An STT-MRAM Based Strong PUF

Soroush Khaleghi

Paolo Vinella

Soumya Banerjee

Wenjing Rao

Nanoarch 2016 – Beijing, China

ECE Department

University of Illinois at Chicago

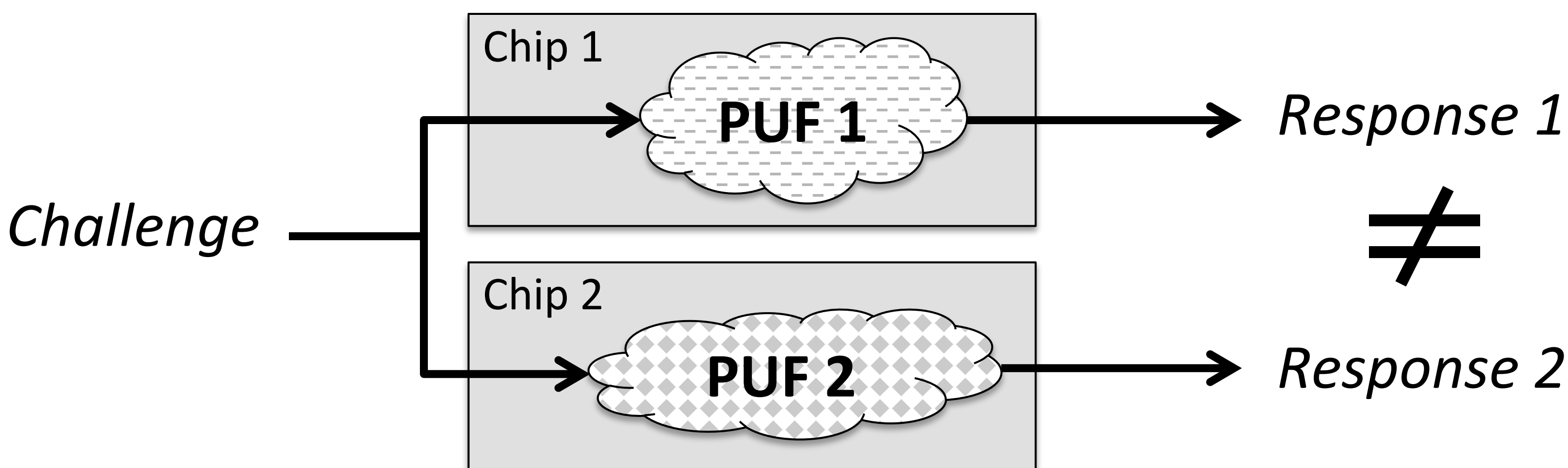
ELECTRICAL AND COMPUTER ENGINEERING
COLLEGE OF ENGINEERING

UIC

What is a PUF?

- No two chips are exactly the same
  - Due to manufacturing *process variations*

- **PUF:** Physically Unclonable Function
  - A device, based on physical disorders of chips



- **CRP:** Challenge-Response Pair

PUFs at a Glance

- Manufactured with the same layout
- A unique function per chip
  - *Challenge-Response Pairs (**CRPs**)*
- Physically unclonable
  - Impossible to avoid random process variations
- Unpredictable behavior
  - Unless by testing all CRPs
  - Known CRPs cannot be used to predict responses to new challenges

Security Advantages

- Keys are generated on demand
  - No need to program the key
  - No non-volatile memory required

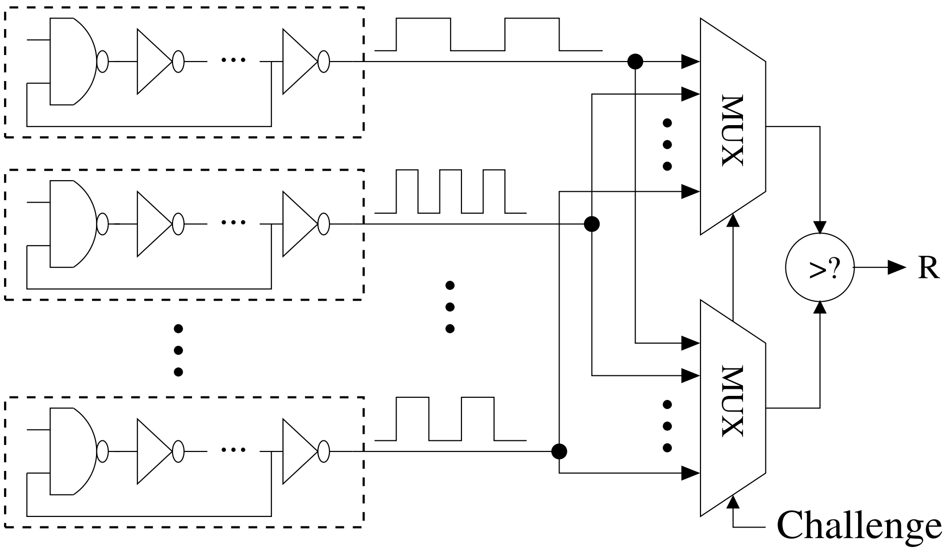
- No need to store information on chip
  - Unlike conventional digital storage
  - Security achieved through a *Challenge-Response* mechanism

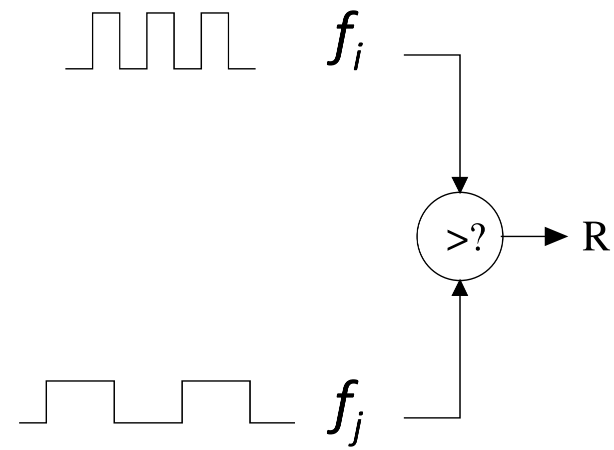
- No attack when the chip is OFF

- Resilient against *invasive* attacks
  - The PUF would be changed/destroyed

Weak PUFs

❑ **Example:** *Ring-Oscillator (RO) based* PUF*





❖ n ROs ==> $\binom{n}{2}$ CRPs : $O(n^2)$

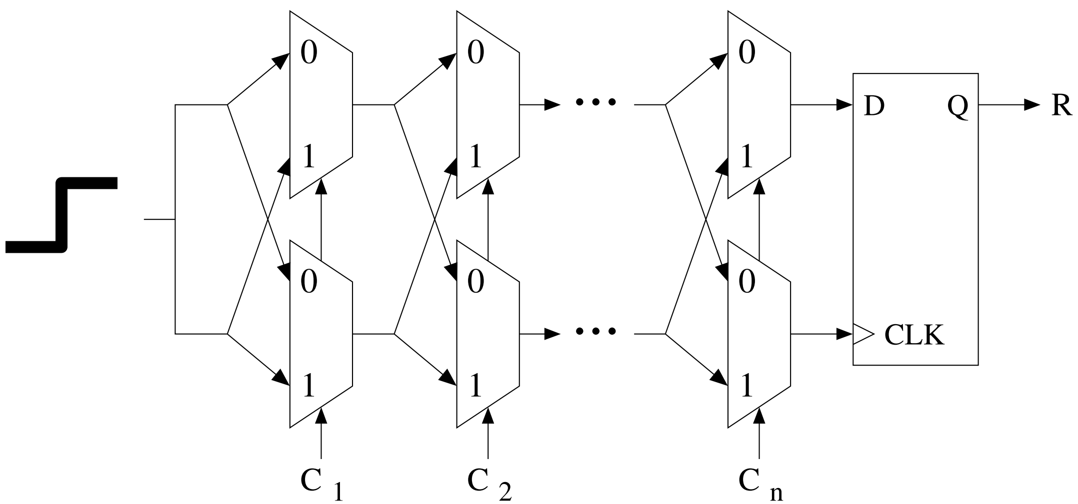
➢ **Weak PUF:** Limited number of independent CRPs

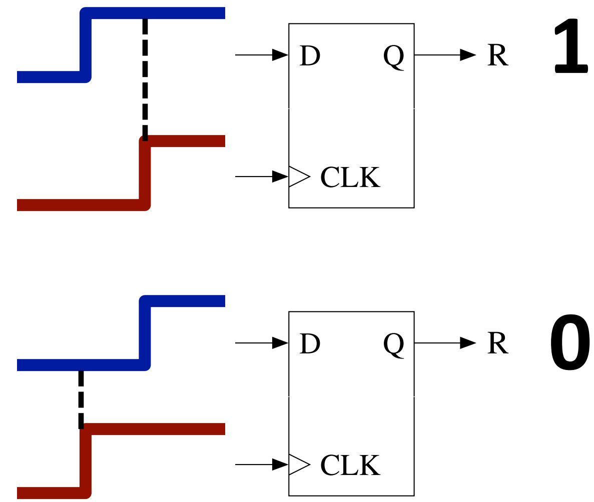
- *Polynomial* w.r.t. the number of components

* G. Sush and S. Devadas, *IEEE/ACM Design Automation Conference*, 2007

Strong PUFs

- **Example:** *Arbiter* PUF*





  - *2n* Multiplexers ==> 2^n CRPs : $O(2^n)$

- **Strong PUF:** Huge number of independent CRPs
  - *<u>Exponential</u>* w.r.t. the number of components

* S. Devadas et al, *IEEE International Conference on RFID*, 2008

Weak PUF vs. Strong PUF

Weak PUF

- **Limited** number of CRPs
  - *Polynomial*
- CRPs must be kept **secret**
  - Otherwise, the attacker can fully characterize the PUF
- Applications
  - Key generation, fingerprint

Strong PUF

- **Huge** number of CRPs
  - *Exponential*
- CRPs are **not secret**
  - *Infeasible* to fully recover the truth-table
- Applications
  - Device authentication, logic obfuscation, etc.

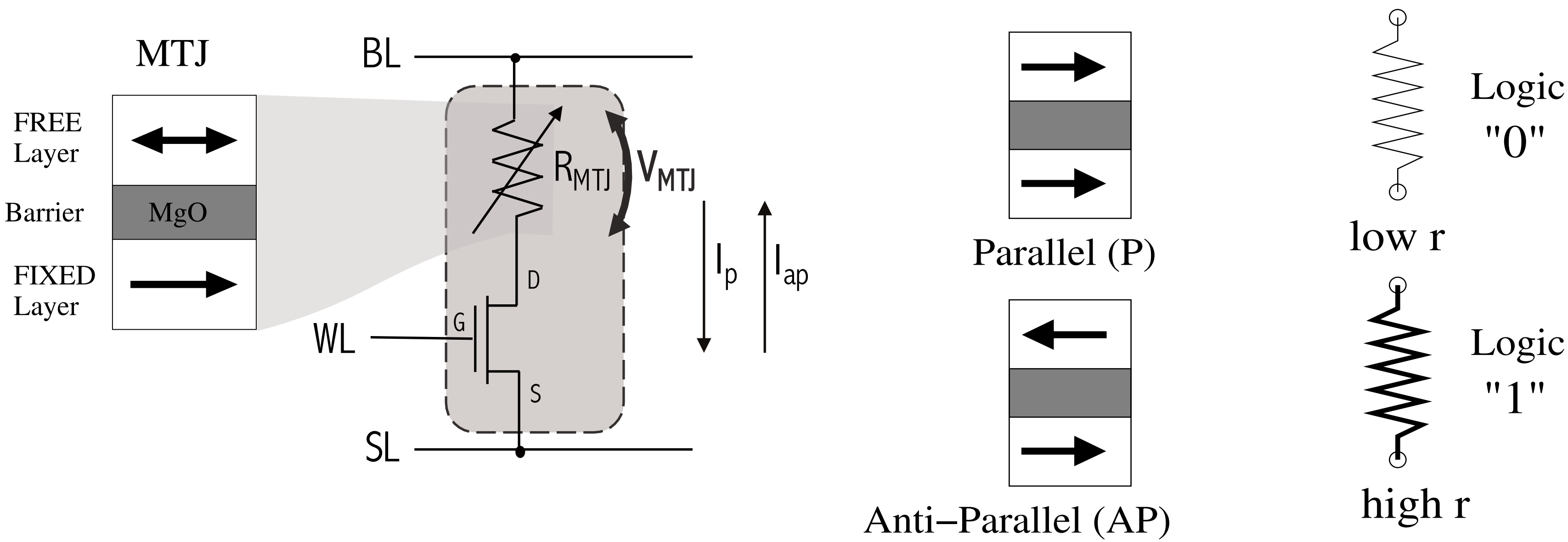
Overview of the Proposed Work

1) Proposing a strong PUF based on STT-MRAM devices
   - ❖ Previous work: an STT-MRAM based **weak PUF**
   - ❖ Introducing the idea of *Group Formation*
   - ❖ The proposed **strong PUF**

2) Generalizing the idea of ***Group Formation***
   - ❖ How to make a strong PUF in general?
   - ❖ Applying the idea of group formation to RO-based weak PUF

Introduction to STT-MRAM

- Spin-Transfer Torque Magnetic RAM (STT-MRAM)
  - A nano device, with Magnetic Tunnel Junction (MTJ) as its storage

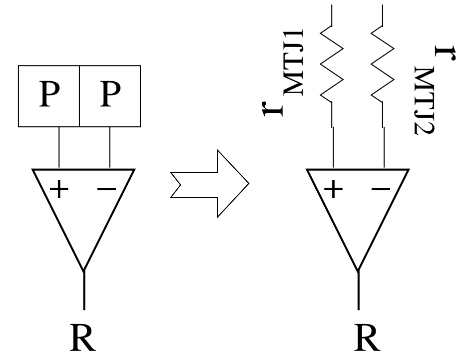


- Two states:
  1) *Parallel (**P**)*: **low** resistance, associated with **logic 0**
  2) *Anti-Parallel (**AP**)*: **high** resistance, associated with **logic 1**

An STT-MRAM based Weak PUF*

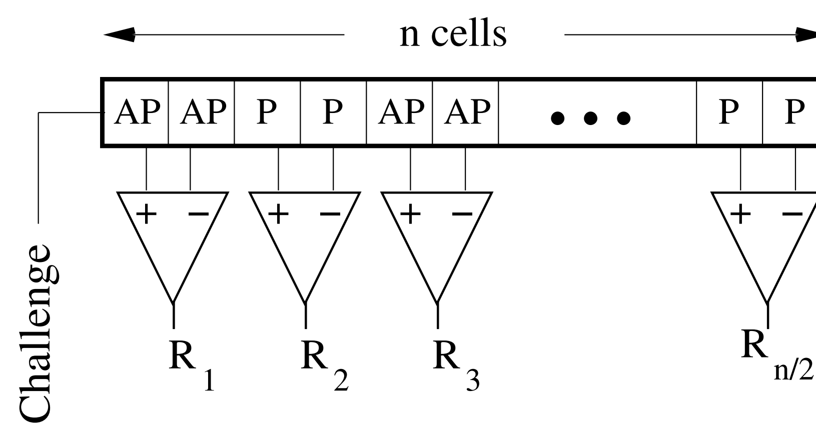
- Main idea
  - Two identical cells with the same magnetization

$$R = \begin{cases} 0 & \text{if } r_{MTJ1} > r_{MTJ2} \\ 1 & \text{if } r_{MTJ1} < r_{MTJ2} \end{cases}$$



- Architecture
  - *n/2* pairs ==> *2* $^{n/2}$ CRPs

❖ Only 2 independent CRPs
1) All pairs set to state *P*
2) All pairs set to state *AP*



✓ Weak PUF

* L. Zhang et al, *IEEE International Symposium on Circuits and Systems*, 2014

Weak PUF vs. Strong PUF

- PUFs are based on noisy analog features
  - STT-MRAM: resistances of the MTJ devices
  - Arbiter, RO-based: gate delays

- Analog features “collapsing” into digital bits ==> PUF
  - STT-MRAM: Resistance comparison of two cells

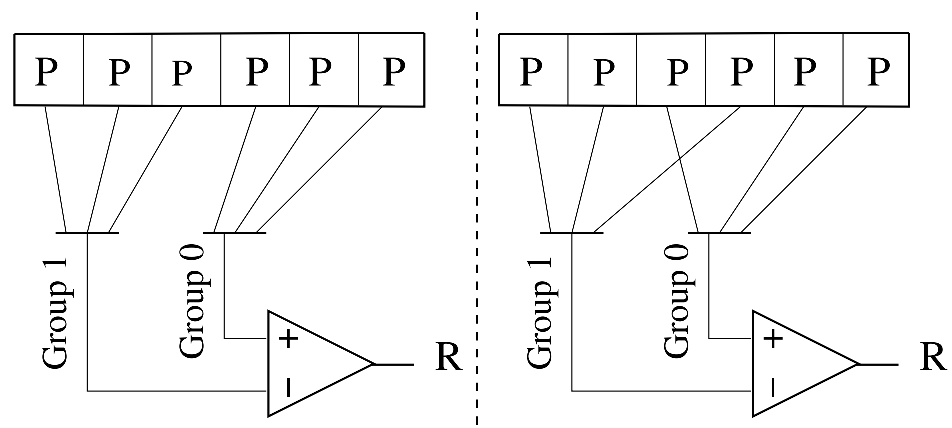
- Analog features can offer an unlimited number of CRPs
  - Infinite precision

- Weak PUF vs. Strong PUF
  - How much of such infinite precision is exploited before collapsing into digital?

Strong PUF Component 1: Group Formation

- Previous *Weak* PUF:
  - Comparing the resistances of two **single** cells
- **Group Formation:**
  - Comparing the resistances of two **groups** of cells

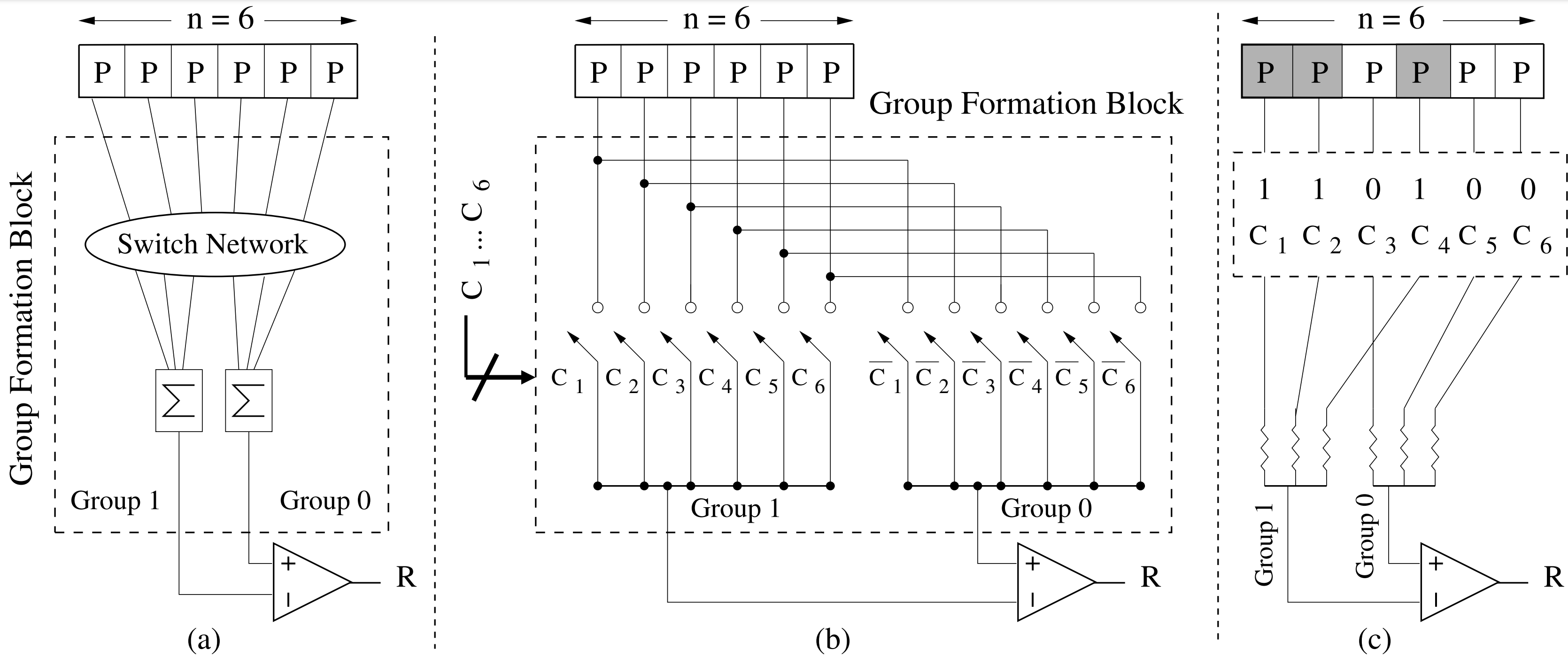
- Example:
  - 6 STT-MRAM cells
  - 3 cells per group
  - Fixed magnetization
  - Group 1 vs. Group 0



(a) R = 0 or 1
(b) R = 0 or 1

❖ <u>Configurable</u> grouping: **10 independent CRPs**

Group Formation Block



- Two groups (*Group 1* and *Group 0*) with 3 cells
- Each cell can join <u>either</u> of groups, but <u>not both simultaneously</u>
- Challenge bits: C_1 to C_6 , controlling 12 switches

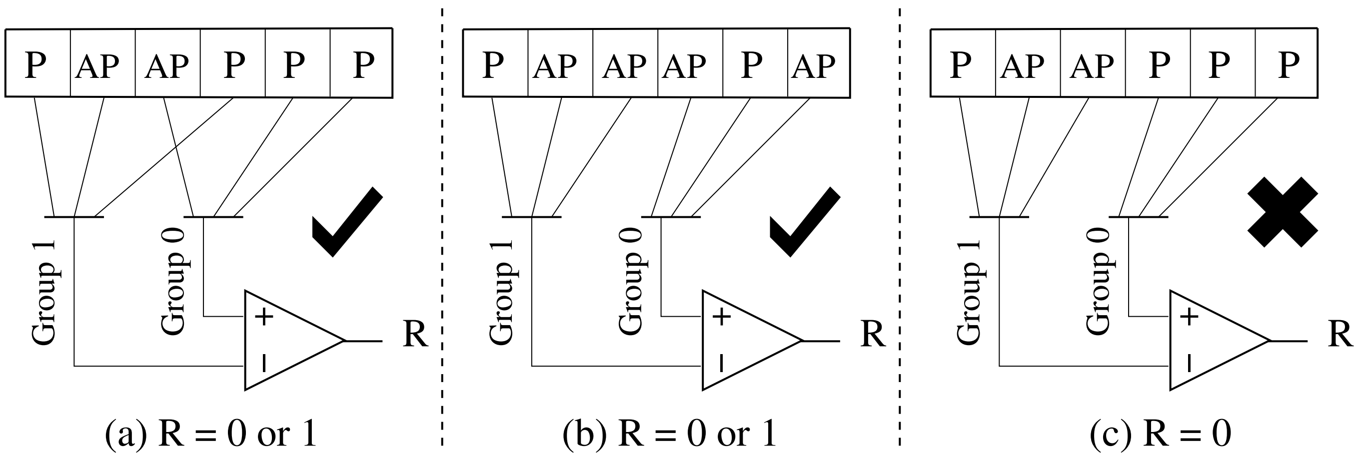
❑ Example:

- *Group 1*: Cells in Grey   *Group 0*: cells in white

Strong PUF Component 2: Bit Pattern

- **Bit Pattern:**
  - Changing the magnetization of cells in each group (assumed to be fixed so far)

- Example:



- Same number of cells in states *P* and *AP* in both groups

- **20 independent CRPs** (per 6 cells) for every group choice

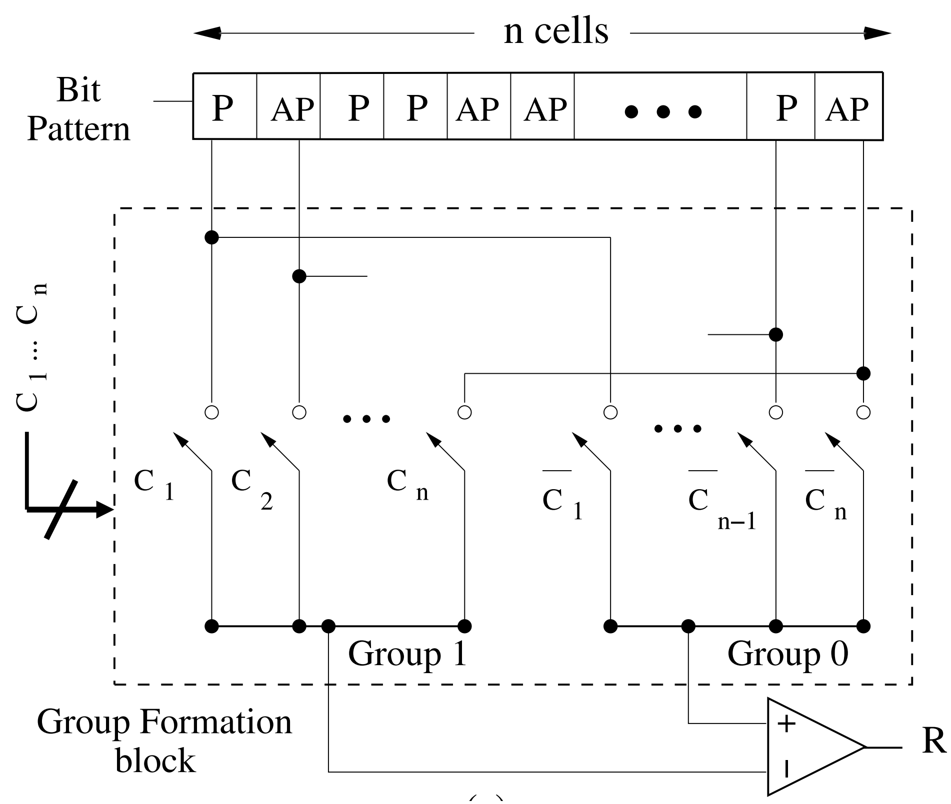
Proposed STT-MRAM Based Strong PUF

- *n/2* cells per group
- Each cell can join either of groups, but not both simultaneously
- Groups with less than *n/2* cells: not allowed by the architecture
  - To avoid using the info. of smaller groups to determine the larger ones

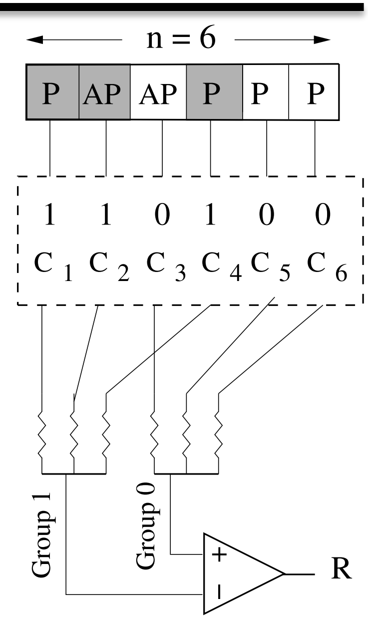
❖ *Challenges:*

1) Group Formation
2) Bit Pattern Selection

❖ *Responses:* 1 or 0 (1-bit)



Analysis of the Proposed PUF (1/2)



➢ Total resistance of each group

- *<u>Parallel equivalence</u>* of all cells

❑ Example:

- 3 cells per group (two *P*'s and one *AP*)

$$\frac{1}{r_{G1}} = \frac{1}{r_1^P} + \frac{1}{r_2^{AP}} + \frac{1}{r_4^P} \quad and \quad \frac{1}{r_{G0}} = \frac{1}{r_3^{AP}} + \frac{1}{r_5^P} + \frac{1}{r_6^P}$$

➢ Hardware overhead

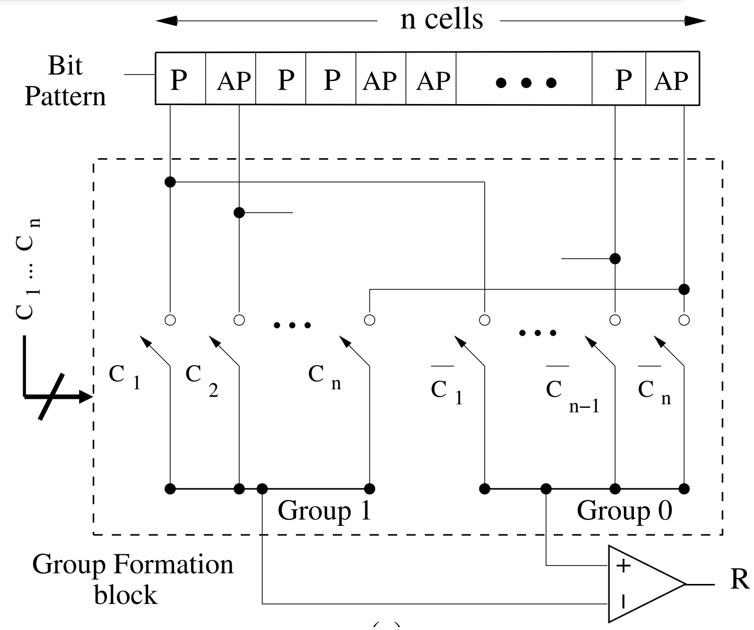
- Previous weak PUF: *n* sense-amplifiers
- Proposed PUF: 1 sense-amplifier + 2*n* switches

Analysis of the Proposed PUF (2/2)

- Number of independent CRPs

  1) Group Formation: $\frac{1}{2}\binom{n}{n/2}$

  2) Bit Pattern Selection: $\sum_{i=0}^{n/2}\binom{\frac{n}{2}}{i}^2$



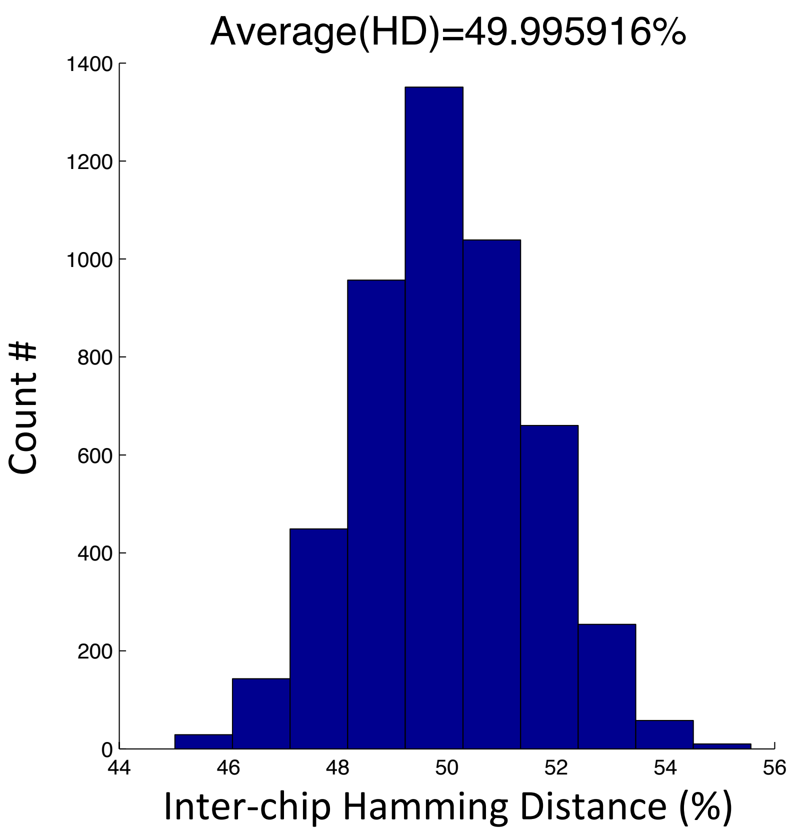
- Total number of independent CRPs

$$\frac{1}{2}\times\binom{n}{\frac{n}{2}}\times\sum_{i=0}^{n/2}\binom{\frac{n}{2}}{i}^2=\frac{1}{2}\binom{n}{\frac{n}{2}}^2$$

Factorial growth of ***independent*** CRPs ==> Strong PUF

Simulation Results: Inter-chip

- Experiment Setup:
  - 1024-bit responses
  - 100 Chips
  - MATLAB model*

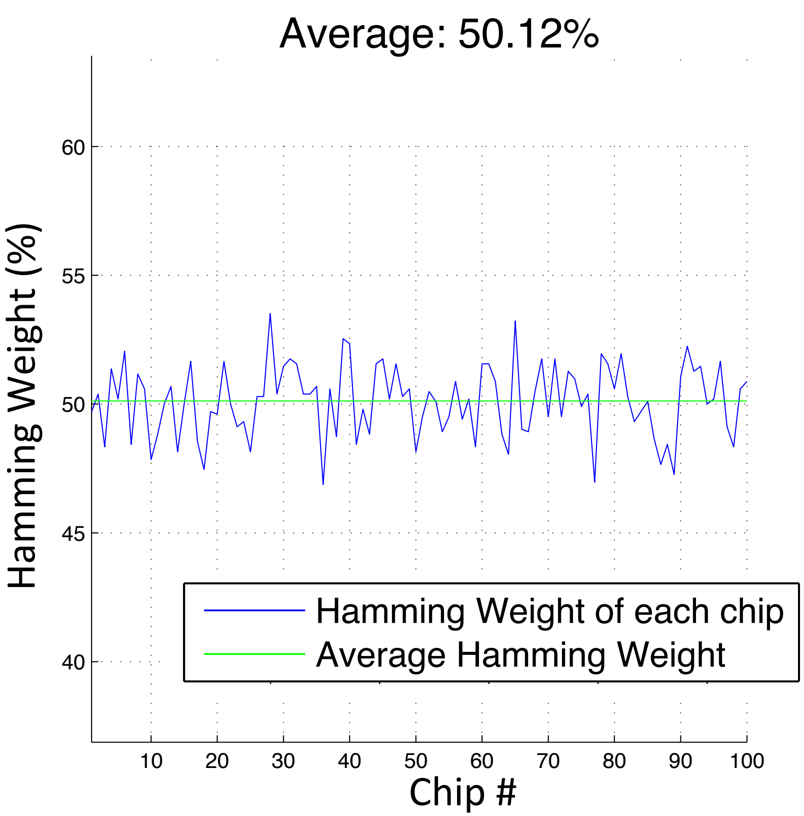


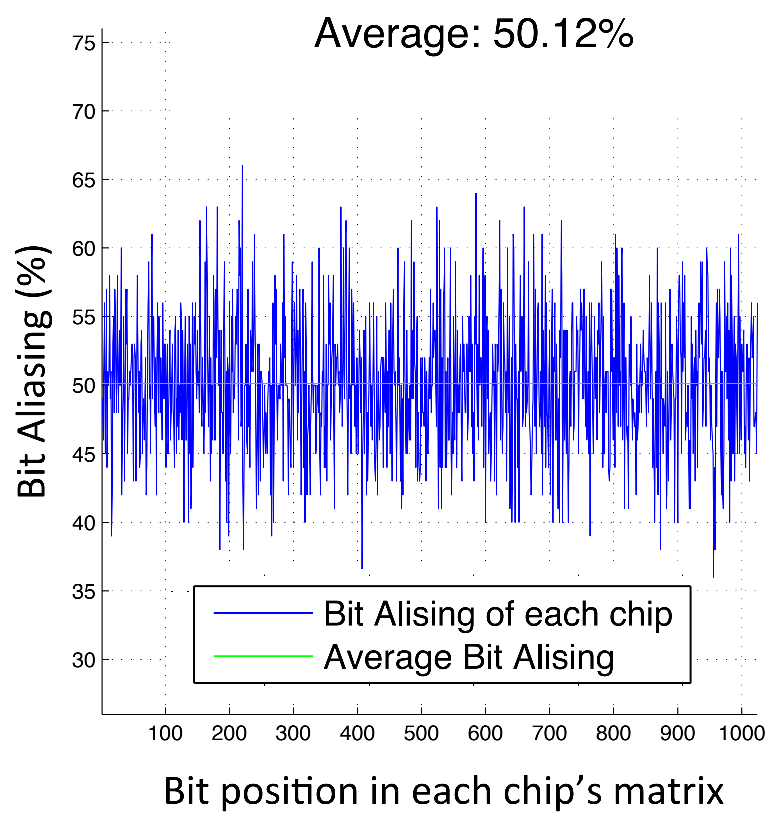
- Inter-chip randomness
  - Hamming Distance

* L. Zhang et al, *IEEE International Symposium on Circuits and Systems*, 2014

Simulation Results: Intra-chip

- Intra-chip randomness
  1) *Hamming Weight:* randomness of **bits** within the *same* response
  2) *Bit Aliasing:* **single bit** randomness among *different* responses





Strong PUF Beyond STT-MRAM

➢ Necessary conditions for making a strong PUF

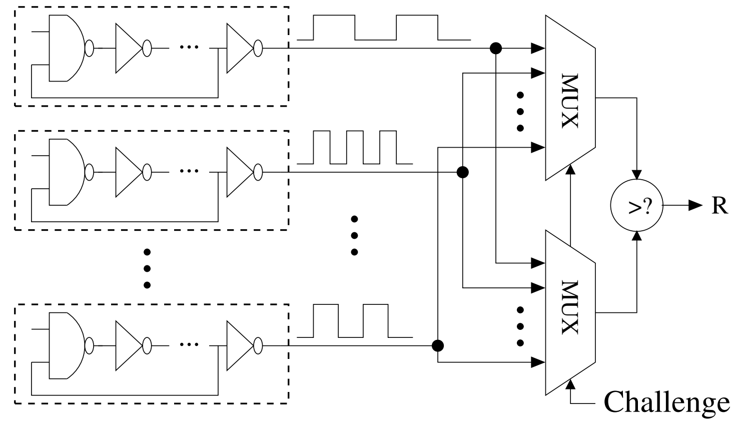
1) **Device-level** compatibility for group formation
   - STT-MRAM: parallel combination of MTJ cells' resistances
   - Arbiter PUF: gate delays
   - Not supported in "SRAM-based power-up PUF" *

2) **Architecture-level** support to achieve independent CRPs
   - STT-MRAM: group formation flexibility
   - Arbiter PUF: path selection

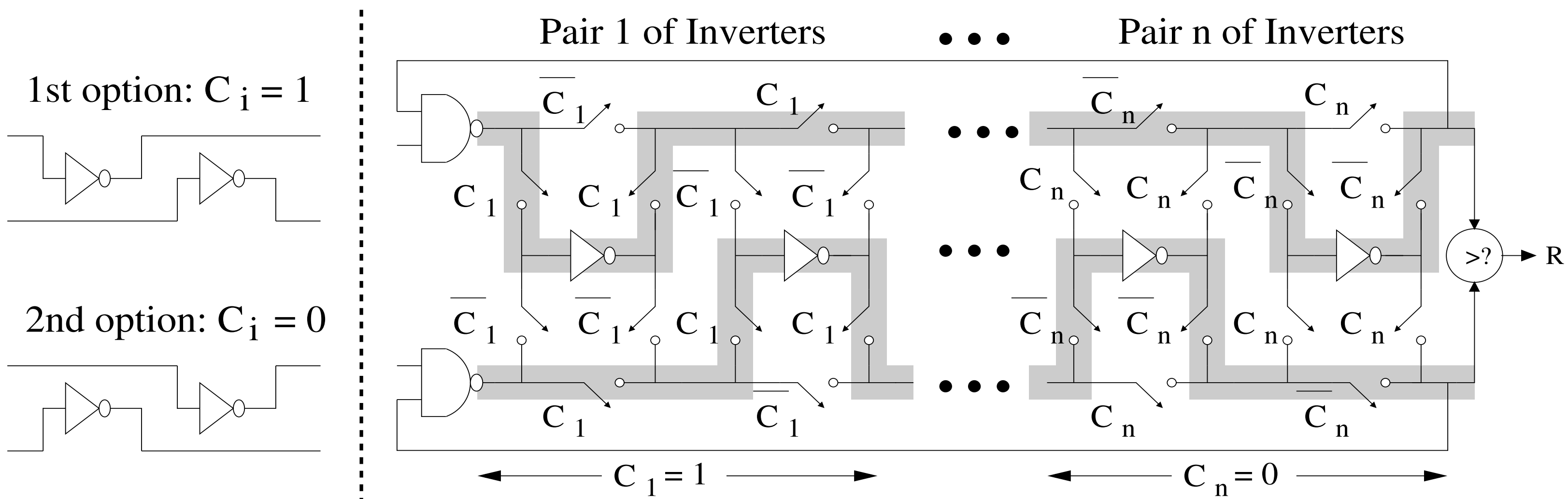
* D. Holcomb et al, *IEEE Transactions on Computers*, 2009

RO-based Strong PUF

- RO-based weak PUF
  - Two ROs compared at a time
  - n ROs ==> $\binom{n}{2}$ CRPs : $O(n^2)$



- RO-based **strong** PUF



- $2n$ Inverters ==> 2^n CRPs : $O(2^n)$

Conclusions

✧ Weak PUF vs. Strong PUF

- How much to exploit the noisy analog feature?

✧ An STT-MRAM based strong PUF

- Based on the idea of Group Formation
  - Fixing the group size
  - Allowing each device to join either of groups, but not both
- Simulation results confirmed high quality of randomness

✧ Making a strong PUF in general

1) Device-level compatibility for group formation
2) Architecture-level support for huge CRPs