

# Security and Privacy, Blatt 3

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

6. 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, at which we are looking anyways. This means, that also  $\forall n > N_3 : w(n) < \frac{1}{p(n)}$  holds.

## Problem 2: Deterministic verifier in IPS

## Problem 3: Anonymous credentials and IPS

## Problem 4: Equivalent definition of computational ZK

## Problem 5: Reducing the error probability 1

