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



Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich