Prüfungsvorbereitung

Christian Grothoff

Berner Fachhochschule

June 9, 2018

Fragegebiete: Crytography

- Blinding (GNS-style, RSA-style, FoT-style)
- Cut-and-choose (FoT, Taler, principle!)
- Bilinear maps & BLS Signatures
- Homomorphic Encryption (idea, not Paillier math)
- Common SMC adversary models
- Efficient computation of DLOG

Fragegebiete: Protocols

- Design goals for secure channels
- Analysis and design of KX protocols
- Constructions of SC from DH-based KX
- Anonymity metrics, mixing, onion routing
- Name systems design goals, GNS cryptography
- Specialized SMC protocol (FoT, Scalarproduct)