CERIAS

The Center for Education and Research in Information Assurance and Security

Sustained Space and Cumulative Complexity Trade-offs for Data-Dependent Memory-Hard Functions

Jeremiah Blocki and Blake Holman
Department of Computer Science, Purdue University

Motivation

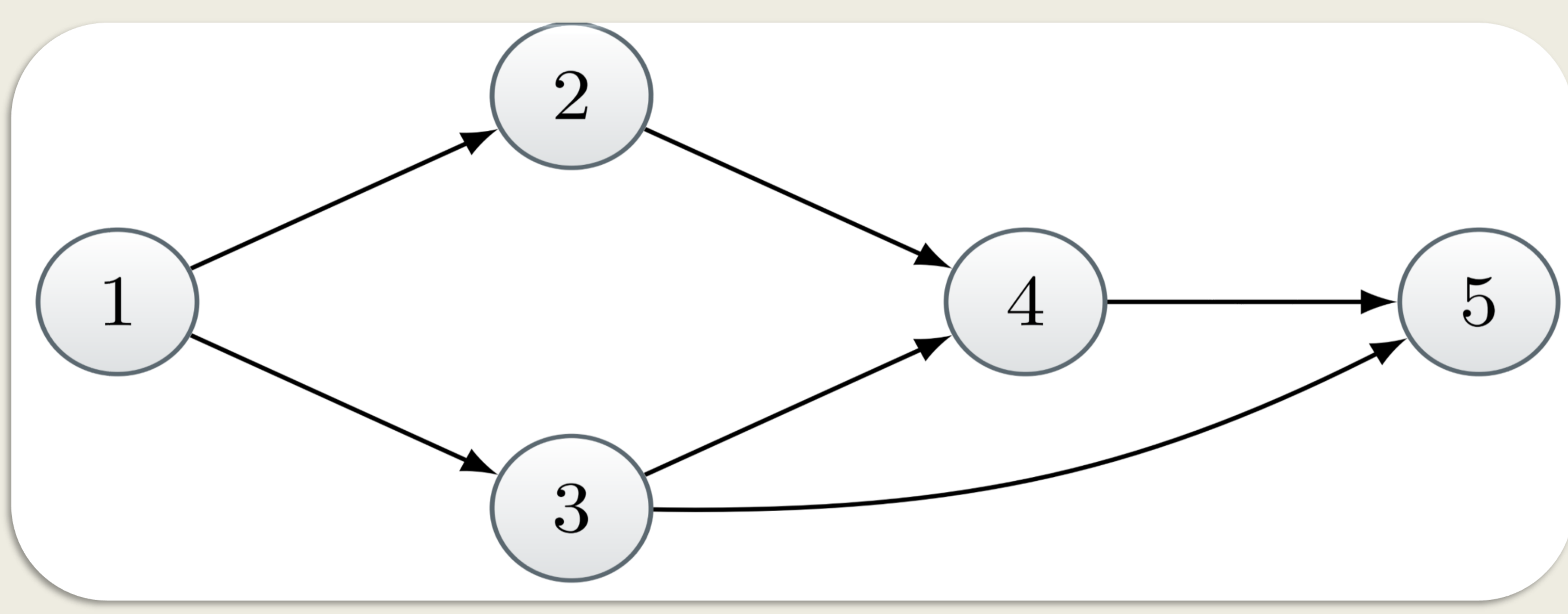
- Billions of user accounts have been affected by password breaches
  - An attacker who obtains hashes of user passwords launches a brute force attack to guess the users' passwords
  - The attacker must evaluate the hash function millions or billions of times
  - Specialized hardware allows attackers to evaluate these functions orders of magnitude faster than standard hardware, but memory cost is relatively uniform across different types of hardware.
- Memory Hard Functions (MHFs) are functions that have high memory cost
- Leaked passwords hashed with MHFs are robust against offline brute-force attacks
- Measures of memory hardness:
  - **Cumulative Complexity (CC):** *The sum (over all steps in the computation) of the memory required to compute the MHF*
  - ***s*-Sustained Space Complexity (*s*-SSC):** *The number of steps required to sustain s bits of memory to computer the MHF.*
- Data-dependent MHFs (dMHFs) are a broad class of MHFs which trade side-channel resistance for easy constructions and asymptotically stronger CC
- **In general, MHFs have weak SSC Guarantees; Can dMHFs perform better?**

Contribution

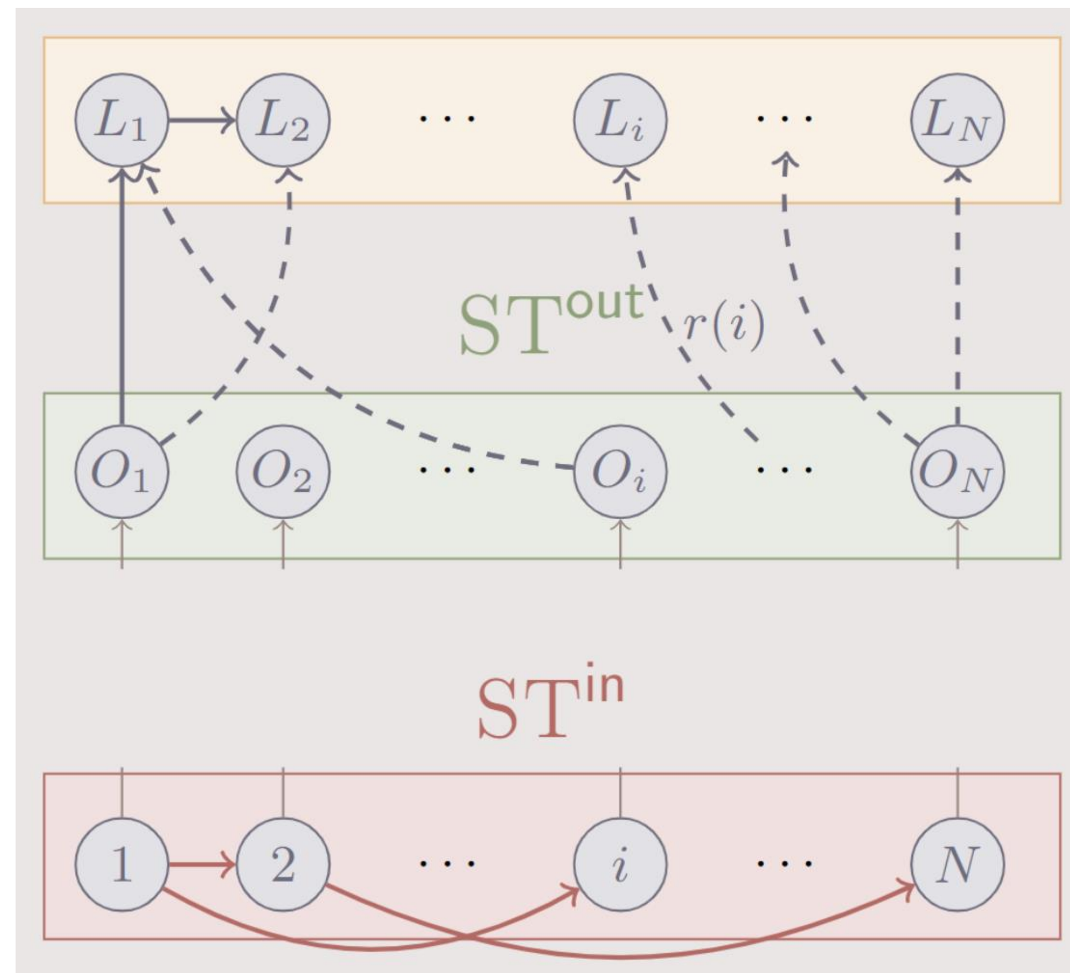
- **dMHFs have much stronger SSC guarantees.**
- We analyze four dMHFs of varying practicality:
  - **Dynamic EGS:** asymptotically maximal SSC, but very impractical
  - **Dynamic DRSample:** practical MHF candidate with almost maximal SSC
  - **Argon2id:** already deployed and widely used, but much weaker SSC than the others
  - **Our Construction**: a theoretical construction with maximal tradeoff with constant indegree

Methods

- Instead analyze pebbling games on graphs
- Each round, pebbles can be placed on any (and all) nodes whose parents are all pebbled
- *Goal: place a pebble on the sink*



- Pebbling: $P_1 = \{1\}, P_2 = \{2,3\}, P_3 = \{3,4\}$, and $P_4 = \{5\}$
- $cc(P) = 1 + 2 + 2 + 1 = 6$
- $2\text{-}ssc(P) = 0 + 1 + 1 + 0 = 2$



Our Construction

- **Dynamic pebbling graphs:** a node v can have a random edge from some prior node $r(v)$ which is only visible to the pebbler once v's predecessor is pebbled
- **ST-Robust graphs:** N inputs/outputs with high connectivity between them
- **Our construction:** $\mathbb{G}_D^N$ (pictured above)
  - ST robust graph with N inputs and N outputs
  - Pebbling graph D overlayed onto the inputs
  - Line graph at the end with random edges to outputs
- **Intuition:** high connectivity between inputs and outputs
  - If a pebbling strategy uses relatively few pebbles, then (with high probability) they need to repebble many inputs
  - The inputs have high CC, so the strategy incurs high cost

Results

- Results of the following form:
  - A pebbling strategy either sustains s pebbles for $\Omega(N)$ steps, or has CC at least C
  - Every graph has CC at most $N^2/2$, so the goal is to require CC $\omega(N^2)$ while keeping s as large as possible
- Graphs with higher than constant indegree lead to MHFs that are Impractical for common applications

Dynamic Graph	Indegree	Sustained Space	Cumulative Cost
Dynamic EGS	$O(\log N)$	$\Omega(N)$	$\Omega(N^3)$
Dynamic DRSample	2	$\Omega\left(N/\log N\right)$	$\Omega\left(N^3/\log N\right)$
Argon2id	2	$\Omega(N^{1-\epsilon})$	$\Omega(N^{2+2\epsilon})$
Our Construction	2	$\Omega(N)$	$\Omega(N^{3-\epsilon})$

- **Open Question:** can we use these pebbling arguments on dynamic graphs directly prove similar SSC/CC trade-offs for their corresponding dMHFs?

References

1. J. Alwen, J. Blocki, and K. Pietrzak. "Sustained space complexity." EUROCRYPT 2018
2. J. Blocki and M. Cinkoske. "A New Connection Between Node and Edge Depth Robust Graphs." ITCS 2021
3. J. Blocki and S. Zhou. "On the depth-robustness and cumulative pebbling cost of Argon2i." TCC 2017
4. J. Blocki, B. Harsha, S. Kang, S. Lee, L. Xing, S. Zhou. "Data-independent memory hard functions: New attacks and stronger constructions." CRYPTO 2019
5. J. Blocki, B. Harsha, and S. Zhou. "On the economics of offline password cracking." SP 2018.

PURDUE UNIVERSITY Discovery Park

CERIAS