

# Security and Privacy, Blatt 4

Franziska Hutter (3295896)  
Felix Truger (3331705)  
Felix Bühler (2973410)

2. Juli 2018

## Problem 1: Transitivity of computational indistinguishability

$D_x$  is computationally indistinguishable from  $D'_x \implies \forall \text{ TM } U, \exists \text{ a negligible function } f, \text{ such that } \forall x \in L :$

$$|Pr[U(D_x, x) = 1] - Pr[U(D'_x, x) = 1]| \leq f(|x|).$$

Analogous for  $D'_x$  and  $D''_x : \exists \text{ a negligible function } g, \text{ such that:}$

$$|Pr[U(D'_x, x) = 1] - Pr[U(D''_x, x) = 1]| \leq g(|x|).$$

Let  $h(|x|) = \max(f(|x|), g(|x|))$ : We can conclude that in the above  $f(|x|)$  and  $g(|x|)$  can be replaced by  $h(|x|)$ . (Note that  $h(|x|)$  is still negligible, as it is just the greater of the both functions.)

We now want to have a look at:

$$|Pr[U(D_x, x) = 1] - Pr[U(D''_x, x) = 1]|$$

Which is equivalent to:

$$|Pr[U(D_x, x) = 1] - Pr[U(D'_x, x) = 1] + Pr[U(D'_x, x) = 1] - Pr[U(D''_x, x) = 1]|$$

Applying triangle inequality, we conclude that:

$$|Pr[U(D_x, x) = 1] - Pr[U(D''_x, x) = 1]| \leq$$

$$|Pr[U(D_x, x) = 1] - Pr[U(D'_x, x) = 1]| + |Pr[U(D'_x, x) = 1] - Pr[U(D''_x, x) = 1]|$$

Thus:

$$|Pr[U(D_x, x) = 1] - Pr[U(D''_x, x) = 1]| \leq 2 \cdot h(|x|)$$

As  $2 \cdot h(|x|)$  is negligible (namely the sum of two negligible functions),  $|Pr[U(D_x, x) = 1] - Pr[U(D''_x, x) = 1]|$  is upper bounded by the negligible function  $j(|x|) := 2 \cdot h(|x|)$ . It follows that  $D_x$  and  $D''_x$  are also computationally indistinguishable.

## Problem 2: Check for $e = 0$ in the Fiat-Shamir identification protocol

Soundness:  $\forall (n, v) \notin L$  and  $\forall \text{ ITMs } P^*$  it shall hold true, that  $Pr[\langle P^*, V' \rangle(n, v) = 1] \leq \frac{1}{2}$ . That means there should not be a Prover that can convince  $V'$  for an  $(n, v) \notin L$  to accept with a high probability. ( $V'$  as described in the problem description.)

We consider  $n = 5$ , hence  $\mathbb{Z}_n^* = \mathbb{Z}_5^* = \{1, 2, 3, 4\}$ . Furthermore we consider  $v = 2$ . Since  $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4$  and  $4^2 \equiv 1 \pmod{5}$ :  $(n, v) = (5, 2) \notin L$ . (There is no square root for 2 in  $\mathbb{Z}_5^*$ .)

We now want to show that there is a Prover  $B$  that can convince  $V'$  to accept upon input  $(5, 2)$  with a probability greater than  $\frac{1}{2}$ :

First note that  $V'$  is deterministic, since it does not use any randomness. Thus if our prover is able to convince  $V'$  once, it is always able to convince it with probability 1 just by repeating the same message flow.

For our example we let  $B$  commit to  $x = 2$ .  $V'$  will then send the challenge  $e = 1$ . We let  $B$  respond with  $y = 3$ .  $V'$  now calculates:  $y^2 \pmod{5} = 4$ .  $x \cdot v^e = 2 \cdot 2 = 4 \pmod{5}$ . Thus the check for  $y^2 = x \cdot v^e$  is successful. Also the check  $y \in \mathbb{Z}_5^*$  is successful.  $V'$  accepts and outputs 1, while actually  $(5, 2) \notin L$ . So we found a Prover  $B$  and an input  $(n, v)$  such that  $\Pr[\langle B, V' \rangle(n, v) = 1] = 1 > \frac{1}{2}$ . Thus  $(B, V')$  is not an IPS, since the soundness is not fulfilled.

### Problem 3: Pedersen commitment scheme without randomness

Commitment scheme  $\mathcal{C} = (\text{Gen}, \text{com}')$ :

- **Computational Hiding:**  $\mathcal{C}$  is computationally hiding if  $\forall$  ppt TM  $A$   $|\text{Adv}_{A, \mathcal{C}}^{\text{hiding}}(\eta)|$  is negligible.

Claim:  $\mathcal{C}$  is not computationally hiding. There is an adversary  $A'$  that has a non-negligible advantage  $|\text{Adv}_{A', \mathcal{C}}^{\text{hiding}}(\eta)| > 0$ . More specifically  $A'$  has the advantage  $|\text{Adv}_{A', \mathcal{C}}^{\text{hiding}}(\eta)| = 1$ .

Proof: Let  $A' = (A'_F, A'_G)$ . The security experiment  $\mathbb{E}_{A', \mathcal{C}}^{\text{hiding}}$  runs as follows:

- $\text{Gen}$  is used to generate a group  $\mathcal{G}$  with generator  $g$  and  $q = |\mathcal{G}|$  a prime.
- $A'_F$  just selects two values  $v_0, v_1 \in \mathbb{Z}_q$ .
- A random  $b \in \{0, 1\}$  is selected and a commitment  $c = \text{com}'((\mathcal{G}, q, g), v_b)$  is calculated.
- Now it is  $A'_G$ 's turn to guess given  $(\mathcal{G}, q, g, h)$  and  $c$ , which  $v_{b'}$  corresponds to that commitment and return  $b'$ .  $A'_G$  works as follows: It calculates  $g^{v_i}$  for each  $v_i \in \{0, 1\}$  and returns  $b' = i$  if  $c = g^{v_i}$ .

– Finally the security game returns 1 if  $b == b'$  and 0 otherwise.

It is obvious, that  $A'_G$  is always able to find the correct  $b'$ . Thus

$$\begin{aligned} Pr[\mathbb{E}_{\mathcal{A}', \mathcal{C}}^{hiding} = 1] &= 1 \\ |Adv_{\mathcal{A}', \mathcal{C}}^{hiding}(\eta)| &= 2 \cdot (Pr[\mathbb{E}_{\mathcal{A}', \mathcal{C}}^{hiding} = 1] - \frac{1}{2}) \\ &= 2 \cdot (1 - \frac{1}{2}) = 2 \cdot \frac{1}{2} = 1 \end{aligned}$$

- **Computational Binding:**  $\mathcal{C}$  is computationally binding if  $\forall$  ppt TM A  $|Adv_{A, \mathcal{C}}^{binding}(\eta)|$  is negligible.

$$|Adv_{A, \mathcal{C}}^{binding}(\eta)| = Pr[\mathbb{E}_{A, \mathcal{C}}^{binding}(1^\eta) = 1]$$

In words the advantage of every possible adversary  $A'$  shall be negligible. The advantage is the probability that  $A'$  is able to find  $v_0 \neq v_1 \in \mathbb{Z}_q$ , such that  $com'((\mathcal{G}, q, g, h), v_0) = c = com'((\mathcal{G}, q, g, h), v_1)$  for a randomly generated  $p = (\mathcal{G}, q, g, h)$ . (Which is the essential point of  $\mathbb{E}_{A, \mathcal{C}}^{binding}$ .)

Assume there were  $v_0, v_1 \in \mathbb{Z}_q, v_0 \neq v_1$ . As we know the commitment is simply calculated as  $g^{v_0}$  for  $v_0$  and  $g^{v_1}$  for  $v_1$ . Thus it would be required, that  $g^{v_0} = g^{v_1}$ . Note that  $\mathcal{G}$  is a cyclic finite Group and  $c \in \mathcal{G}$ . Thus  $g^{v_0} = g^{v_1} \implies v_0 = v_1$  in contradiction to the assumption. It is not possible for any adversary to find an ambiguous commitment. Thus the advantage of all ppt TM A is zero. It follows that  $\mathcal{C}$  is computationally binding.

## Problem 4: Schnorr's protocol - proof of knowledge

In the following we denote the corresponding language for  $R_{DL}$  as  $L_R = \{(\mathcal{G}, q, g, h) | \exists \omega : ((\mathcal{G}, q, g, h), \omega) \in R_{DL}\}$ . By definition the IPS  $(P, V)$  is a proof of knowledge with respect to  $R_{DL}$  and knowledge error  $\kappa$  if it fulfills the requirements of **non-triviality** and **validity**:

- **Non-triviality:**  $\forall x \in L_R : Pr[\langle P, V \rangle(x) = 1] = 1$  (Definition)

It is easy to see, that for any  $x \in L_R$  if the prover behaves correctly,  $V$  would accept with probability 1, because  $V$  directly checks the conditions for  $x \in L_R$  itself.

- **Validity:**  $\exists$  polynomial  $q, \exists$  ITM  $K, \forall$  ITM  $B, \forall x \in L_R, \forall \alpha \in \{0, 1\}^{t(|x|)}$  where  $t$  is the runtimebound of  $B$ :  
 If  $p(x, \alpha) := \Pr[\langle B^\alpha, V \rangle(x) = 1] > \kappa(|x|)$  then  $K^{B_x, \alpha}(x)$  outputs a witness  $\omega \in R(x)$  where the expected runtime of  $K$  is bounded by  $\frac{q(|x|)}{p(x, \alpha) - \kappa(|x|)}$ . (Definition)

Abc