A DRAM based Physical Unclonable Function Capable of Generating >10^{32} Challenge Response Pairs per 1Kbit Array for Secure Chip Authentication

Q. Tang, C. Zhou, *W. Choi, *G. Kang, *J. Park, K. K. Parhi, and C. H. Kim

University of Minnesota, Minneapolis, USA
Korea University, Seoul, Korea

zhoux825@umn.edu

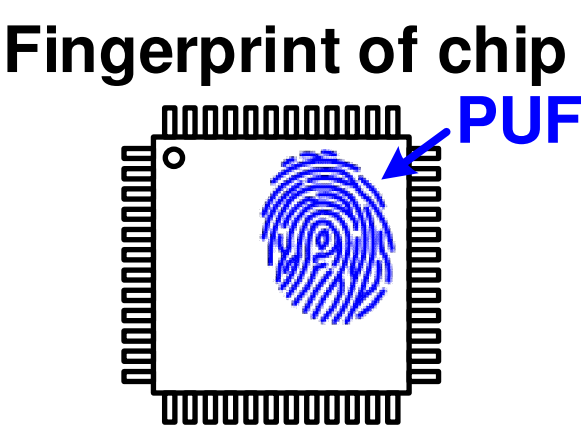
Agenda

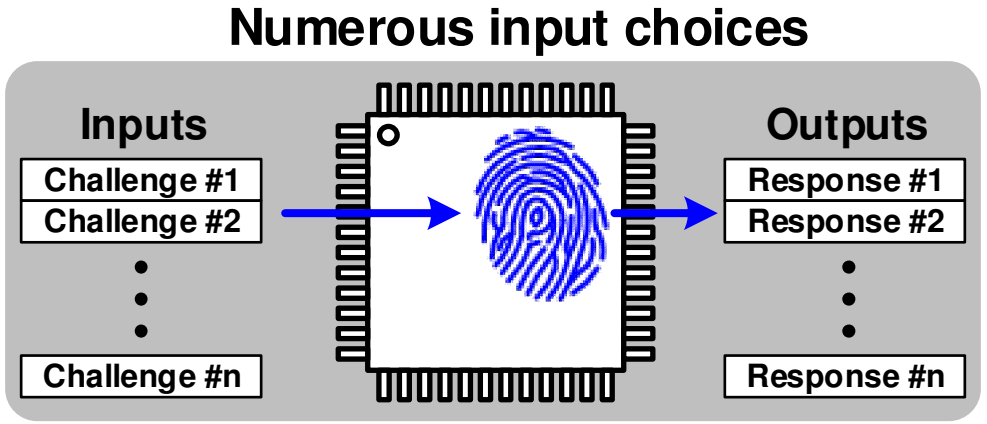
- Background
- Proposed DRAM based Strong PUF
- Enhancing DRAM PUF Uniqueness and Stability
- Hamming Distance Measurements
- Summary

Agenda

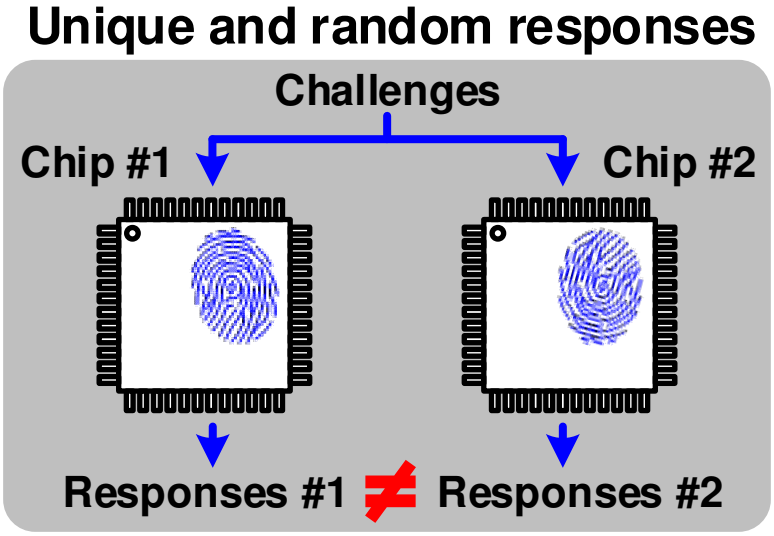
- **Background**
- **Proposed DRAM based Strong PUF**
- **Enhancing DRAM PUF Uniqueness and Stability**
- **Hamming Distance Measurements**
- **Summary**

Physical Unclonable Function (PUF)



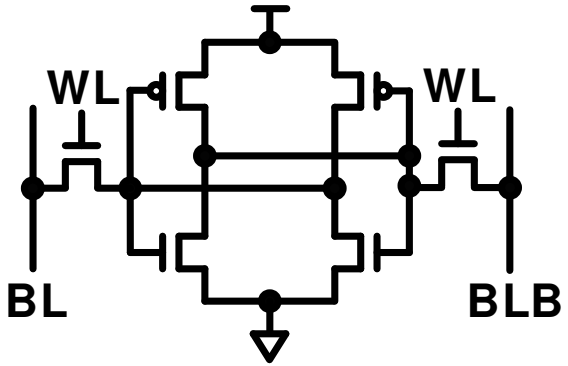


- **Unique and random: Based on inherent process variation**
- **Secure: Large # of challenge-response pairs (CRPs)**

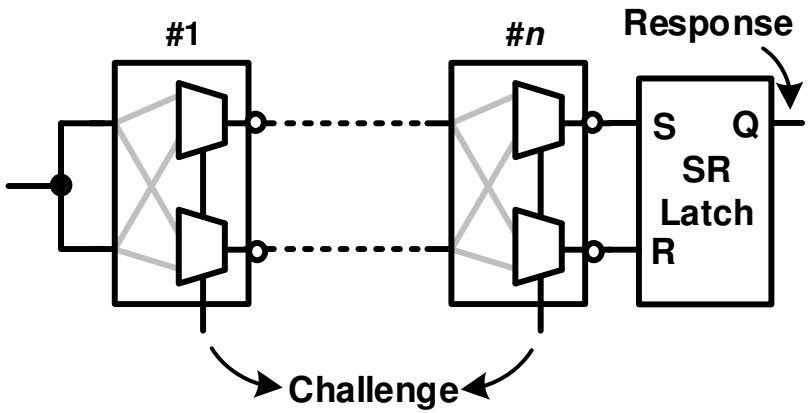


Weak PUF vs. Strong PUF

- **Weak PUF:**
  - **# of CRPs* proportional to # of unit cells**
  - **Example: SRAM PUF**
  - **Application: key generation**

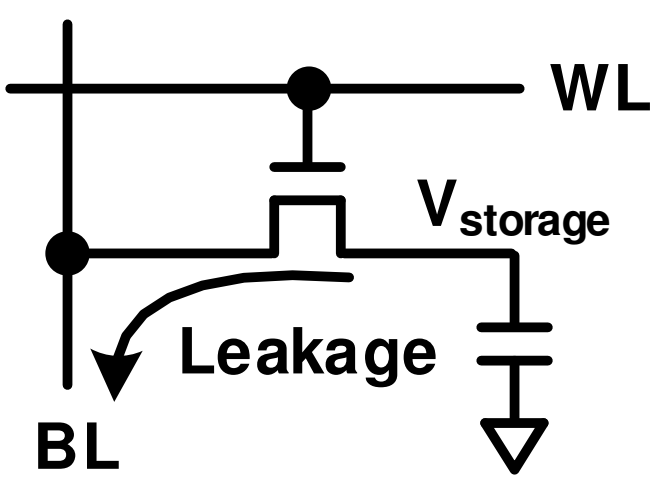


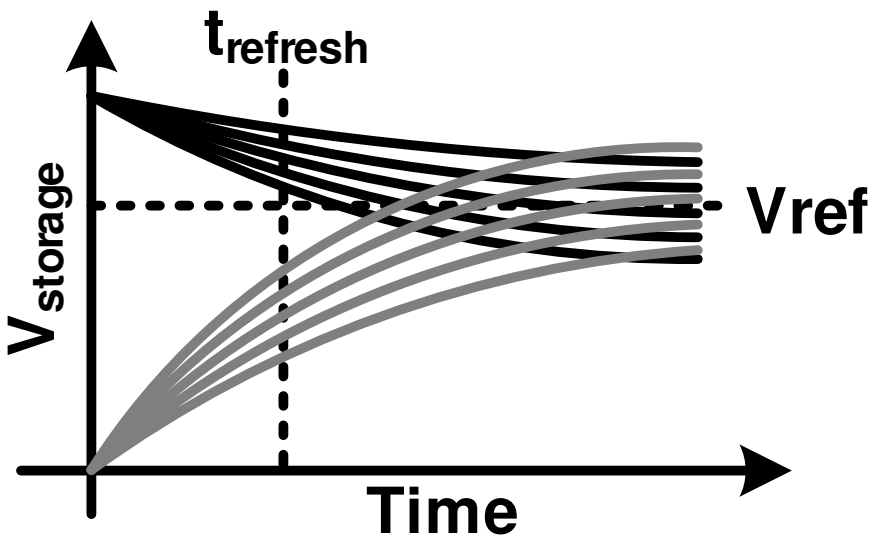
- **Strong PUF:**
  - **# of CRPs exponential to # of unit stages (2^n)**
  - **Example: MUX arbiter PUF**
  - **Application: system authentication**



*CRP: Challenge Response Pair

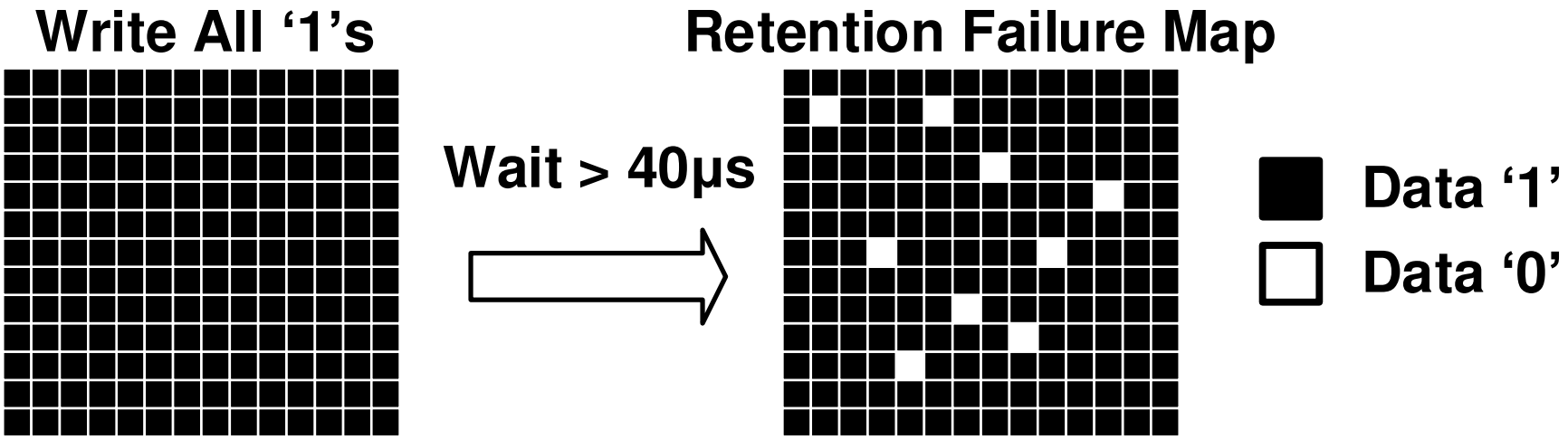
DRAM Retention Characteristics





- Data retention time depends on the leakage current and capacitance of the storage node
- Refresh required before the cell data flips

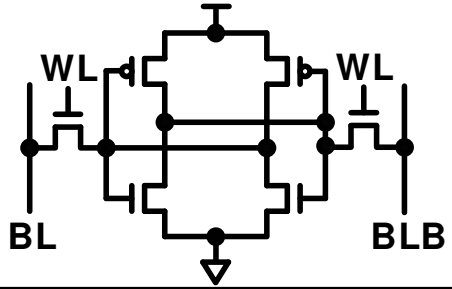
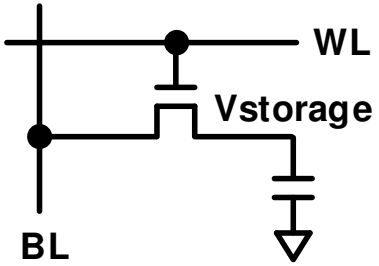
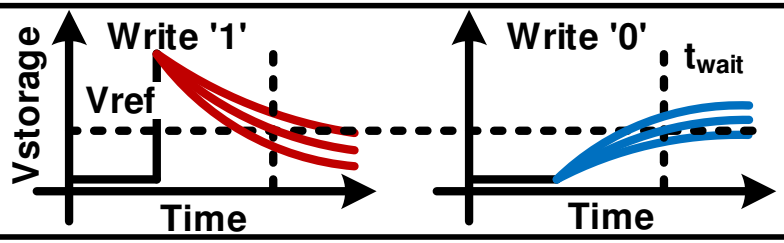
DRAM based PUF



- **Failure locations unique to each chip**
- **Retention time adjusted by word line voltage**
- **Only weak PUF configuration implemented**

S. Rosenblatt, et al., JSSC, 2013 (IBM)

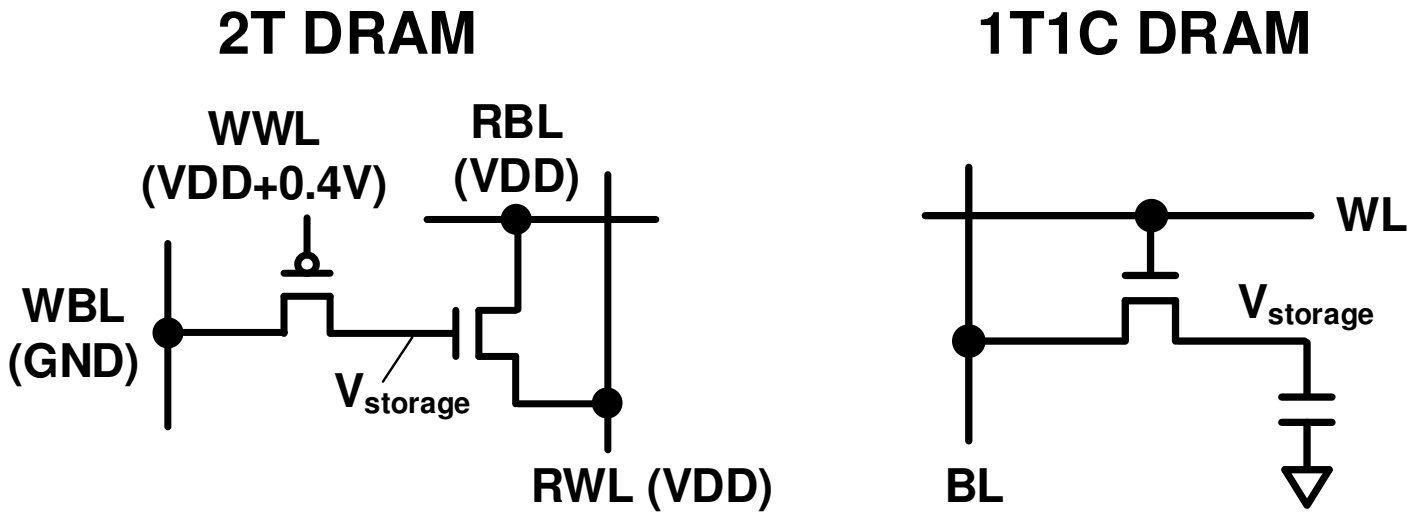
SRAM PUF vs. DRAM PUF

	SRAM PUF	DRAM PUF
Schematic		
Challenge Method	Power up 	
Key Features	• Power off required • Weak PUF configuration only	• Power is kept on • Strong PUF configuration possible • V, T variation can be compensated

Agenda

- Background
- **Proposed DRAM based Strong PUF**
- Enhancing DRAM PUF Uniqueness and Stability
- Hamming Distance Measurements
- Summary

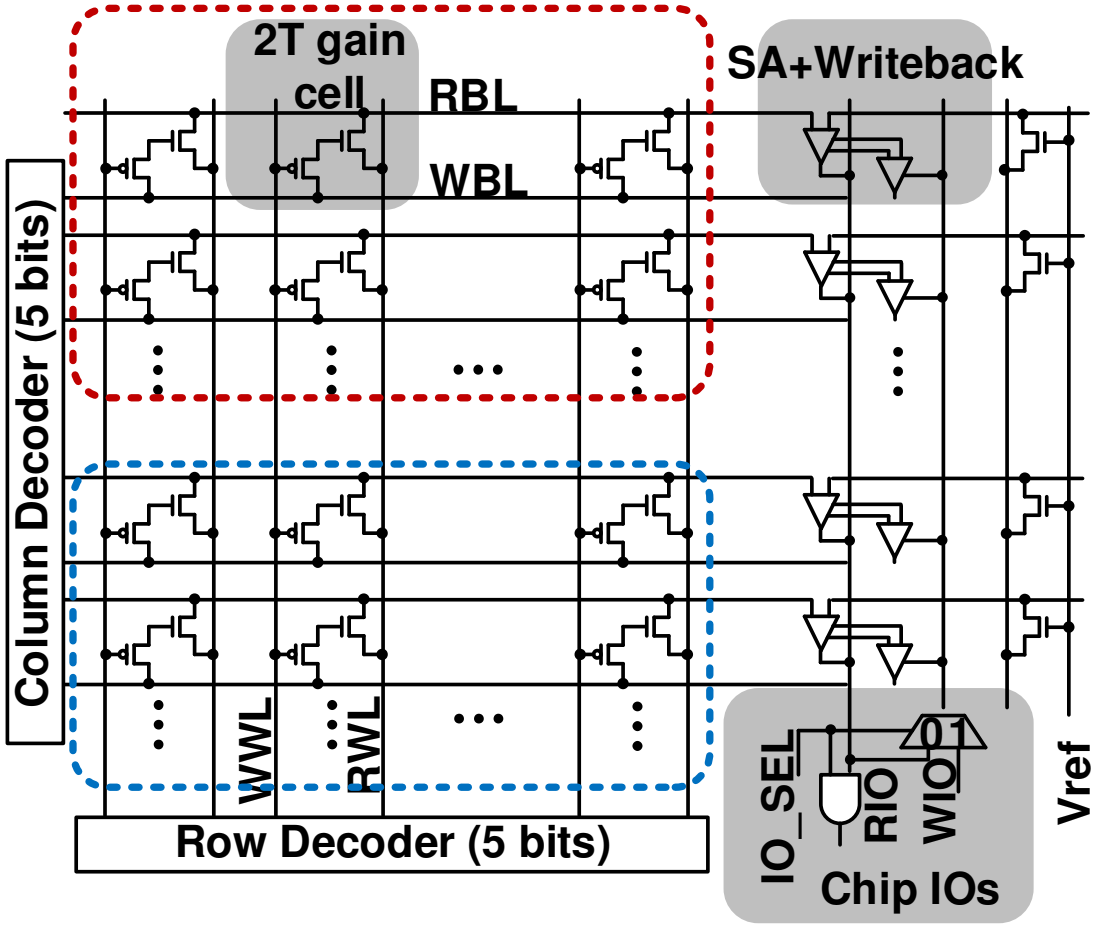
Proposed 2T DRAM based PUF



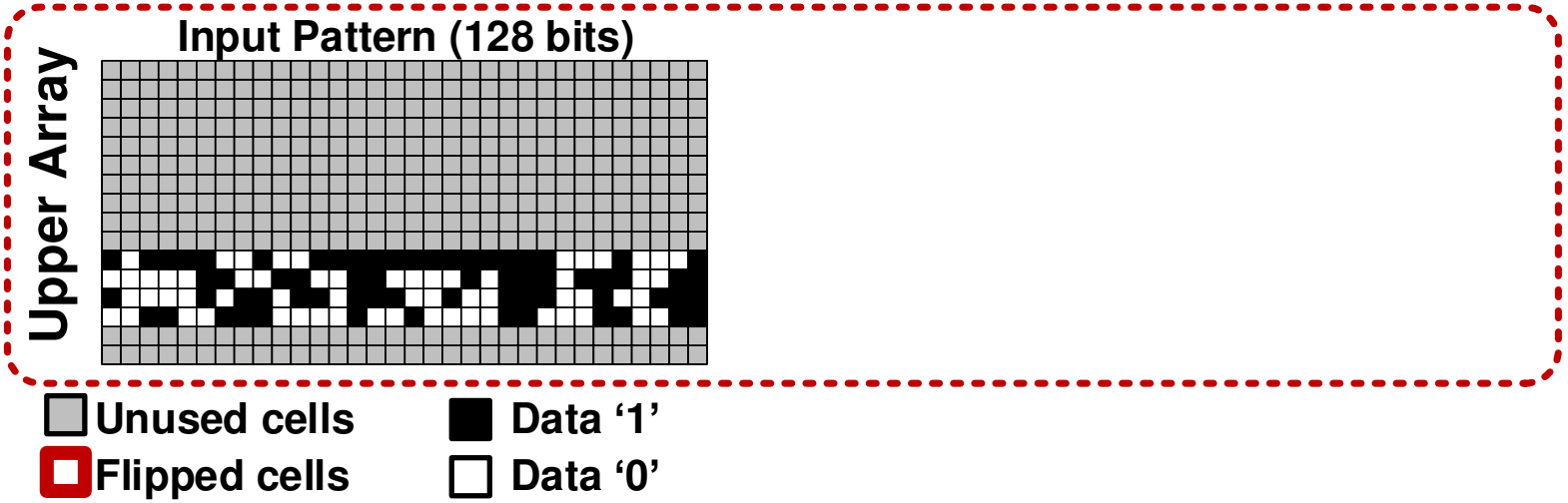
K. Chun, et al., ISSCC 2011, JSSC 2012

- **Logic compatible**
- **Retention time similar to 1T1C**
- **t_{wait} = 10.5ms induces 10% flips @1.2V, 27ºC**

DRAM based Strong PUF Array

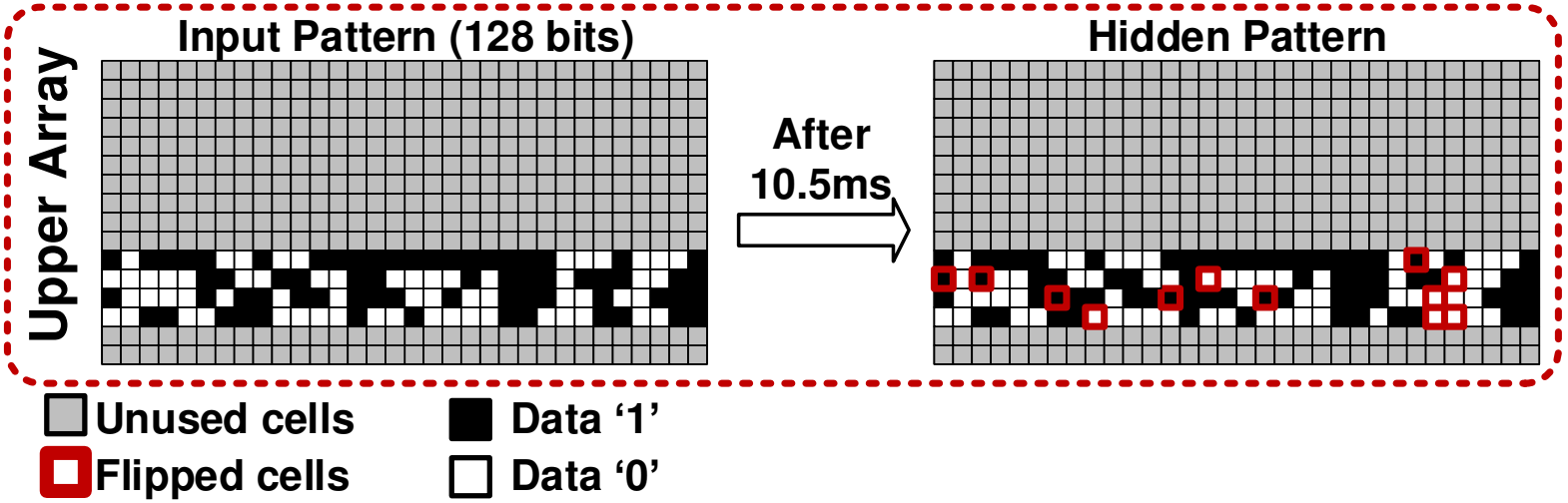


Proposed Authentication Scheme



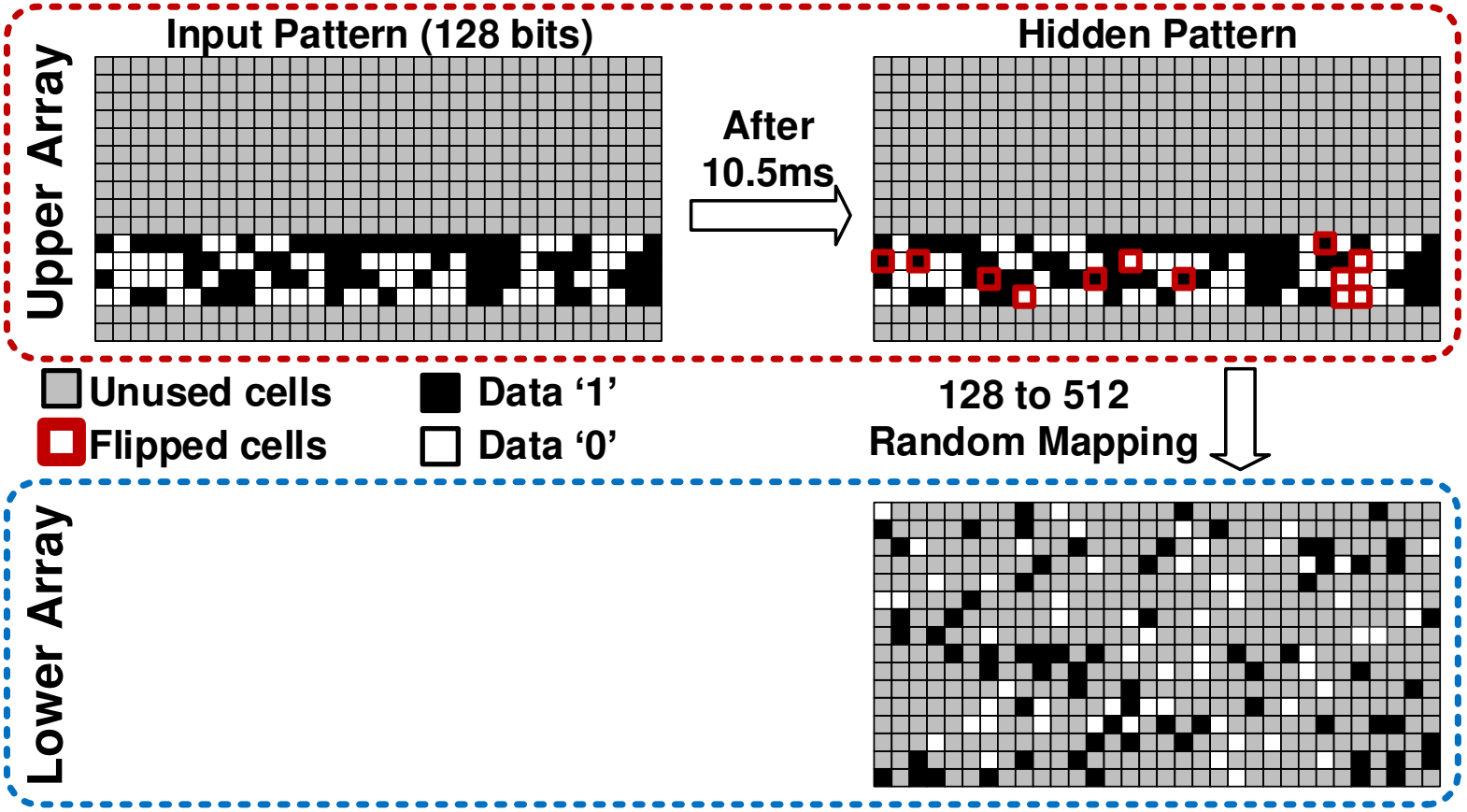
- Step 1: Write a 128 bit pattern to selected upper array
- Challenge: start location (=512) + input data ('1' or '0')

Proposed Authentication Scheme



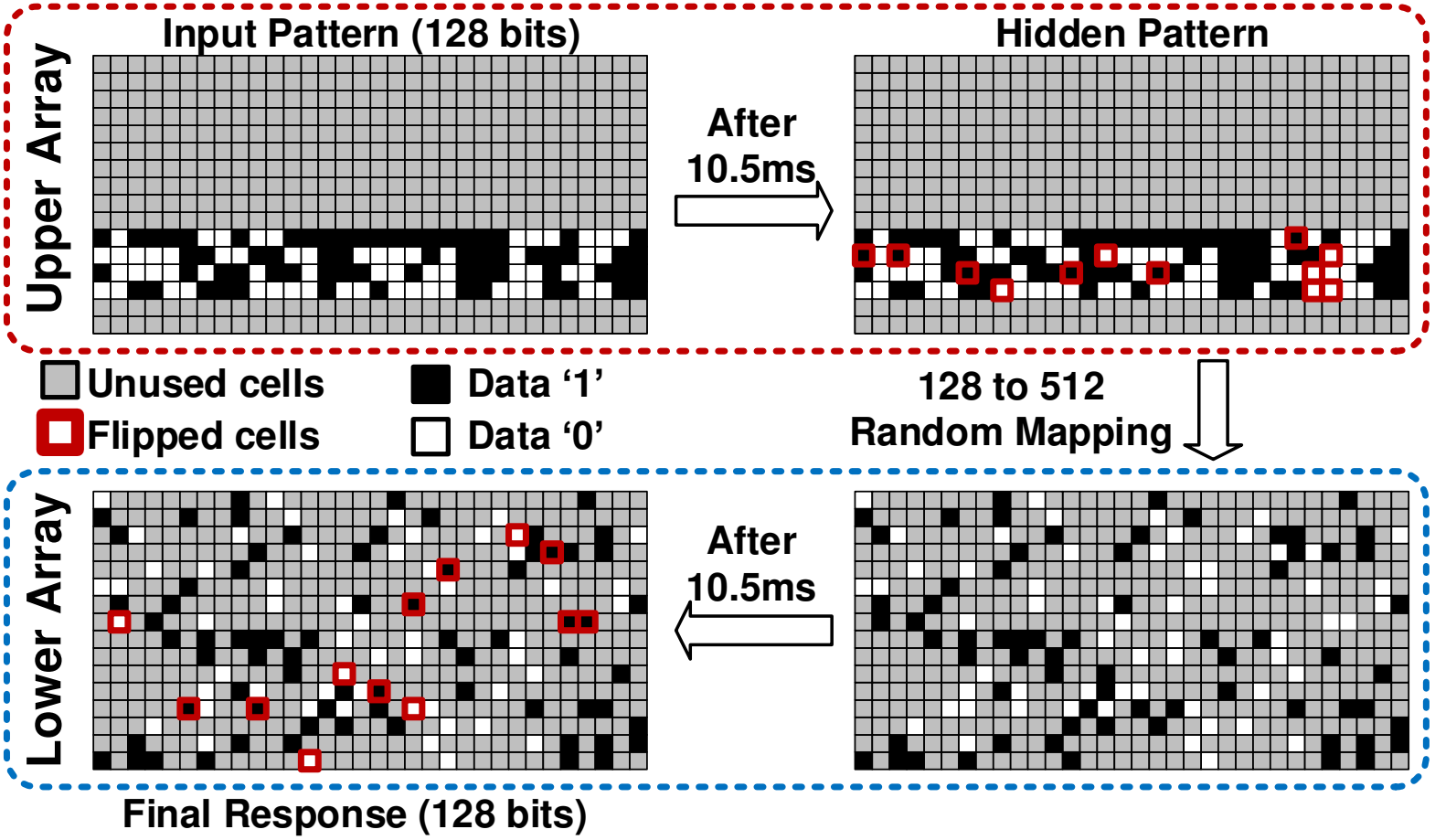
- Step 2: Wait for 10.5ms to induce 10% cell failures
- Internally generated pattern is hidden to outside world

Proposed Authentication Scheme



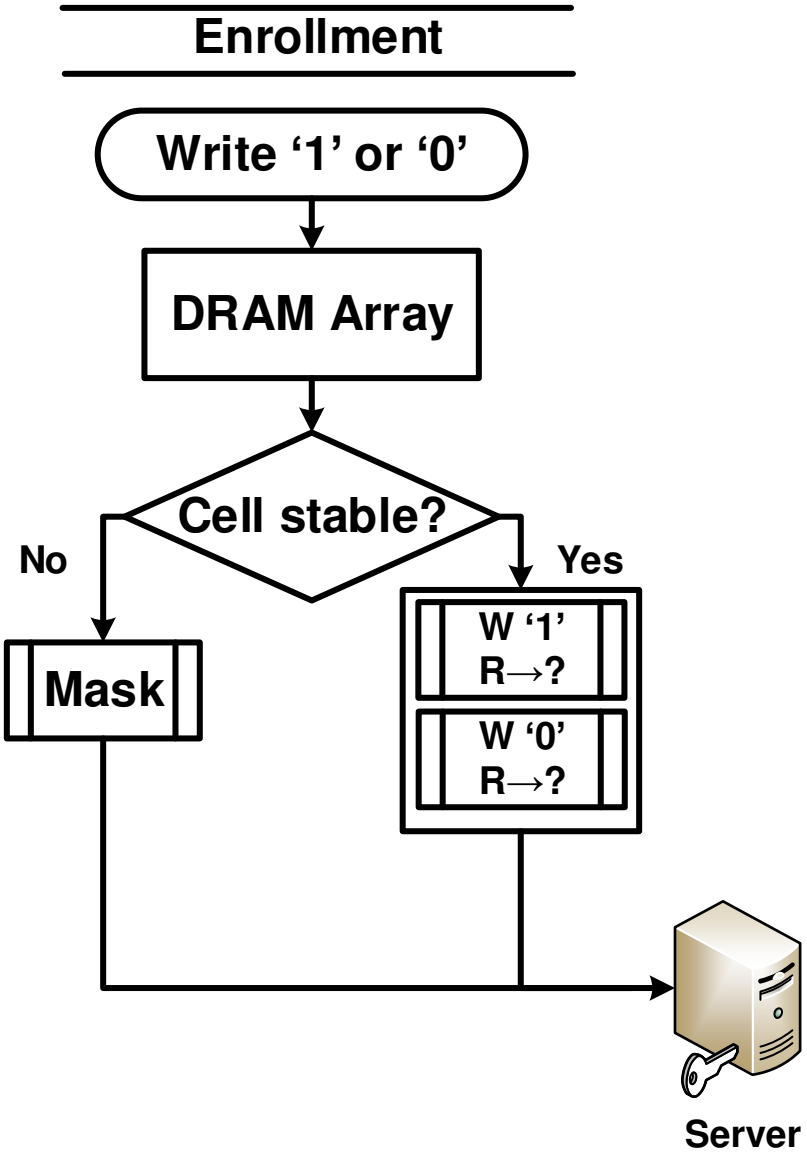
- Step 3: Write hidden pattern to lower array
- Challenge: mapping information (=Permutation(512, 128))

Proposed Authentication Scheme

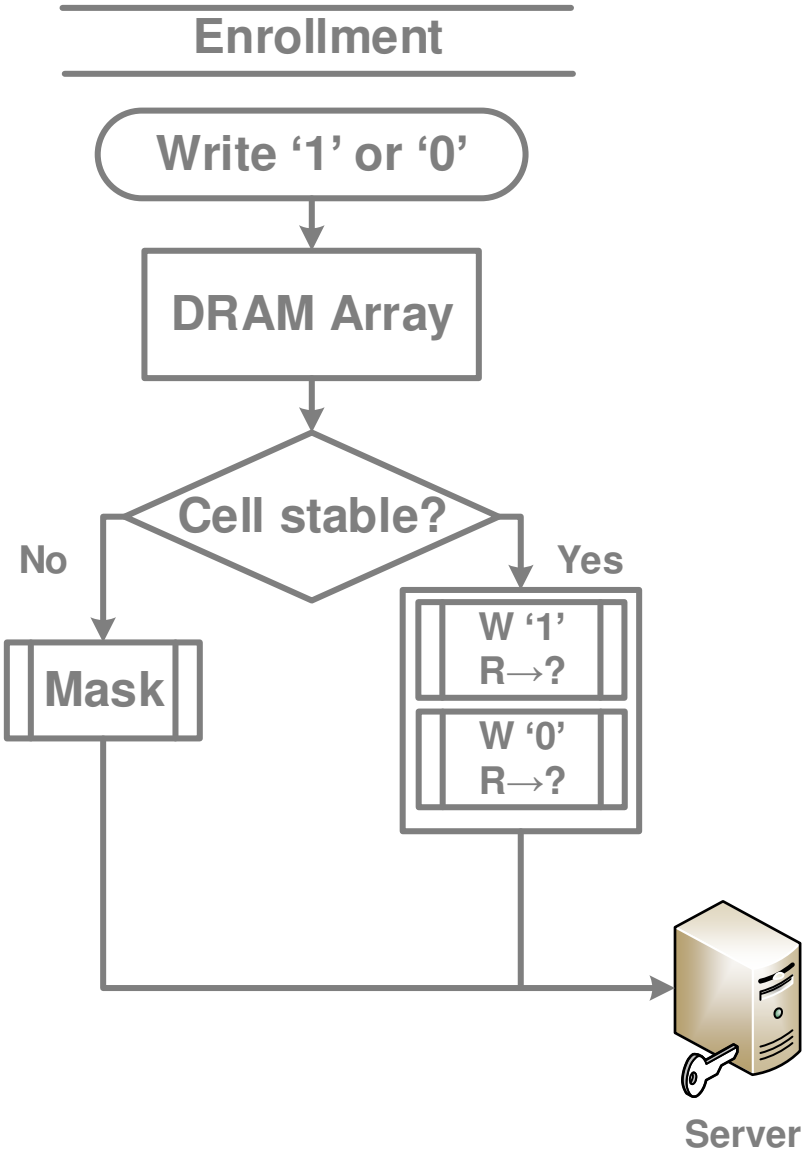


- Step 4: Collect responses from lower array after 10.5ms
- # of Challenges = 512×2×Permutation(512, 128)

Enrollment and Authentication Flow



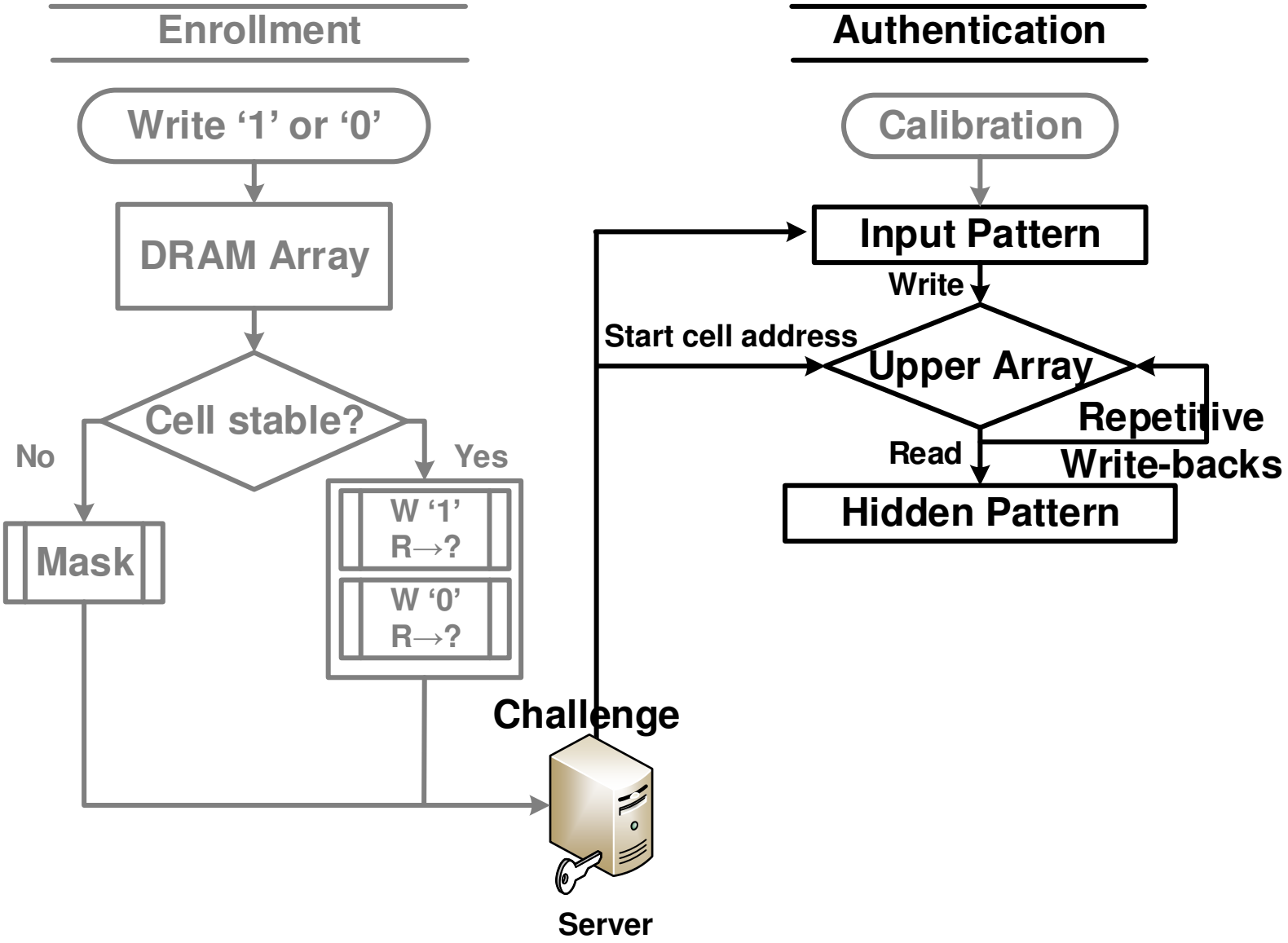
Enrollment and Authentication Flow



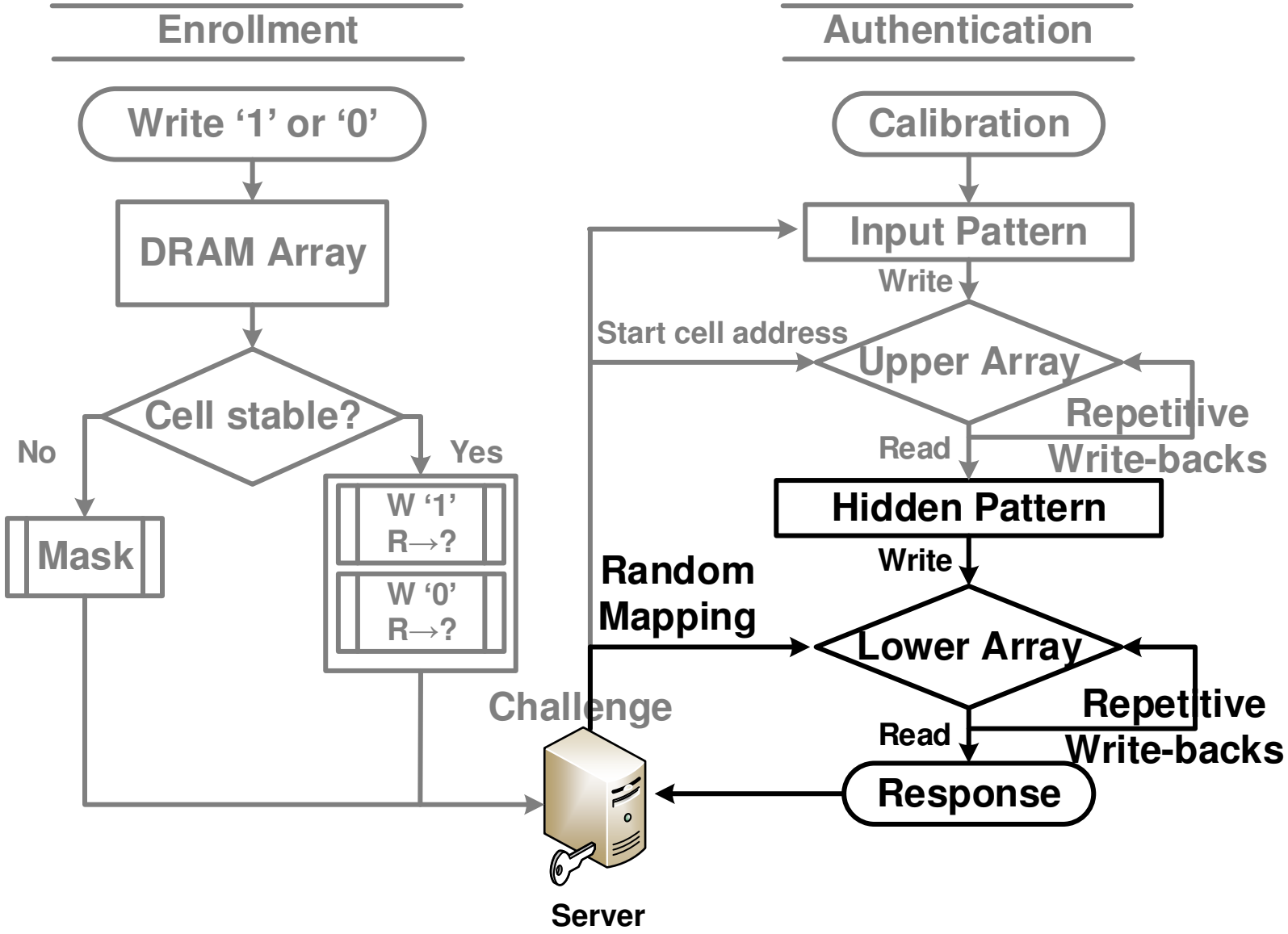
Authentication

Calibration

Enrollment and Authentication Flow



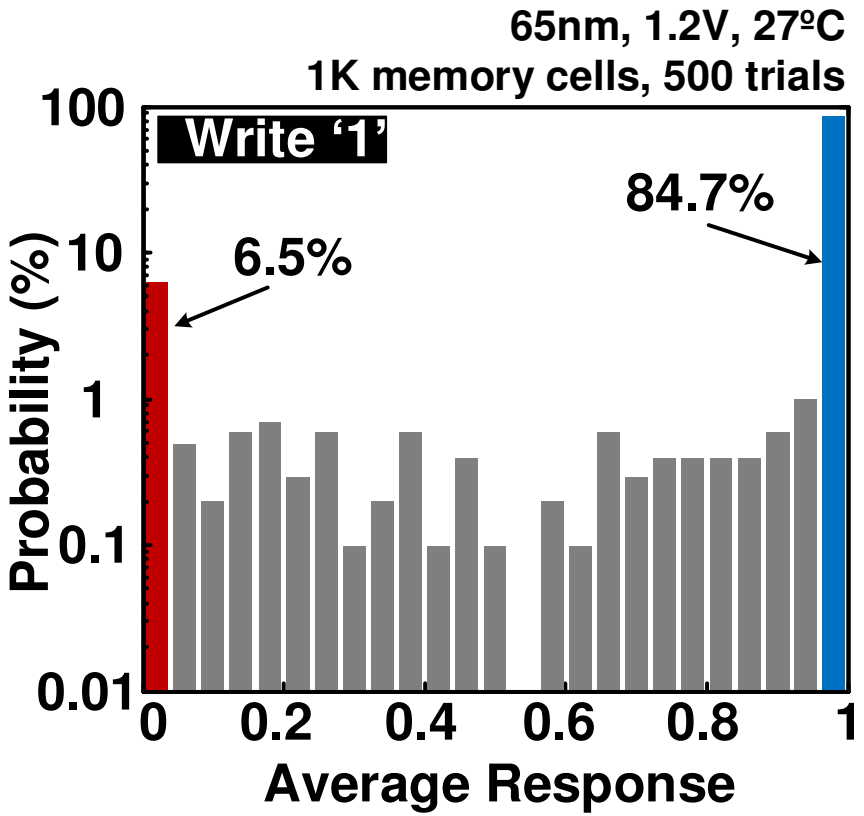
Enrollment and Authentication Flow

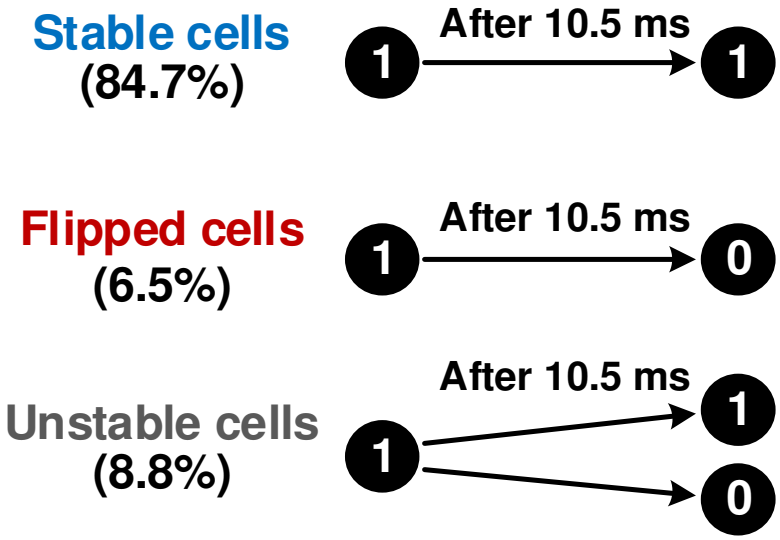


Agenda

- Background
- Proposed DRAM based Strong PUF
- **Enhancing DRAM PUF Uniqueness and Stability**
- Hamming Distance Measurements
- Summary

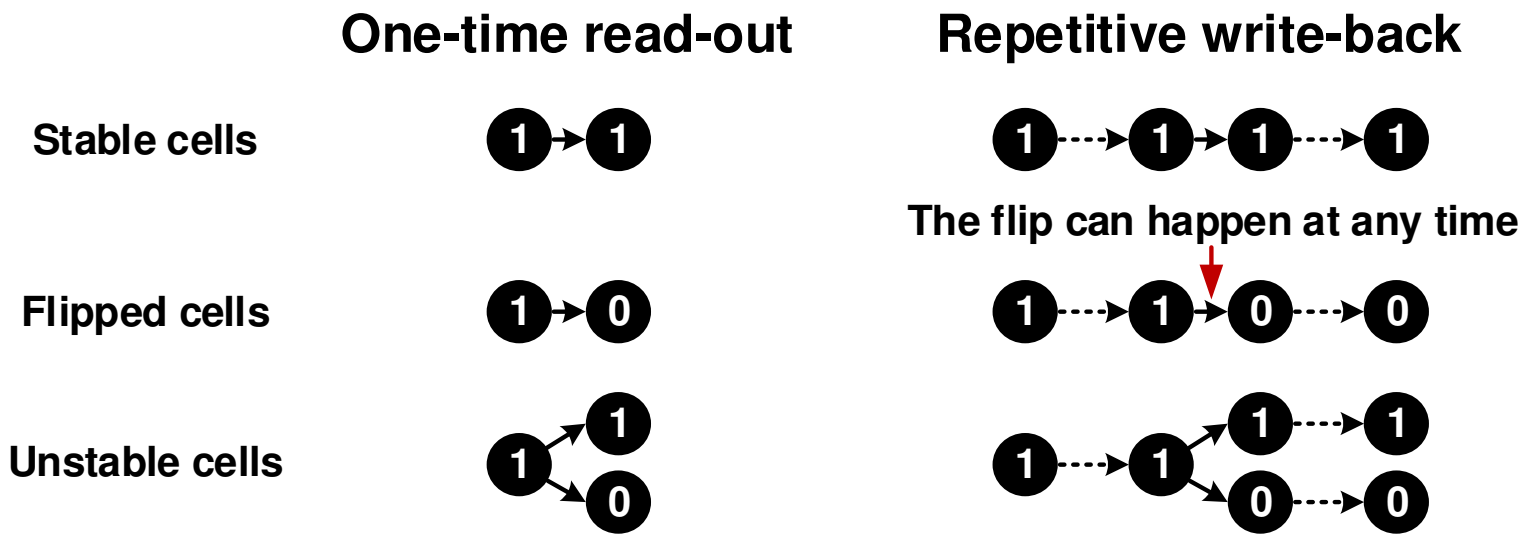
DRAM PUF Response Distribution





- Average response over 500 trials
- More flip cells (red color bar) desired
- Few unstable cells (gray color bar) desired

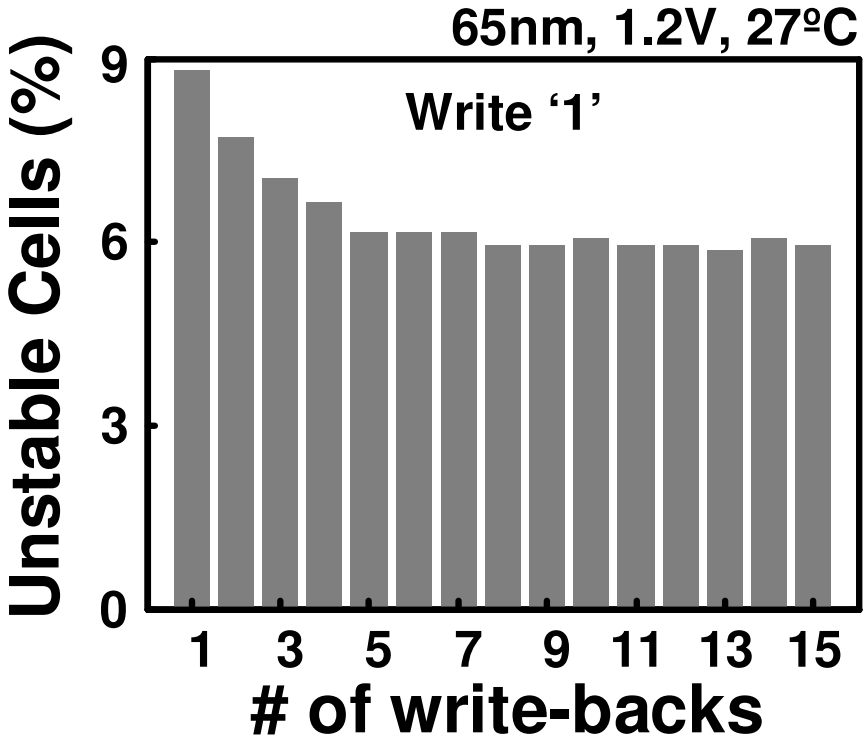
Repetitive Write-back Scheme



- Weak ‘1’ cell tends to be a strong ‘0’ cell, and vice versa
- Repetitive write-back = detect flip in repeated test
  - % of stable cells ↓, % of flip cells ↑, % of unstable cells ↓

Repetitive Write-back Scheme

	No write-backs		10 write-backs	
	W '1'	W '0'	W '1'	W '0'
Always '1'	84.7%	6.5%	81.3%	11.6%
Always '0'	6.5%	86.3%	12.7%	83.2%
Unstable	8.8%	7.2%	6.0%	5.2%

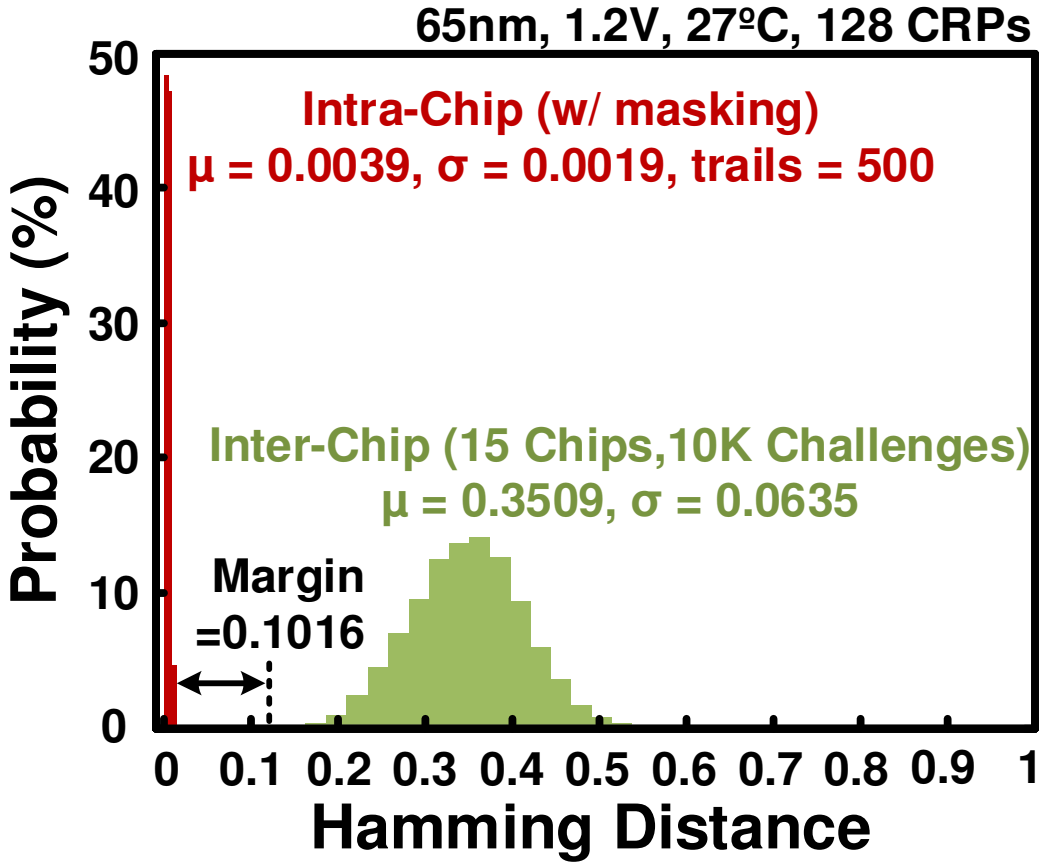


- # of flipped cells increases: better uniqueness
- # of unstable cells decreases: better stability

Agenda

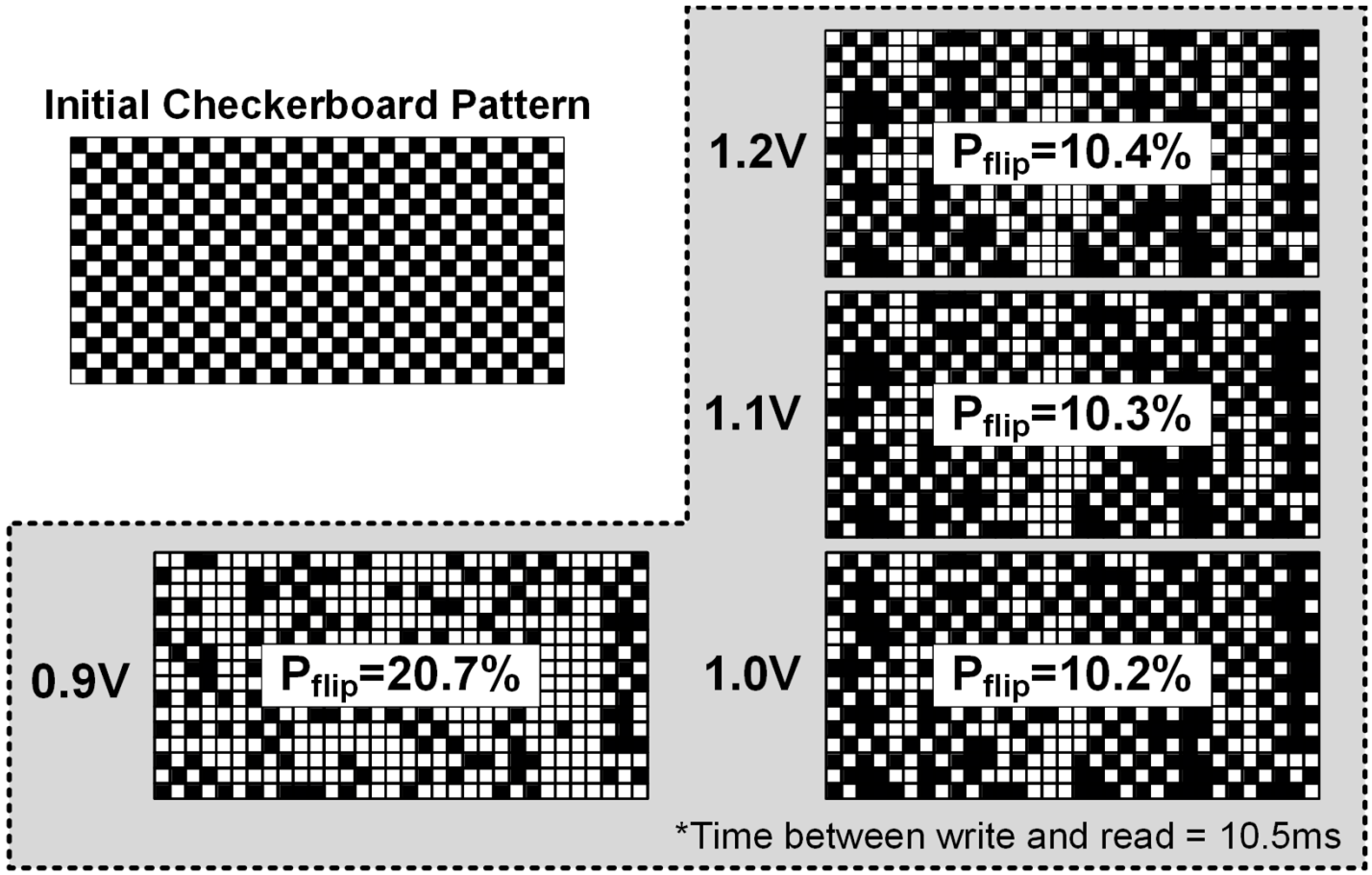
- Background
- Proposed DRAM based Strong PUF
- Enhancing DRAM PUF Uniqueness and Stability
- **Hamming Distance Measurements**
- Summary

Intra- and Inter-chip Hamming Distance



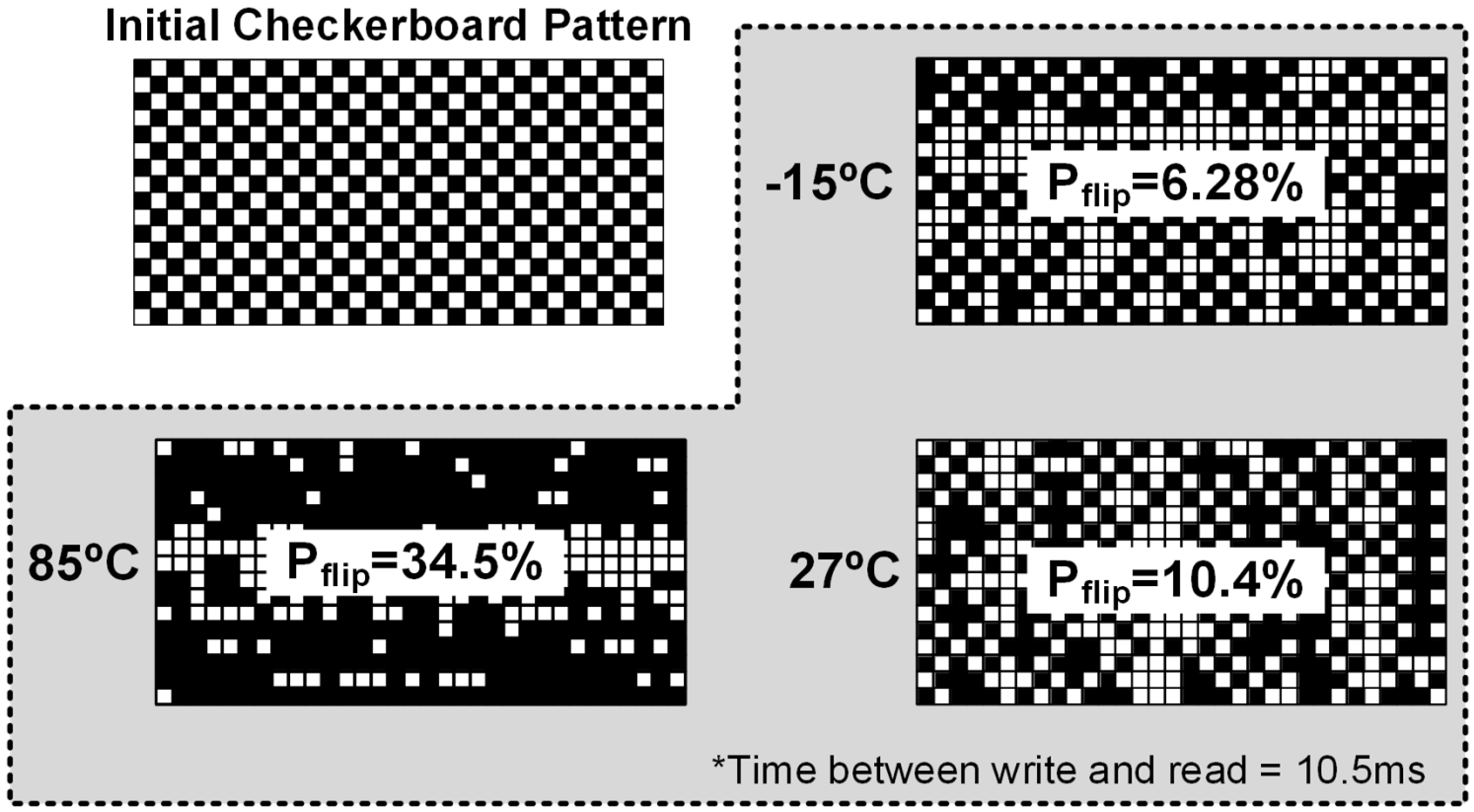
- Inter-chip HD avg ≠ 0.5 due to a flip ratio of 10%
- 0.102 margin → reliable authentication

Retention Map vs. Supply Voltage



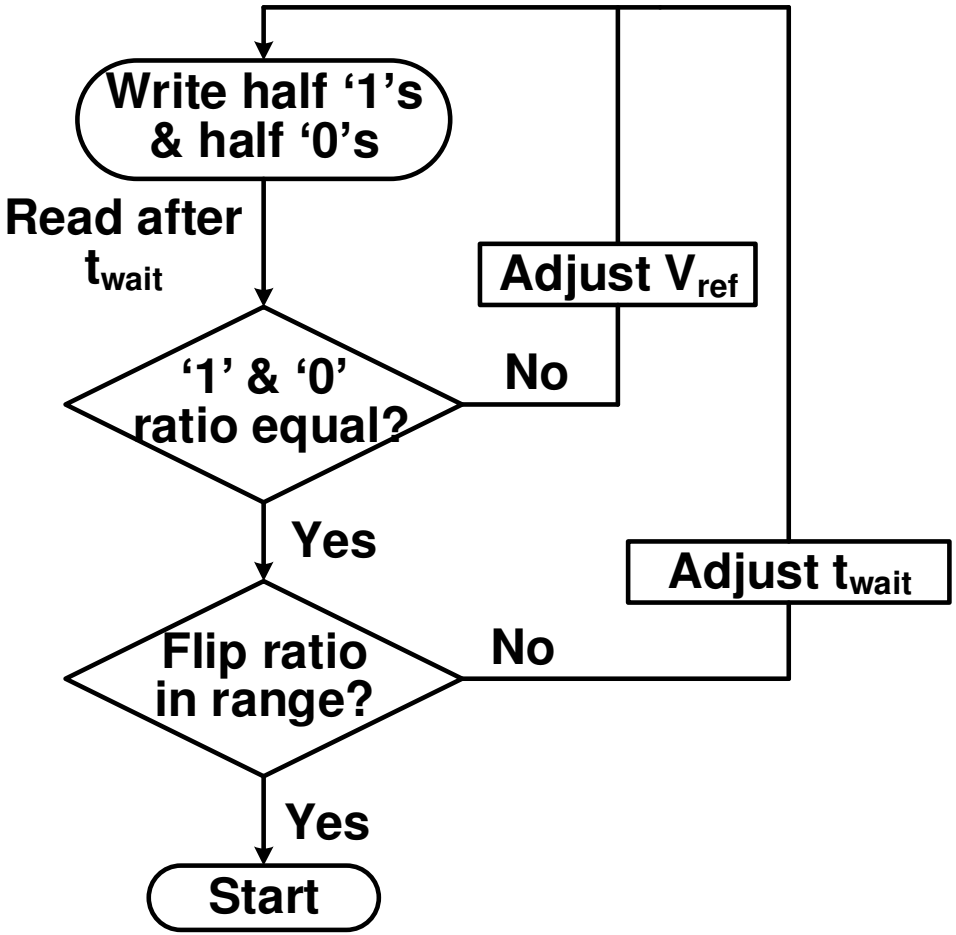
- **Desired flipping probability range: 9%<P_{flip}<11%**

Retention Map vs. Temperature



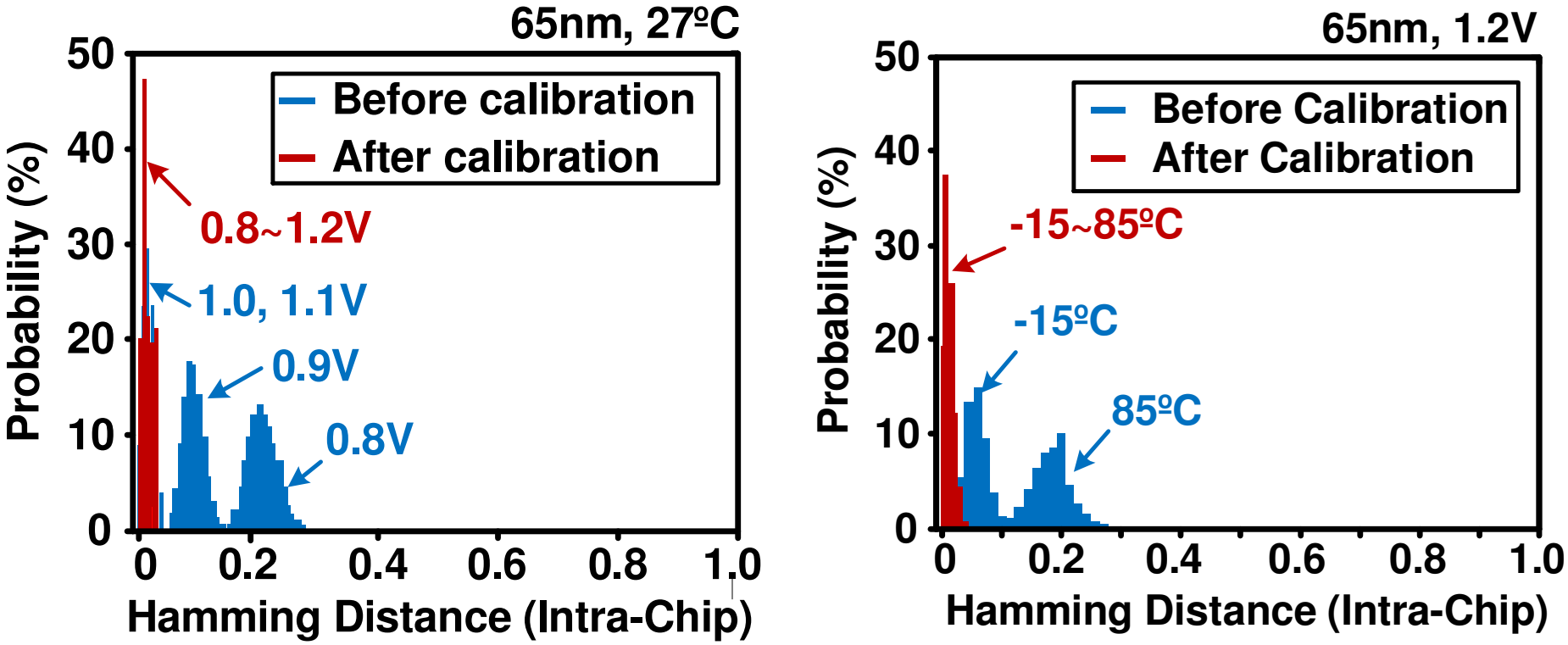
- **Desired flipping probability range: 9%<P_{flip}<11%**

Calibration Flow



- **Target retention failure rate: 9%~11%**
- **Calibration performed before each authentication request**

Intra-chip HD under Different V and T



- μ and σ of the intra-chip Hamming distance distribution are getting smaller after calibration

Summary

- **A 2T DRAM based "Strong" PUF demonstrated in 65nm LP CMOS**
- **Number of CRPs > 10^{32}**
- **A repetitive write-back scheme proposed to enhance PUF uniqueness and stability**
- **A calibration scheme mitigates voltage and temperature effects**

Acknowledgement

- **This work was supported in part by the National Science Foundation under Grant CNS-1441639, and in part by the Semiconductor Research Corporation under Contract 2014-TS-2560.**