MPRI SECURE: Proofs of Security Protocols

TD: Signed Diffie-Hellman Key-Exchange

Adrien Koutsos

2026/2027

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

0.1 Signature Scheme and EUF-CMA

An signature scheme $(\mathsf{pk}, \mathsf{sk}, \mathsf{sign}, \mathsf{check})$ comprises:

- 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 $\mathsf{n} \in \{0,1\}^\eta$ by some party A. The public key $\mathsf{pk}(\mathsf{n})$ is shared with everybody, e.g. using a key server, while the secret key $\mathsf{sk}(\mathsf{n})$ must remain secret. The signature $\sigma = \mathsf{sign}(m, \mathsf{sk}(\mathsf{n}))$ of a message m is computed using the private key $\mathsf{sk}(\mathsf{n})$, and proves that m originated from A. This signature can be verified by anyone using the public key $\mathsf{pk}(\mathsf{n})$ and the signature checking function $\mathsf{check}(_, _, _)$. To this end, we must have that:

$$\forall \mathsf{n} \in \{0,1\}^\eta.\ \forall m.\ \mathsf{check}(\mathsf{sign}(m, \mathsf{sk}(\mathsf{n})), m, \mathsf{pk}(\mathsf{n})) = \mathsf{true}$$

Unforgeability A signature scheme is computationally unforgeable when no adversary can build valid signatures, even if it is provided the 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 MACs.

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

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

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

Question 1. *Design a rule schemata for EUF-CMA for signatures.*

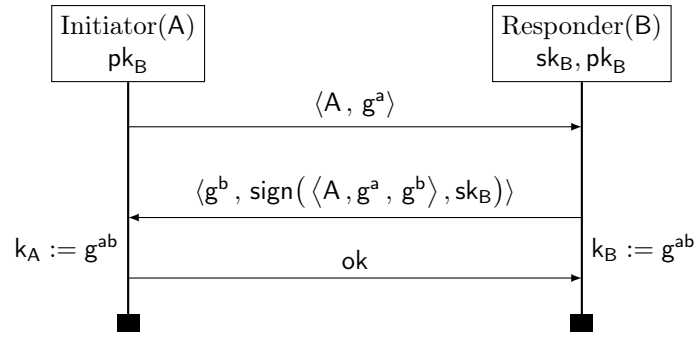
1 Signed Diffie-Hellman

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 protocol aims at establishing 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 g^a to B;

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



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

Figure 1: The signed Diffie-Hellman protocol Signed-DH.

- 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).

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

Let $\mathcal{I}$ be a finite set of identities.

Question 2. *Write the processes:*

- $P(A, i)$ *representing the* i*-th session of the initiator* $A \in \mathcal{I}$*;*
- $B(j)$ *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 A_i^0 *and* A_i^1 *for* $P(A, i)$*, and* B_j *for* $B(j)$*. Moreover, the random exponents sampled by* $P(A, i)$ *and* $B(j)$ *will be, respectively,* $a_{A,i}$ *and* b_j*.*

Let $N, M \in \mathbb{N}$. We consider the top-level process Q:

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

Question 3. *For any trace* $\mathtt{tr} : A_i^1 \in \mathcal{T}_{io}$*, write a term* $\mathsf{accept}_Q@\mathtt{tr}$ *representing the acceptance check of* $P(A, i)$*. To do this, we may use* $\mathsf{in}_Q@\mathtt{tr}$*, which represents the messages inputted at the end of* $\mathtt{tr}$*.*

Question 4. *Give the definition of* $\mathsf{out}_Q@\mathtt{tr}$*, for any trace* $\mathtt{tr} : \mathsf{c} \in \mathcal{T}_{io}$*, where* c *is any of the channels* A_i^0*,* A_i^1 *or* B_j*.*

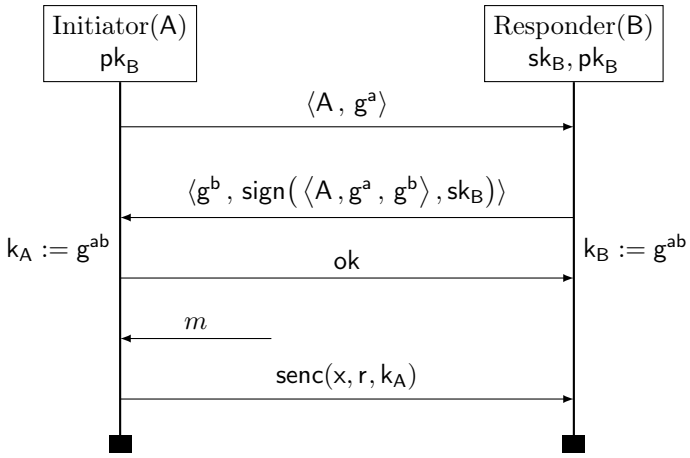
Key-Agreement Intuitively, the Signed-DH protocol has the key agreement property if, for any trace $\mathtt{tr} \in \mathcal{T}_{\mathsf{io}}$, for any identity A, if $P(\mathsf{A}, i)$ ends in an accepting state, then there exists a session j of B such that:

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

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

Question 5. *For any* $\mathtt{tr} : A_i^1 \in \mathcal{T}_{io}$*, write a term* $\mathsf{derived\text{-}key}_Q^A@\mathtt{tr}$ *representing the key derived by* $P(A, i)$*.*
Similarly, write a term $\mathsf{derived\text{-}key}_Q^B@\mathtt{tr}$ *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* $\mathtt{tr} \in \mathcal{T}_{io}$*.*



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

Figure 2: The signed Diffie-Hellman protocol with a single message exchanged $\mathsf{Signed\text{-}DH_m}$

1.2 Security Proof

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

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

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

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 $\mathsf{n} \in \mathcal{N}$ such that $\mathsf{n} \notin \mathit{st}(t)$, prove that the formula:*

$$[g^{\mathsf{n}} \neq t]$$

is valid in any computational model where O_η is asymptotically large, in the sense that $1/\mathsf{O}_\eta$ 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 $(\mathit{pk}, \mathit{sk}, \mathit{sign}, \mathit{check})$ 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.*

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 $\mathsf{senc}(m, \mathsf{r}, \mathsf{k_A})$[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 $\mathsf{Signed\text{-}DH_m^{id}}$, 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 $\mathit{Signed\text{-}DH_m}$ and $\mathit{Signed\text{-}DH_m^{id}}$.*

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.

[2] r is the symmetric encryption randomness.

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:

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

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 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 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.*

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]*.*

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 Signed-DH$_{\mathsf{m}}$

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

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

[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.