RSAConference2021
May 17 – 20 | Virtual Experience

SESSION ID: CRYP-R05C

On The Cost of ASIC Hardware Crackers: A SHA-1 Case Study

Mustafa Khairallah

Research Scientist
Nanyang Technological University, Singapore
Twitter handle: @muskhairallah
Joint work with: Anupam Chattopadhyay, Gaëtan Leurent, Zakaria Najm, Thomas Peyrin, Vesselin Velichkov

Research Questions

- Can the financial cost of the collision attacks against SHA-1 be reduced?
- What is the difference between generic attacks and cryptanalytic attacks in terms of cost and implementation?
- What actual security an 80-bit collision-resistant hash function provides in practice?

History

- SHA-1 was selected as a replacement to SHA-0 in 1995.
- It was broken in 2005 by Wang et al.
- It was practically broken in 2017 by Stevens et al. using a GPU cluster. This was done using what is known as identical-prefix collision.
- In 2019, another attack (chosen-prefix attack) was implemented by Leurent and Peyrin.

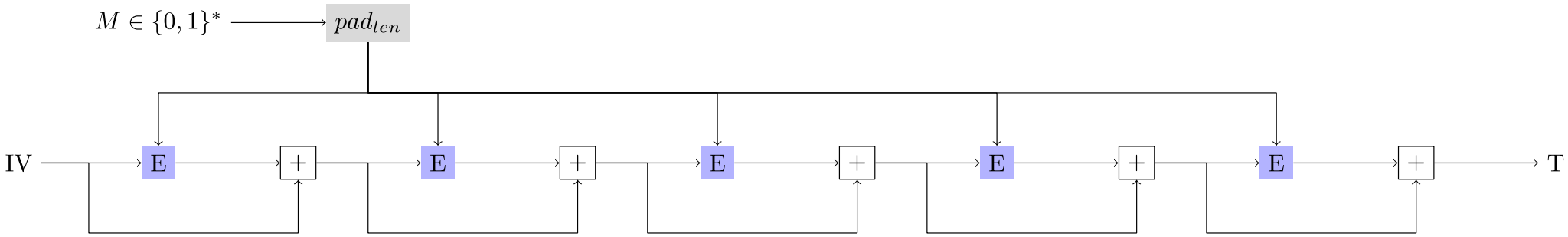
Hash Functions and Collision Resistance

$M' \in \{0,1\}^* \longrightarrow$ Hash Function $\longrightarrow T \in \{0,1\}^t$

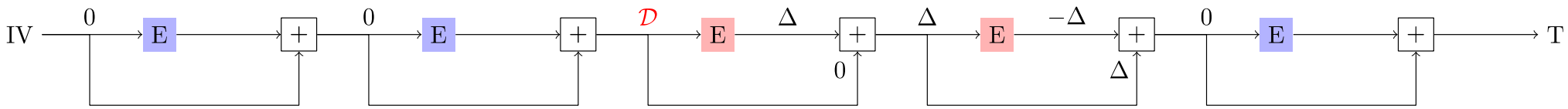
Collision Resistance

$M \in \{0,1\}^* \longrightarrow$ Hash Function $\longrightarrow T \in \{0,1\}^t$

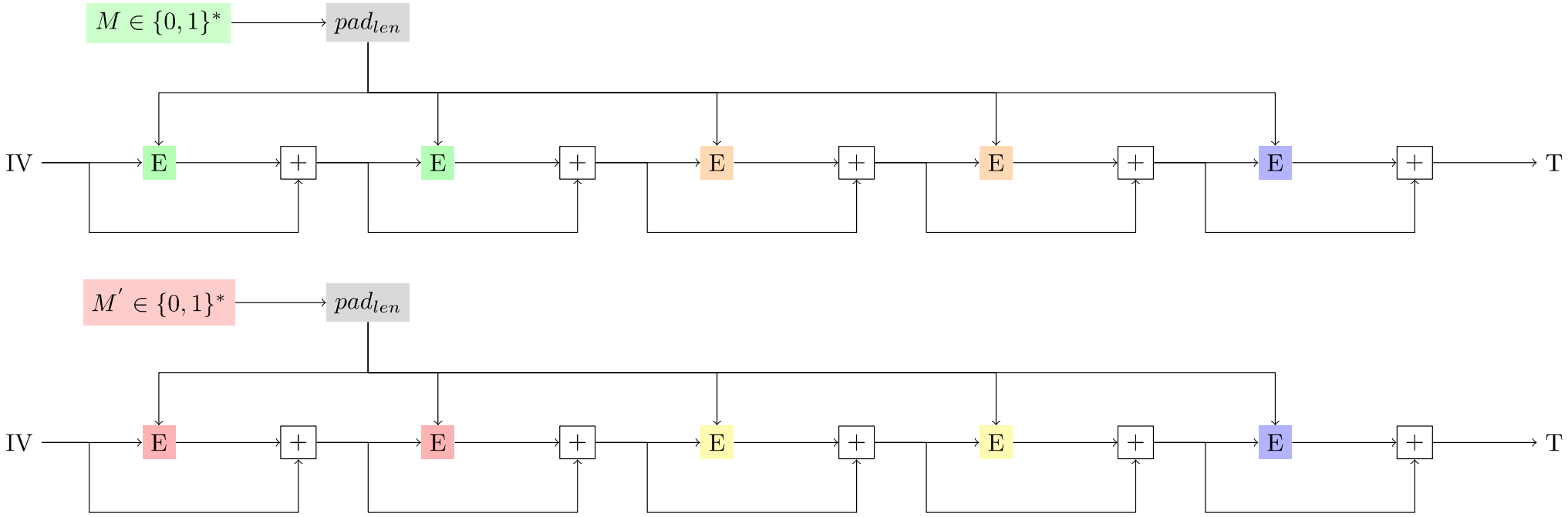
The Merkle-Damgard Construction



Differential Cryptanalysis

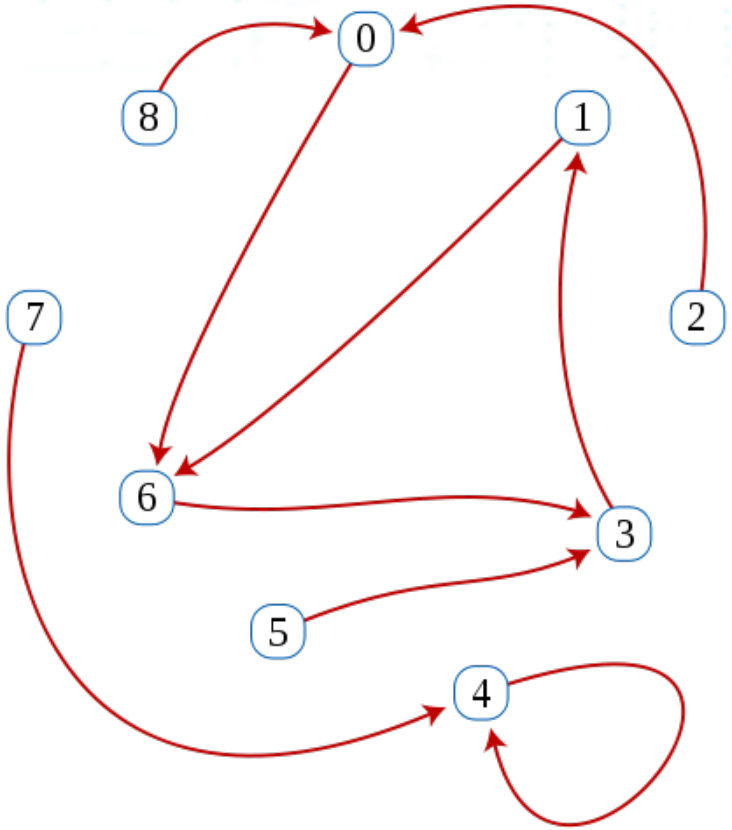


Chosen-Prefix Attack



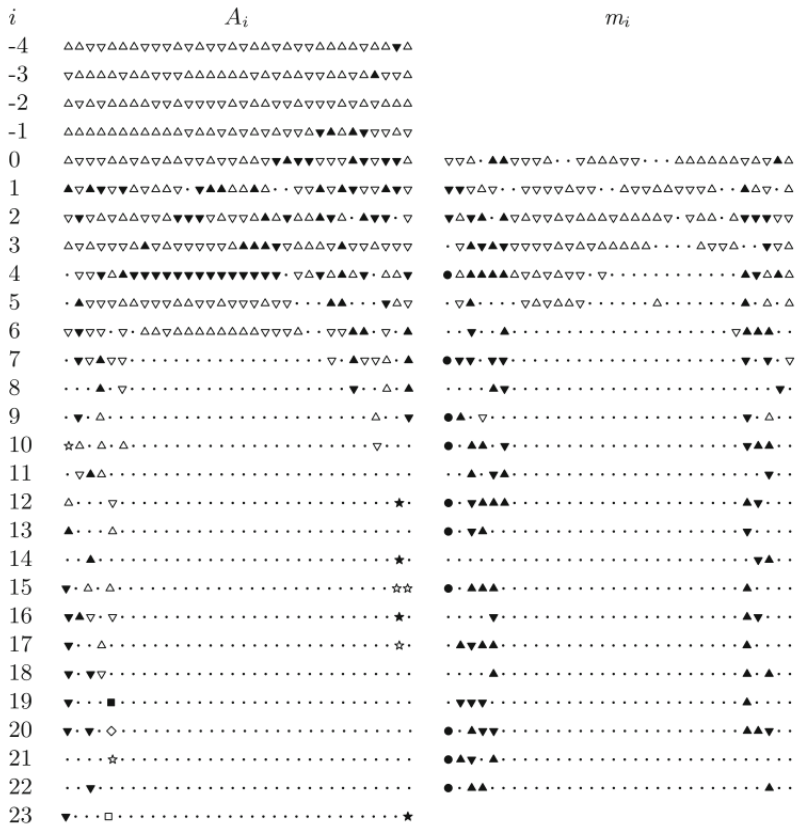
Collision Search in Functional Graphs

x	$f(x)$
0	6
1	6
2	0
3	1
4	4
5	3
6	3
7	4
8	0

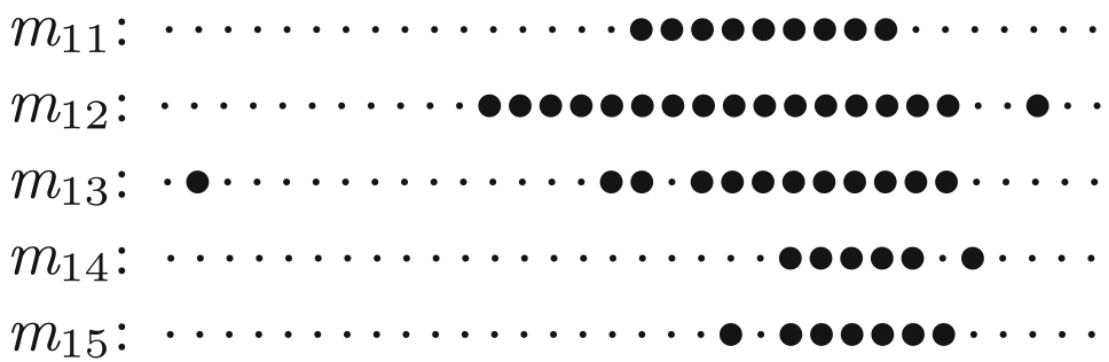


Differential Cryptanalysis of SHA-1

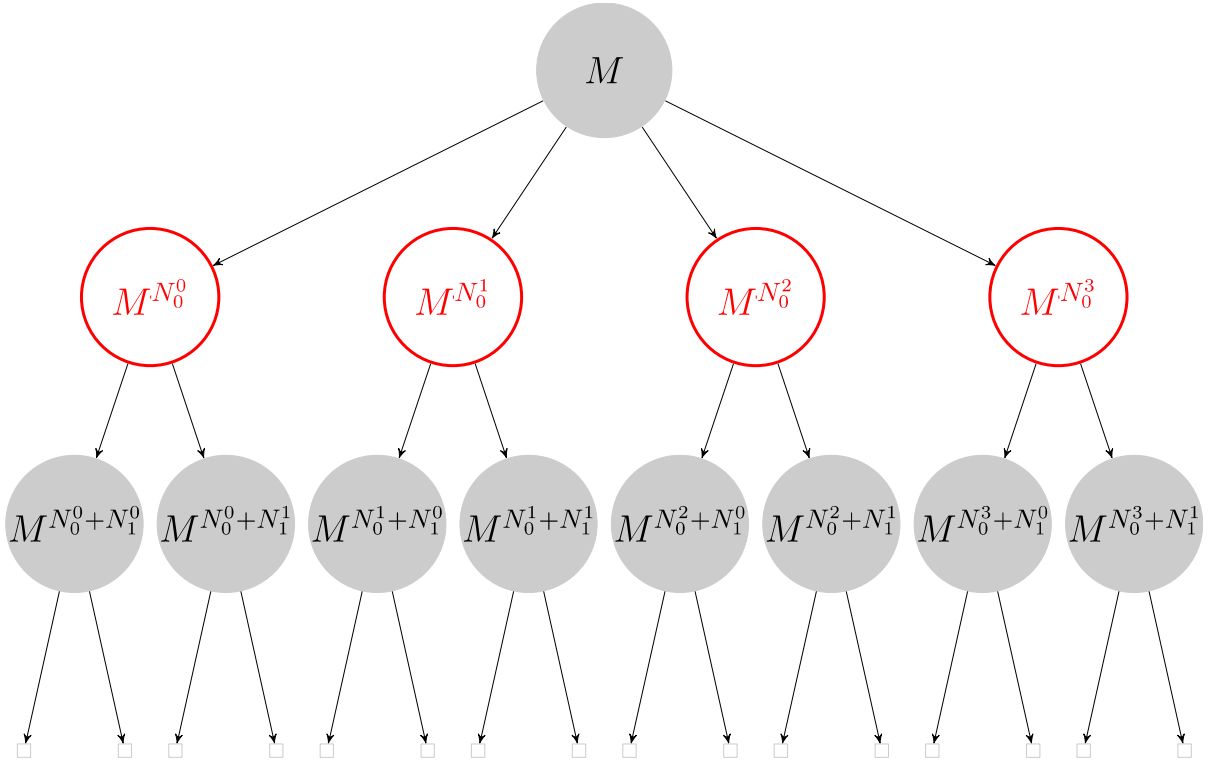
Differential Path



Neutral Bits



Solution Tree

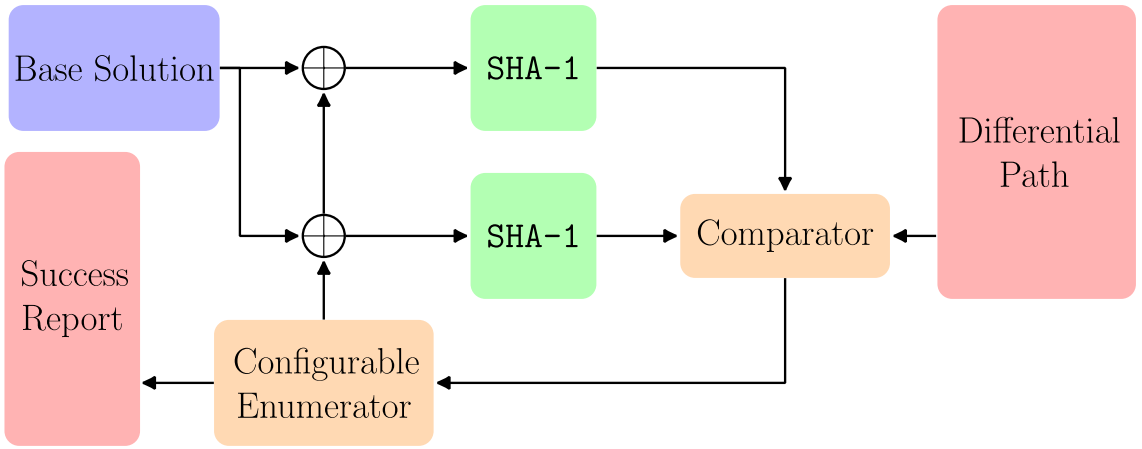


Goals

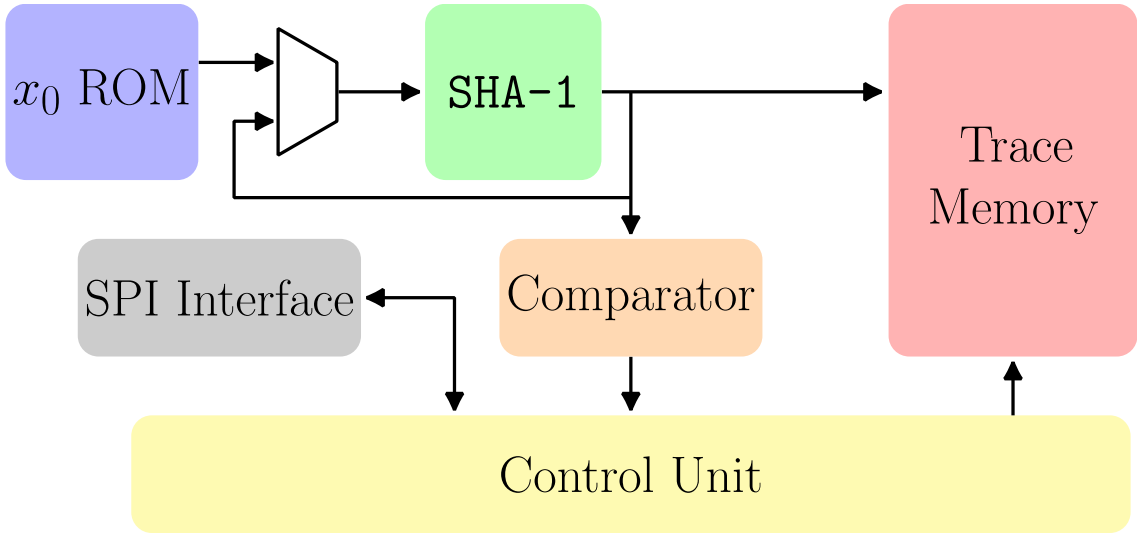
- Compare the cost of building a SHA-1 attack cluster using ASIC and GPU, for the following attacks:
  - 128-bit collision (i.e. attack on 64-bit collision resistance): generic attack.
  - 160-bit collision (i.e. attack on 80-bit collision resistance): generic attack.
  - Chosen-prefix attack: differential cryptanalysis.

SHA-1 Attack Cores

Neutral Bit Search

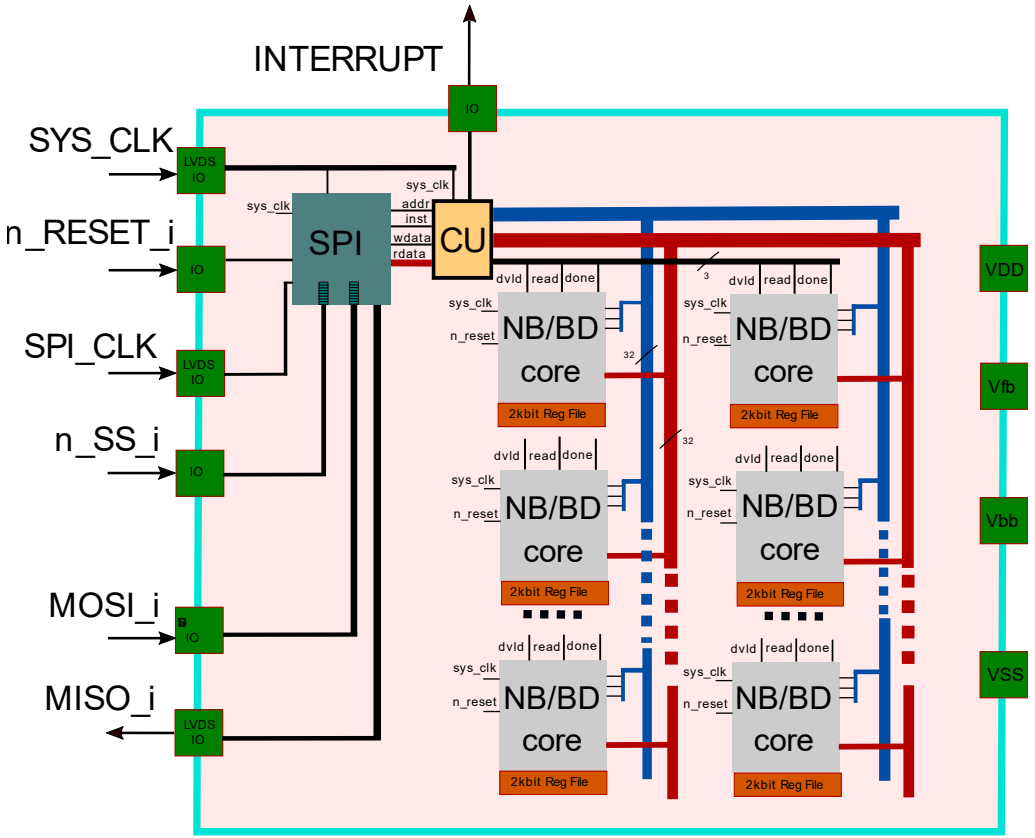


Birthday Attack

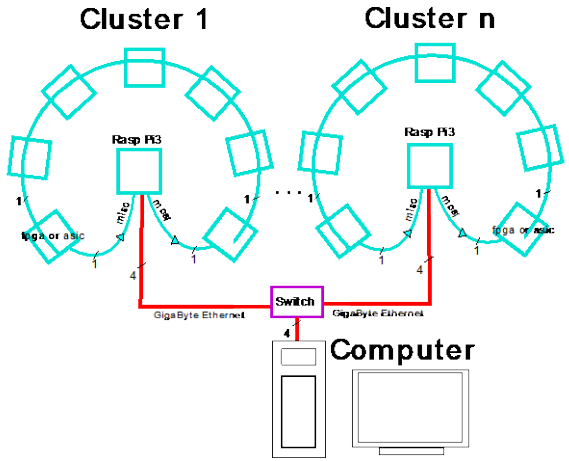


ASIC System Architecture

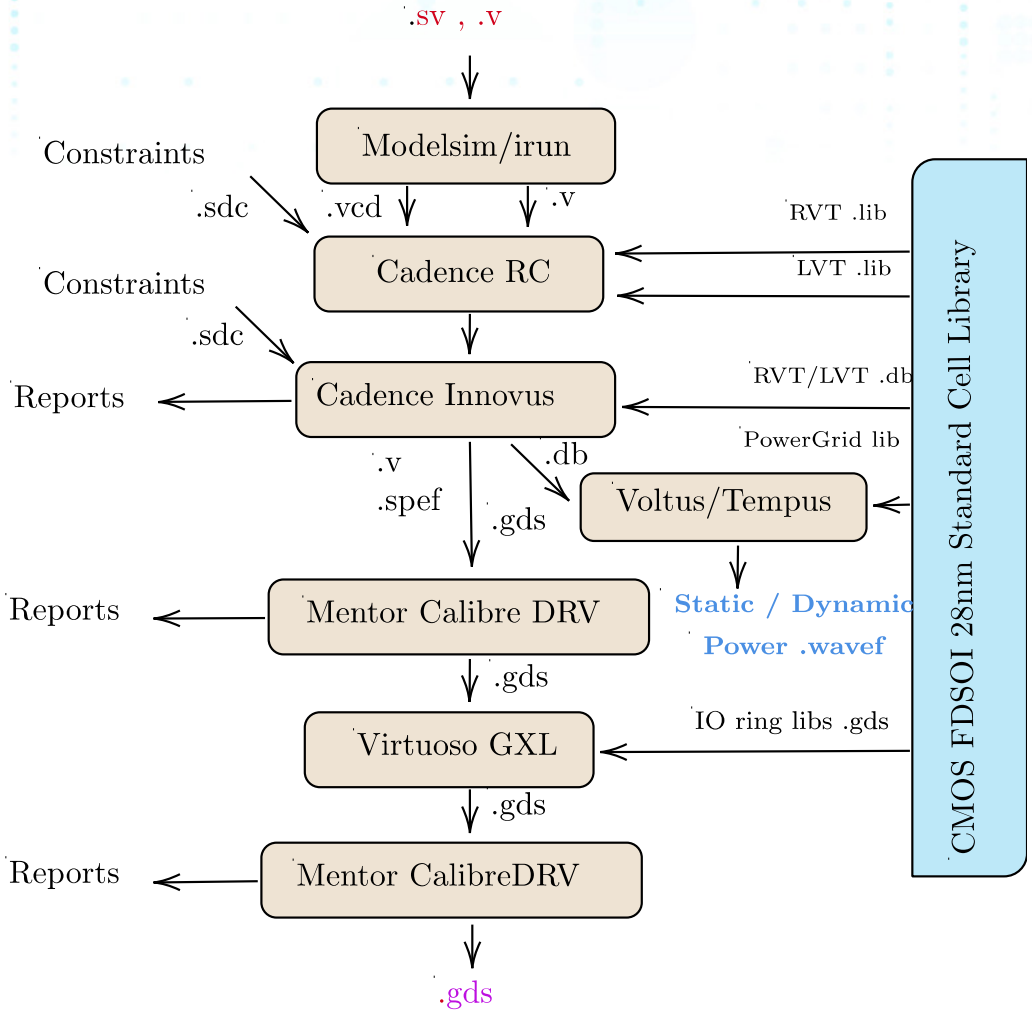
Chip



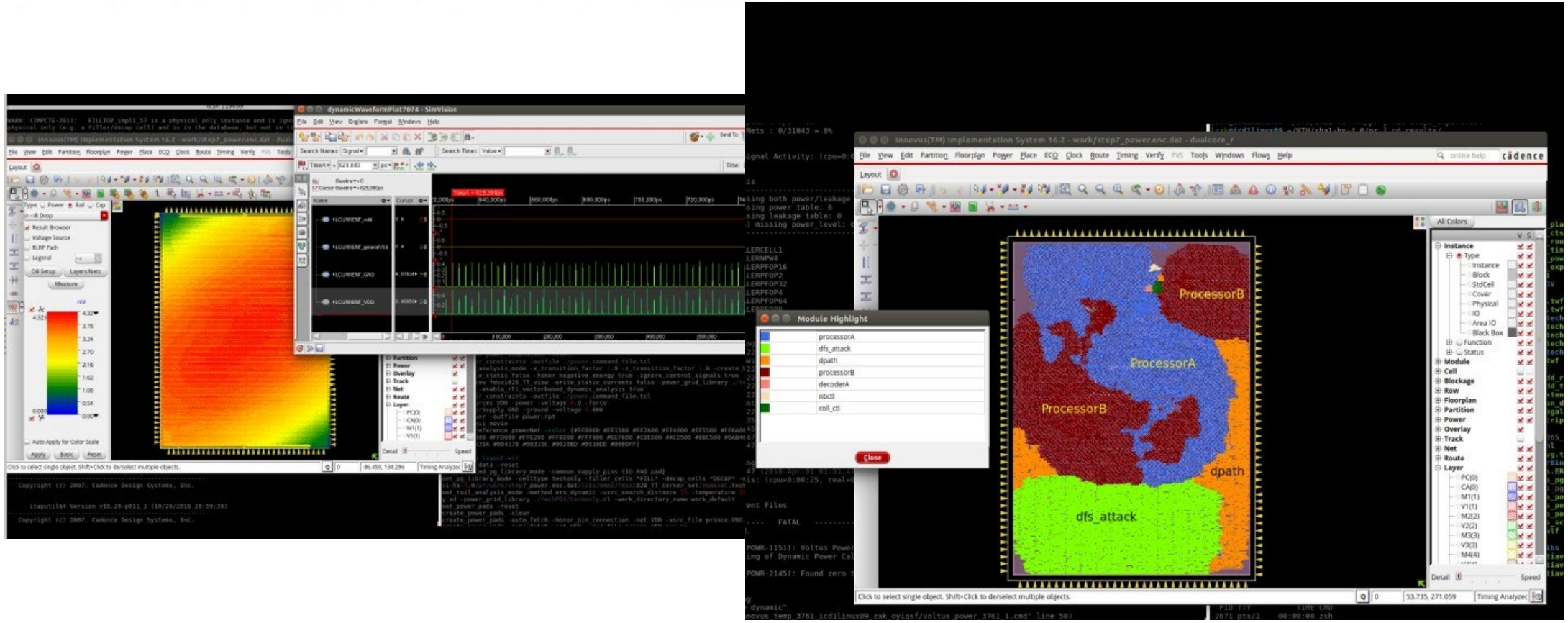
Network



Design and Simulation Flow



Simulations and implementation



Amortized cost of a collision attack: Running the cluster over 3 years

Attack	ASIC	Renting GPU	Buying GPU
128-bit collision	781-8k USD	43k USD	61k USD
Differential Collision	1.6k-32.1k USD	43k USD	26k USD
160-bit collision	51M USD	4B USD	2.5B USD

The attack runs in time between 1 month (most expensive) and 1 year (cheapest). For GPU the cost is almost constant regardless of the attack duration as the cost scales linearly. For ASIC, spending larger initial budget reduces the amortized cost.

Cost of building the machine

Attack	ASIC
128-bit collision on SHA-1 (Partial collision)	257-8.5k USD
Chosen-prefix attack	1.6k-32.1k USD
160-bit collision on SHA-1	11M-263B USD

Research Questions

- Can the financial cost of the collision attacks against SHA-1 be reduced?
  - Yes, but only for big players and big-budget organizations.
- What is the difference between generic attacks and cryptanalytic attacks in terms of cost and implementation?
  - While the differential attack and the 128-bit collision attack have roughly the same computational complexity, the 128-bit collision attack is significantly cheaper, due to its simplicity.
- What actual security an 80-bit collision-resistant hash function provides in practice?
  - A billion-dollar entity can, in the near future, break 80-bit collision resistance using a generic attack, in one month or less.

RSAConference2021

Thanks for watching

Mustafa Khairallah, mustafa.khairallah@ntu.edu.sg