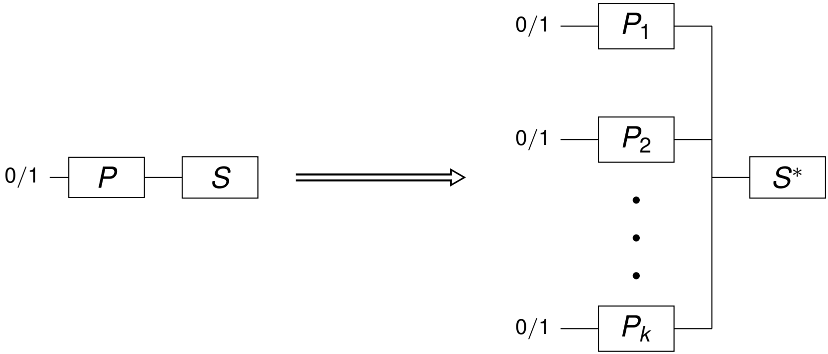
Hardness Amplification for Weakly Verifiable Cryptographic Primitives

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?



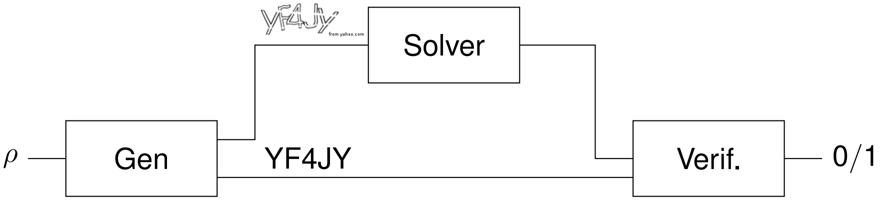
Hardness Amplification Facts

- 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



- Small solutions space.
- Solver cannot 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.

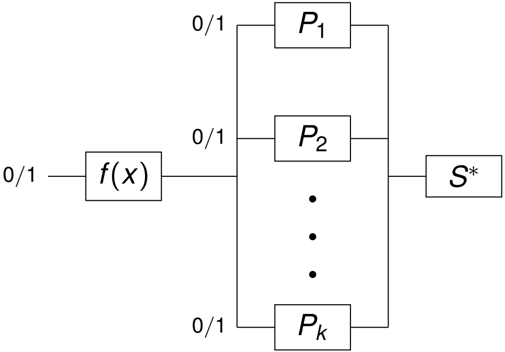
Threshold and Monotone Functions

Threshold function

$$f_K(b_1, \dots, b_n) = \begin{cases} 1 \text{ if } \sum_{i=1}^{n} b_i \geq K \\ 0 \text{ otherwise.} \end{cases}$$

Monotone function

$$f(b_0, \dots, b_n) : \{0,1\}^n \to \{0,1\}$$

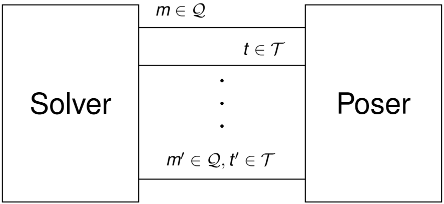


Gap Amplification

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 [**?**]

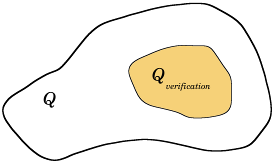
Goal

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

Weakly Verifiable	+	Dynamic	+	Interactive

Hint queries

- The solver asks hint queries.
- Hint queries can prevent verification queries from succeeding.
- Use hash function to partition query domain [**?**].
- Can ask hints only on $\mathcal{Q} \setminus \mathcal{Q}_{verification}$.
- Substantial success probability for partitioned domain

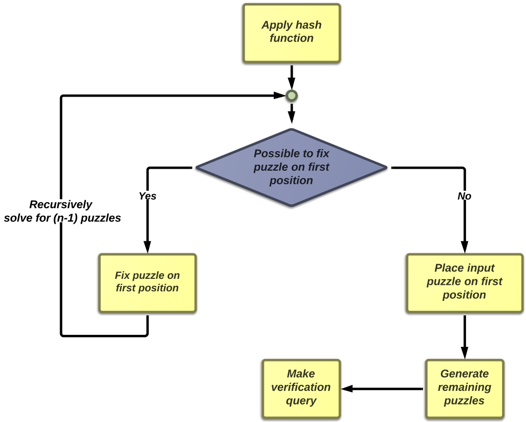


$$hash \leftarrow \mathcal{H}$$

$$hash : \mathcal{Q} \rightarrow \{0, 1, \ldots, 2(h + v) - 1\}$$

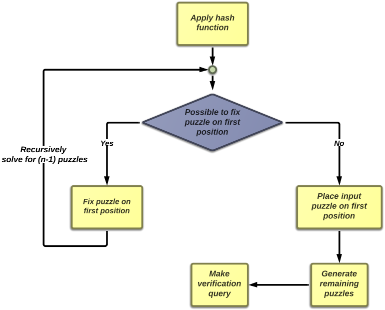
$$\mathcal{Q}_{verification} := q \in \mathcal{Q} : hash(q) = 0$$

Approach overview



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.



?	1	1	$\cdots\cdots$	1

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

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

Discussion

- Not clear whether it is possible to improve the result

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

- Tried to improve it. ✗
- Tried to show it is optimal. ✗

Questions

Bibliography

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