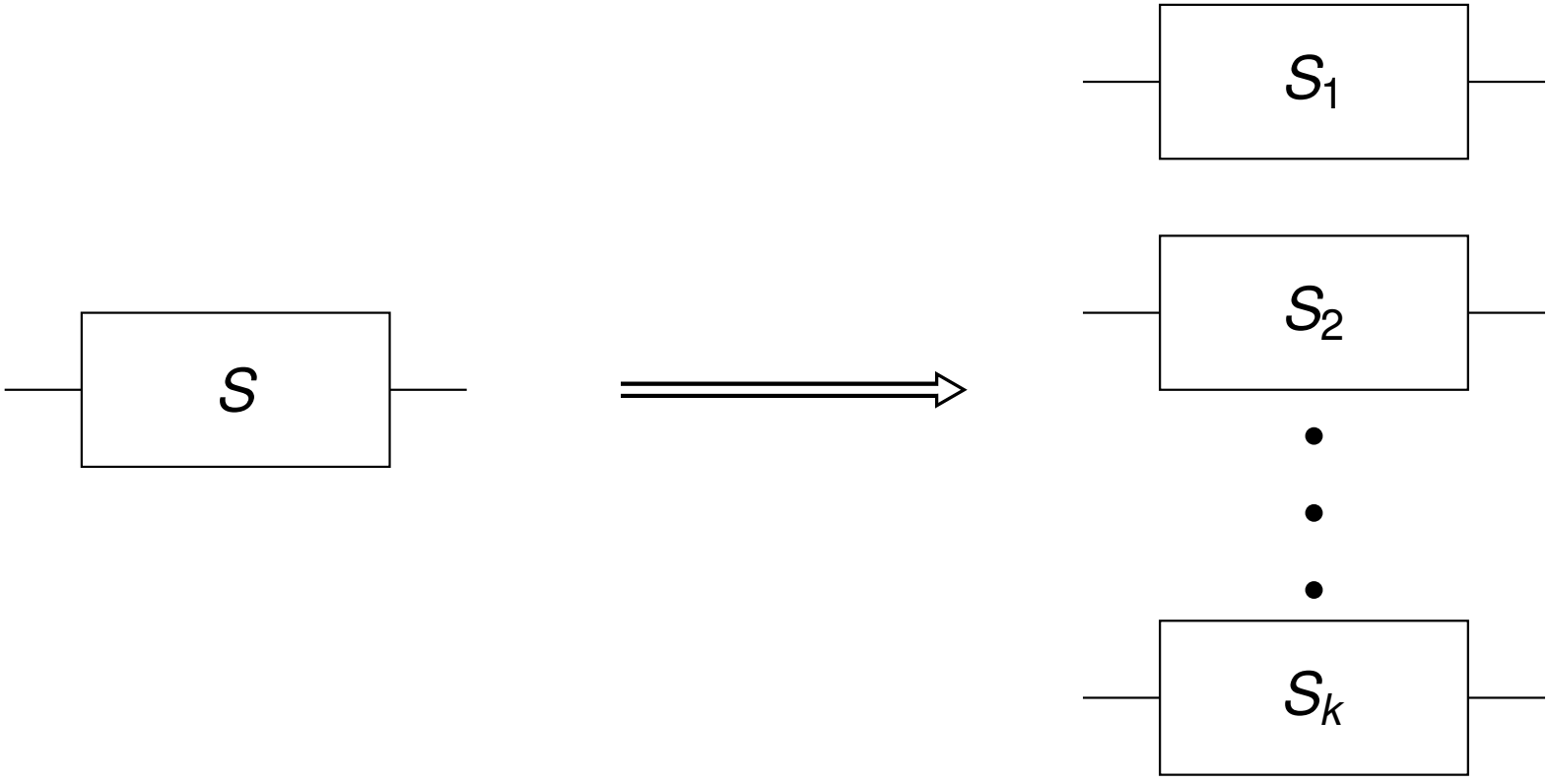
Hardness Amplification for Weakly Verifiable Cryptographic Primitives

Grzegorz Mąkosa

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

Hardness Amplification

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



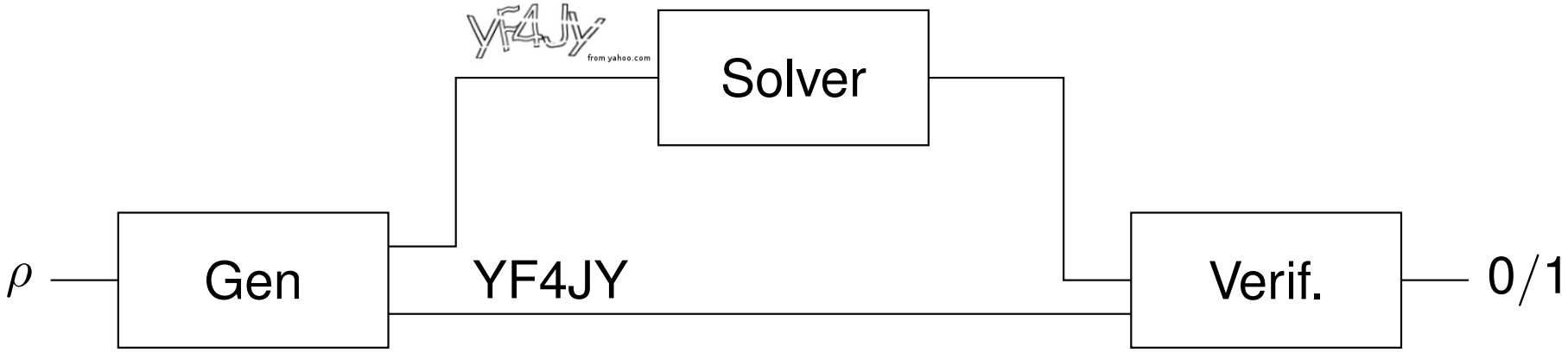
Hardness Amplification Facts

- Weak one-way function $\Longrightarrow$ strong one-way function
- What about MAC, signature schemes, CAPTCHAs?

Agenda

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

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

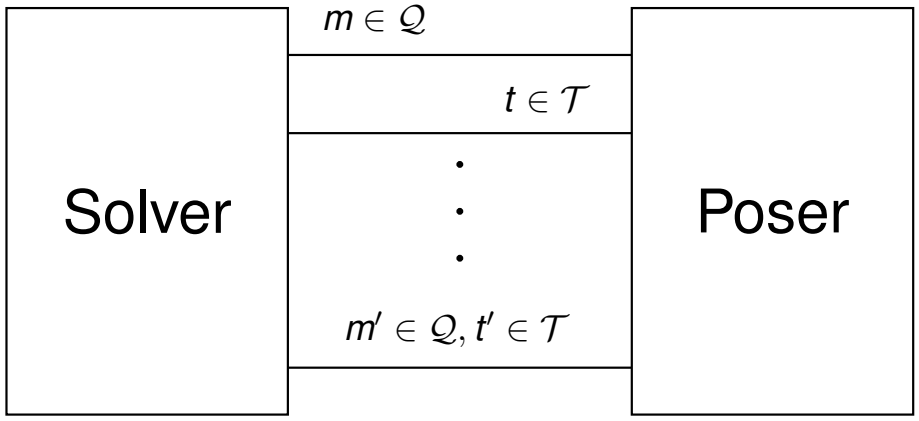
Threshold functions
Binary functions

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

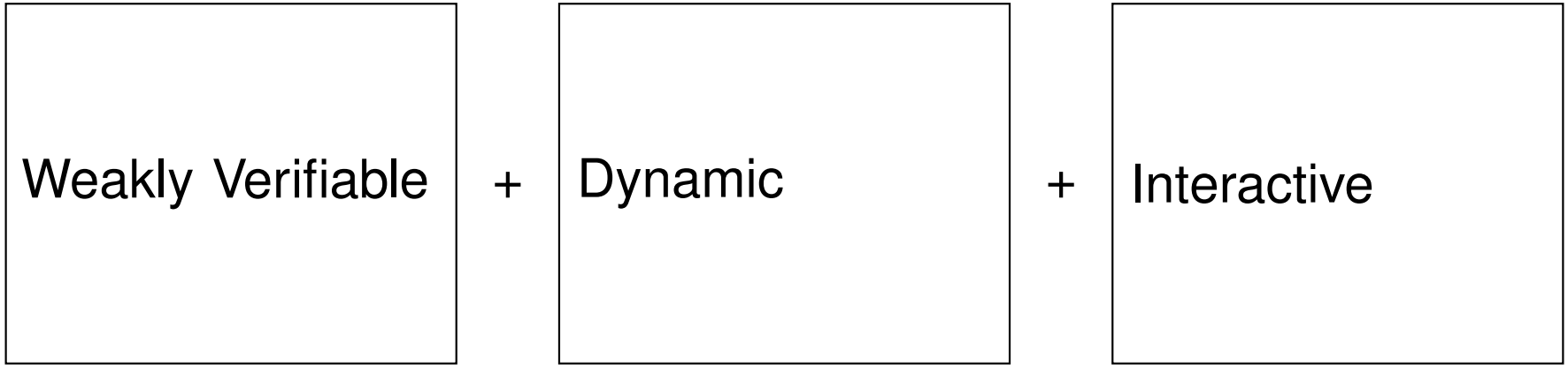
- Binding property of the bit commitment protocols.

Previous works

- Weakly verifiable puzzles [CHS05]
- Dynamic weakly verifiable puzzles and threshold functions [**?**]
- Interactive puzzles and monotone function [**?**]

Goal

- Define puzzles that generalize MAC, CAPTCHA, bit commitments.
- Hardness amplification result for these puzzles.



Dynamic interactive puzzles

- Cannot run the solver multiple times.
- Hint queries from previous runs can prevent verification queries from succeeding.
- Use hash function to partition query domain [**?**].

Weakly verifiable puzzles

- Cannot check whether the solution is correct.
- For a special case where all puzzles have to be solved.
- Look at remaining $n - 1$ puzzles that are generated.

Results

Let C be a solver for parallel repetition of puzzles

$$\geq \Pr_{u \leftarrow \mu_\delta^k}[g(u) = 1] + \varepsilon,$$

then D with high probability satisfies

$$\geq \frac{1}{16(h+v)}\left(\delta + \frac{\varepsilon}{6k}\right). \tag{0.1}$$

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.