Data-Independent Memory Hard Functions: New Attacks and Stronger Constructions

Jeremiah Blocki[1], Ben Harsha[1], Siteng Kang[2], Seunghoon Lee[1]
Lu Xing[1], and Samson Zhou[3]
1. Purdue 2. Penn State 3. Indiana University

https://eprint.iacr.org/2018/944 (CRYPTO 2019)
https://github.com/antiparallel-drsbrg-argon/Antiparallel-DRS-BRG

Goal: Protect low entropy secrets against brute force attacks

Memory Hard Functions: Password Hashing

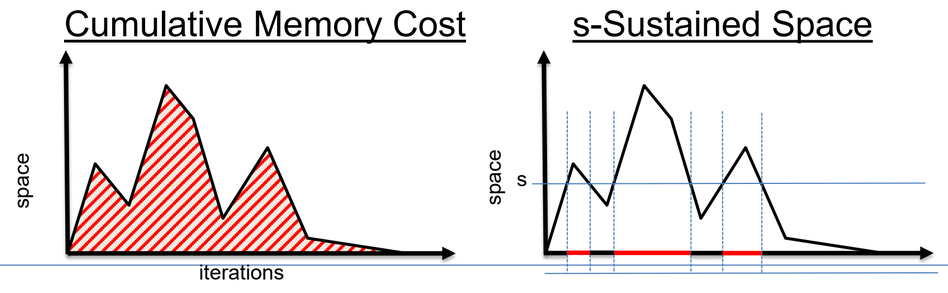
- Evaluating requires lots of memory for duration of computation
- Brute-Force Attacks: Expensive on ASICs

Data-Independent Memory Hard Functions (iMHFs): side-channel resistant

Design a provably memory-hard iMHF?

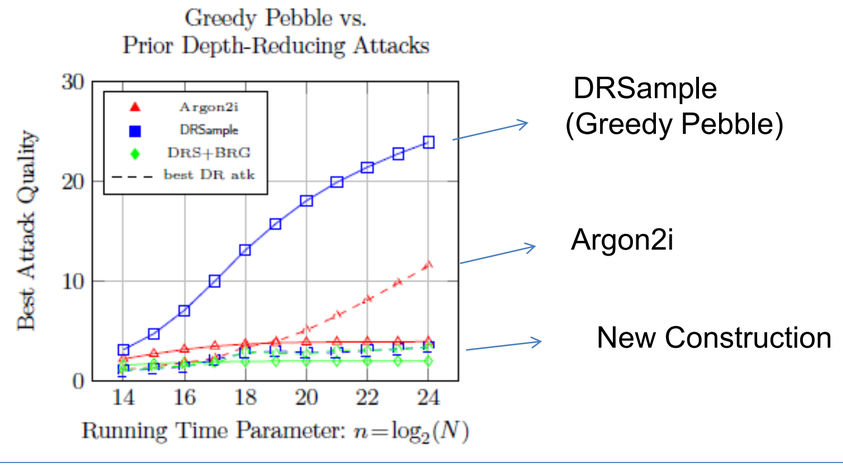
PHC Winner Argon2i: vulnerable to depth-reducing attacks [AB16,AB17,BZ17]

DRSample [ABH17]: Asymptotically optimal CMC (Constants? Sustained Space?)

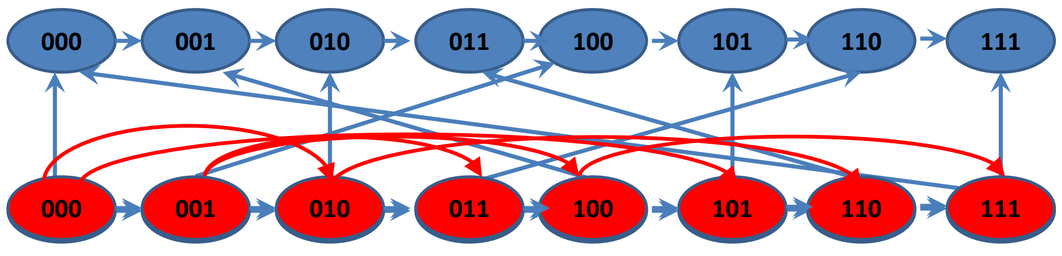


- New Pebbling Reduction: Memory Hardness of Practical iMHFs captured by graph pebbling.
- State of the art construction of hard to pebble graph (DRSample+BRG)
  - First practical construction with high sustained space complexity
- New Techniques for Constructing Small Depth-Reducing Sets
  - Cryptanalysis of iMHFs/Proofs of Space
- Inherently Sequential Round Function

Sequential attack on DRSample



State of the Art iMHF (DRSample+BRG)



New Construction: DRSample + Bit Reversal Graph
(First layer of BRG replaced with depth-robust DAG)

Theorem: Any sequential pebbling of DRS+BRG either has Cumulative Cost $\Omega(N^2)$

Theorem: Any parallel pebbling of DRS+BRG either has

1. Cumulative Cost $\omega(N^2)$, or
2. At least $s = \Omega(N/\log N)$ pebbles for $t = \Omega(N)$ rounds

Theorem: Under plausible conjectures (see paper) any parallel pebbling of DRS+BRG has cumulative cost $\Omega(N^2 \log\log N / \log N)$

PhD Students

- Ben Harsha
- Seunghoon Lee

Undergraduate Involvement:

- Michael Cinkoske
- Siteng Kang

Course Integration: Passwords and Human Authentication

Broader Impacts

- Stronger tools to protect low-entropy secrets
- Informs future Password Hashing Standards
- Tools to analyze Proofs of Space and Replication (Ecofriendly Replacement for POW)

NSF Award ID#: **1755708**