# MPRI 2.30: Proofs of Security Protocols

## TD: Signed Diffie-Hellman Key-Exchange

Adrien Koutsos

2022/2023

*Questions marked with a star ($\star$) can be omitted without impacting the rest of the exercise.*

### 0.1 Signature Scheme and EUF-CMA

A signature scheme $(\mathcal{S}, \mathsf{pk}, \mathsf{sk}, \mathsf{sign}, \mathsf{check})$ is an *asymmetric* cryptographic scheme comprising:

- a finite set of key seeds $\mathcal{S}$;
- public and private key-generation functions $\mathsf{pk}(\_)$ and $\mathsf{sk}(\_)$;
- a signature function $\mathsf{sign}(\_, \_)$;
- and a signature checking function $\mathsf{check}(\_, \_, \_)$.

The public and private keys are generated from a key seed $\mathsf{n} \in \mathcal{S}$ by some party $\mathsf{A}$. The public key is shared with everybody, e.g. using some key server, while the secret key must never be shared by $\mathsf{A}$. The signature $\sigma = \mathsf{sign}(m, \mathsf{sk}(\mathsf{n}))$ of a message is computed using the private key $\mathsf{sk}(\mathsf{n})$, and proves that $m$ indeed originated from $\mathsf{A}$. This signature can be checked by anyone using the corresponding public key $\mathsf{pk}(\mathsf{n})$ and the signature checking function $\mathsf{check}(\_, \_, \_)$. To this end, it is required that $\mathsf{check}$ and $\mathsf{sign}$ verify the functional property:

$$\forall \mathsf{n} \in \mathcal{S}, \forall m. \mathsf{check}(\mathsf{sign}(m, \mathsf{sk}(\mathsf{n})), m, \mathsf{pk}(\mathsf{n})) = \mathsf{true}$$

**Remark 1.** *For the sack of conciseness, the security parameter $\eta$ has been omitted in the definitions above. Actually, all the functions of a signature scheme take as additional argument $\eta$ (in unary). Also, the set of key seeds $\mathcal{S}$ is actually a* family *of sets $(\mathcal{S}_\eta)_{\eta \in \mathbb{N}}$, indexed by $\eta$.*

**Unforgeability** A signature scheme is computationally unforgeable when no adversary can build valid signatures, even if it knows the public key $\mathsf{pk}(\mathsf{n})$ and has access to a signing oracle. This cryptographic assumption is the asymmetric counter-part to the unforgeability assumption for keyed cryptographic hashes.

**Definition 1.** A signature scheme $(\mathcal{S}, \mathsf{pk}, \mathsf{sk}, \mathsf{sign}, \mathsf{check})$ is *unforgeable against chosen-message attacks* (EUF-CMA) iff. for every PPTM $\mathcal{A}$:

$$\mathsf{Pr}_{\mathsf{n} \in \mathcal{S}} \left(\mathcal{A}^{\mathcal{O}_{\mathsf{sign}(\cdot, \mathsf{sk}(\mathsf{n}))}}(1^\eta, \mathsf{pk}(\eta)) = \langle m \,,\, \sigma\rangle,\ m \text{ not queried to } \mathcal{O}_{\mathsf{sign}(\cdot, \mathsf{sk}(\mathsf{n}))} \text{ and } \mathsf{check}(\sigma, m, \mathsf{sk}(\mathsf{n}))\right)$$

is negligible $\in \eta$, where $\mathsf{n}$ is drawn uniformly at random in $\mathcal{S}$.

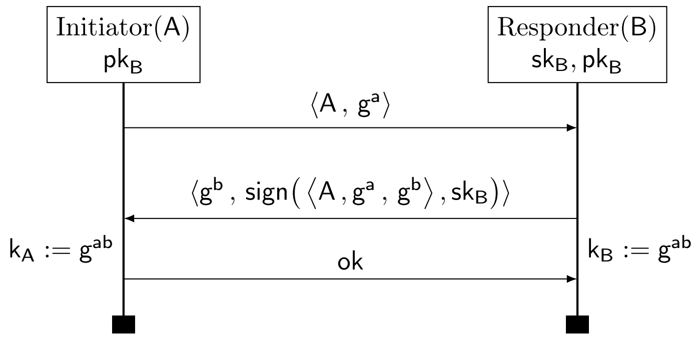
**Question 1.** *Design a rule schemata for EUF-CMA for signatures when $\mathcal{S} = \{0, 1\}^\eta$.*

*Solution.*

$$\mathsf{check}(\sigma, m, \mathsf{sk}(\mathsf{n})) \dot{\rightarrow} \dot{\bigvee_{u \in \mathcal{S}}} m \doteq u$$

where:

- $\sigma, m$ are ground terms and $\mathsf{n}$ a name in $\mathcal{N}$;
- $\mathsf{n}$ appears in $\sigma, \mathsf{n}$ only in subterms of the form $\mathsf{pk}(\cdot)$ or $\mathsf{sign}(\cdot, \mathsf{sk}(\mathsf{n}))$;
- $\mathcal{S} = \{u \mid \mathsf{sign}(u, \mathsf{sk}(\mathsf{n})) \in \mathsf{st}(m, \sigma)\}$ ■




**Notation:** $\mathsf{sk_B} \equiv \mathsf{sk}(\mathsf{n_B})$, $\mathsf{pk_B} \equiv \mathsf{pk}(\mathsf{n_B})$.

Figure 1: Signed-DH, The Signed Diffie-Hellman Protocol

# 1 Signed Diffie-Hellman

The Signed Diffie-Hellman protocol is a key-exchange protocol. This is a two party protocol, between an Initiator with identity A and a responder B. The goal of the protocol is to establish a **shared secret** key k between A and B. This key can then be used as a *symmetric* encryption key in future communications between A and B.

Let $(\mathcal{G}, \mathsf{e}, +)$ be a finite cyclic group[1], and g a generator of $\mathcal{G}$. Exponentiation of an element $\mathsf{x} \in \mathcal{G}$ by $y \in \mathbb{N}$ is written $x^y := \underbrace{x + \cdots + x}_{y \text{ times}}$. The Signed-DH protocol, depicted in Figure 1, works roughly as follows:

- A samples uniformly at random a secret exponent a, and sends the public value $\mathsf{g^a}$ to B;
- idem for B, which samples the secret b, and sends $\mathsf{g^b}$ to A in a signed message, and computes the shared secret key $\mathsf{g^{ab}} = (\mathsf{g^a})^{\mathsf{b}}$;
- if the signature is valid, A computes the shared secret key $\mathsf{g^{ab}} = (\mathsf{g^b})^{\mathsf{a}}$ and sends ok (if the signature check fails, A sends ko).

Essentially, the idea is that $\mathsf{g^{ab}}$ should not be computable from the public values $\mathsf{g^a}, \mathsf{g^b}$ without knowing one of the secret exponents a or b.

We consider a scenario with many initiators, each running many sessions, but with a single responder B, common to all initiators. The responder B also runs many sessions.

## 1.1 Modeling

**Question 2.** *Write the processes:*

- *$P(A, i)$ representing the $i$-th session of the initiator A;*
- *$B(j)$ representing the $j$-th session of the responder B.*

*Note that there is a single B, which accepts to talk to any initiator $A \in \mathcal{I}$.*

*We will use the channel $\mathsf{c}^i_{A_0}$ and $\mathsf{c}^i_{A_1}$ for $P_{\mathsf{A}}(i)$, and $\mathsf{c}^j_B$ for $B(j)$. Moreover, the random exponents sampled by $P(A, i)$ and $B(j)$ will be, respectively, $a_i$ and $b_j$.*

*Solution.*

$$\begin{aligned} P(A,i) \;:=\;& \nu\, \mathsf{a}_{\mathsf{A},i}.\ \mathbf{in}(\mathsf{c}^{\mathtt{i}}_{\mathtt{A}_0}, \_).\ \mathbf{out}(\mathsf{c}^{\mathtt{i}}_{\mathtt{A}_0}, \langle \mathsf{A}\,,\, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \rangle). \\ & \qquad \mathbf{in}(\mathsf{c}^{\mathtt{i}}_{\mathtt{A}_1}, \mathsf{x}).\ \mathsf{if}\ \mathsf{check}(\pi_2\,\mathsf{x}, \langle \mathsf{A}\,,\, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}}\,,\, \pi_1\,\mathsf{x} \rangle\,,\, \mathsf{pk_B}) \\ & \qquad\qquad \mathsf{then}\ \mathbf{out}(\mathsf{c}^{\mathtt{i}}_{\mathtt{A}_1}, \mathsf{ok}) \\ & \qquad\qquad \mathsf{else}\ \mathbf{out}(\mathsf{c}^{\mathtt{i}}_{\mathtt{A}_1}, \mathsf{ko})) \end{aligned}$$

$$B(j) \;:=\; \nu\, \mathsf{b}_j.\ \ \mathbf{in}(\mathsf{c}^{\mathtt{j}}_{\mathtt{B}}, \mathsf{y}).\ \mathbf{out}(\mathsf{c}^{\mathtt{j}}_{\mathtt{B}}, \langle \mathsf{g}^{\mathsf{b}_j}\,,\, \mathsf{sign}(\langle \pi_1\,\mathsf{y}\,,\, \pi_2\,\mathsf{y}\,,\, \mathsf{g}^{\mathsf{b}_j} \rangle\,,\, \mathsf{sk_B})\rangle) \quad \blacksquare$$

[1] Actually a family of groups indexed by the security parameter.

Let $\mathcal{I}$ be a finite set of identities, and $N, M \in \mathbb{N}$. We consider the top-level process $\mathsf{Q}$:

$$\nu\, \mathsf{n_B}.\ \big(!_{\mathsf{A}\in\mathcal{I}}\, !_{i\leq N}\ P(\mathsf{A}, i)\big) \mid \big(!_{i\leq M}\ B(j)\big)$$

**Question 3.** *For any trace $\mathtt{tr} \diamond \mathsf{c}^i_{A_1} \in \mathcal{T}_{io}$, write a term $\mathsf{accept}_Q@\mathtt{tr}$ representing the acceptance check of $P(A, i)$. To do this, we may use the term $\mathsf{in_Q}@\mathtt{tr}$, which represents the messages inputted at the end of $\mathtt{tr}$.*

*Solution.*

$$\mathsf{accept}_{\mathcal{Q}}@\mathtt{tr} := \mathsf{check}(\pi_2\, \mathsf{in_Q}@\mathtt{tr}, \langle \mathsf{A}\,, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}}\,, \pi_1\, \mathsf{in_Q}@\mathtt{tr}\rangle\,, \mathsf{pk_B}) \qquad \blacksquare$$

**Question 4.** *Give the definition of $\mathsf{out_Q}@\mathtt{tr}$, for any trace $\mathtt{tr} \diamond \mathsf{c} \in \mathcal{T}_{io}$, where $\mathsf{c}$ is any of the channels $\mathsf{c}^i_{A_0}$, $\mathsf{c}^i_{A_1}$ or $\mathsf{c}^j_B$.*

*Solution.*

$$\mathsf{out_Q}@\mathtt{tr} := \begin{cases} \langle \mathsf{A}\,, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \rangle & \text{if } \mathtt{tr} \diamond \mathsf{c}^{\mathsf{i}}_{\mathsf{A}_0} \\ \text{if } \mathsf{accept}_{\mathcal{Q}}@\mathtt{tr} \text{ then ok else ko} & \text{if } \mathtt{tr} \diamond \mathsf{c}^{\mathsf{i}}_{\mathsf{A}_1} \\ \langle \mathsf{g}^{\mathsf{b}_j}\,, \mathsf{sign}(\big\langle \pi_1\, \mathsf{in_Q}@\mathtt{tr}\,, \pi_2\, \mathsf{in_Q}@\mathtt{tr}\,, \mathsf{g}^{\mathsf{b}_j} \big\rangle\,, \mathsf{sk_B})\rangle & \text{if } \mathtt{tr} \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \end{cases}$$

$\blacksquare$

**Key-Agreement** Intuitively, the $\mathsf{Signed\text{-}DH}$ protocol has the key agreement property if, for any trace $\mathtt{tr} \in \mathcal{T}_{\mathsf{io}}$, for any identity $\mathsf{A}$, if $P(\mathsf{A}, i)$ ended in an accepting state, then there exists a session $j$ of $\mathsf{B}$ such that:

- $P(\mathsf{A}, i)$ and $B(j)$ are properly interleaved;
- $P(\mathsf{A}, i)$ and $B(j)$ both derived the key $\mathsf{g}^{\mathsf{a}_i \mathsf{b}_j}$.

We are now going to translate this property into a (set of) formulas of the logic.

**Question 5.** *For any $\mathtt{tr} \diamond \mathsf{c}^i_{A_1} \in \mathcal{T}_{io}$, write a term $\mathsf{derived\text{-}key}^A_Q@\mathtt{tr}$ representing the key derived by $P(A, i)$.*

*Similarly, write a term $\mathsf{derived\text{-}key}^B_Q@\mathtt{tr}$ representing the key derived by $B(j)$.*

*Solution.*

$$\begin{aligned} \mathsf{derived\text{-}key}^{\mathsf{A}}_{\mathsf{Q}}@\mathtt{tr} &:= (\pi_1\, \mathsf{in_Q}@\mathtt{tr})^{\mathsf{a}_{\mathsf{A},i}} && \text{if } \mathtt{tr} \diamond \mathsf{c}^{\mathsf{i}}_{\mathsf{A}_1} \\ \mathsf{derived\text{-}key}^{\mathsf{B}}_{\mathsf{Q}}@\mathtt{tr} &:= (\pi_2\, \mathsf{in_Q}@\mathtt{tr})^{\mathsf{b}_j} && \text{if } \mathtt{tr} \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \end{aligned} \qquad \blacksquare$$

**Question 6.** *Using everything above, give a set of formulas stating that the $\mathsf{Signed\text{-}DH}$ protocol has the key-agreement property for any trace $\mathtt{tr} \in \mathcal{T}_{io}$.*

*Solution.* For any trace $\mathtt{tr} \in \mathcal{T}_{\mathsf{io}}$, for any $\mathtt{tr}_1 \diamond \mathsf{c}^{\mathsf{i}}_{\mathsf{A}_0}$ and $\mathtt{tr}_3 \diamond \mathsf{c}^{\mathsf{i}}_{\mathsf{A}_1}$ such that $\mathtt{tr}_1 \leq \mathtt{tr}_3 \leq \mathtt{tr}$:

$$\mathsf{accept}_{\mathcal{Q}}@\mathtt{tr}_3 \mathrel{\dot{\rightarrow}} \dot{\bigvee_{\substack{\mathtt{tr}_2 \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \\ \mathtt{tr}_1 \leq \mathtt{tr}_2 \leq \mathtt{tr}_3}}} \mathsf{derived\text{-}key}^{\mathsf{A}}_{\mathsf{Q}}@\mathtt{tr}_3 \doteq \mathsf{derived\text{-}key}^{\mathsf{B}}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}\, \mathsf{b}_j} \qquad \blacksquare$$

## 1.2 Security Proof

We are now going to prove that $\mathsf{Signed\text{-}DH}$ has the key-agreement property.

**Question 7.** *For any $\mathtt{tr} \in \mathcal{T}_{io}$, give the set of honest signatures $\mathcal{S}$:*

$$\big\{m \mid \mathsf{sign}(m, \mathsf{sk}(\mathsf{n})) \in \mathsf{st}(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr})\big\}$$

*Solution.* The only honest signatures of the protocol $\mathcal{Q}$ are computed by $\mathsf{B}$, hence:

$$\mathcal{S} = \Big\{ \big\langle \pi_1\, \mathsf{in_Q}@\mathtt{tr}'\,, \pi_2\, \mathsf{in_Q}@\mathtt{tr}'\,, \mathsf{g}^{\mathsf{b}_j} \big\rangle \mid \mathtt{tr}' \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \leq \mathtt{tr}_3 \Big\} \qquad \blacksquare$$

**Question 8** ($\star$). *Let $(\mathcal{G}, \mathsf{e}, +)$ be a family of cyclic groups of order $\mathsf{O}_\eta$. For any ground term $t$ and name $\mathsf{n} \in \mathcal{N}$ such that $\mathsf{n} \notin \mathit{st}(t)$, prove that the following rule:*

$$\mathsf{g}^{\mathsf{n}} \doteq t \sim \mathit{false}$$

*is valid in any computational model where $\mathsf{O}_\eta$ is asymptotically large, in the sense that $1/\mathsf{O}_\eta$ is negligible.*

*Solution.* Let $\mathcal{M}$ be a computational model such that $\mathsf{O}_\eta$ is asymptotically large.

$$\begin{aligned}
&\Pr_\rho([\![\mathsf{g}^{\mathsf{n}} \doteq t]\!]_{\mathcal{M}}(1^\eta, \rho)) \\
=\; &\sum_{w \in \Sigma^*} \Pr_\rho([\![\mathsf{g}^{\mathsf{n}}]\!]_{\mathcal{M}}(1^\eta, \rho) = w \wedge [\![t]\!]_{\mathcal{M}}(1^\eta, \rho) = w) \\
=\; &\sum_{w \in [\![\mathcal{G}]\!]_{\mathcal{M}}} \Pr_\rho([\![\mathsf{g}^{\mathsf{n}}]\!]_{\mathcal{M}}(1^\eta, \rho) = w \wedge [\![t]\!]_{\mathcal{M}}(1^\eta, \rho) = w) && \text{(since } \mathsf{g}^{\mathsf{n}} \in [\![\mathcal{G}]\!]_{\mathcal{M}}) \\
=\; &\sum_{w \in [\![\mathcal{G}]\!]_{\mathcal{M}}} \Pr_\rho([\![\mathsf{g}^{\mathsf{n}}]\!]_{\mathcal{M}}(1^\eta, \rho) = w) \times \Pr_\rho([\![t]\!]_{\mathcal{M}}(1^\eta, \rho) = w) && \text{(by independence)}
\end{aligned}$$

Let $q_\eta$ is the quotient of $2^\eta$ by $\mathsf{O}_\eta$. Then:

$$\Pr_\rho([\![\mathsf{g}^{\mathsf{n}}]\!]_{\mathcal{M}}(1^\eta, \rho) = w) \leq \frac{q_\eta + 1}{2^\eta}$$

since there are at most $q_\eta + 1$ value of $[\![\mathsf{n}]\!]_{\mathcal{M}}(1^\eta, \rho)$ such that $[\![\mathsf{g}^{\mathsf{n}}]\!]_{\mathcal{M}}(1^\eta, \rho) = w$ (as $[\![\mathsf{g}]\!]_{\mathcal{M}}$ is a generator of $[\![\mathcal{G}]\!]_{\mathcal{M}}$). Consequently:

$$\begin{aligned}
&\sum_{w \in [\![\mathcal{G}]\!]_{\mathcal{M}}} \Pr_\rho([\![\mathsf{g}^{\mathsf{n}}]\!]_{\mathcal{M}}(1^\eta, \rho) = w) \times \Pr_\rho([\![t]\!]_{\mathcal{M}}(1^\eta, \rho) = w) && \text{(by independence)} \\
\leq\; &\sum_{w \in [\![\mathcal{G}]\!]_{\mathcal{M}}} \frac{q_\eta + 1}{2^\eta} \times \Pr_\rho([\![t]\!]_{\mathcal{M}}(1^\eta, \rho) = w) \\
\leq\; &\frac{q_\eta + 1}{2^\eta} \times \sum_{w \in [\![\mathcal{G}]\!]_{\mathcal{M}}} \Pr_\rho([\![t]\!]_{\mathcal{M}}(1^\eta, \rho) = w) \\
\leq\; &\frac{q_\eta + 1}{2^\eta}
\end{aligned}$$

We conclude using the fact that:

$$\frac{q_\eta + 1}{2^\eta} = \frac{\lfloor \frac{2^\eta}{\mathsf{O}_\eta} \rfloor}{2^\eta} + \frac{1}{2^\eta} \leq \frac{\frac{2^\eta}{\mathsf{O}_\eta}}{2^\eta} + \frac{1}{2^\eta} \leq \frac{1}{\mathsf{O}_\eta} + \frac{1}{2^\eta} \in \mathsf{negl}(\eta) \qquad \blacksquare$$

**Question 9.** *Prove that* Signed-DH *has the key-agreement property by showing that the formulas of Question 6 are valid in any computational model where:*

- *the signature scheme $(\mathcal{S}, \mathit{pk}, \mathit{sk}, \mathit{sign}, \mathit{check})$ is* EUF-CMA;
- *$(\mathcal{G}, \mathsf{e}, +)$ is a family of cyclic groups of order $\mathsf{O}_\eta$ such that $1/\mathsf{O}_\eta$ is negligible.*

*Solution.* Let $\mathtt{tr} \in \mathcal{T}_{\mathsf{io}}$, $\mathtt{tr}_1 \diamond \mathsf{c}^{\mathsf{i}}_{\mathsf{A}_0}$ and $\mathtt{tr}_3 \diamond \mathsf{c}^{\mathsf{i}}_{\mathsf{A}_1}$ such that $\mathtt{tr}_1 \leq \mathtt{tr}_3 \leq \mathtt{tr}$. Let:

$$\phi \stackrel{\text{def}}{=} \dot{\bigvee_{\substack{\mathtt{tr}_2 \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \\ \mathtt{tr}_1 \leq \mathtt{tr}_2 \leq \mathtt{tr}_3}}} \mathsf{derived\text{-}key}^{\mathsf{A}}_{\mathsf{Q}}@\mathtt{tr}_3 \doteq \mathsf{derived\text{-}key}^{\mathsf{B}}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}\, \mathsf{b}_j}$$

We want to give a derivation of:

$$\vdash \mathsf{accept}_{\mathcal{Q}}@\mathtt{tr}_3 \dot{\rightarrow} \phi \tag{1}$$

Applying the rule for EUF-CMA, and using the result of Question 7, we know that the following judgement is derivable:

$$\mathsf{accept}_{\mathcal{Q}}@\mathtt{tr}_3 \vdash \dot{\bigvee_{u \in \mathcal{S}}} u \doteq \langle \mathsf{A}\,, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}}\,, \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3 \rangle$$

I.e.:

$$\mathsf{accept}_Q@\mathtt{tr}_3 \vdash \dot{\bigvee_{\substack{\mathtt{tr}_2 \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \\ \mathtt{tr}_2 \leq \mathtt{tr}_3}}} \left\langle \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2\, , \pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2\, , \mathsf{g}^{\mathsf{b}_j} \right\rangle \doteq \langle \mathsf{A}\, , \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}}\, , \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3 \rangle$$

Using the pair injectivity rules:

$$\mathsf{accept}_Q@\mathtt{tr}_3 \vdash \dot{\bigvee_{\substack{\mathtt{tr}_2 \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \\ \mathtt{tr}_2 \leq \mathtt{tr}_3}}} \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{A} \mathbin{\dot\wedge} \pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \mathbin{\dot\wedge} \mathsf{g}^{\mathsf{b}_j} \doteq \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3 \tag{2}$$

is derivable.

We can start the derivation of the formula in Equ. (1):

$$\dfrac{\dfrac{\dfrac{(2)}{\mathsf{accept}_Q@\mathtt{tr}_3 \vdash \dot\bigvee_{\substack{\mathtt{tr}_2 \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \\ \mathtt{tr}_2 \leq \mathtt{tr}_3}} \begin{array}{c}\pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{A} \dot\wedge \\ \pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \dot\wedge \\ \mathsf{g}^{\mathsf{b}_j} \doteq \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3\end{array}} \qquad \mathsf{accept}_Q@\mathtt{tr}_3, \dot\bigvee_{\substack{\mathtt{tr}_2 \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \\ \mathtt{tr}_2 \leq \mathtt{tr}_3}} \begin{array}{c}\pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{A} \dot\wedge \\ \pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \dot\wedge \vdash \phi \\ \mathsf{g}^{\mathsf{b}_j} \doteq \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3\end{array}}{\mathsf{accept}_Q@\mathtt{tr}_3 \vdash \phi}\ \text{Cut}}{\vdash \mathsf{accept}_Q@\mathtt{tr}_3 \mathbin{\dot\rightarrow} \phi}\ \text{L-}\dot\rightarrow$$

Continuing the derivation of the right branch:

$$\dfrac{\begin{array}{c}\pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{A} \dot\wedge \\ \mathsf{accept}_Q@\mathtt{tr}_3, \pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \dot\wedge \vdash \phi \\ \mathsf{g}^{\mathsf{b}_j} \doteq \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3\end{array} \qquad \text{for any } \mathtt{tr}_2 \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \text{ s.t. } \mathtt{tr}_2 \leq \mathtt{tr}_3}{\mathsf{accept}_Q@\mathtt{tr}_3, \dot\bigvee_{\substack{\mathtt{tr}_2 \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}} \\ \mathtt{tr}_2 \leq \mathtt{tr}_3}} \begin{array}{c}\pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{A} \dot\wedge \\ \pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \dot\wedge \vdash \phi \\ \mathsf{g}^{\mathsf{b}_j} \doteq \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3\end{array}}\ \text{L-}\dot\vee \tag{3}$$

Let $\mathtt{tr}_2 \diamond \mathsf{c}^{\mathsf{j}}_{\mathsf{B}}$ s.t. $\mathtt{tr}_2 \leq \mathtt{tr}_3$. If $\mathtt{tr}_2 \leq \mathtt{tr}_1$, then Equ. (3) is derivable as follows:

$$\dfrac{\dfrac{}{\pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \vdash \bot}}{\begin{array}{c}\pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{A} \dot\wedge \\ \mathsf{accept}_Q@\mathtt{tr}_3, \pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \dot\wedge \vdash \phi \\ \mathsf{g}^{\mathsf{b}_j} \doteq \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3\end{array}}\ \text{Weak} + \text{R-}\bot$$

using the rule of Question 8 and the fact that when $\mathtt{tr}_2 \leq \mathtt{tr}_1$, $\mathsf{a}_{\mathsf{A},i}$ does not appears in the subterms of $\pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2$ (said otherwise, when when $\mathtt{tr}_2 \leq \mathtt{tr}_1$, $\mathsf{a}_{\mathsf{A},i}$, the term $\pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2$ must be equal to a name that has not yet been sampled).

Finally, assume $\mathtt{tr}_1 \leq \mathtt{tr}_2 \leq \mathtt{tr}_3$, we finish the derivation of Equ. (3):

$$\dfrac{\begin{array}{l}\pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{A} \dot\wedge \\ \mathsf{accept}_Q@\mathtt{tr}_3, \pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \dot\wedge \vdash \mathsf{derived\text{-}key}^{\mathsf{A}}_{\mathsf{Q}}@\mathtt{tr}_3 \doteq \mathsf{derived\text{-}key}^{\mathsf{B}}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}\, \mathsf{b}_j} \\ \mathsf{g}^{\mathsf{b}_j} \doteq \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3\end{array}}{\begin{array}{c}\pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{A} \dot\wedge \\ \mathsf{accept}_Q@\mathtt{tr}_3, \pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \dot\wedge \vdash \phi \\ \mathsf{g}^{\mathsf{b}_j} \doteq \pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr}_3\end{array}}\ \text{R-}\dot\vee$$

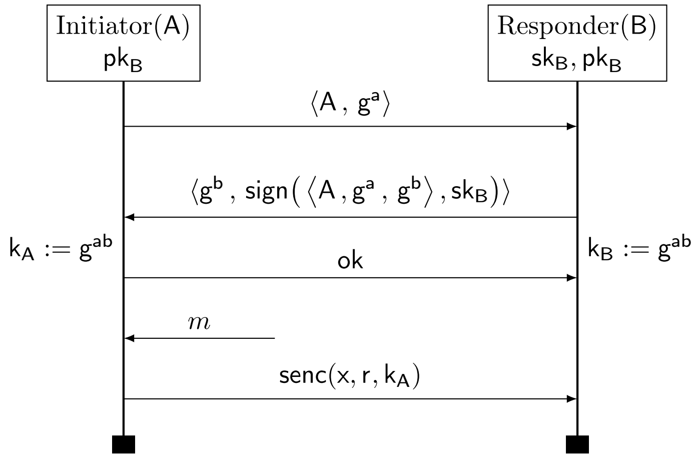
We conclude easily using basic equality reasonings and the fact that:

$$\mathsf{derived\text{-}key}^{\mathsf{B}}_{\mathsf{Q}}@\mathtt{tr}_2 \doteq (\pi_2\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr})^{\mathsf{b}_j} \qquad \mathsf{derived\text{-}key}^{\mathsf{A}}_{\mathsf{Q}}@\mathtt{tr}_3 \doteq (\pi_1\, \mathsf{in}_{\mathsf{Q}}@\mathtt{tr})^{\mathsf{a}_{\mathsf{A},i}} \qquad \blacksquare$$

## 1.3 Signed DH with Message

We now go further in the modeling, and consider that Alice sends a message to Bob using the derived key and a symmetric encryption $\mathsf{senc}(m, \mathsf{r}, \mathsf{k}_{\mathsf{A}})^2$. To be as general as possible, we do not fix the content of the message Alice sends to Bob. Instead, we assume the worse, and let the adversary choose it. The protocol $\mathsf{Signed\text{-}DH_m}$ is depicted in Figure 2.

[2] $\mathsf{r}$ is the symmetric encryption randomness.




**Notation:** $\mathsf{sk_B} \equiv \mathsf{sk}(\mathsf{n_B})$, $\mathsf{pk_B} \equiv \mathsf{pk}(\mathsf{n_B})$

Figure 2: $\mathsf{Signed\text{-}DH_m}$, the Signed Diffie-Hellman Protocol with a Single Message

Our goal is to prove that $\mathsf{Signed\text{-}DH_m}$ is indistinguishable from an idealized version of the protocol $\mathsf{Signed\text{-}DH_m^{id}}$, where the content of the message sent has been replaced by a message of the same length, with all bits set to zero.

**Question 10.** *Write the real-world and ideal-world protocols $\mathsf{Signed\text{-}DH_m}$ and $\mathsf{Signed\text{-}DH_m^{id}}$.*

*Solution.* The process for $\mathsf{B}$ is unchanged. We give the process for the initiator in $\mathsf{Signed\text{-}DH_m}$ below:

$$
\begin{aligned}
P_m(A,i) \;:=\; \nu\, \mathsf{a}_{\mathsf{A},i}.\ & \mathbf{in}(\mathtt{c}^{\mathtt{i}}_{\mathtt{A}_0}, \_).\ \mathbf{out}(\mathtt{c}^{\mathtt{i}}_{\mathtt{A}_0}, \langle \mathsf{A}\,,\, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}}\rangle). \\
& \mathbf{in}(\mathtt{c}^{\mathtt{i}}_{\mathtt{A}_1}, \mathsf{x}).\ \mathsf{if}\ \mathsf{check}(\pi_2\,\mathsf{x}, \langle \mathsf{A}\,, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}}\,,\, \pi_1\,\mathsf{x}\rangle\,, \mathsf{pk_B})\ \mathsf{then} \\
& \qquad \mathbf{out}(\mathtt{c}^{\mathtt{i}}_{\mathtt{A}_1}, \mathsf{ok}). \\
& \qquad \mathbf{in}(\mathtt{c}^{\mathtt{i}}_{\mathtt{A}_2}, \mathsf{m}). \\
& \qquad \nu\, \mathsf{r}_{\mathsf{A},i}. \\
& \qquad \mathbf{out}(\mathtt{c}^{\mathtt{i}}_{\mathtt{A}_2}, \mathsf{senc}(\mathsf{m}, \mathsf{r}_{\mathsf{A},i}, \pi_1\,\mathsf{x}^{\mathsf{a}_{\mathsf{A},i}})) \\
& \quad \mathsf{else}\ \mathbf{out}(\mathtt{c}^{\mathtt{i}}_{\mathtt{A}_1}, \mathsf{ko}))
\end{aligned}
$$

The initiator process $P_m^{\mathrm{id}}(A,i)$ in the ideal protocol is identical to $P_m(A,i)$, except that the last output is replaced by:

$$\mathbf{out}(\mathtt{c}^{\mathtt{i}}_{\mathtt{A}_2}, \mathsf{senc}(0^{|\mathsf{m}|}, \mathsf{r}_{\mathsf{A},i}, \pi_1\,\mathsf{x}^{\mathsf{a}_{\mathsf{A},i}})) \qquad \blacksquare$$

To do this proof, we are going to make two cryptographic assumptions. We require that:

- the symmetric encryption used satisfies the *symmetric* IND-CCA$_1^{\mathcal{G}}$ assumption;
- the group used satisfy the *Decisional Diffie-Hellman* assumption.

**Symmetric IND-CCA$_1^{\mathcal{G}}$** The symmetric IND-CCA$_1^{\mathcal{G}}$ assumption on a symmetric encryption scheme $(\mathsf{senc}(\_,\_,\_), \mathsf{sdec}(\_,\_))$ is very similar to the asymmetric one. The only differences are:

- instead of giving the public key to the adversary, it has access to an symmetric encryption oracle;
- symmetric keys are assumed to be randomly generated group elements, obtained by putting $\mathsf{g}$ to an exponent sampled uniformly at random.

We omit the precise description of the game here, and admit that the ground rule:

$$\frac{\mathsf{len}(t_0) = \mathsf{len}(t_1)}{\vec{u}, \mathsf{senc}(t_0, \mathsf{r}, \mathsf{g^n}) \sim \vec{u}, \mathsf{senc}(t_1, \mathsf{r}, \mathsf{g^n})}\ \text{IND-CCA}_1^{\mathcal{G}}$$

is sound, when:

i) $\mathsf{r} \in \mathcal{N}$ does not appear in $\vec{u}, t_0, t_1$;

ii) $\mathsf{n} \in \mathcal{N}$ appears only terms of the form $\mathsf{senc}(v, \mathsf{r}_0, \mathsf{g}^{\mathsf{n}})$ where $\mathsf{r}_0 \in \mathcal{N}$ or $\mathsf{sdec}(v, \mathsf{g}^{\mathsf{n}})$ in $\vec{u}, t_0, t_1$;

iii) for all name $\mathsf{r}_0$ such that $\mathsf{senc}(v, \mathsf{r}_0, \mathsf{g}^{\mathsf{n}})$ is a subterm of $\vec{u}, t_0, t_1$, all occurrences of $\mathsf{r}_0$ are in the subterm $\mathsf{senc}(v, \mathsf{r}_0, \mathsf{g}^{\mathsf{n}})$.

**Question 11** ($\star$)**.** *From the description and rule above, give the definition of the* IND-CCA$_1^{\mathcal{G}}$ *cryptographic assumption. Explain why item iii) is necessary for the rule soundness.*

*Solution.* A symmetric encryption scheme $(\mathsf{senc}(\_,\_,\_), \mathsf{sdec}(\_,\_))$ satisfies the IND-CCA$_1^{\mathcal{G}}$ assumption iff. for every PPTM $\mathcal{A}$ with access to:

- a left-right oracle $\mathcal{O}_{\mathsf{LR}}^{b,\mathsf{n}}(\cdot,\cdot)$:

$$\mathcal{O}_{\mathsf{LR}}^{b,\mathsf{n}}(m_0, m_1) \stackrel{\text{def}}{=} \begin{cases} \mathsf{senc}(m_b, \mathsf{r}, \mathsf{g}^{\mathsf{n}}) & \text{if } \mathsf{len}(m_1) = \mathsf{len}(m_2) \quad (\mathsf{r} \textit{ fresh}) \\ 0 & \text{otherwise} \end{cases}$$

- a decryption oracle $\mathcal{O}_{\mathsf{sdec}}^{\mathsf{n}}$ such that for any $\mathsf{x}$:

$$\mathcal{O}_{\mathsf{sdec}}^{\mathsf{n}}(\mathsf{x}) \stackrel{\text{def}}{=} \mathsf{sdec}(\mathsf{x}, \mathsf{g}^{\mathsf{n}})$$

- and an encryption oracle $\mathcal{O}_{\mathsf{senc}}^{\mathsf{n}}$ such that for any $\mathsf{x}$:

$$\mathcal{O}_{\mathsf{senc}}^{\mathsf{n}}(\mathsf{x}) \stackrel{\text{def}}{=} \mathsf{senc}(\mathsf{x}, \mathsf{r}, \mathsf{g}^{\mathsf{n}}) \qquad (\mathsf{r} \text{ fresh})$$

where $\mathcal{A}$ can call $\mathcal{O}_{\mathsf{LR}}$ once, and cannot call $\mathcal{O}_{\mathsf{sdec}}$ after $\mathcal{O}_{\mathsf{LR}}$, then:

$$\left|\ \mathsf{Pr}_{\mathsf{n}}\left(\mathcal{A}^{\mathcal{O}_{\mathsf{LR}}^{1,\mathsf{n}}, \mathcal{O}_{\mathsf{sdec}}^{\mathsf{n}}, \mathcal{O}_{\mathsf{senc}}^{\mathsf{n}}}(1^\eta) = 1\right) - \ \mathsf{Pr}_{\mathsf{n}}\left(\mathcal{A}^{\mathcal{O}_{\mathsf{LR}}^{0,\mathsf{n}}, \mathcal{O}_{\mathsf{sdec}}^{\mathsf{n}}, \mathcal{O}_{\mathsf{senc}}^{\mathsf{n}}}(1^\eta) = 1\right)\ \right|$$

is negligible in $\eta$, where $\mathsf{n}$ is drawn uniformly in $\{0,1\}^\eta$.

Condition *iii)* is here to account for the freshness of the encryption name in the oracle $\mathcal{O}_{\mathsf{senc}}^{\mathsf{n}}$: since the name r is sampled by the challenger, it must not be directly accessible to the adversary. ■

**Decisional Diffie-Hellman** A cyclic group family $(\mathcal{G}, \mathsf{e}, +)$ satisfies the Decisional Diffie-Hellman assumption (DDH) if no adversary can distinguish values sampled from $(\mathsf{g}^a, \mathsf{g}^b, \mathsf{g}^{ab})$ from values sampled from $(\mathsf{g}^a, \mathsf{g}^b, \mathsf{g}^c)$ (where $a, b$ and $c$ are uniformly sampled at random in $\{0,1\}^\eta$) with non-negligible probability. Formally, for every PPTM $\mathcal{A}$:

$$\left|\Pr_{a,b}\left(\mathcal{A}(1^\eta, \mathsf{g}^a, \mathsf{g}^b, \mathsf{g}^{ab})\right) - \Pr_{a,b,c}\left(\mathcal{A}(1^\eta, \mathsf{g}^a, \mathsf{g}^b, \mathsf{g}^c)\right)\right|$$

must be negligible in $\eta$, when $a, b$ and $c$ are uniform samplings in $\{0,1\}^\eta$.

**Question 12** ($\star$)**.** *Give a cyclic group family such that the* DDH *assumption does not hold.*

*Solution.* The DDH problem is trivial in additive groups, e.g.:

$$(\mathbb{Z}/2^\eta\,\mathbb{Z}, 0.+)_{\eta \in \mathbb{N}}$$

■

**Question 13** ($\star$)**.** *Show that* DDH *is a stronger assumption (i.e. harder to met) than the* DLog *assumption*[3]*.*

*Solution.* We show that if there exists an efficient algorithm $\mathcal{A}$ for the DLog problem, then there exists an efficient algorithm $\mathcal{B}$ for the DDH problem.

Given a DDH triple $(\mathsf{g}^a, \mathsf{g}^b, Z)$, $\mathcal{B}$ computes $a$ and $b$ from, respectively, $\mathsf{g}^a$ and $\mathsf{g}^b$, using $\mathcal{A}$. It then compute $Z' = \mathsf{g}^{a \cdot b}$, and checks whether $Z' = Z$. ■

[3]The discrete logarithm assumption DLog state that PPTM can compute $a$ from $\mathsf{g}^a$ with non-negligible probability, where $a$ is sampled uniformly at random.

**Question 14.** *Design a rule schemata for the* DDH *assumption. First, design the simplest rule possible capturing the* DDH *assumption.*

*Then, design a more general rule, which allows the application of the* DDH *assumption under an arbitrary context. Prove that the generalized variant is admissible from the simpler variant using standard rules of the indistinguishability logic.*

*Solution.* The following simple rule capturing the DDH assumption:

$$\frac{}{\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}} \sim \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}}\ \text{DDH}$$

where $\mathsf{a}, \mathsf{b}$ and $\mathsf{c}$ are *names*.

It is trivial to show that this rule is satisfied in computational model $\mathcal{M}$ where the group family $\left(\llbracket\mathcal{G}\rrbracket_{\mathcal{M}}(1^\eta)\right)_{\eta\in\mathbb{N}}$ satisfies the DDH assumption.

This rule can be generalized in several ways.

**First generalization** For any context $C$ such that $\mathsf{a}, \mathsf{b}, \mathsf{c} \notin \mathsf{st}(C)$, we consider the following rule applying DDH under $C$:

$$\frac{}{C[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}] \sim C[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}]}\ \text{DDH}_c$$

We show that this rule is satisfied in any computational model where DDH holds by giving a derivation of DDH$_c$ using DDH and usual valid rules. The proof is by structural induction on the context $C$.

- Case 1: $C$ is the smallest context, i.e. $(C[x, y, z] = x, y, z)$. Then we conclude immediately using DDH.
- Case 3: $(C[x, y, z] = C_0[x, y, z], f(C_1[x, y, z], \ldots, C_n[x, y, z]))$ where $f$ is a function symbol. Then:

$$\frac{\begin{array}{l} C_0[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}], C_1[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}], \ldots, C_n[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}] \\ \sim\ C_0[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}], C_1[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}], \ldots, C_n[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}] \end{array}}{\begin{array}{l} C_0[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}], f\left(C_1[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}], \ldots, C_n[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}]\right) \\ \sim\ C_0[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}], f\left(C_1[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}], \ldots, C_n[\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}]\right) \end{array}}\ \text{FA}$$

  We conclude by induction hypothesis.
- Case 3: $C$ does not contain any function symbols (otherwise we use the induction step in case 2). Hence $(C[x, y, z] = x, y, z, \mathsf{n}_0, \ldots, \mathsf{n}_l)$ where for all $i$, $\mathsf{n}_i \in \mathcal{N}$ is a name. Note that we assume, w.l.o.g., that $x, y$ and $z$ appear only once (if this is not the case, we apply the Dup rule).

  By applying the Dup rule again, we assume w.l.o.g. that all names are distinct.

  Since $\mathsf{a} \notin \mathsf{st}(C)$, we know that $\mathsf{n}_l \neq \mathsf{a}$ (idem for $\mathsf{b}$ and $\mathsf{c}$). Hence:

$$\mathsf{n}_l \notin \mathsf{st}\left(\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}, \mathsf{n}_0, \ldots, \mathsf{n}_{l-1}\right) \qquad \mathsf{n}_l \notin \mathsf{st}\left(\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}, \mathsf{n}_0, \ldots, \mathsf{n}_{l-1}\right)$$

  Consequently, we can apply the Fresh rule to get rid of $\mathsf{n}_l$. Repeating this last step for $\mathsf{n}_{l-1}, \ldots, \mathsf{n}_1$, we get the derivation:

$$\frac{\begin{array}{c} \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}} \sim \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}} \\ \vdots \\ \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}, \mathsf{n}_0, \ldots, \mathsf{n}_{l-1} \sim \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}, \mathsf{n}_0, \ldots, \mathsf{n}_{l-1} \end{array}}{\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}}, \mathsf{n}_0, \ldots, \mathsf{n}_l \sim \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}}, \mathsf{g}^{\mathsf{c}}, \mathsf{n}_0, \ldots, \mathsf{n}_l}\ \text{Fresh}$$

  We conclude using DDH.

**Second generalization** The DDH rule can be generalized by allowing it to be applied simultaneously on multiple DDH triples, potentially overlapping. E.g., with two triples:

$$\frac{}{\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_0}, \mathsf{g}^{\mathsf{b}_1}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_1} \sim \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{c}_0}, \mathsf{g}^{\mathsf{b}_1}, \mathsf{g}^{\mathsf{c}_1}} \tag{4}$$

Observe that the same $\mathsf{a}$ is involved in two DDH triples: $(\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_0})$ and $(\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_1}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_1})$.

This rule can be shown valid using the simple DDH rule plus some usual rules:

$$\dfrac{\dfrac{\dfrac{}{\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{c}_0}, \mathsf{g}^{\mathsf{b}_1}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_1} \sim \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{c}_0}, \mathsf{g}^{\mathsf{b}_1}, \mathsf{g}^{\mathsf{c}_1}}\ \mathrm{DDH}_c \qquad \dfrac{\ldots}{(\mathsf{g}^{\mathsf{a}})^{\mathsf{b}_1} = \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_1}}}{\dfrac{\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{c}_0}, \mathsf{g}^{\mathsf{b}_1}, (\mathsf{g}^{\mathsf{a}})^{\mathsf{b}_1} \sim \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{c}_0}, \mathsf{g}^{\mathsf{b}_1}, \mathsf{g}^{\mathsf{c}_1}}{\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_0}, \mathsf{g}^{\mathsf{b}_1}, (\mathsf{g}^{\mathsf{a}})^{\mathsf{b}_1} \sim \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{c}_0}, \mathsf{g}^{\mathsf{b}_1}, \mathsf{g}^{\mathsf{c}_1}}\ \mathrm{DDH}_c + \textsc{Trans}}\ \mathrm{R} \qquad \dfrac{\ldots}{\mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_1} = (\mathsf{g}^{\mathsf{a}})^{\mathsf{b}_1}}}{\mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_0}, \mathsf{g}^{\mathsf{b}_1}, \mathsf{g}^{\mathsf{a}\cdot\mathsf{b}_1} \sim \mathsf{g}^{\mathsf{a}}, \mathsf{g}^{\mathsf{b}_0}, \mathsf{g}^{\mathsf{c}_0}, \mathsf{g}^{\mathsf{b}_1}, \mathsf{g}^{\mathsf{c}_1}}\ \mathrm{R}$$

Generalizing to any number of triples, we get the rule:

$$\frac{}{(\mathsf{g}^{\mathsf{a}_i})_{1\leq i\leq l}, (\mathsf{g}^{\mathsf{b}_j})_{1\leq j\leq m}, (\mathsf{g}^{\mathsf{a}_i\cdot\mathsf{b}_j})_{\substack{1\leq i\leq l\\1\leq j\leq m}} \sim (\mathsf{g}^{\mathsf{a}_i})_{1\leq i\leq l}, (\mathsf{g}^{\mathsf{b}_j})_{1\leq j\leq m}, (\mathsf{g}^{\mathsf{c}_{i,j}})_{\substack{1\leq i\leq l\\1\leq j\leq m}}}\ \mathrm{DDH}_m$$

where $(\mathsf{a}_i)_{1\leq i\leq l}, (\mathsf{g}^{\mathsf{b}_j})_{1\leq j\leq m}$ and $(\mathsf{c}_{i,j})_{\substack{1\leq i\leq l\\1\leq j\leq m}}$ are all names in $\mathcal{N}$.

The soundness proof for this rule is similar to the one for the rule in Equ. (4). We omit it.

**Final generalization** Finally, both generalization (application under context and multiple DDH triples) can be used at the same time, which yield the rules:

$$\frac{}{C\left[(\mathsf{g}^{\mathsf{a}_i})_{1\leq i\leq l}, (\mathsf{g}^{\mathsf{b}_j})_{1\leq j\leq m}, (\mathsf{g}^{\mathsf{a}_i\cdot\mathsf{b}_j})_{\substack{1\leq i\leq l\\1\leq j\leq m}}\right] \sim C\left[(\mathsf{g}^{\mathsf{a}_i})_{1\leq i\leq l}, (\mathsf{g}^{\mathsf{b}_j})_{1\leq j\leq m}, (\mathsf{g}^{\mathsf{c}_{i,j}})_{\substack{1\leq i\leq l\\1\leq j\leq m}}\right]}\ \mathrm{DDH}_m$$

where $(\mathsf{a}_i)_{1\leq i\leq l}, (\mathsf{g}^{\mathsf{b}_j})_{1\leq j\leq m}$ and $(\mathsf{c}_{i,j})_{\substack{1\leq i\leq l\\1\leq j\leq m}}$ are all names in $\mathcal{N}$, and $C$ is a context such that none of the DDH names occur in $C$. This rule soundness is shown using the same reasoning than in the last two rules. Again, we omit the details. ■

### Security of $\mathsf{Signed\text{-}DH_m}$

**Question 15.** *Prove that* $\mathsf{Signed\text{-}DH}_m \approx \mathsf{Signed\text{-}DH}^{id}_m$ *in any computational model where:*

- *the signature scheme* $(\mathcal{S}, \mathsf{pk}, \mathsf{sk}, \mathsf{sign}, \mathsf{check})$ *is EUF-CMA;*
- $(\mathcal{G}, \mathsf{e}, +)$ *is a family of cyclic groups of order* $\mathsf{O}_\eta$ *such that* $1/\mathsf{O}_\eta$ *is negligible.*
- *the symmetric encryption scheme* $(\mathsf{senc}(\_,\_,\_), \mathsf{sdec}(\_,\_))$ *is* $\text{IND-CCA}_1^{\mathcal{G}}$*;*
- *the group family* $(\mathcal{G}, \mathsf{e}, +)$ *satisfies the* DDH *assumption.*