MPRI SECURE: Proofs of Security Protocols

TD: Signed Diffie-Hellman Key-Exchange

Adrien Koutsos

2025/2026

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 $\{0,1\}^\eta$.

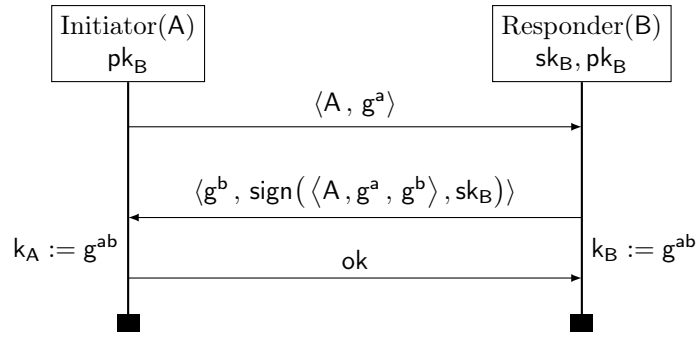
Question 1. *Design a rule schemata for EUF-CMA for signatures.*

Solution.

$$\mathsf{check}(\sigma, m, \mathsf{sk}(\mathsf{n})) \vdash \bigvee_{u \in \mathcal{S}} m = u$$

where:

- σ, m are ground terms and n a name in $\mathcal{N}$;
- n appears in σ 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: The signed Diffie-Hellman protocol Signed-DH.

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 $\mathsf{g^a}$ 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).

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*.*

Solution.

$$
\begin{aligned}
P(A,i) \;:=\; & \nu\, \mathsf{a}_{\mathsf{A},i}.\ \mathbf{in}(\mathsf{A}^0_\mathsf{i}, \_).\ \mathbf{out}(\mathsf{A}^0_\mathsf{i}, \langle \mathsf{A}\,,\, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \rangle).\\
& \qquad \mathbf{in}(\mathsf{A}^1_\mathsf{i}, \mathsf{x}).\ \mathbf{out}(\mathsf{A}^1_\mathsf{i}, \mathsf{if}\ \mathsf{check}(\pi_2(\mathsf{x}), \langle \mathsf{A}\,,\mathsf{g}^{\mathsf{a}_{\mathsf{A},i}}\,,\,\pi_1(\mathsf{x})\rangle\,,\mathsf{pk_B}))\\
& \qquad\qquad \mathsf{then\ ok}\\
& \qquad\qquad \mathsf{else\ ko}\\
B(j) \;:=\; & \nu\, \mathsf{b}_j.\ \ \mathbf{in}(\mathsf{B}_\mathsf{j}, \mathsf{y}).\ \mathbf{out}(\mathsf{B}_\mathsf{j}, \langle \mathsf{g}^{\mathsf{b}_j}\,,\, \mathsf{sign}(\langle \pi_1(\mathsf{y})\,,\,\pi_2(\mathsf{y})\,,\,\mathsf{g}^{\mathsf{b}_j}\rangle\,,\mathsf{sk_B})\rangle) \quad \blacksquare
\end{aligned}
$$

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

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

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

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

Solution.

$$\mathsf{accept}_\mathcal{Q}@\mathtt{tr} := \mathsf{check}(\pi_2(\mathsf{in}_\mathsf{Q}@\mathtt{tr}), \langle \mathsf{A}\,, \mathsf{g}^{\mathsf{a}_\mathbf{A},i}\,,\ \pi_1(\mathsf{in}_\mathsf{Q}@\mathtt{tr})\rangle\,, \mathsf{pk}_\mathsf{B})$$ ■

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

Solution.

$$\mathsf{out}_\mathsf{Q}@\mathtt{tr} := \begin{cases} \langle \mathsf{A}\,,\, \mathsf{g}^{\mathsf{a}_\mathbf{A},i}\rangle & \text{if } \mathtt{tr} : \mathsf{A}^0_\mathtt{i} \\ \mathsf{if\ accept}_\mathcal{Q}@\mathtt{tr}\ \mathsf{then\ ok\ else\ ko} & \text{if } \mathtt{tr} : \mathsf{A}^1_\mathtt{i} \\ \langle \mathsf{g}^{\mathsf{b}_j}\,,\, \mathsf{sign}(\langle \pi_1(\mathsf{in}_\mathsf{Q}@\mathtt{tr})\,, \pi_2(\mathsf{in}_\mathsf{Q}@\mathtt{tr})\,,\, \mathsf{g}^{\mathsf{b}_j}\rangle\,, \mathsf{sk}_\mathsf{B})\rangle & \text{if } \mathtt{tr} : \mathsf{B}_\mathtt{j} \end{cases}$$

■

Key-Agreement Intuitively, the Signed-DH protocol has the key agreement property if, for any trace $\mathtt{tr} \in \mathcal{T}_{io}$, 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 $\mathsf{g}^{\mathsf{a}_\mathbf{A},i\ \mathsf{b}_j}$.

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

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

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

Solution.

$$\begin{aligned} \mathsf{derived\text{-}key}^\mathsf{A}_\mathsf{Q}@\mathtt{tr} &:= (\pi_1(\mathsf{in}_\mathsf{Q}@\mathtt{tr}))^{\mathsf{a}_\mathbf{A},i} && \text{if } \mathtt{tr} : \mathsf{A}^1_\mathtt{i} \\ \mathsf{derived\text{-}key}^\mathsf{B}_\mathsf{Q}@\mathtt{tr} &:= (\pi_2(\mathsf{in}_\mathsf{Q}@\mathtt{tr}))^{\mathsf{b}_j} && \text{if } \mathtt{tr} : \mathsf{B}_\mathtt{j} \end{aligned}$$ ■

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

Solution. For any trace $\mathtt{tr} \in \mathcal{T}_{io}$, for any $\mathtt{tr}_1 : \mathsf{A}^0_\mathtt{i}$ and $\mathtt{tr}_3 : \mathsf{A}^1_\mathtt{i}$ such that $\mathtt{tr}_1 \le \mathtt{tr}_3 \le \mathtt{tr}$:

$$\mathsf{accept}_\mathcal{Q}@\mathtt{tr}_3 \rightarrow \bigvee_{\substack{\mathtt{tr}_2 : \mathsf{B}_\mathtt{j} \\ \mathtt{tr}_1 \le \mathtt{tr}_2 \le \mathtt{tr}_3}} \mathsf{derived\text{-}key}^\mathsf{A}_\mathsf{Q}@\mathtt{tr}_3 = \mathsf{derived\text{-}key}^\mathsf{B}_\mathsf{Q}@\mathtt{tr}_2 = \mathsf{g}^{\mathsf{a}_\mathbf{A},i\ \mathsf{b}_j}$$ ■

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 $\mathcal{S}$:*

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

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

$$\mathcal{S} = \left\{\langle \pi_1(\mathsf{in}_\mathsf{Q}@\mathtt{tr}')\,, \pi_2(\mathsf{in}_\mathsf{Q}@\mathtt{tr}')\,,\, \mathsf{g}^{\mathsf{b}_j}\rangle \mid \mathtt{tr}' : \mathsf{B}_\mathtt{j} \le \mathtt{tr}_3\right\}$$ ■

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

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

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

Solution. Let $\mathbb{M}$ be a computational model such that O_η is asymptotically large. We let $[\![\mathcal{G}]\!]^\eta_{\mathbb{M}}$ be the η-the group in the model $\mathbb{M}$ (thus $[\![\mathcal{G}]\!]^\eta_{\mathbb{M}}$ is of order O_η).

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

Let q_η is the quotient of 2^η by O_η. Then:

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

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

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

We conclude using the fact that:

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

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 $(\mathsf{pk}, \mathsf{sk}, \mathsf{sign}, \mathsf{check})$ 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.*

Solution. Let $\mathtt{tr} \in \mathcal{T}_{\mathsf{io}}$, $\mathtt{tr}_1 : \mathsf{A}^0_{\mathsf{i}}$ and $\mathtt{tr}_3 : \mathsf{A}^1_{\mathsf{i}}$ such that $\mathtt{tr}_1 \leq \mathtt{tr}_3 \leq \mathtt{tr}$. Let:

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

We want to give a derivation of:

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

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

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

I.e.:

$$\mathsf{accept}_{\mathcal{Q}}@\mathtt{tr}_3 \vdash \bigvee_{\substack{\mathtt{tr}_2:\mathsf{B}_j \\ \mathtt{tr}_2 \leq \mathtt{tr}_3}} \left\langle \pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2)\,, \pi_2(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2)\,, \mathsf{g}^{\mathsf{b}_j} \right\rangle = \langle \mathsf{A}\,, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}}\,, \pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_3)\rangle$$

Using the pair injectivity rules:

$$\mathsf{accept}_{\mathcal{Q}}@\mathtt{tr}_3 \vdash \bigvee_{\substack{\mathtt{tr}_2:\mathsf{B}_j \\ \mathtt{tr}_2 \leq \mathtt{tr}_3}} \pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{A} \wedge \pi_2(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \wedge \mathsf{g}^{\mathsf{b}_j} = \pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_3) \qquad (2)$$

is derivable.

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

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

Continuing the derivation of the right branch:

$$\dfrac{\mathsf{accept}_{\mathcal{Q}}@\mathtt{tr}_3, \begin{array}{r}\pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{A} \wedge \\ \pi_2(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \wedge \vdash \phi \\ \mathsf{g}^{\mathsf{b}_j} = \pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_3)\end{array} \quad \text{for any } \mathtt{tr}_2 : \mathsf{B}_j \text{ s.t. } \mathtt{tr}_2 \leq \mathtt{tr}_3}{\mathsf{accept}_{\mathcal{Q}}@\mathtt{tr}_3, \bigvee_{\substack{\mathtt{tr}_2:\mathsf{B}_j \\ \mathtt{tr}_2 \leq \mathtt{tr}_3}} \begin{array}{r}\pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{A} \wedge \\ \pi_2(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \wedge \vdash \phi \\ \mathsf{g}^{\mathsf{b}_j} = \pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_3)\end{array}}\ \text{L-}\vee \qquad (3)$$

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

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

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 $\pi_2(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2)$ (said otherwise, when $\mathtt{tr}_2 \leq \mathtt{tr}_1$, $\mathsf{a}_{\mathsf{A},i}$, the term $\pi_2(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2)$ 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):

$$\dfrac{\mathsf{accept}_{\mathcal{Q}}@\mathtt{tr}_3, \begin{array}{r}\pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{A} \wedge \\ \pi_2(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \wedge \vdash \mathsf{derived\text{-}key}^{\mathsf{A}}_{\mathcal{Q}}@\mathtt{tr}_3 = \mathsf{derived\text{-}key}^{\mathsf{B}}_{\mathcal{Q}}@\mathtt{tr}_2 = \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}\,\mathsf{b}_j} \\ \mathsf{g}^{\mathsf{b}_j} = \pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_3)\end{array}}{\mathsf{accept}_{\mathcal{Q}}@\mathtt{tr}_3, \begin{array}{r}\pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{A} \wedge \\ \pi_2(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_2) = \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \wedge \vdash \phi \\ \mathsf{g}^{\mathsf{b}_j} = \pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}_3)\end{array}}\ \text{R-}\vee$$

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

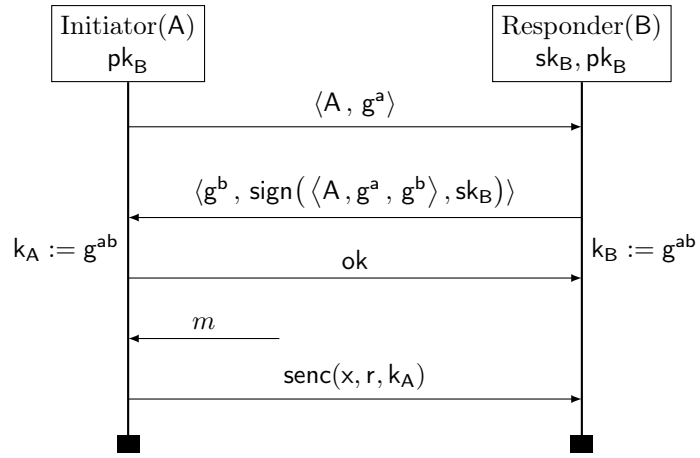
$$\mathsf{derived\text{-}key}^{\mathsf{B}}_{\mathcal{Q}}@\mathtt{tr}_2 = (\pi_2(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr}))^{\mathsf{b}_j} \qquad \mathsf{derived\text{-}key}^{\mathsf{A}}_{\mathcal{Q}}@\mathtt{tr}_3 = (\pi_1(\mathsf{in}_{\mathcal{Q}}@\mathtt{tr})))^{\mathsf{a}_{\mathsf{A},i}} \qquad \blacksquare$$

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 $\mathsf{Signed\text{-}DH}_{\mathsf{m}}$ is depicted in Figure 2.

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

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

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

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

$$\begin{aligned} P_m(A,i) \;:=\; & \nu\, \mathsf{a}_{\mathsf{A},i}.\ \mathbf{in}(\mathsf{A}^0_{\mathsf{i}}, \_).\ \mathbf{out}(\mathsf{A}^0_{\mathsf{i}}, \langle \mathsf{A}, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}} \rangle).\\ & \mathbf{in}(\mathsf{A}^1_{\mathsf{i}}, \mathsf{x}).\ \mathsf{if}\ \mathsf{check}(\pi_2(\mathsf{x}), \langle \mathsf{A}, \mathsf{g}^{\mathsf{a}_{\mathsf{A},i}}, \pi_1(\mathsf{x}) \rangle, \mathsf{pk_B})\ \mathsf{then}\\ & \qquad \mathbf{out}(\mathsf{A}^1_{\mathsf{i}}, \mathsf{ok}).\\ & \qquad \mathbf{in}(\mathsf{A}^2_{\mathsf{i}}, \mathsf{m}).\\ & \qquad \nu\, \mathsf{r}_{\mathsf{A},i}.\\ & \qquad \mathbf{out}(\mathsf{A}^2_{\mathsf{i}}, \mathsf{senc}(\mathsf{m}, \mathsf{r}_{\mathsf{A},i}, \pi_1(\mathsf{x}^{\mathsf{a}_{\mathsf{A},i}}))) \end{aligned}$$

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:

$$\mathbf{out}(\mathsf{A}^2_{\mathsf{i}}, \mathsf{senc}(0^{|\mathsf{m}|}, \mathsf{r}_{\mathsf{A},i}, \pi_1(\mathsf{x}^{\mathsf{a}_{\mathsf{A},i}})))$$ ■

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 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 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.*

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 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 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 η, where 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 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.*

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, g^a and g^b, using $\mathcal{A}$. It then compute $Z' = \mathsf{g}^{a \cdot b}$, and checks whether $Z' = Z$. ■

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.*

[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.

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 a, b and c are *names*.

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

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

  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 b and 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 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 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:

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

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

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

where $(\mathsf{a}_i)_{1\le i\le l}, (\mathsf{g}^{\mathsf{b}_j})_{1\le j\le m}$ and $(\mathsf{c}_{i,j})_{\substack{1\le i\le l\\1\le j\le m}}$ 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:

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

where $(\mathsf{a}_i)_{1\le i\le l}, (\mathsf{g}^{\mathsf{b}_j})_{1\le j\le m}$ and $(\mathsf{c}_{i,j})_{\substack{1\le i\le l\\1\le j\le m}}$ 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 Signed-DH$_\mathsf{m}$

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

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