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 A. The public key is shared with everybody, e.g. using some key server, while the secret key must never be shared by 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 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 check and 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 η has been omitted in the definitions above. Actually, all the functions of a signature scheme take as additional argument η (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 η.*

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* ($\mathsf{EUF\text{-}CMA}$) iff. for every PPTM $\mathcal{A}$:

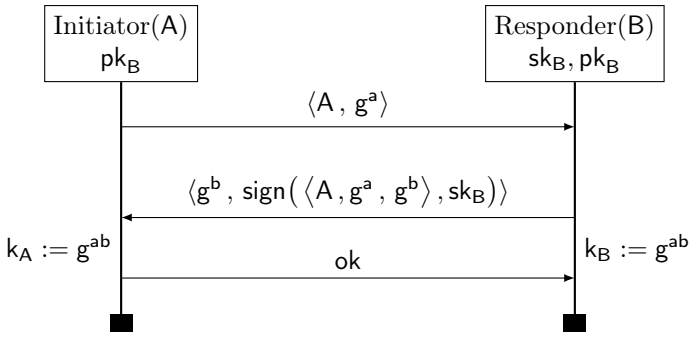
$$\mathsf{Pr}_{\mathsf{n} \in \mathcal{S}} \left(\mathcal{A}^{\mathcal{O}_{\mathsf{sign}(\cdot, \mathsf{sk}(\mathsf{n}))}}(1^\eta, \mathsf{pk}(\eta)) = \langle m\,,\, \sigma \rangle,\ m \text{ not queried to } \mathcal{O}_{\mathsf{sign}(\cdot, \mathsf{sk}(\mathsf{n}))} \text{ and } \mathsf{check}(\sigma,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

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

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

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.



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

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:*

- $P(\mathsf{A}, i)$ *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* $\mathsf{A} \in \mathcal{I}$*.*

We will use the channel $\mathsf{c}^i_{\mathsf{A}_0}$ *and* $\mathsf{c}^i_{\mathsf{A}_1}$ *for* $P_\mathsf{A}(i)$*, and* c^j_B *for* $B(j)$*. Moreover, the random exponents sampled by* $P(\mathsf{A}, i)$ *and* $B(j)$ *will be, respectively,* a_i *and* b_j*.*

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

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

Question 3. *For any trace* $\mathsf{tr} \diamond \mathsf{c}^i_{\mathsf{A}_1} \in \mathcal{T}_{io}$*, write a term* $\mathsf{accept_Q}@\mathsf{tr}$ *representing the acceptance check of* $P(\mathsf{A}, i)$*. To do this, we may use the term* $\mathsf{in_Q}@\mathsf{tr}$*, which represents the messages inputted at the end of* tr*.*

Question 4. *Give the definition of* $\mathsf{out_Q}@\mathsf{tr}$*, for any trace* $\mathsf{tr} \diamond \mathsf{c} \in \mathcal{T}_{io}$*, where* c *is any of the channels* $\mathsf{c}^i_{\mathsf{A}_0}$*,* $\mathsf{c}^i_{\mathsf{A}_1}$ *or* c^j_B*.*

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

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

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

1.2 Security Proof

We are now going to prove that Signed-DH has the key-agreement property.

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

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

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

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

is valid in any computational model where O_η is asymptotically large, in the sense that $1/O_\eta$ is negligible.

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

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.

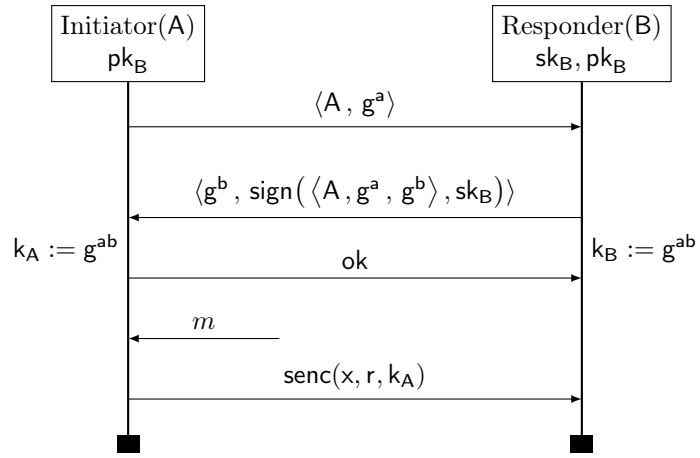
Our goal is to prove that $\mathsf{Signed\text{-}DH_m}$ is indistinguishable from an idealized version of the protocol $\mathsf{Signed\text{-}DH^{id}_m}$, where the content of the message sent has been replaced by a message of the same length, with all bits set to zero.

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

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

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

[2] 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

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 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 $\mathsf{senc}(v, \mathsf{r}_0, \mathsf{g^n})$ where $\mathsf{r}_0 \in \mathcal{N}$ or $\mathsf{sdec}(v, \mathsf{g^n})$ in $\vec{u}, t_0, t_1$;

iii) for all name r_0 such that $\mathsf{senc}(v, \mathsf{r}_0, \mathsf{g^n})$ is a subterm of $\vec{u}, t_0, t_1$, all occurrences of r_0 are in the subterm $\mathsf{senc}(v, \mathsf{r}_0, \mathsf{g^n})$.

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.*

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 η, 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.*

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

[3]The discrete logarithm assumption DLog state that PPTM can compute a from 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.*

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

Question 15. *Prove that* $\mathsf{Signed\text{-}DH_m} \approx \mathsf{Signed\text{-}DH_m^{id}}$ *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* O_η *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.*