Bandwidth Hard Functions for ASIC Resistance

Ling Ren and Srinivas Devadas

TCC - Nov. 2017

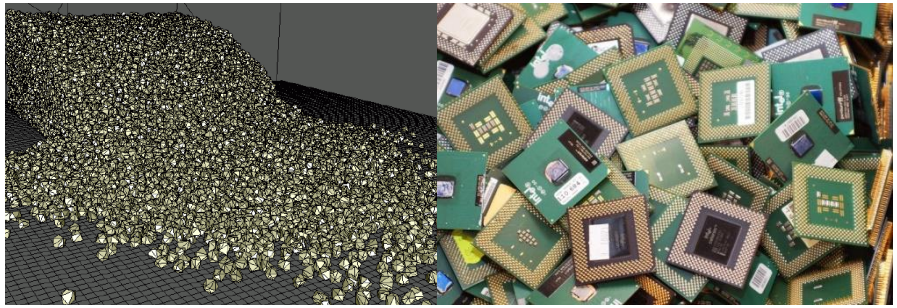
Memory-hard → ASIC resistant?

[Percival'09 (scrypt)]
[Password hashing competition: Argon2, Catena, Lyra2, yescrypt]
[Corrigan-Gibbs et al.'16 (Balloon)],
[Alwen et al. stoc'15, crypto'16, eurocrypt'17, ccs'17]

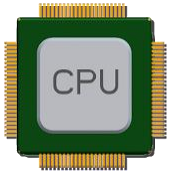
Bandwidth-hard:
definitions and constructions

What is the ASIC Advantage?

Advertised Capacity:
4.73 Th/s

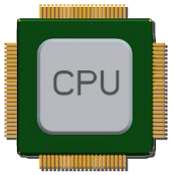


>200,000x faster than



$$ \$\text{ per eval}() : \frac{\text{capital}}{\#\text{ of lifetime eval}()} + \text{electricity} $$

What is the ASIC Advantage?



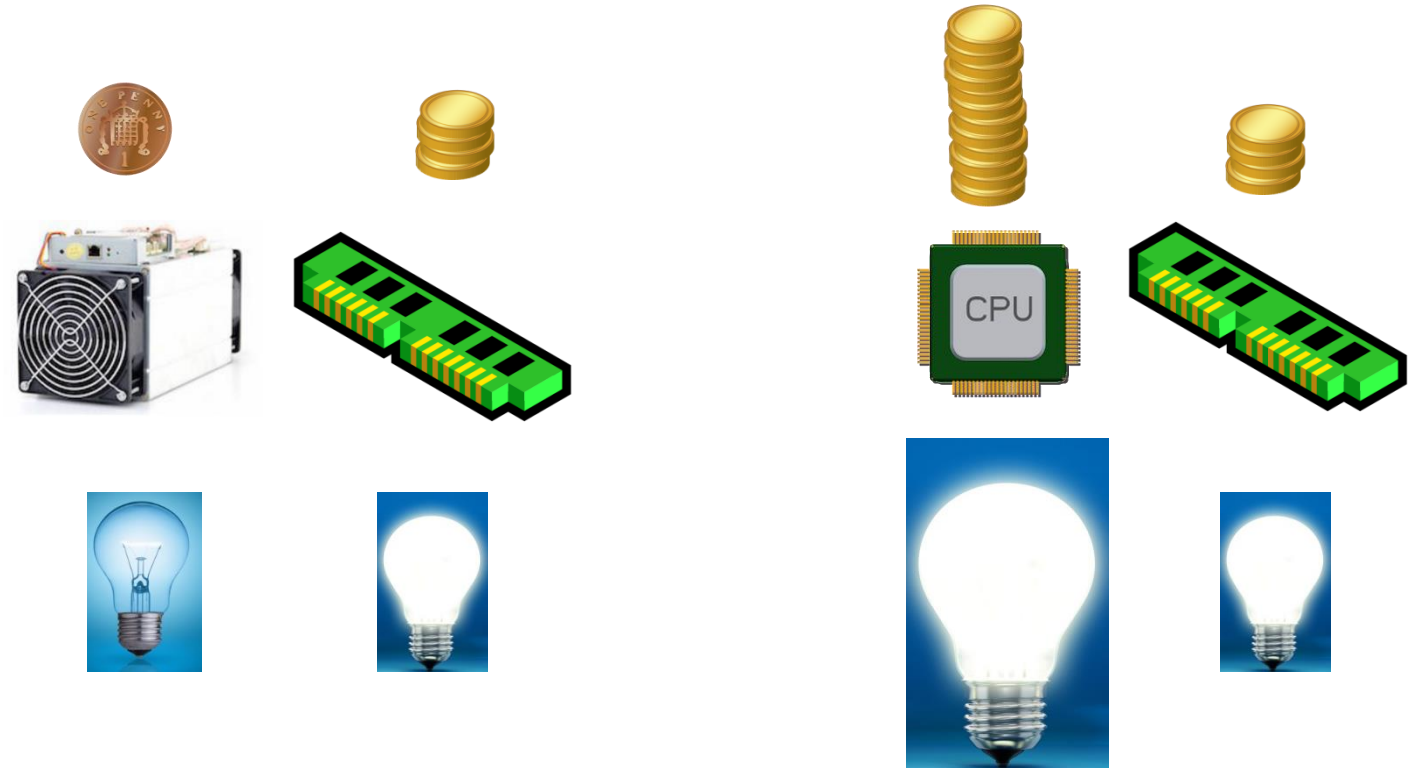
$$ per eval(): amortized capital + electricity

Reducing ASIC Advantage

Memory-hard functions [Percival'09 (scrypt)]:

"A natural way to reduce the advantage provided by an attacker's ability to construct highly parallel circuits is to **increase the size of the circuit.**"

Reducing ASIC Advantage



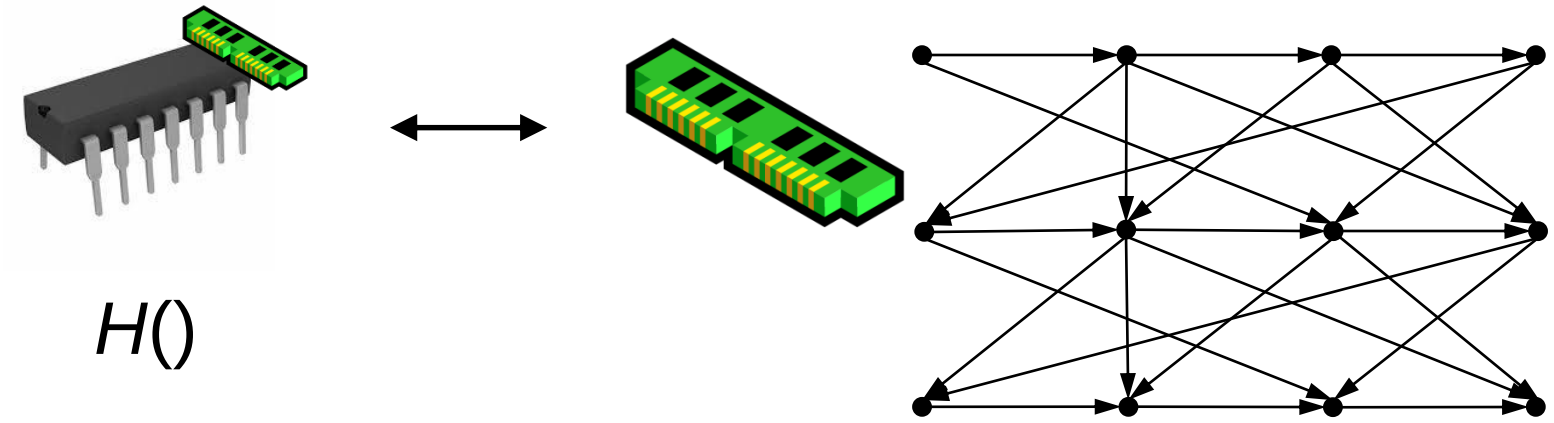
(memory-hard) (bandwidth-hard)

$$ per eval(): amortized capital + electricity

How to Define Bandwidth Hardness?

Model

- Graph labeling, compute *H* in a DAG
- Give the adversary a cache



H()

A Natural Definition

[Abadi et al.'05]
[Dwork et al.'03]

- f() is memory-bound if:
  - Computable with *B* memory accesses
  - Not computable with < *cB* memory accesses

    even using a cache of size *M*

- Hard to construct; rules out all *ST* tradeoff

Bandwidth-hard functions

- Will charge for computation as well
- An honest user transfers *B* bits, computes on *R* bits, and incurs electricity (energy) cost

$$\frac{C_b * B + C_r * R}{C_b' * B' + C_r' * R'}$$

- Similarly for the adversary

Bandwidth-hard functions

- f() is bandwidth-hard iff:

$$\frac{C_b * B + C_r * R}{C_b' * B' + C_r' * R'} = O(1)$$

  - C_b : cost of transferring 1 bit
  - C_r : cost of computing H on 1 bit
  - B and R: # bits transferred vs. computed on
  - Apostrophe: for the adversary

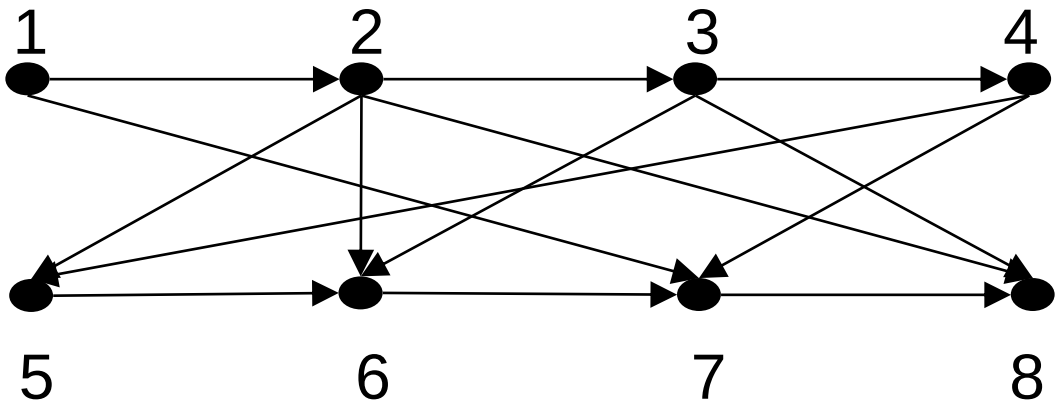
1pJ$\approx C_r' \ll C_r$ $\quad C_r' = o(C_r)$

1nJ$\approx C_b' \approx C_b \approx C_r$ $\quad \theta(C_r) = \theta(C_b') = \theta(C_b)$

Are existing constructions bandwidth-hard?

Red-Blue Pebble Game

- red = in cache, blue = in memory
- Can place a red if all predecessors have red *(R)*
- Can change red ←→ blue *(B)*

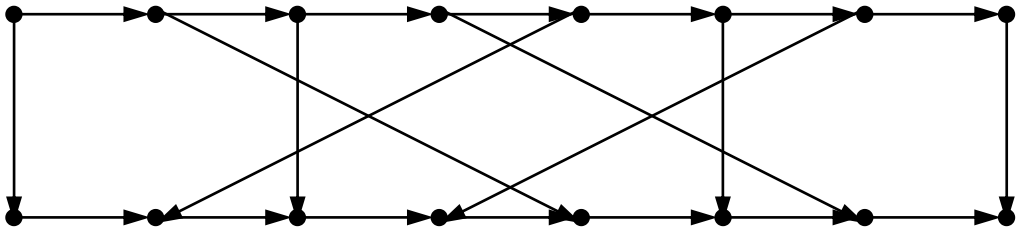


Open: equivalence to **the RO with cache model?**

Data-independent Schemes

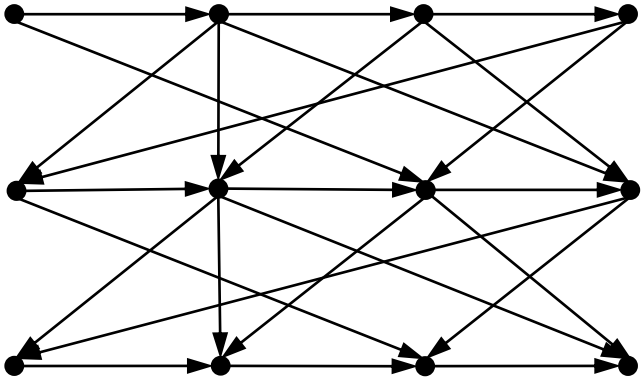
- Under the red-blue pebble game model,

  [Catena-BRG]

  and

  [Balloon]

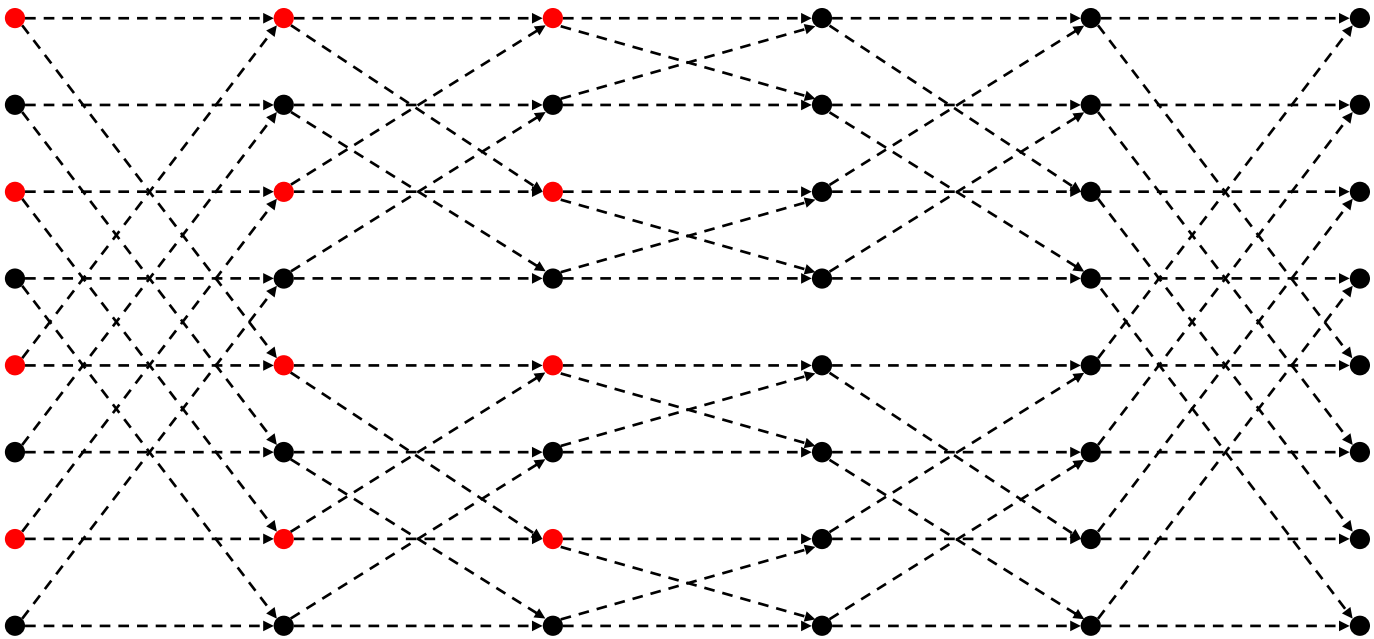
  

  are bandwidth-hard.

  They are also sequentially memory-hard

Data-independent Schemes

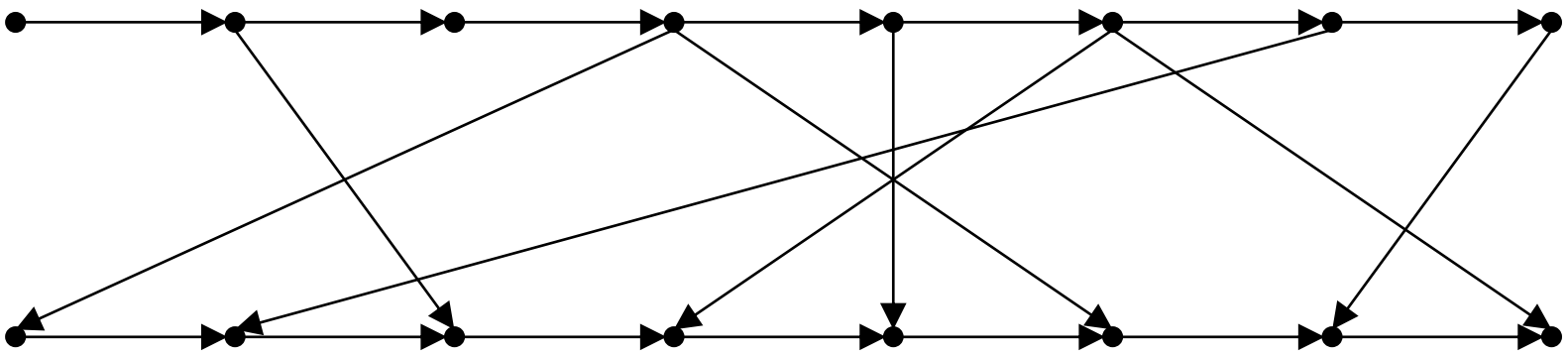
- A sequentially memory-hard function is not necessarily bandwidth hard



Data-dependent Scheme: Scrypt

- Memory-hard under parallelism [Alwen et al.'17]

- Bandwidth-hard only if $N > M \frac{C_b'}{C_r'}$



A2 Terminator 110MH/s Scrypt ASIC Miner WITH Power Supply

459 recent views

Priced at $1,279.99 DISCOUNTS

Quantity: 1

Add to cart

Sold by Deep_In_the_Mines

125 Bonanza transactions
100% positive rating

Summary

- Two aspects of ASIC resistance
  - Capital cost ← memory-hard
  - Electricity cost ← bandwidth-hard
- Most but not all MHFs are bandwidth-hard
- Bandwidth-hardness kicks in only under certain parameters

Thank you!