Hardness amplification for weakly verifiable cryptographic primitives

Grzegorz Mąkosa

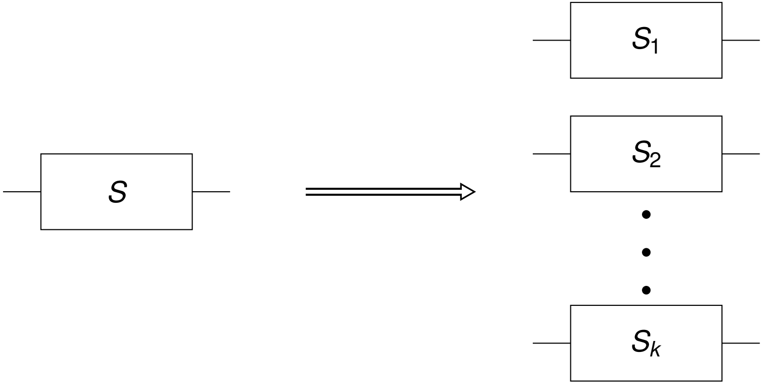
Advisors: Prof. Dr. Thomas Holenstein, Dr. Robin Künzler
Department of Computer Science, ETH Zürich

Agenda

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

Hardness Amplification

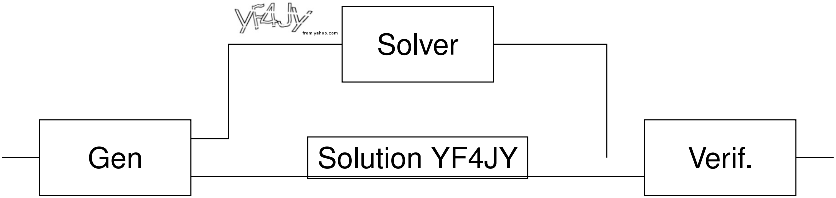
Is solving parallel repetition of problems substantially harder than a single instance of a problem?



Weakly Verifiable Puzzles

1. An algorithm G generates a puzzle p together with some secrecy information s.
2. A solver given p has to find a correct solution.
3. It is hard for the solver to verify the correctness of a solution given only p.
4. A verification algorithm has access to s which makes the task of checking the correctness of a solution easy.

Weakly Verifiable Primitives - Example



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