Security and Privacy, Blatt 5

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

5. Juli 2018

Problem 1: Schnorr's protocol - special honest verifier zero-knowledge

It is easy to see, that (P, V) as given for Schnorr's protocol has the form of a Σ-protocol with commitment a, challenge e and response z. The "special honest verifier ZK" property requires: $\exists$ ppt simulator M such that $\forall x \in L_R$ and $e \in \{0,1\}^t : M(x,e) = Trans_{V^e}^{P}(x)$ where $Trans_{V^e}^{P}(x)$ is the Transcript of an interaction between P and V using challenge e on input x.

Problem 2: Homomorphic properties of algorithms

Problem 3: Building circuits for functions

Problem 4: Garbled circuits

Problem 5: 51%-Attack on Bitcoin