Security and Privacy, Blatt 3

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

12. Juni 2018

Problem 1: Sum of negligible functions

Definition: v is negligible $\implies \exists N \in \mathbb{N}$ such that $\forall n > N$ and for all positive polynomials p: $v(n) < \frac{1}{p(n)}$

v and v' negligible: $\exists N_1, N_2 \in \mathbb{N}$, such that:
$\forall n > N_1 : v(n) < \frac{1}{p(n)}$
$\forall n > N_2 : v'(n) < \frac{1}{p(n)}$
(by Definition)

Let $w(n) = v(n) + v'(n)$: For w to be negligible, we need an $N_3 \in \mathbb{N}$, such that $\forall n > N_3 : w(n) < \frac{1}{p(n)}$. We conclude from the above, that $\forall n > (N_1 + N_2) : v(n) + v'(n) < \frac{1}{p(n)} + \frac{1}{p(n)}$, Thus $N_3 = N_1 + N_2 \implies \forall n > N_3 : w(n) < \frac{2}{p(n)}$.
Since we're looking at the inverses of *all* positive polynomials, we can easily generate $\frac{1}{p(n)}$ from $\frac{2}{p(n)}$ by multiplying $p(n)$ by 2, which makes just another polynomial $2p(n)$, at which we are looking anyways. This means, that also $\forall n > N_3 : w(n) < \frac{1}{p(n)}$ holds for all positive polynomials p.

Problem 2: Deterministic verifier in IPS

V deterministic $\implies$ V does not use any randomness. Thus the output of V for a given input (i.e. under same conditions) is always the same. That means, that one can think of a prover P' that just replays the messages from P to V. By definition there are only polynomially many messages. Thus a deterministic P' can be constructed to convince V.

Witnesses:
$x \in L$: The witness w consists just of the messages, which P' has to send to V such that V accepts on (x, w). This witness must exist for $x \in L$, because otherwise the probability for V to accept would be 0 (in contradiction to the definition of IPS).
$x \notin L$: On the other hand there can not be a witness that leads to V accepting if $x \notin L$. Otherwise V would always accept when w is used, making the probability for V to accept 1, which again contradicts the definition of IPS.

This shows us for $L \in \mathcal{IP}$ if V is a deterministic verifier for L, that $L \in \mathcal{NP}$ holds.

Problem 3: Anonymous credentials and IPS

Problem 4: Equivalent definition of computational ZK

Problem 5: Reducing the error probability 1 ★