Security and Privacy, Blatt 4

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

21. Juni 2018

Problem 1: Transitivity of computational indistinguishability

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

Problem 3: Pedersen commitment scheme without randomness

Problem 4: Schnorr's protocol - proof of knowledge