Crypto Engineering - verifying security protocols
2022/2023

Exercices

Exercise 1

- Solve the following syntactic unification problems. If there is no unifier, explain why

  1. $f(x,y) \stackrel{?}{=} f(h(a),x)$
  2. $f(x,y) \stackrel{?}{=} f(h(x),x)$
  3. $f(x,a) \stackrel{?}{=} f(h(b),b)$
  4. $f(x,x) \stackrel{?}{=} f(h(y),y)$

- Now solve each of the above, modulo commutativity of f, i.e. $\forall x, y \quad f(x,y) = f(y,x)$.

Exercise 2

We recall the rules of the Deduction System for Dolev Yao theory: $T_0 \vdash s$, where $\llbracket \_ \rrbracket_{\_}$ represents a symmetric encryption scheme, $\{\ \_\ \}_{\_}$ an asymmetric encryption scheme, and we suppose that $pr(u)$ is the inverse secret key associated to $pk(u)$:

$$(\mathbf{A}) \quad \frac{u \in T_0}{T_0 \vdash u} \qquad\qquad (\mathbf{UL}) \quad \frac{T_0 \vdash \langle u,v \rangle}{T_0 \vdash u}$$

$$(\mathbf{P}) \quad \frac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \langle u,v \rangle} \qquad\qquad (\mathbf{UR}) \quad \frac{T_0 \vdash \langle u,v \rangle}{T_0 \vdash v}$$

$$(\mathbf{C}) \quad \frac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \llbracket u \rrbracket_v} \qquad\qquad (\mathbf{D}) \quad \frac{T_0 \vdash \llbracket u \rrbracket_v \qquad T_0 \vdash v}{T_0 \vdash u}$$

$$(\mathbf{AD}) \quad \frac{T_0 \vdash \{\ u\ \}_{pk(v)} \qquad T_0 \vdash pr(v)}{T_0 \vdash u} \qquad\qquad (\mathbf{AC}) \quad \frac{T_0 \vdash u \qquad T_0 \vdash pk(v)}{T_0 \vdash \{\ u\ \}_{pk(v)}}$$

The set of **Syntactic Subterms** of a term t, denoted by $S(t)$, is the smallest set such that:

- $t \in S(t)$
- $\langle u,v \rangle \in S(t) \Rightarrow u, v \in S(t)$
- $\llbracket u \rrbracket_v \in S(t) \Rightarrow u, v \in S(t)$

For a set T of terms, we define $S(T) = \bigcup_{t \in T} S(t)$.

The following algorithm allows to decide if $T_0 \vdash w$ (where $T \vdash^{\leq 1} s$ means that s can be obtained from T using only one rule from the Deduction System):

McAllester's Algorithm

Input : T_0, w

$T \leftarrow T_0$;

while ($\exists s \in S(T_0 \cup \{w\})$ such that $T \vdash^{\leq 1} s$ and $s \notin T$)

$T \leftarrow T \cup \{s\}$;

Output :$w \in T$

Using the above algorithm, prove or disprove that a passive Dolev Yao intruder can deduce the message s with the initial knowledge T_0.

1.) $T_0 = \{a, k\}$ and $s = \langle a, \{\!\{a\}\!\}_k \rangle$

2.) $T_0 = \{a, k, n1, \{\!\{k2\}\!\}_{\langle n1,n2\rangle}, \{\!\{\langle n2, \{\!\{n1\}\!\}_{\langle n3,n3\rangle}\rangle\}\!\}_k\}$ and $s = k2$

3.) $T_0 = \{a, b, k1, k2, \{\!\{k4\}\!\}_{\langle k1,k3\rangle}, \{\!\{\langle k2, n\rangle\}\!\}_{\langle k2,k1\rangle}, \{\!\{\langle k2, k3\rangle\}\!\}_{\langle k4,k1\rangle}\}$ and $s = k4$

Solution :

1.) It is true that $T_0 \vdash \langle a, \{\!\{a\}\!\}_k \rangle$, since we can build the following proof:

$$(P)\dfrac{(A)\dfrac{a \in T_0}{T_0 \vdash a} \qquad (C)\dfrac{(A)\dfrac{a \in T_0}{T_0 \vdash a} \qquad (A)\dfrac{k \in T_0}{T_0 \vdash k}}{T_0 \vdash \{\!\{a\}\!\}_k}}{T_0 \vdash \langle a, \{\!\{a\}\!\}_k \rangle}$$

2.) It is true that $T_0 \vdash k2$, since we can build the following proof:

$$(D)\dfrac{(A)\dfrac{\{\!\{k2\}\!\}_{\langle n1,n2\rangle} \in T_0}{T_0 \vdash \{\!\{k2\}\!\}_{\langle n1,n2\rangle}} \qquad (P)\dfrac{(A)\dfrac{n1 \in T_0}{T_0 \vdash n1} \qquad (UL)\dfrac{(D)\dfrac{(A)\dfrac{\{\!\{\langle n2, \{\!\{n1\}\!\}_{\langle n3,n3\rangle}\rangle\}\!\}_k \in T_0}{T_0 \vdash \{\!\{\langle n2, \{\!\{n1\}\!\}_{\langle n3,n3\rangle}\rangle\}\!\}_k} \qquad (A)\dfrac{k \in T_0}{T_0 \vdash k}}{T_0 \vdash \langle n2, \{\!\{n1\}\!\}_{\langle n3,n3\rangle}\rangle}}{T_0 \vdash n2}}{T_0 \vdash \langle n1, n2\rangle}}{T_0 \vdash k2}$$

3.) It is not true that $T_0 \vdash k4$. We use the locality result of Mc Allester.

Compute the set of subterms:

$S(T_0 \cup \{s\}) = \{a, b, k1, k2, \{\!\{k4\}\!\}_{\langle k1,k3\rangle}, \{\!\{\langle k2, n\rangle\}\!\}_{\langle k2,k1\rangle}, \{\!\{\langle k2, k3\rangle\}\!\}_{\langle k4,k1\rangle}, k4, \langle k1, k3\rangle, k3,$
$\langle k2, n\rangle, \langle k2, k1\rangle, n, \langle k2, k3\rangle, \langle k4, k1\rangle\}$.

We have to compute the set T_1 of all messages in $S(T_0 \cup \{s\})$ that can be derived from T_0, and then to check if $s \in T_1$ or not.

We put $T_1 \Leftarrow T_0 = \{a, b, k1, k2, \{\!\{k4\}\!\}_{\langle k1,k3\rangle}, \{\!\{\langle k2, n\rangle\}\!\}_{\langle k2,k1\rangle}, \{\!\{\langle k2, k3\rangle\}\!\}_{\langle k4,k1\rangle}\}$.

The only new message that is also in $S(T_0 \cup \{s\})$ and that can be obtained in one step from T_1 is $\langle k2, k1\rangle$: we apply (P) to $k2 \in T_1$ and $k1 \in T_1$, and we get $\langle k2, k1\rangle$.
We add $\langle k2, k1\rangle$ to T_1:
$T_2 \Leftarrow T_1 \cup \{\langle k2, k1\rangle\} = \{a, b, k1, k2, [\![k4]\!]_{\langle k1,k3\rangle}, [\![\langle k2, n\rangle]\!]_{\langle k2,k1\rangle}, [\![\langle k2, k3\rangle]\!]_{\langle k4,k1\rangle}, \langle k2, k1\rangle\}$.

Next, the only new message that is also in $S(T_0 \cup \{s\})$ and that can be obtained in one step from T_2 is $\langle k2, n\rangle$: we apply (D) to $[\![\langle k2, n\rangle]\!]_{\langle k2,k1\rangle} \in T_2$ and $\langle k2, k1\rangle \in T_2$, and we get $\langle k2, n\rangle$.
We add $\langle k2, n\rangle$ to T_2:
$T_3 \Leftarrow T_2 \cup \{\langle k2, kn\rangle\} = \{a, b, k1, k2, [\![k4]\!]_{\langle k1,k3\rangle}, [\![\langle k2, n\rangle]\!]_{\langle k2,k1\rangle}, [\![\langle k2, k3\rangle]\!]_{\langle k4,k1\rangle}, \langle k2, k1\rangle, \langle k2, n\rangle\}$.

Next, the only new message that is also in $S(T_0 \cup \{s\})$ and that can be obtained in one step from T_3 is n: we apply (UR) to $\langle k2, n\rangle \in T_1$, and we get n.
We add n to T_3:
$T_4 \Leftarrow T_3 \cup \{n\} = \{a, b, k1, k2, [\![k4]\!]_{\langle k1,k3\rangle}, [\![\langle k2, n\rangle]\!]_{\langle k2,k1\rangle}, [\![\langle k2, k3\rangle]\!]_{\langle k4,k1\rangle}, \langle k2, k1\rangle, \langle k2, n\rangle, n\}$.

From here we cannot apply any rules in order to get new messages in $S(T_0 \cup \{s\})$ from T_4, because:

- *(UR), (UL), (P), (C) do not generate nothing new (not in T_1) from $S(T_0 \cup \{s\})$ in one step.*
- *(D): we alredy applied (D) to $[\![\langle k2, n\rangle]\!]_{\langle k2,k1\rangle}$, and we can not apply (D) neither to $[\![k4]\!]_{\langle k1,k3\rangle}$ since $\langle k1, k3\rangle \notin T_4$, nor to $[\![\langle k2, k3\rangle]\!]_{\langle k4,k1\rangle}$ since $\langle k4, k1\rangle \notin T_4$.*

And now we can see that $s = k4 \notin T_4$, and hence, using the locality result of Mc Allester, we conclude that $T_0 \nvdash k4$.

Exercise 3
Consider the following protocol:

$$\begin{array}{llcll} 1. & A & \rightarrow & B & : \{\!|\, \langle A, N_a\rangle \,|\!\}_{pk(B)} \\ 2. & B & \rightarrow & A & : \langle \{\!|\, \langle A, K\rangle \,|\!\}_{pk(A)}, [\![N_a]\!]_K\rangle \\ 3. & A & \rightarrow & B & : \{\!|\, \langle\langle A, B\rangle, K\rangle \,|\!\}_{pk(B)} \end{array}$$

Assume that $\{\!|\, \_ \,|\!\}_\_$ is an asymmetric encryption scheme, $pk(x)$ (respectively $pr(x)$) is the public key (respectively private key) of participant x.

1. Consider a session between two honest participants a and b and show that k (the instantiation of variable K in this session) remains secret in presence of a passive Dolev-Yao intruder.

2. We assume now that the adversary i is active (he controls the network).

   1.) Consider the scenario corresponding to a session of a as initiator with i, and to a session of b as responder.

Suppose that the initial knwoledge of the intruder i is the set $T_1 = \{a, b, pk(a), pk(b), pk(i), pr(i)\}$, i.e. we suppose that a and b are honest. Suppose that at the end, b will think that he is talking and sharing a secret value k with a. Can you find an attack where the intruder i will learn k?

2.) Can you correct the protocol? Justify your answer.

Solution :

1. *The set of messages T_1 that a passive intruder get from a session between two honest participants a and b, plus the set of terms he already know initially is the set* $T_1 = \{a, b, pk(a), pk(b), pk(i), pr(i), \{\langle a, n_a\rangle\}_{pk(b)}, \langle \{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k\rangle, \{\langle\langle a, b\rangle, k\rangle\}_{pk(b)}\}$. *Now we show that $T_1 \not\vdash k$ using the locality result of Mc Allester.*

   Compute the set of subterms:
   $$S(T_1 \cup \{k\}) = \{a, b, pk(a), pk(b), pk(i), pr(i), \{\langle a, n_a\rangle\}_{pk(b)}, \langle \{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k\rangle,$$
   $$\{\langle\langle a, b\rangle, k\rangle\}_{pk(b)}, \langle a, n_a\rangle, n_a, \{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k, \langle a, k\rangle, k, \langle\langle a, b\rangle, k\rangle, \langle a, b\rangle\}.$$

   We have to compute the set T of all messages in $S(T_1 \cup \{k\})$ that can be derived from T_1, and then to check if $k \in T$ or not.

   We put $T \Leftarrow T_1 = \{a, b, pk(a), pk(b), pk(i), pr(i), \{\langle a, n_a\rangle\}_{pk(b)}, \langle \{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k\rangle, \{\langle\langle a, b\rangle, k\rangle\}_{pk(b)}\}$.

   The only new messages that are also in $S(T_1 \cup \{k\})$ and that can be obtained in one step from T are $\{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k, \langle a, b\rangle$:

   - *we apply (UL) to $\langle \{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k\rangle$ and we get $\{\langle a, k\rangle\}_{pk(a)}$.*
   - *we apply (UR) to $\langle \{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k\rangle$ and we get $[\![n_a]\!]_k$.*
   - *we apply (P) to a and b and we get $\langle a, b\rangle$.*

   We add all these new messages to T: $T \Leftarrow T \cup \{\{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k, \langle a, b\rangle\} = \{a, b, pk(a), pk(b), pk(i), pr(i), \{\langle a, n_a\rangle\}_{pk(b)}, \langle \{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k\rangle, \{\langle\langle a, b\rangle, k\rangle\}_{pk(b)}, \{\langle a, k\rangle\}_{pk(a)}, [\![n_a]\!]_k, \langle a, b\rangle\}$.

   From here we cannot apply any rules in order to get new messages in $S(T_1 \cup \{k\})$ from T, because:

   - *(UR), (UL), (P), (C) do not generate nothing new (not in T) from $S(T_1 \cup \{k\})$ in one step.*
   - *(D): we can not apply (D) to get new messages since all $pr(a), pr(b), k$ do not belong to T.*

   And now we can check that $k \notin T$, and hence, using the locality result of Mc Allester, we conclude that $T_1 \not\vdash k$.

2. *Consider now the case of an active adversary.*

1.) The attacker i can mount the following man-in-the-middle attack (and i can deduce k):

$$\begin{array}{lll} 1.1. & a \longrightarrow i : & \{\ \langle a, n_a \rangle\ \}_{pk(i)} \\ 2.1. & i(a) \longrightarrow b : & \{\ \langle a, n_a \rangle\ \}_{pk(b)} \\ 2.2. & b \longrightarrow i(a) : & \langle \{\ \langle a, k \rangle\ \}_{pk(a)}, [\![a_a]\!]_k \rangle \\ 1.2. & i \longrightarrow a : & \langle \{\ \langle a, k \rangle\ \}_{pk(a)}, [\![a_a]\!]_k \rangle \\ 1.3. & a \longrightarrow i : & \{\ \langle \langle a, i \rangle, k \rangle\ \}_{pk(i)} \\ 2.3. & i(a) \longrightarrow b : & \{\ \langle \langle a, b \rangle, k \rangle\ \}_{pk(b)} \end{array}$$

2.) A corrected version (see the TP):

$$\begin{array}{lllll} 1. & A & \rightarrow & B & : \{\ \langle A, N_a \rangle\ \}_{pk(B)} \\ 2. & B & \rightarrow & A & : \langle \{\ \langle B, K \rangle\ \}_{pk(A)}, [\![N_a]\!]_K \rangle \\ 3. & A & \rightarrow & B & : \{\ \langle \langle A, B \rangle, K \rangle\ \}_{pk(B)} \end{array}$$

Exercise 4

Consider the following (Needham-Schroeder-Lowe) protocol:

$$\begin{array}{lllll} 1. & A & \rightarrow & B & : \{\ \langle A, N_a \rangle\ \}_{pk(B)} \\ 2. & B & \rightarrow & A & : \{\ \langle N_a, \langle N_b, B \rangle \rangle\ \}_{pk(A)} \\ 3. & A & \rightarrow & B & : \{\ N_b\ \}_{pk(B)} \end{array}$$

Assume that $\{\ \_\ \}_\_$ is an asymmetric encryption scheme, $pk(x)$ (respectively $pr(x)$) is the public key (respectively private key) of participant x. This protocols ensures secrecy of N_b, and injective agreement from the perspective of both the initiator and the responder. Show that the following modified version of Needham-Schroeder-Lowe protocol:

$$\begin{array}{lllll} 1. & A & \rightarrow & B & : \{\ \langle A, N_a \rangle\ \}_{pk(B)} \\ 2. & B & \rightarrow & A & : \{\ \langle N_a, N_b \oplus B \rangle\ \}_{pk(A)} \\ 3. & A & \rightarrow & B & : \{\ N_b\ \}_{pk(B)} \end{array}$$

is not correct. It allows an attack on both the secrecy of N_b and on the authentication of B. This arises because $\oplus$ has algebraic properties that the free algebra assumption ignores: for instance, it is associative, commutative, and has the cancellation property $X \oplus X = 0$. What can you say about the following protocol?

$$\begin{array}{lllll} 1. & A & \rightarrow & B & : \{\ \langle A, N_a \rangle\ \}_{pk(B)} \\ 2. & B & \rightarrow & A & : \{\ \langle N_a \oplus B, N_b \rangle\ \}_{pk(A)} \\ 3. & A & \rightarrow & B & : \{\ N_b\ \}_{pk(B)} \end{array}$$

Solution : *The attacker i can mount the following man-in-the-middle attack (and i can deduce n_b):*

$$\begin{array}{lll} 1.1. & a \longrightarrow i : & \{\ \langle a, n_a \rangle\ \}_{pk(i)} \\ 2.1. & i(a) \longrightarrow b : & \{\ \langle a, n_a \rangle\ \}_{pk(b)} \\ 2.2. & b \longrightarrow i(a) : & \{\ \langle n_a, n_b \oplus b \rangle\ \}_{pk(a)} \\ 1.2. & i \longrightarrow a : & \{\ \langle n_a, n_b \oplus b \rangle\ \}_{pk(a)} \\ 1.3. & a \longrightarrow i : & \{\ (n_b \oplus b) \oplus i\ \}_{pk(i)} \\ 2.3. & i(a) \longrightarrow b : & \{\ n_b\ \}_{pk(b)} \end{array}$$

In the step 1.2, a will interpret $n_b \oplus b$ as $n'_b \oplus i$ with $n'_b = (n_b \oplus b) \oplus i$.
Interestingly, the following protocol

$$\begin{array}{lllll} 1. & A & \rightarrow & B & : \{\ \langle A, N_a \rangle\ \}_{pk(B)} \\ 2. & B & \rightarrow & A & : \{\ \langle N_a \oplus B, N_b \rangle\ \}_{pk(A)} \\ 3. & A & \rightarrow & B & : \{\ N_b\ \}_{pk(B)} \end{array}$$

is also flawed. The attacker i can mount the following man-in-the-middle attack (and i can deduce n_b):

$$\begin{array}{lll} 1.1. & a \longrightarrow i : & \{\ \langle a, n_a \rangle\ \}_{pk(i)} \\ 2.1. & i(a) \longrightarrow b : & \{\ \langle a, n_a \oplus i \oplus b \rangle\ \}_{pk(b)} \\ 2.2. & b \longrightarrow i(a) : & \{\ \langle n_a \oplus i, n_b \rangle\ \}_{pk(a)} \\ 1.2. & i \longrightarrow a : & \{\ \langle n_a \oplus i, n_b \rangle\ \}_{pk(a)} \\ 1.3. & a \longrightarrow i : & \{\ (n_b\ \}_{pk(i)} \\ 2.3. & i(a) \longrightarrow b : & \{\ n_b\ \}_{pk(b)} \end{array}$$

In the step 2.1, b will interpret $n_a \oplus i \oplus b$ as n'_a, and for this reason, in step 2.2 he will answer $\{\ \langle n'_a \oplus b, n_b \rangle\ \}_{pk(a)}$ which is the same as $\{\ \langle n_a \oplus i, n_b \rangle\ \}_{pk(a)}$.

Exercise 5

In this exercice, $(\_, \_)$ represents concatenation, and $\{\_\}_{\_}^{\_}$ represents a probabilistic symmetric encryption scheme (the randomness used is explicit now). We recall that two messages m_0 and m_1 are equivalent in the Dolev Yao model (written $m_0 \sim m_1$) if there is a renaming (a bijection) σ_K of keys of m_1 and a renaming σ_R of random coins of m_1 such that $\mathbf{pat}(m_0) = \mathbf{pat}(m_1)\sigma_K\sigma_R$.

Prove or disprove the symbolic equivalence $\sim$ in the Dolev Yao model of the following pairs of messages $m_0 \overset{?}{\sim} m_1$:

$$\begin{array}{lll} 1.) & m_0 = (\{(1, \{0\}_{k_1}^{r'})\}_k^r, \{0\}_k^{r'}), & m_1 = (\{(1, 0)\}_{k_3}^{r'}, \{1\}_{k_3}^s) \\ 2.) & m_0 = ((\{(0, \{1\}_k^{r'})\}_{k_1}^r, \{1\}_k^{r'}), k_1), & m_1 = ((\{(0, \{1\}_k^{r'})\}_{k_1}^r, \{1\}_k^{r''}), k_1) \\ 3.) & m_0 = (\{(0, \{1\}_k^{r'})\}_k^r, \{0\}_{k'}^{r'}), & m_1 = (\{0\}_k^{r'}, \{0\}_k^s) \end{array}$$

Solution :

1. *We have that $\mathbf{pat}(m_0) = (\square^r, \square^{r'})$, $\mathbf{pat}(m_1) = (\square^{r'}, \square^s)$. Hence for the bijective renaming $\sigma_R = \{r' \mapsto r, s \mapsto r'\}$ we have that $\mathbf{pat}(m_0) = \mathbf{pat}(m_1)\sigma_R$, and hence $m_0 \sim m_1$.*

2. *We have that $\mathbf{pat}(m_0) = ((\{(0, \square^{r'})\}_{k_1}^r, \square^{r'}), k_1)$, $\mathbf{pat}(m_1) = ((\{(0, \square^{r'})\}_{k_1}^r, \square^{r''}), k_1)$. Since there is no bijective renaming σ_R such that $\mathbf{pat}(m_0) = \mathbf{pat}(m_1)\sigma_R$, we conclude that $m_0 \not\sim m_1$.*

3. *We have that $\mathbf{pat}(m_0) = (\square^r, \square^{r'})$, $\mathbf{pat}(m_1) = (\square^{r'}, \square^s)$. Hence for the bijective renaming $\sigma_R = \{r' \mapsto r, s \mapsto r'\}$ we have that $\mathbf{pat}(m_0) = \mathbf{pat}(m_1)\sigma_R$, and hence $m_0 \sim m_1$.*

Exercise 6

We recall that a family of distributions $\mathcal{E}$ is called **polynomial-time constructible**, if there is a ppt-algorithm $\Psi_{\mathcal{E}}$, such that the output of $\Psi_{\mathcal{E}}(\eta)$ is distributed identically to $\mathcal{E}_\eta$. Given two families of distributions $\mathcal{D}$ and $\mathcal{E}$, we define $\mathcal{D}\|\mathcal{E}$ by

$$(\mathcal{D}\|\mathcal{E})_\eta = [x \leftarrow^R \mathcal{D}_\eta; y \leftarrow^R \mathcal{E}_\eta :\ (x, y)]$$

Prove or disprove the following assertions (where $\approx$ is the computational indistingushability relation over distributions):

- If $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}^0 \approx \mathcal{E}^1$ and $\mathcal{D}^0, \mathcal{D}^1, \mathcal{E}^0, \mathcal{E}^1$ are all polynomial-time constructible, then $(\mathcal{D}^0\|\mathcal{E}^0) \approx (\mathcal{D}^1\|\mathcal{E}^1)$.
- If $(\mathcal{D}^0\|\mathcal{E}^0) \approx (\mathcal{D}^1\|\mathcal{E}^1)$ then $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}^0 \approx \mathcal{E}^1$.

Solution :

- *Let $\mathcal{D}^0, \mathcal{D}^1, \mathcal{E}^0, \mathcal{E}^1$ be polynomial-time constructible families of distributions, and assume that $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}^0 \approx \mathcal{E}^1$. Let us prove that $(\mathcal{D}^0\|\mathcal{E}^0) \approx (\mathcal{D}^1\|\mathcal{E}^1)$.*

  We shall prove that $(\mathcal{D}^0\|\mathcal{E}^0) \approx (\mathcal{D}^1\|\mathcal{E}^0)$ and $(\mathcal{D}^1\|\mathcal{E}^0) \approx (\mathcal{D}^1\|\mathcal{E}^1)$. The equivalence $(\mathcal{D}^0\|\mathcal{E}^0) \approx (\mathcal{D}^1\|\mathcal{E}^1)$ will follow then by transitivity of $\approx$.

  The first assertion $(\mathcal{D}^0\|\mathcal{E}^0) \approx (\mathcal{D}^1\|\mathcal{E}^0)$ was already proven during the lectures. Let us prove $(\mathcal{D}^1\|\mathcal{E}^0) \approx (\mathcal{D}^1\|\mathcal{E}^1)$.

  Suppose that $(\mathcal{D}^1\|\mathcal{E}^0) \not\approx (\mathcal{D}^1\|\mathcal{E}^1)$, and let $\mathcal{A}$ be a ppt-adversary that can distinguish $(\mathcal{D}^1\|\mathcal{E}^0)$ and $(\mathcal{D}^1\|\mathcal{E}^1)$ with non-negligible advantage.

  Define an adversary $\mathcal{B}$ by

  $$\mathcal{B}(\eta, y) = [x \leftarrow^R \Psi_{\mathcal{D}^1}(\eta); b' \leftarrow^R \mathcal{A}(\eta, (x, y)) :\ b']$$

  We can see that if y is distributed according to $\mathcal{E}^i_\eta$, then the argument of $\mathcal{A}$ is distributed according to $(\mathcal{D}^1\|\mathcal{E}^i)_\eta$. Then

  $Adv^{\mathcal{E}^0,\mathcal{E}^1}(\mathcal{B}) = Pr[b' = 1 | y \leftarrow^R \mathcal{E}^0_\eta; b' \leftarrow^R \mathcal{B}(\eta, y)] - Pr[b' = 1 | y \leftarrow^R \mathcal{E}^1_\eta; b' \leftarrow^R \mathcal{B}(\eta, y)]$

  $= Pr[b' = 1 | y \leftarrow^R \mathcal{E}^0_\eta; x \leftarrow^R \Psi_{\mathcal{D}^1}(\eta); b' \leftarrow^R \mathcal{A}(\eta, (x, y))] - Pr[b' = 1 | y \leftarrow^R \mathcal{E}^1_\eta; x \leftarrow^R \Psi_{\mathcal{D}^1}(\eta); b' \leftarrow^R \mathcal{A}(\eta, (x, y))]$

  $= Pr[b' = 1 | y \leftarrow^R \mathcal{E}^0_\eta; x \leftarrow^R \mathcal{D}^1_\eta; b' \leftarrow^R \mathcal{A}(\eta, (x, y))] - Pr[b' = 1 | y \leftarrow^R \mathcal{E}^1_\eta; x \leftarrow^R \mathcal{D}^1_\eta; b' \leftarrow^R \mathcal{A}(\eta, (x, y))]$

  $= Pr[b' = 1 | x \leftarrow^R \mathcal{D}^1_\eta; y \leftarrow^R \mathcal{E}^0_\eta; b' \leftarrow^R \mathcal{A}(\eta, (x, y))] - Pr[b' = 1 | x \leftarrow^R \mathcal{D}^1_\eta; y \leftarrow^R \mathcal{E}^1_\eta; b' \leftarrow^R \mathcal{A}(\eta, (x, y))]$

  $= Adv^{\mathcal{D}^1\|\mathcal{E}^0,\mathcal{D}^1\|\mathcal{E}^1}(\mathcal{A})$

  Hence the advantage of $\mathcal{B}$ in distinguishing $\mathcal{E}^0$ and $\mathcal{E}^1$is equal to the advantage of $\mathcal{A}$ in distinguishing $(\mathcal{D}^0\|\mathcal{E}^0)$ and $(\mathcal{D}^1\|\mathcal{E}^1)$.

- *Assume that $(\mathcal{D}^0 \| \mathcal{E}^0) \approx (\mathcal{D}^1 \| \mathcal{E}^1)$. We must prove $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}^0 \approx \mathcal{E}^1$. We prove the second assertion, $\mathcal{E}^0 \approx \mathcal{E}^1$. The first one is similar.*

  Suppose that $\mathcal{E}^0 \not\approx \mathcal{E}^1$, and let $\mathcal{A}$ be a ppt-adversary that can distinguish $\mathcal{E}^0$ and $\mathcal{E}^1$ with non-negligible advantage.

  Define an adversary $\mathcal{B}$ by

  $$\mathcal{B}(\eta, (x, y)) = [b' \leftarrow^R \mathcal{A}(\eta, y) : \ b']$$

  Then $Adv^{\mathcal{D}^0\|\mathcal{E}^0, \mathcal{D}^1\|\mathcal{E}^1}(\mathcal{B}) = Pr[b' = 1|(x, y) \leftarrow^R (\mathcal{D}^0\|\mathcal{E}^0)_\eta; b' \leftarrow^R \mathcal{B}(\eta, (x, y))] - Pr[b' = 1|(x, y) \leftarrow^R (\mathcal{D}^1\|\mathcal{E}^1)_\eta; b' \leftarrow^R \mathcal{B}(\eta, (x, y))]$

  $= Pr[b' = 1|x \leftarrow^R \mathcal{D}^0_\eta; y \leftarrow^R \mathcal{E}^0_\eta; b' \leftarrow^R \mathcal{A}(\eta, y)] - Pr[b' = 1|x \leftarrow^R \mathcal{D}^1_\eta; y \leftarrow^R \mathcal{E}^1_\eta; b' \leftarrow^R \mathcal{A}(\eta, y)]$

  $= Pr[b' = 1|y \leftarrow^R \mathcal{E}^0_\eta; b' \leftarrow^R \mathcal{A}(\eta, y)] - Pr[b' = 1|y \leftarrow^R \mathcal{E}^1_\eta; b' \leftarrow^R \mathcal{A}(\eta, y)]$

  $= Adv^{\mathcal{E}^0, \mathcal{E}^1}(\mathcal{A})$

  Hence the advantage of $\mathcal{B}$ in distinguishing $(\mathcal{D}^0\|\mathcal{E}^0)$ and $(\mathcal{D}^1\|\mathcal{E}^1)$ is equal to the advantage of $\mathcal{A}$ in distinguishing $\mathcal{E}^0$ and $\mathcal{E}^1$.

Exercise 7
We use $\oplus$ to denote the usual bitwise xor over equal-length bitstrings, e.g. $0011 \oplus 1110 = 1101$, and $01 \oplus 00 = 01$.
Given two families of distributions $\mathcal{D}$ and $\mathcal{E}$, such that for any η, both $\mathcal{D}_\eta$ and $\mathcal{E}_\eta$ are distributions over strings of length η, we define $\mathcal{D} \oplus \mathcal{E}$ by

$$(\mathcal{D} \oplus \mathcal{E})_\eta = [x \leftarrow^R \mathcal{D}_\eta; y \leftarrow^R \mathcal{E}_\eta : \ (x \oplus y)]$$

.

Prove or disprove the following assertions (where $\approx$ is the computational indistingushability relation over distributions):

- If $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}$ is polynomial-time constructible, then $(\mathcal{D}^0 \oplus \mathcal{E}) \approx (\mathcal{D}^1 \oplus \mathcal{E})$.
- If $(\mathcal{D}^0 \oplus \mathcal{E}) \approx (\mathcal{D}^1 \oplus \mathcal{E})$ then $\mathcal{D}^0 \approx \mathcal{D}^1$.

Solution :

- *Let $\mathcal{E}$ be a polynomial-time constructible family of distributions, and assume that $\mathcal{D}^0 \approx \mathcal{D}^1$. Let us prove that $(\mathcal{D}^0 \oplus \mathcal{E}) \approx (\mathcal{D}^1 \oplus \mathcal{E})$.*

  Suppose that $(\mathcal{D}^0 \oplus \mathcal{E}) \not\approx (\mathcal{D}^1 \oplus \mathcal{E})$, and let $\mathcal{A}$ be a ppt-adversary that can distinguish $(\mathcal{D}^0 \oplus \mathcal{E})$ and $\mathcal{D}^1 \oplus \mathcal{E}$ with non-negligible advantage.

  Define an adversary $\mathcal{B}$ by

  $$\mathcal{B}(\eta, x) = [y \leftarrow^R \Psi_\mathcal{E}(\eta); b' \leftarrow^R \mathcal{A}(\eta, x \oplus y) : \ b']$$

We can see that if x is distributed according to $\mathcal{D}^i_\eta$, then the argument of $\mathcal{A}$ is distributed according to $(\mathcal{D}^i \oplus \mathcal{E})_\eta$. Then

$Adv^{\mathcal{D}^0,\mathcal{D}^1}(\mathcal{B}) = Pr[b' = 1|x \leftarrow^R \mathcal{D}^0_\eta; b' \leftarrow^R \mathcal{B}(\eta, x)] - Pr[b' = 1|y \leftarrow^R \mathcal{D}^1_\eta; b' \leftarrow^R \mathcal{B}(\eta, x)]$

$= Pr[b' = 1|x \leftarrow^R \mathcal{D}^0_\eta; y \leftarrow^R \Psi_\mathcal{E}(\eta); b' \leftarrow^R \mathcal{A}(\eta, x \oplus y)] - Pr[b' = 1|x \leftarrow^R \mathcal{D}^1_\eta; y \leftarrow^R \Psi_\mathcal{E}(\eta); b' \leftarrow^R \mathcal{A}(\eta, x \oplus y)]$

$= Pr[b' = 1|x \leftarrow^R \mathcal{D}^0_\eta; y \leftarrow^R \mathcal{E}_\eta; b' \leftarrow^R \mathcal{A}(\eta, x \oplus y)] - Pr[b' = 1|x \leftarrow^R \mathcal{D}^1_\eta; y \leftarrow^R \mathcal{E}_\eta; b' \leftarrow^R \mathcal{A}(\eta, x \oplus y)]$

$= Adv^{\mathcal{D}^0 \oplus \mathcal{E}, \mathcal{D}^1 \oplus \mathcal{E}}(\mathcal{A})$

Hence the advantage of $\mathcal{B}$ in distinguishing $\mathcal{D}^0$ and $\mathcal{D}^1$ is equal to the advantage of $\mathcal{A}$ in distinguishing $(\mathcal{D}^0 \oplus \mathcal{E})$ and $(\mathcal{D}^1 \oplus \mathcal{E})$.

- *The assertion is false.*

  Let $\mathcal{D}^0_\eta$ be the distribution that return the string 0^η with probability 1, and all other strings of length η with probability 0, that is,

  $Pr[d = 0^\eta | d \leftarrow^R \mathcal{D}^0_\eta] = 1$

  and for any string $w \in \{0,1\}^\eta$, such that $w \neq 0^\eta$, $Pr[d = w | d \leftarrow^R \mathcal{D}^0_\eta] = 0$.

  Let $\mathcal{D}^1_\eta$ be the distribution that return the string 1^η with probability 1, and all other strings of length η with probability 0, that is,

  $Pr[d = 1^\eta | d \leftarrow^R \mathcal{D}^1_\eta] = 1$

  and for any string $w \in \{0,1\}^\eta$, such that $w \neq 1^\eta$, $Pr[d = w | d \leftarrow^R \mathcal{D}^1_\eta] = 0$.

  Let $\mathcal{E}_\eta$ be the uniform distribution over the strings of length η, that is, for any string $w \in \{0,1\}^\eta$,

  $Pr[d = w | d \leftarrow^R \mathcal{D}^1_\eta] = 1/2^\eta$.

  Then $(\mathcal{D}^0 \oplus \mathcal{E}) = (\mathcal{D}^1 \oplus \mathcal{E})$, since both are the uniform distribution over the strings of length η, and hence $(\mathcal{D}^0 \oplus \mathcal{E}) \approx (\mathcal{D}^1 \oplus \mathcal{E})$. But obviously, $\mathcal{D}^0 \not\approx \mathcal{D}^1$.

  Consider for example the adversary $\mathcal{A}$ defined by:

$$\mathcal{A}(\eta, x) = if\ x = 0^\eta\ then\ return\ 1\ else\ return\ 0.$$