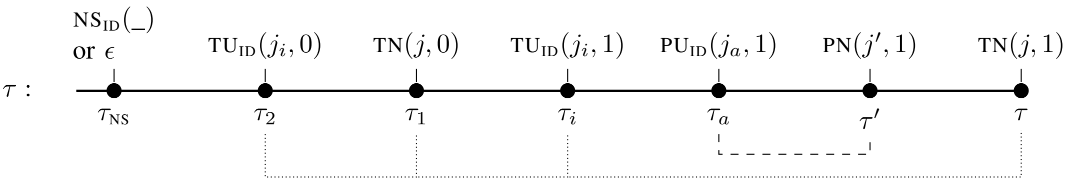
Hence:

$$\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \rightarrow \neg\mathsf{inc\text{-}accept}_{\tau'}^{\text{ID}} \qquad \text{when } \tau_{\text{NS}} \prec_\tau \tau_a \prec_\tau \tau_2 \tag{123}$$

d) Part 2: Using (115) and (123), we know that we can focus on the (partial) SUPI sessions that started after τ_i, i.e. the sessions with transcript of the from $\lambda_{\tau_a}^{\tau'}$, where $\tau_a = \_, \text{PU}_{\text{ID}}(j_a, 1)$, $\tau' = \_, \text{PN}(j', 1)$ and $\tau_i \prec_\tau \tau_a \prec_\tau \tau'$. Formally, we have:

$$\begin{aligned}(\mathsf{f} \wedge \theta_{\text{PN}}) &\leftrightarrow \bigwedge_{\substack{\tau'=\_,\text{PN}(\_,1) \\ \tau_1 \prec_\tau \tau'}} \neg\mathsf{inc\text{-}accept}_{\tau'}^{\text{ID}} \\ &\leftrightarrow \bigwedge_{\substack{\tau'=\_,\text{PN}(\_,1) \\ \tau_1 \prec_\tau \tau'}} \left((\mathsf{f} \wedge \mathsf{accept}_{\tau'}^{\text{ID}}) \rightarrow \neg\mathsf{inc\text{-}accept}_{\tau'}^{\text{ID}}\right) \\ &\leftrightarrow \bigwedge_{\substack{\tau'=\_,\text{PN}(j',1) \\ \tau_0'=\_,\text{PN}(j',0) \\ \tau_a=\_,\text{PU}_{\text{ID}}(j_a,1) \\ \tau_1 \prec_\tau \tau' \\ \tau_0' \prec_\tau \tau_a \prec_\tau \tau'}} \left(\left(\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'}\right) \rightarrow \neg\mathsf{inc\text{-}accept}_{\tau'}^{\text{ID}}\right) && \text{(By (113))} \\ &\leftrightarrow \bigwedge_{\substack{\tau_a=\_,\text{PU}_{\text{ID}}(j_a,1) \\ \tau'=\_,\text{PN}(j',1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \left(\left(\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'}\right) \rightarrow \neg\mathsf{inc\text{-}accept}_{\tau'}^{\text{ID}}\right) && \text{(By (115) and (123))}\end{aligned}$$

We represent graphically the shape of the interleavings that we need to consider:



e) Part 3: We are now going to show that if at least one partial SUPI session that started after τ_i accepts (i.e. $\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'}$ holds), then we have $\sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\text{N}}^{\text{ID}}) \neq \mathsf{n}^j$. First, from what we showed in **Part 2**, and using (112) we know that:

$$\begin{aligned}\neg\left(\mathsf{f} \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\text{N}}^{\text{ID}}) = \mathsf{n}^j\right) &\leftrightarrow \bigvee_{\substack{\tau_a=\_,\text{PU}_{\text{ID}}(j_a,1) \\ \tau'=\_,\text{PN}(j',1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \wedge \mathsf{inc\text{-}accept}_{\tau'}^{\text{ID}} \\ &\rightarrow \bigvee_{\substack{\tau_a=\_,\text{PU}_{\text{ID}}(j_a,1) \\ \tau'=\_,\text{PN}(j',1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'}\end{aligned}$$

In a first time, assume that for every $\tau_a = \_, \text{PU}_{\text{ID}}(j_a, 1)$ and $\tau' = \_, \text{PN}(j', 1)$ such that $\tau_i \prec_\tau \tau_a \prec_\tau \tau'$ we have:

$$\left(\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \wedge \neg\mathsf{inc\text{-}accept}_{\tau'}^{\text{ID}}\right) \rightarrow \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\text{N}}^{\text{ID}}) \neq \mathsf{n}^j \tag{124}$$

Then we know that:

$$\bigvee_{\substack{\tau_a=\_,\text{PU}_{\text{ID}}(j_a,1) \\ \tau'=\_,\text{PN}(j',1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \rightarrow \neg\left(\mathsf{f} \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\text{N}}^{\text{ID}}) = \mathsf{n}^j\right)$$

Therefore:

$$\neg\left(\mathsf{f} \wedge \sigma_\tau^{\mathsf{in}}(\mathsf{session}_{\text{N}}^{\text{ID}}) = \mathsf{n}^j\right) \leftrightarrow \bigvee_{\substack{\tau_a=\_,\text{PU}_{\text{ID}}(j_a,1) \\ \tau'=\_,\text{PN}(j',1) \\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \tag{125}$$

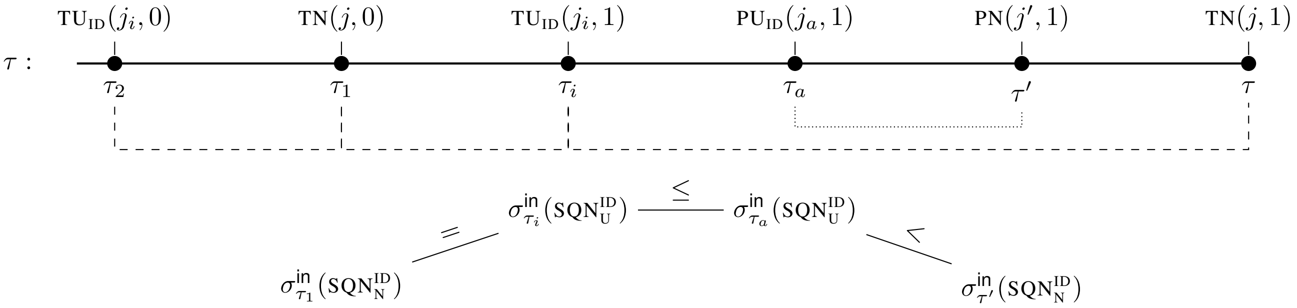
We now give the proof of (124). Let $\tau_a = \_, \text{PU}_{\text{ID}}(j_a, 1)$ and $\tau' = \_, \text{PN}(j', 1)$ such that $\tau_i \prec_\tau \tau_a \prec_\tau \tau'$. We know that:

$$\left(\lambda_{\tau_a}^{\tau'} \wedge \neg \text{inc-accept}_{\tau'}^{\text{ID}}\right) \;\rightarrow\; \sigma_{\tau_a}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}) < \sigma_{\tau'}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}})$$

And that:

$$\mathsf{f} \;\rightarrow\; \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) = \sigma_{\tau_i}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}})$$

Moreover by **(B1)** we know that $\sigma_{\tau_i}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}}) \leq \sigma_{\tau_a}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}})$. We summarize this graphically:



We deduce that:

$$\left(\mathsf{f} \wedge \lambda_{\tau_a}^{\tau'} \wedge \neg \text{inc-accept}_{\tau'}^{\text{ID}}\right) \;\rightarrow\; \sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) < \sigma_{\tau'}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}})$$

Moreover:

$$\sigma_{\tau_1}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) < \sigma_{\tau'}^{\text{in}}(\text{SQN}_{\text{N}}^{\text{ID}}) \;\rightarrow\; \Bigg(\bigvee_{\substack{\tau_x = \text{PN}(j_x,1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \text{inc-accept}_{\tau_x}^{\text{ID}}\Bigg) \vee \Bigg(\bigvee_{\substack{\tau_x = \text{TN}(j_x,1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \text{inc-accept}_{\tau_x}^{\text{ID}}\Bigg)$$

For every $\tau_x = \text{PN}(j_x, 1)$ such that $\tau_1 \prec_\tau \tau_x \prec_\tau \tau'$ we have $j_x \neq j$. Therefore:

$$\begin{aligned}\bigvee_{\substack{\tau_x = \text{PN}(j_x,1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \text{inc-accept}_{\tau_x}^{\text{ID}} \;&\rightarrow\; \bigvee_{\substack{\tau_x = \text{PN}(j_x,1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \sigma_{\tau_x}(\text{session}_{\text{N}}^{\text{ID}}) = \mathsf{n}^{j_x}\\ &\rightarrow\; \sigma_{\tau}^{\text{in}}(\text{session}_{\text{N}}^{\text{ID}}) \neq \mathsf{n}^{j}\end{aligned}$$

And:

$$\begin{aligned}\bigvee_{\substack{\tau_x = \text{TN}(j_x,1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \text{inc-accept}_{\tau_x}^{\text{ID}} \;&\rightarrow\; \bigvee_{\substack{\tau_x = \text{TN}(j_x,1)\\ \tau_1 \prec_\tau \tau_x \prec_\tau \tau'}} \sigma_{\tau_x}^{\text{in}}(\text{session}_{\text{N}}^{\text{ID}}) = \mathsf{n}^{j_x}\\ &\rightarrow\; \sigma_{\tau}^{\text{in}}(\text{session}_{\text{N}}^{\text{ID}}) \neq \mathsf{n}^{j}\end{aligned}$$

This concludes the proof of (124).

The proofs in **Part 1** to **3** only used the fact that τ is a valid symbolic trace. We never used the fact that τ is a basic trace. Therefore, carrying out the same proof, we can show that:

$$\neg\left(\underline{\mathsf{f}} \wedge \sigma_{\underline{\tau}}^{\text{in}}(\text{session}_{\text{N}}^{\nu_\tau(\text{ID})}) = \mathsf{n}^{j}\right) \;\leftrightarrow\; \bigvee_{\substack{\tau_a = \_, \text{PU}_{\text{ID}}(j_a,1)\\ \tau' = \_, \text{PN}(j',1)\\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \underline{\mathsf{f}} \wedge \lambda_{\underline{\tau_a}}^{\underline{\tau'}} \tag{126}$$

f) Part 4: Let $\tau_a = \_, \text{PU}_{\text{ID}}(j_a, 1)$ and $\tau' = \_, \text{PN}(j', 1)$ be such that $\tau_i \prec_\tau \tau_a \prec_\tau \tau'$. Observing that:

$$\left(\mathsf{n}^{j'}, \mathsf{n}^{j'}\right) \in \text{reveal}_{\tau_0} \qquad \left(\{\langle \text{ID}\,,\, \sigma_{\tau_a}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_a}}, \{\langle \nu_\tau(\text{ID})\,,\, \sigma_{\underline{\tau_a}}^{\text{in}}(\text{SQN}_{\text{U}}^{\nu_\tau(\text{ID})})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_a}}\right) \in \text{reveal}_{\tau_0}$$

$$\left(\text{Mac}_{\mathsf{k}_{\mathsf{m}}^{\text{ID}}}^{1}(\langle\{\langle \text{ID}\,,\, \sigma_{\tau_a}^{\text{in}}(\text{SQN}_{\text{U}}^{\text{ID}})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_a}}\,,\, g(\phi_{\tau_a}^{\text{in}})\rangle), \text{Mac}_{\mathsf{k}_{\mathsf{m}}^{\nu_\tau(\text{ID})}}^{1}(\langle\{\langle \nu_\tau(\text{ID})\,,\, \sigma_{\underline{\tau_a}}^{\text{in}}(\text{SQN}_{\text{U}}^{\nu_\tau(\text{ID})})\rangle\}_{\mathsf{pk}_{\text{N}}}^{\mathsf{n}_{\mathsf{e}}^{j_a}}\,,\, g(\phi_{\underline{\tau_a}}^{\text{in}})\rangle)\right) \in \text{reveal}_{\tau_0}$$

It is straightforward to show that we have a derivation of:

$$\frac{\phi_{\tau}^{\text{in}}, \text{l-reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}}{\phi_{\tau}^{\text{in}}, \text{l-reveal}_{\tau_0}, \lambda_{\tau_a}^{\tau'} \;\sim\; \phi_{\underline{\tau}}^{\text{in}}, \text{r-reveal}_{\tau_0}, \lambda_{\underline{\tau_a}}^{\underline{\tau'}}}\ \text{Simp}$$

Using (125) and (126), and combining the derivation above with the derivation in (107), we can build the following derivation:

$$\dfrac{\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0},}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \neg\left(\bigvee_{\substack{\tau_a = \_,\mathrm{PU_{ID}}(j_a,1)\\ \tau' = \_,\mathrm{PN}(j',1)\\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \mathsf{f} \wedge \lambda^{\tau'}_{\tau_a}\right) \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \neg\left(\bigvee_{\substack{\tau_a = \_,\mathrm{PU_{ID}}(j_a,1)\\ \tau' = \_,\mathrm{PN}(j',1)\\ \tau_i \prec_\tau \tau_a \prec_\tau \tau'}} \underline{\mathsf{f}} \wedge \lambda^{\underline{\tau'}}_{\underline{\tau_a}}\right)}\,(\mathsf{Dup}, \mathsf{FA})^*}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{f} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^j \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\mathsf{f}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{session}^{\nu_\tau(\mathrm{ID})}_{\mathrm{N}}) = \mathsf{n}^j}\,R \tag{127}$$

We know that:

$$[\mathsf{f}]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} = \begin{array}{l} \text{if } \mathsf{f} \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}) \wedge \sigma^{\mathsf{in}}_{\tau}(\mathsf{session}^{\mathrm{ID}}_{\mathrm{N}}) = \mathsf{n}^j \\ \quad \text{then } \mathsf{suc}(\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_0}) \\ \quad \text{else } \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_0} \end{array}$$

Similarly:

$$[\underline{\mathsf{f}}]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} = \begin{array}{l} \text{if } \underline{\mathsf{f}} \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}}) \wedge \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{session}^{\nu_\tau(\mathrm{ID})}_{\mathrm{N}}) = \mathsf{n}^j \\ \quad \text{then } \mathsf{suc}(\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}}) \\ \quad \text{else } \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}} \end{array}$$

Hence, using (127) and the fact that:

$$\left(\sigma^{\mathsf{in}}_{\tau}(\mathsf{sync}^{\mathrm{ID}}_{\mathrm{U}}), \sigma^{\mathsf{in}}_{\underline{\tau}}(\mathsf{sync}^{\nu_\tau(\mathrm{ID})}_{\mathrm{U}})\right) \in \mathsf{reveal}_{\tau_0} \qquad \left(\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau_0}, \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau_0}}\right) \in \mathsf{reveal}_{\tau_0}$$

We have a derivation of:

$$\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, [\mathsf{f}]\mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, [\underline{\mathsf{f}}]\mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}\,\mathsf{Simp} \tag{128}$$

g) Part 5: Using **(J10)**, we know that:

$$\mathsf{accept}^{\mathrm{ID}}_{\tau} \ \leftrightarrow \bigvee_{\substack{\tau_i = \_,\mathrm{TU_{ID}}(j_i,1)\\ \tau_1 = \_,\mathrm{TN}(j,0)\\ \tau_2 = \_,\mathrm{TU_{ID}}(j_i,0)\\ \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \left(\mathsf{full\text{-}tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i}\right)$$

We split between the cases $\tau_i \prec_\tau \tau_{\mathrm{NS}}$ and $\tau_i \not\prec_\tau \tau_{\mathrm{NS}}$:

$$\leftrightarrow \bigvee_{\substack{\tau_i = \_,\mathrm{TU_{ID}}(j_i,1)\\ \tau_1 = \_,\mathrm{TN}(j,0)\\ \tau_2 = \_,\mathrm{TU_{ID}}(j_i,0)\\ \tau_2 \prec_\tau \tau_1 <_\tau \tau_i \prec_\tau \tau_{\mathrm{NS}}}} \left(\mathsf{full\text{-}tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i}\right) \vee \bigvee_{\substack{\tau_i = \_,\mathrm{TU_{ID}}(j_i,1)\\ \tau_1 = \_,\mathrm{TN}(j,0)\\ \tau_2 = \_,\mathrm{TU_{ID}}(j_i,0)\\ \tau_{\mathrm{NS}} \prec_\tau \tau_2 <_\tau \tau_1 \prec_\tau \tau_i}} \left(\mathsf{full\text{-}tr}^{\mathsf{n}:\tau_1,\tau}_{\mathsf{u}:\tau_2,\tau_i}\right)$$

If $\tau_i \prec_\tau \tau_{\mathrm{NS}}$ then $\nu_{\tau_2}(\mathrm{ID}) = \nu_{\tau_i}(\mathrm{ID}) \neq \nu_\tau(\mathrm{ID})$, and if $\tau_i \not\prec_\tau \tau_{\mathrm{NS}}$ then $\nu_{\tau_2}(\mathrm{ID}) = \nu_{\tau_i}(\mathrm{ID}) = \nu_\tau(\mathrm{ID})$. It follows, using **(J10)** on $\underline{\tau}$, that:

$$\bigvee_{\substack{\underline{\mathrm{ID}} \in \mathsf{copies\text{-}id}(\mathrm{ID})\\ \underline{\mathrm{ID}} \neq \nu_\tau(\mathrm{ID})}} \mathsf{accept}^{\underline{\mathrm{ID}}}_{\underline{\tau}} \leftrightarrow \bigvee_{\substack{\tau_i = \_,\mathrm{TU_{\underline{ID}}}(j_i,1)\\ \tau_1 = \_,\mathrm{TN}(j,0)\\ \tau_2 = \_,\mathrm{TU_{\underline{ID}}}(j_i,0)\\ \tau_2 \prec_\tau \tau_1 <_\tau \tau_i \prec_\tau \tau_{\mathrm{NS}}}} \left(\mathsf{full\text{-}tr}^{\mathsf{n}:\underline{\tau_1},\underline{\tau}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau_i}}\right) \qquad \mathsf{accept}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}} \leftrightarrow \bigvee_{\substack{\tau_i = \_,\mathrm{TU}_{\nu_\tau(\mathrm{ID})}(j_i,1)\\ \tau_1 = \_,\mathrm{TN}(j,0)\\ \tau_2 = \_,\mathrm{TU}_{\nu_\tau(\mathrm{ID})}(j_i,0)\\ \tau_{\mathrm{NS}} <_\tau \tau_2 \prec_\tau \tau_1 \prec_\tau \tau_i}} \left(\mathsf{full\text{-}tr}^{\mathsf{n}:\underline{\tau_1},\underline{\tau}}_{\mathsf{u}:\underline{\tau_2},\underline{\tau_i}}\right)$$

Hence, using (110) if $\tau_i \prec_\tau \mathrm{NS_{ID}}$, and (128) if $\tau_i \not\prec_\tau \mathrm{NS_{ID}}$, we can build the following derivation:

$$\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}^{\mathrm{ID}}_{\tau} \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \mathsf{sync\text{-}diff}^{\nu_\tau(\mathrm{ID})}_{\underline{\tau}}}\,\mathsf{Simp}$$

h) Part 6: Observe that:

$$\mathsf{net\text{-}e\text{-}auth}_\tau(\mathrm{ID}, j) \ \leftrightarrow\ \mathsf{accept}^{\mathrm{ID}}_{\tau} \qquad \underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathrm{ID}, j) \ \leftrightarrow \bigvee_{\underline{\mathrm{ID}} \in \mathsf{copies\text{-}id}(\mathrm{ID})} \mathsf{accept}^{\underline{\mathrm{ID}}}_{\underline{\tau}}$$

We therefore easily obtain the derivation:

$$\dfrac{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi^{\mathsf{in}}_{\tau}, \mathsf{l\text{-}reveal}_{\tau_0}, \mathsf{net\text{-}e\text{-}auth}_\tau(\mathrm{ID}, j) \ \sim\ \phi^{\mathsf{in}}_{\underline{\tau}}, \mathsf{r\text{-}reveal}_{\tau_0}, \underline{\mathsf{net\text{-}e\text{-}auth}_{\tau}}(\mathrm{ID}, j)}$$

Finally, using **(J10)**, we know that:

$$\bigvee_{\mathrm{ID}\in\mathcal{S}_{\mathsf{id}}} \mathsf{accept}_{\tau}^{\mathrm{ID}} \;\leftrightarrow\; \bigvee_{\mathrm{ID}\in\mathcal{S}_{\mathsf{bid}}} \mathsf{accept}_{\tau}^{\mathrm{ID}} \;\leftrightarrow\; \mathsf{net\text{-}e\text{-}auth}_{\tau}^{\mathrm{ID}}$$

Moreover:

$$\bigvee_{\mathrm{ID}\in\mathcal{S}_{\mathsf{id}}} \mathsf{accept}_{\underline{\tau}}^{\mathrm{ID}} \;\leftrightarrow\; \bigvee_{\mathrm{ID}\in\mathcal{S}_{\mathsf{bid}}} \left(\bigvee_{\underline{\mathrm{ID}}\in\mathsf{copies\text{-}id}(\mathrm{ID})} \mathsf{accept}_{\underline{\tau}}^{\underline{\mathrm{ID}}} \right) \;\leftrightarrow\; \bigvee_{\mathrm{ID}\in\mathcal{S}_{\mathsf{bid}}} \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathrm{ID}, j)$$

It follows that:

$$\dfrac{\dfrac{\dfrac{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \bigvee_{\mathrm{ID}\in\mathcal{S}_{\mathsf{bid}}} \mathsf{net\text{-}e\text{-}auth}_{\tau}^{\mathrm{ID}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \bigvee_{\mathrm{ID}\in\mathcal{S}_{\mathsf{bid}}} \underline{\mathsf{net\text{-}e\text{-}auth}_{\underline{\tau}}}(\mathrm{ID}, j)}\ \mathsf{Simp}}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, \bigvee_{\mathrm{ID}\in\mathcal{S}_{\mathsf{id}}} \mathsf{accept}_{\tau}^{\mathrm{ID}} \sim \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, \bigvee_{\mathrm{ID}\in\mathcal{S}_{\mathsf{id}}} \mathsf{accept}_{\underline{\tau}}^{\mathrm{ID}}}\ R}{\phi_{\tau}^{\mathsf{in}}, \mathsf{l\text{-}reveal}_{\tau_0}, t_{\tau} \;\sim\; \phi_{\underline{\tau}}^{\mathsf{in}}, \mathsf{r\text{-}reveal}_{\tau_0}, t_{\underline{\tau}}}\ \mathsf{FA}$$

Which concludes this proof.