Hardness Amplification for Weakly Verifiable Cryptographic Primitives

Grzegorz Mąkosa

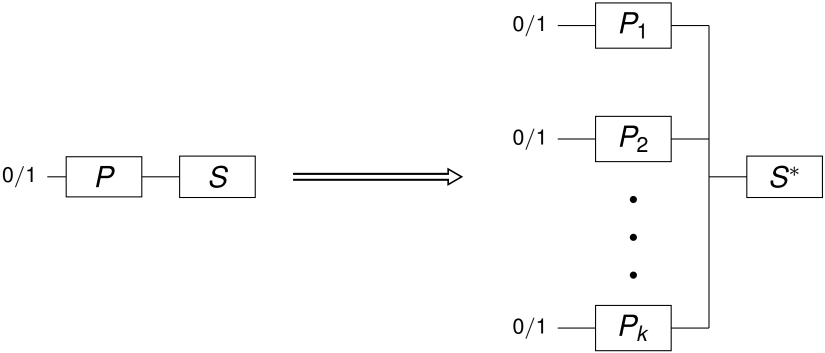
Advisors: Prof. Dr. Thomas Holenstein, Dr. Robin Künzler
Department of Computer Science, ETH Zürich

Notes:

Let's get started. Thank you for coming today. My name is Grzegorz Makosa. I am a master student. This morning I would like to present some of the results of my master Thesis that I have been writing under the supervision of Prof. Holenstein and Dr. Kunzler.

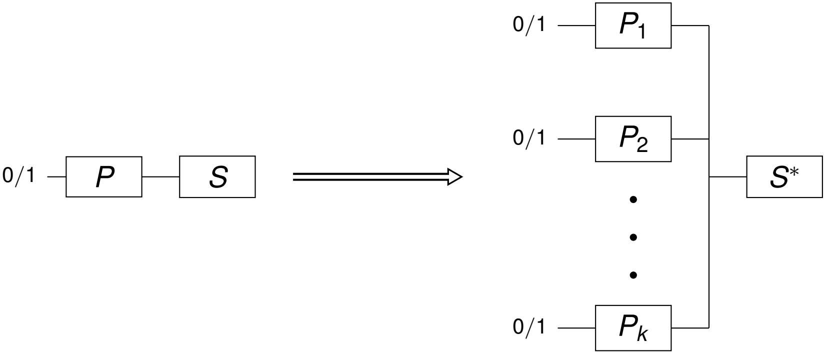
Hardness Amplification

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



Hardness Amplification

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



Agenda

- Motivation
- Background
  - Weakly Verifiable Puzzles
  - Threshold and Monotone Functions
  - Dynamic Puzzles
  - Interactive Puzzles
- Previous Works
- My Results
- Discussion and Questions

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

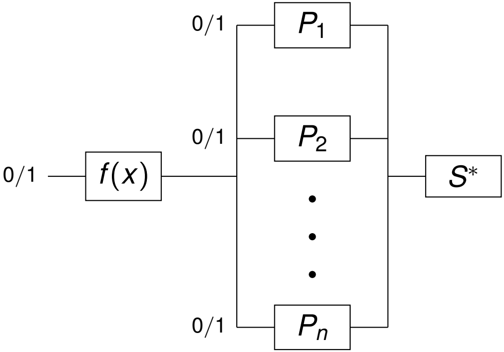
Threshold and Monotone Functions

Threshold function

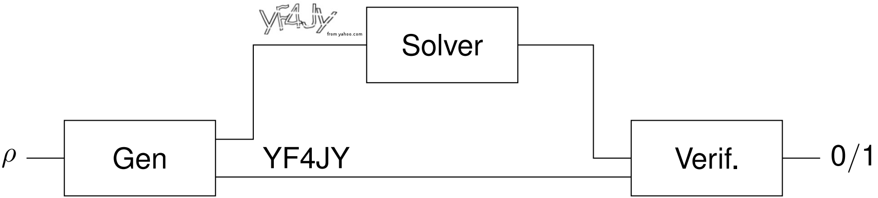
$$f_K(b_1, \ldots, b_n) = \begin{cases} 1 \text{ if } \sum_{i=1}^{n} b_i \geq K \\ 0 \text{ otherwise.} \end{cases}$$

Monotone function

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



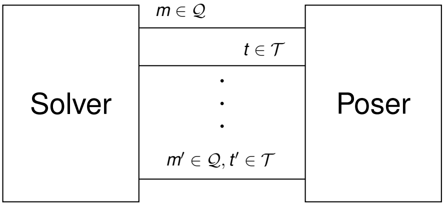
Weakly Verifiable Puzzles - CAPTCHA



- Small solutions space.
- Solver cannot efficiently verify correctness of solutions.

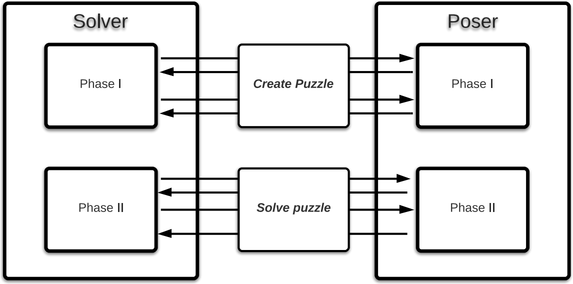
Dynamic Puzzles Example

- Game-based security definition of MAC.



- Set of messages $\mathcal{Q}$
- Hint - solution for $q \in \mathcal{Q}$
- Set of hint indices $\mathcal{H} \subseteq \mathcal{Q}$
- Verification query solution for $q \in \mathcal{Q} \setminus \mathcal{H}$.
- Number of hint and verification queries limited.

Interactive puzzle - commitment protocols



Hardness amplification results

- Weakly verifiable puzzles e.g. CAPTCHA, [CHS05]
- Dynamic weakly verifiable puzzles + threshold functions e.g. MAC,[DIJK09]
- Interactive weakly verifiable puzzles + monotone function e.g. commitment protocols, [HS11]

Goal

- Define puzzle that generalize MAC, CAPTCHA, bit commitments.
- Amplify hardness by parallel repetition.

Monotone functions	+	Dynamic weakly verifiable puzzles	+	Interactive weakly verifi-able puzzles

Reduction

- A - solving a single puzzle is hard
- B - solving parallel repetition is hard

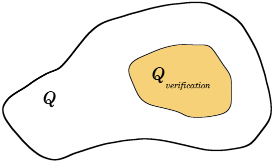
$$A \implies B$$

$$\neg B \implies \neg A$$

- Given a good solver C for parallel repetition
- Reduce C to a solver for single puzzle

Problem: conflicting hint queries

- The solver C can be run multiple times.
- Hint queries prevent verification queries from succeeding.
- Use hash function to partition query domain [DIJK09].
- Can ask hints only on $\mathcal{Q} \setminus \mathcal{Q}_{verification}$.
- Substantial success probability for partitioned domain.

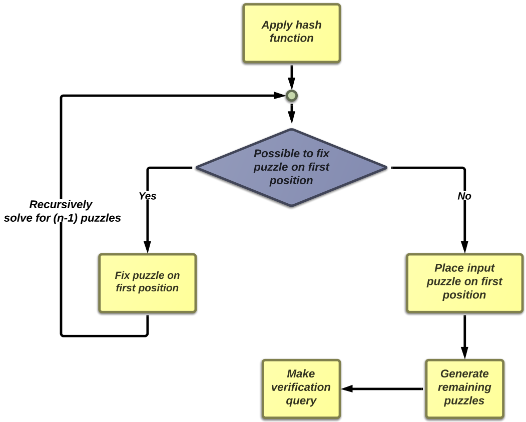


$$hash \leftarrow \mathcal{H}$$

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

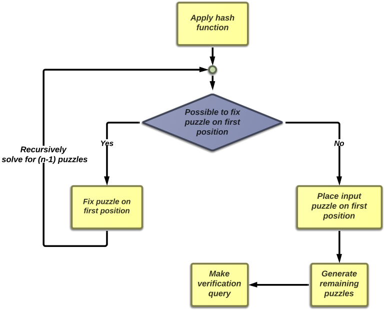
$$\mathcal{Q}_{verification} := q \in \mathcal{Q} : hash(q) = 0$$

Approach overview



Problem: verifying the solution

- Cannot verify correctness of a solution for input puzzle.
- Possible for generated puzzles.



$$\underbrace{\boxed{?}\ \overbrace{\boxed{1}\boxed{1}\ \cdots\cdots\ \boxed{1}}^{<\ \delta^{k-1}}}_{\geq\ \delta^{k}}$$

Result

Given a solver for parallel repetition of puzzles that satisfies

$$\geq \delta^k + \varepsilon \qquad (\geq \Pr[g(u_1, \ldots, u_k) = 1] + \varepsilon),$$

where $\Pr[u_i = 1] = \delta$.

We devise a solver for a single puzzle that satisfies (almost surely)

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

Discussion

- Not clear whether it is possible to improve the result

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

- Improve it? ✗
- Is it 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.

Yevgeniy Dodis, Russell Impagliazzo, Ragesh Jaiswal, and Valentine Kabanets.
Security amplification for interactive cryptographic primitives.
In *Theory of cryptography*, pages 128–145. Springer, 2009.

Thomas Holenstein and Grant Schoenebeck.
General hardness amplification of predicates and puzzles.
In *Theory of Cryptography*, pages 19–36. Springer, 2011.

Notes:

1. What is weak one-way function: there exists a polynomial that lower bounds the failure probability of every polynomial time algorithm. Goldreich p.35.
2. What is strong one-way function?
3. Why it may not be optimal?
4. What did you try to show that it is possible to improve your results?
5. Is it computational or information theoretic result?
6. What kind of security-games for MAC are modeled by DWVP?
7. Why sequential repetition implies security amplification?
8. What if the number of puzzles in the sequential repetition is very big i.e. our result holds only with high probability?
9. Does repeating the whole algorithm may help and increase the success probability?
10. What is the cryptographic primitive?
11. What is the cryptographic scheme?
12. Is there a simple proof for sequential repetition?
13. Why is it not possible to fix all coordinates? Give examples in n-dim space.
14. Try to justify why we have this form of the theorem, what does it mean? and what w

Notes:

1. Where does the proof break when you want to apply it to the large surplus
2. When does the proof breaks? – exactly and why we do not have to care about it too much
3. What it the intuition behind the surplus?
4. Be manage to explain the function on the right hand-side.
5. Why do we need to consider two surpluses
6. How does the optimization problem for gap amplification looks like?
7. Why we cannot perfect hardness amplification?
8. Why $\Pr[c \in \mathcal{G}_1 \setminus \mathcal{G}_0]$ is small but we still have a large surplus
9. Why can we assume that the verification algorithm can be deterministic
10. Followup question: what is proven in DIJK09
11. Followup question: why is the hint circuit H probabilistic
12. Is defining the puzzle only by poser is not artificial as an instance is defined by a pair poser-solver
13. There are no examples of puzzles that are both interactive and dynamic what about this?
14. Number of rounds for which parallel repetition works as i.e. the intuition behind the > 3-round protocols

Notes:

1. Why does obsevation 5.1 is true?
2. What is function what is relation
3. Why WVP does not imply one-way function
4. Is it possible that sampling does not work?
5. Is number of hint and verification queries limitation for the solver or the verify
6. Why do we iterate $\frac{1}{\varepsilon}$ times in Gen, is it efficient, when it might not be efficient what happens with $h + v$ then?
7. Think about different computational contexts for this theorem. Under what conditions for h, v, ε does it make sense
8. Be able to explain the definition in DIJK09.
9. What is the Coron's proof about? Why it does not work?
10. k-wise independent functions; how do they look like?
11. Random questions about hash functions
12. (if not covered in the presentation) is your result optimal?
13. Relation with soundness error of four-round protocols