Security and Privacy, Blatt 4

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

25. Juni 2018

Problem 1: Transitivity of computational indistinguishability

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

Soundness: $\forall (n, v) \notin L$ and $\forall$ 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 $4^2 \equiv 1 \bmod 5$: $(n, v) = (5, 2) \notin L$. (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: $y^2 \bmod 5 = 4$. $x \cdot v^e = 2 \cdot 2 = 4 \bmod 5$. 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

Problem 4: Schnorr's protocol - proof of knowledge