Hardness amplification for weakly verifiable cryptographic primitives

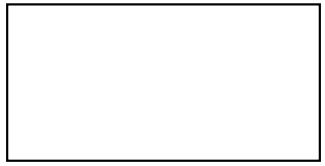
Grzegorz Mąkosa

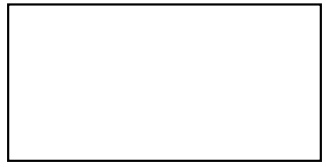
Advisors: Prof. Dr. Thomas Holenstein, Dr. Robin Künzler
Department of Computer Science, ETH Zürich

Agenda

- Motivation and problem statement
- Background and related work
- My contribution
- Results
- Discussion

Hardness Amplification





Weakly Verifiable Cryptographic Primitives

Dynamic Cryptographic Primitives

Interactive Cryptographic Primitives

Previous work of Cannetti, Halevi, and Steiner

Previous work DIJK

Previous work HS

My contribution I

My contribution II

Discussion

Questions