Hardness amplification for weakly verifiable cryptographic primitives

Grzegorz Mąkosa

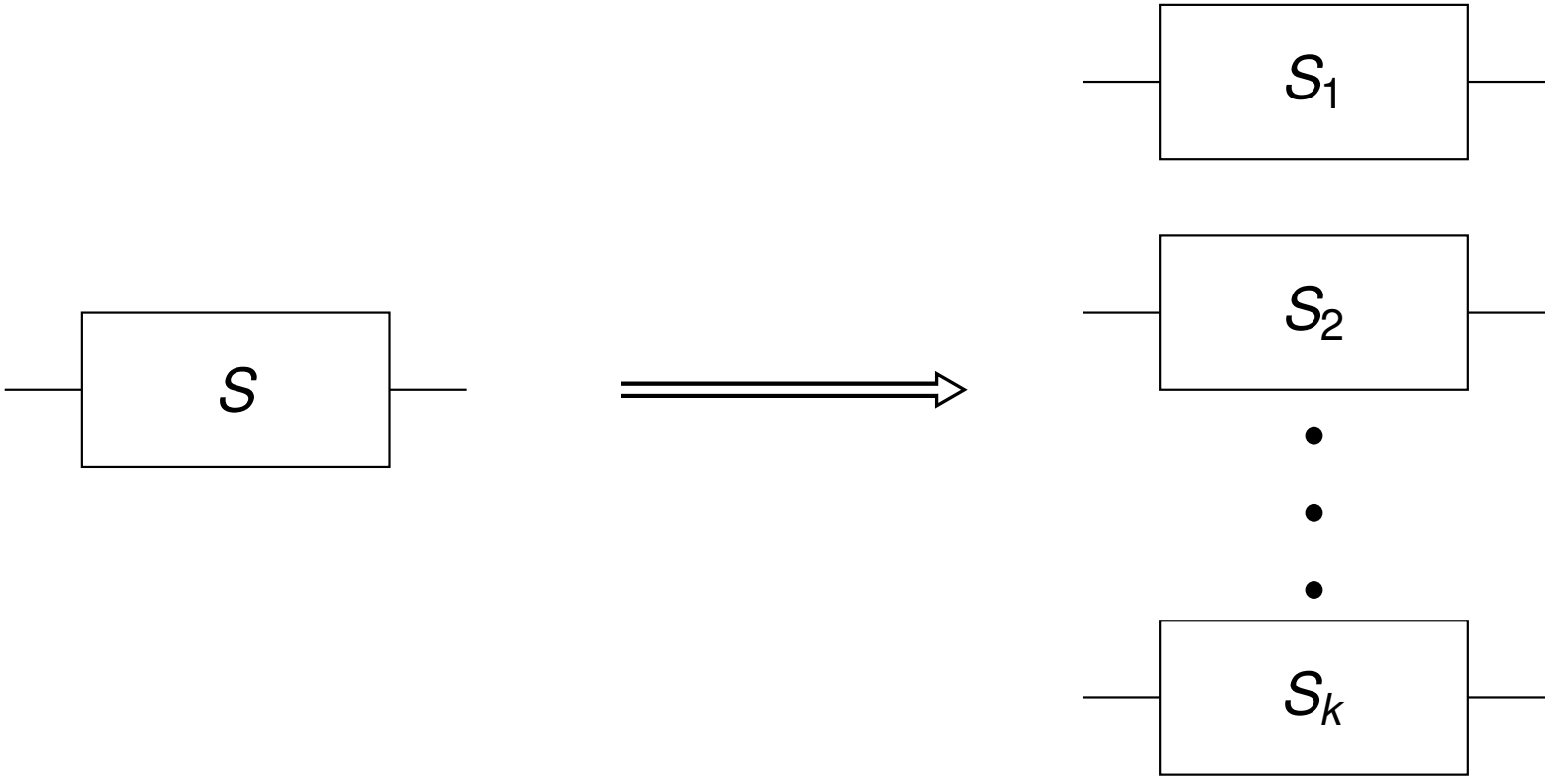
Advisors: Prof. Dr. Thomas Holenstein, Dr. Robin Künzler
Department of Computer Science, ETH Zürich

Agenda

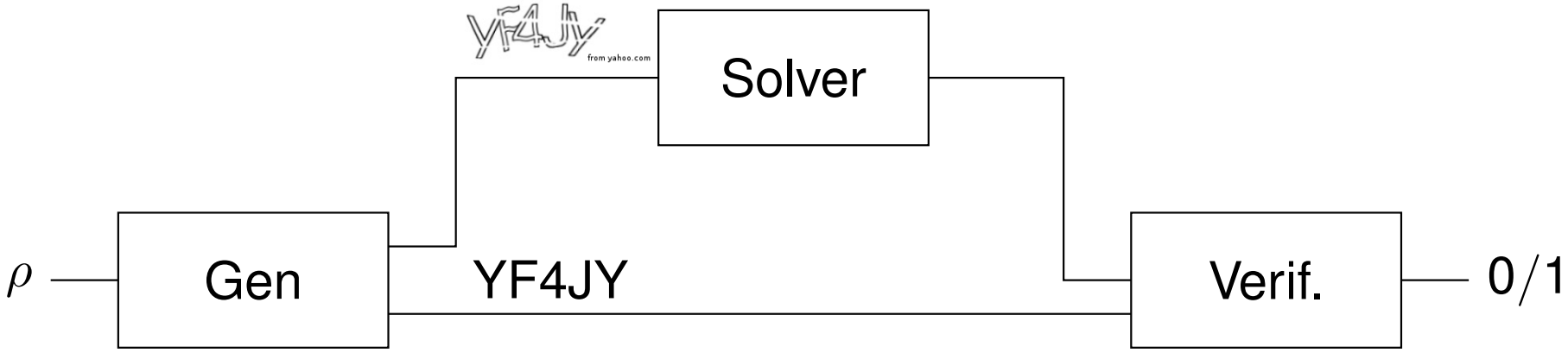
- Motivation and problem statement
- Background and related work
- My contribution
- Results
- Discussion

Hardness Amplification

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



Weakly Verifiable Puzzles - CAPTCHA



Assumptions

- Small solutions space.
- Solver cannot have a way to efficiently verify its solutions.

Weakly Verifiable Puzzles

- Introduces by Cannetti, Halevi, Steiner [CHS05]
- An algorithm *G* generates a puzzle *p* together with some secrecy information *s*.
- A solver given *p* has to find a correct solution.
- It is hard for the solver to verify the correctness of a solution given only *p*.
- A verification algorithm has access to *s* which makes the task of checking the correctness of a solution easy.

Threshold and Binary Monotone Functions

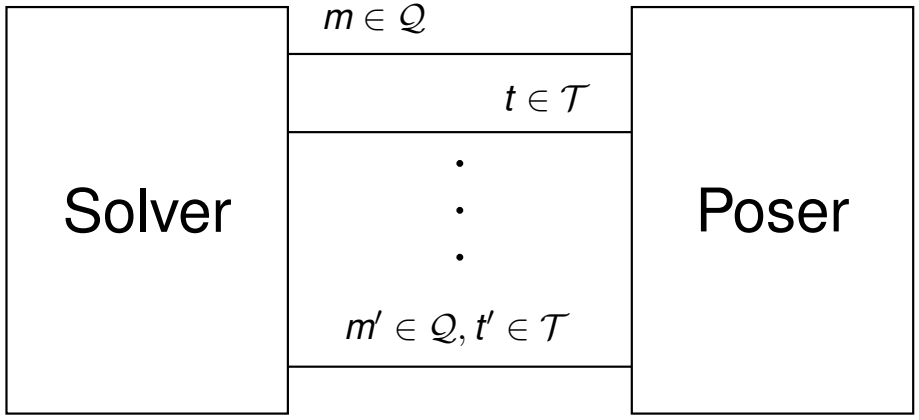
Threshold functions
Binary functions

Gap Amplification

Difference between human and computer algorithms solutions.

Dynamic Puzzles Example

- Game based security definition of MAC.



Dynamic Puzzle Definition (Informal)

- Given a set of indices $\mathcal{Q}$
- Hints : Solver can ask for solutions on any $q \in \mathcal{Q}$
- Verification: Solver solves a puzzle on $q \in \mathcal{Q}$ for which it has not asked for a hint before.
- Number of hint and verification queries limited.
- Generalize breaking MACs and signature schemes
- Introduced by Dodis et al. [**?**]

Interactive Puzzles Example

- Binding property of the bit commitment protocols.

Goal

Give a single proof for puzzles that are dynamic, interactive, and weakly verifiable.

Weakly Verifiable

+

Dynamic Puzzles

+

Interactive Puzzles

Previous work of Cannetti, Halevi, and Steiner

Previous work DIJK

Previous work HS

My contribution I

My contribution II

Discussion

Questions

Bibliography

Ran Canetti, Shai Halevi, and Michael Steiner.
Hardness amplification of weakly verifiable puzzles.
In *Theory of Cryptography*, pages 17–33. Springer, 2005.