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

Previous works HS

Previous works DIJK

My contribution I

My contribution II

Discussion

Questions