Security and Privacy, Blatt 3

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

19. Juni 2018

Problem 1: Sum of negligible functions

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

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 $p'(n) = 2p(n)$, at which we are looking anyway. This means, that there is also an N_4, such that $\forall n > N_4 : w(n) < \frac{1}{p'(n)}$.

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

2. Give an IPS for L and prove its properties

IPS (P, V). Protocol on input c:

Prover P		Verifier V
Compute *name*, *age*, *residence*, k, r and $x =$ "Name: *name*, Age: *age*, Residence: *residence*" such that $c = E(x, k, r) \land age \geq 18$	$\xrightarrow{name,\ age\ residence,\ k,\ r}$	Compute $x' =$ "Name: *name*, Age: *age*, Residence: *residence*" and $c' = E(x', k, r)$ **if** ($c' == c$ && $age \geq 18$) **then** output 1 **else** output 0.

Proof of properties:

- Completeness: It is obvious that for any $c \in L$, V will accept with probability 1, because V does not use any randomness and directly receives all necessary information from P to conclude $c \in L$.
  Thus $Pr[\langle P, V\rangle(c) = 1 \mid c \in L] = 1 \geq \frac{2}{3}$.
- Soundness: $\forall c' \notin L$ and $\forall$ ITMs P^*: Since V is directly checking the properties for c' itself, there is obviously no chance that any prover would fool V on any $c' \notin L$ to accept upon such a c'.
  Thus $Pr[\langle P, V\rangle(c') = 1 \mid c' \notin L] = 0 \leq \frac{1}{3}$

1. Show: $L \in \mathcal{NP}$

In the above protocol we see, that V is deterministic (i.e. V does not use any randomness and always has the same output under same conditions). Furthermore $\langle P, V\rangle$ is an IPS for L. As we know from problem 2, these are exactly the conditions for $L \in \mathcal{NP}$.

Problem 4: Equivalent definition of computational ZK

Problem 5: Reducing the error probability 1 ★

Assuming there is an IPS (P, V) as described in (i), i.e. an IPS for L that has completeness bound 1 and soundness bound $\frac{1}{3}$: One could easily think of another IPS (P', V') that just repeats the original (P, V) $n \in \mathbb{N}$ times and lets V' accept only if V accepted in every single run of (P, V).
Since we started with completeness bound 1, V' will (also) accept with probability $1^n = 1$ for $x \in L$.
On the other hand, we started with soundness bound $\frac{1}{3}$, which means V would accept for $x \notin L$ with a probability lower than or equal to $\frac{1}{3}$. For V' we can conclude that it accepts with a probability lower than or equal to $\frac{1}{3^n}$.
Thus we can choose n such that the soundnes bound is lowered to a value arbitrarily close to 0.
In particular we want to have a soundness bound of $2^{-p(|x|)} = \frac{1}{2^{p(|x|)}}$ for every polynomial p. V' can have polynomial runtime according to the definition of IPS. Thus we are not bound to repeat the proving process only in a linear manner (like $n \in \mathbb{N}$ times). We can also repeat it $p(|x|)$ times resulting in a probability of V'' to accept for $x \notin L$ of $\frac{1}{3^{p(|x|)}}$. Thus we have a new soundness bound for V'', that is lower than $2^{-p(|x|)}$, while (obviously) the completeness bound remains 1. Hence (i) $\implies$ (ii).
In the other direction, if we have an IPS with completeness bound 1 and soundness bound $2^{-p(|x|)}$ for every polynomial (ii), we are obviously able to always find a $p(x)$ such that $2^{-p(|x|)} \leq \frac{1}{3}$. Thus (ii) $\implies$ (i) and subsequently (i) $\Leftrightarrow$ (ii).