清華大學
Tsinghua University

Extending 1kb RRAM Array from Weak PUF to Strong PUF by Employment of SHA Module

Rui Liu[1], Huaqiang Wu[2], Yachuan Pang[2], He Qian[2]
and Shimeng Yu[1]
[1]Arizona State University, AZ, USA
[2]Tsinghua University, Beijing, CN

Email: rliu51@asu.edu

http://faculty.engineering.asu.edu/shimengyu/

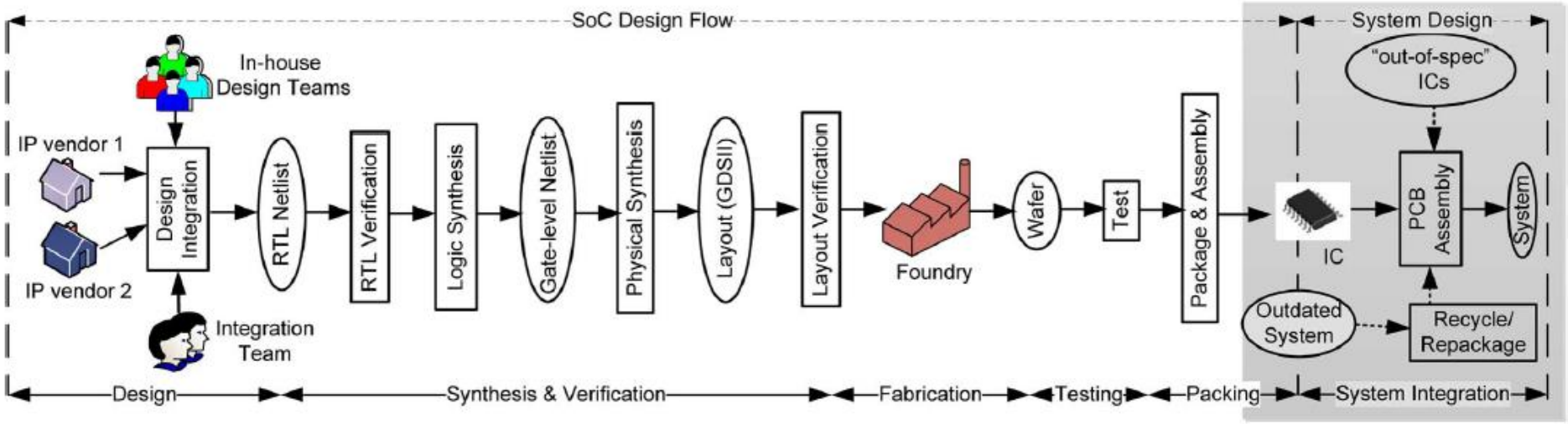
Outline

- **Introduction**
  - Physical Unclonable Function
  - RRAM
- **RRAM PUF Architecture for Authentication**
  - RRAM strong PUF architecture
  - Implementation strategy for PUF
- **Performance Evaluation on 1kb RRAM arrays**
  - PUF Performance Metric
  - Uniqueness, Uniformity, Diffuseness and Reproducibility
- **Machine Learning Attack Evaluation**
- **Conclusion**

Outline

- **Introduction**
  - Physical Unclonable Function
  - RRAM
- **RRAM PUF Architecture for Authentication**
  - RRAM strong PUF architecture
  - Implementation strategy for PUF
- **Performance Evaluation on 1kb RRAM arrays**
  - PUF Performance Metric
  - Uniqueness, Uniformity, Diffuseness and Reproducibility
- **Machine Learning Attack Evaluation**
- **Conclusion**

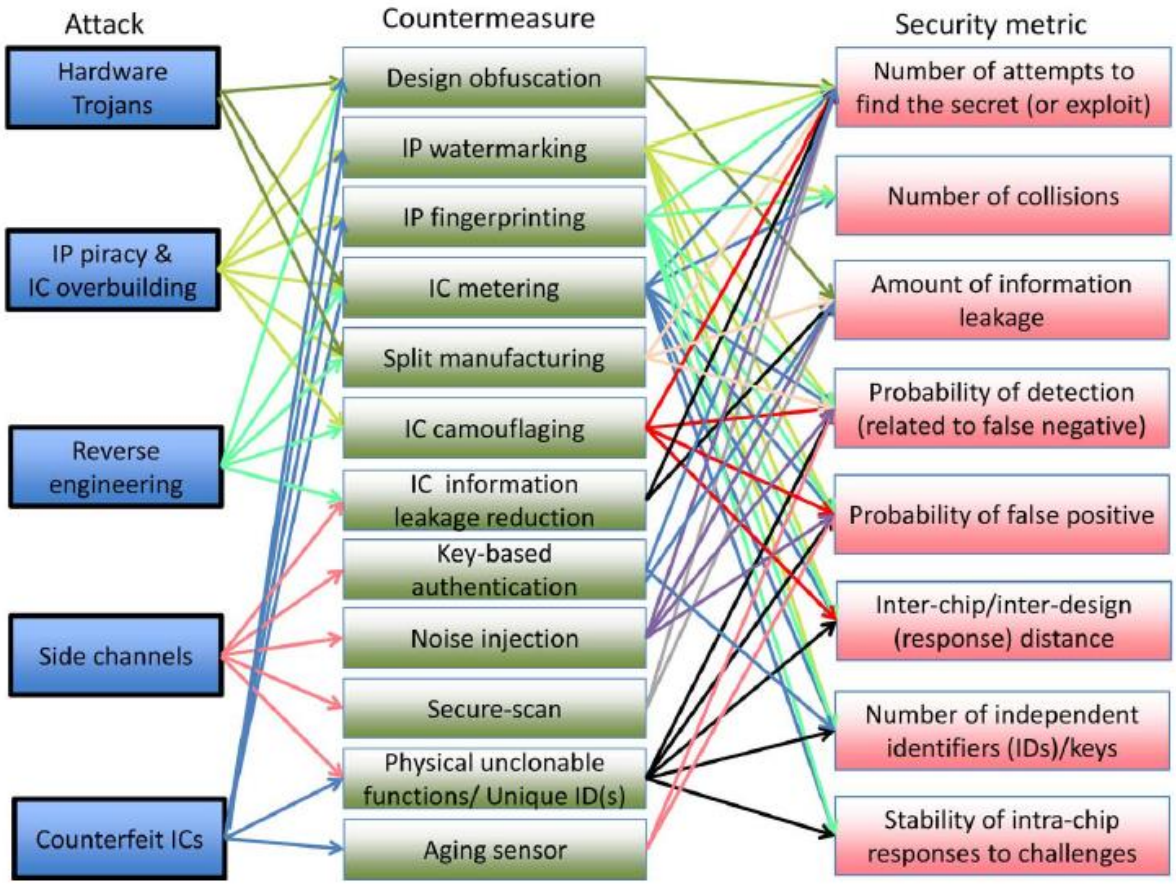
Semiconductor supply chain: IC design flow



Global trends in IC design, manufacturing, and distribution → **emerging hardware security problems** ↑

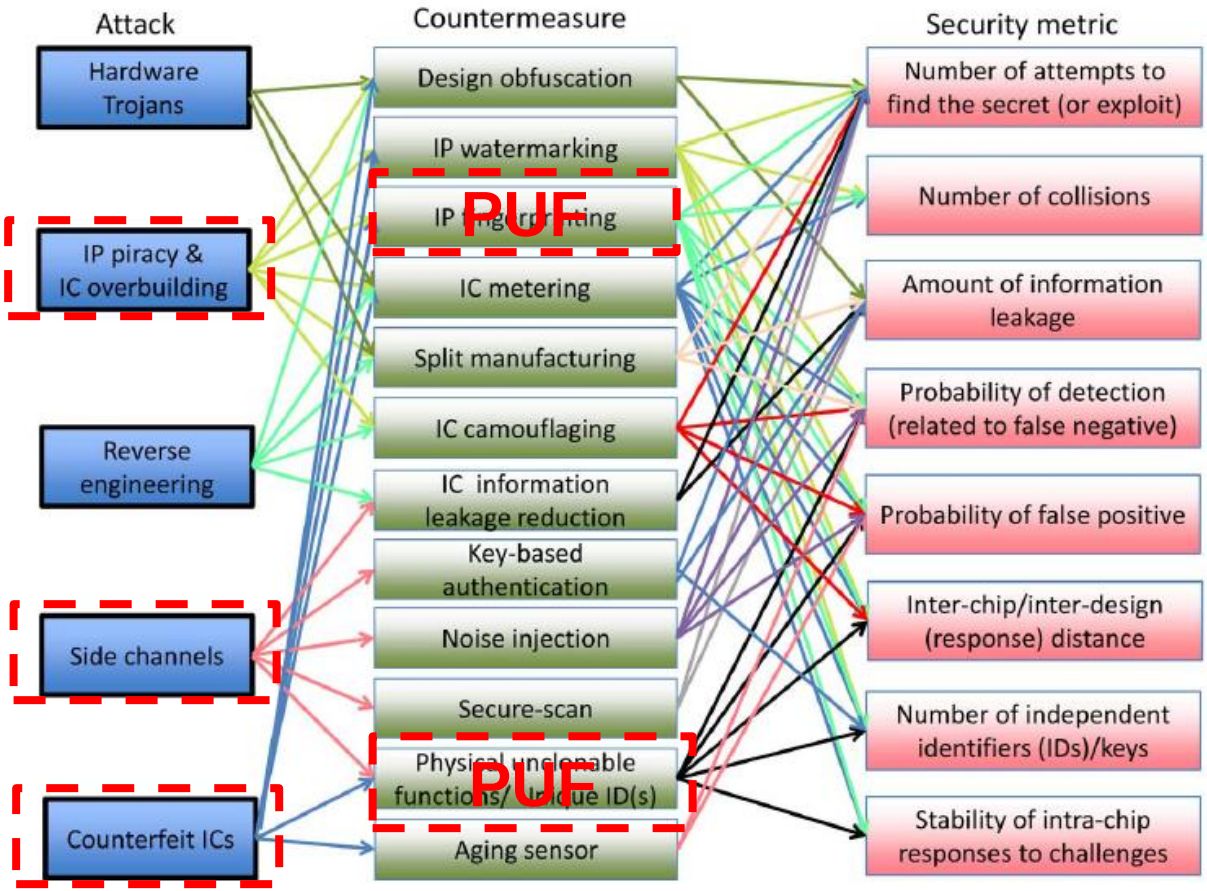
M. Rostami *et al*, IEEE Proc. Aug 2014

Hardware-based Threat in IC Supply Chain



M. Rostami *et al*, IEEE Proc. Aug 2014

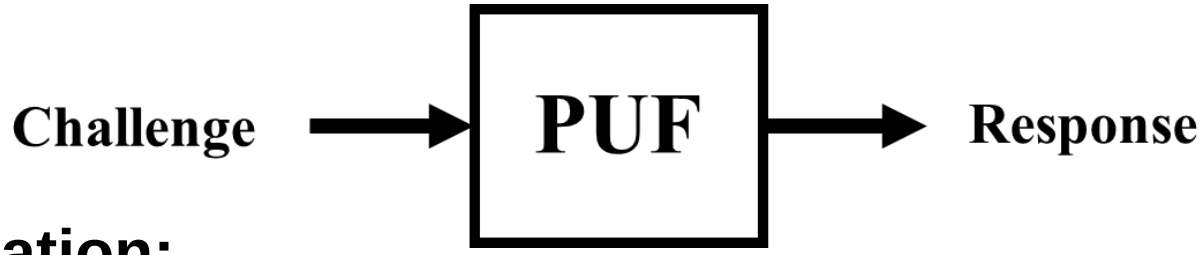
Hardware-based Threat in IC Supply Chain



M. Rostami *et al*, IEEE Proc. Aug 2014

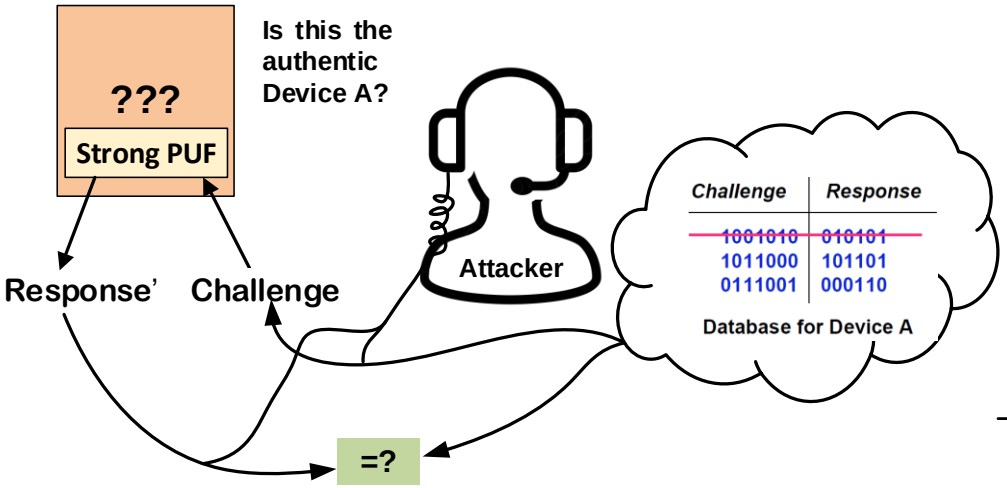
Physical Unclonable Function (PUF)

PUF: map a set of challenges to a set of responses based on an **intractably** complex **physical** system.

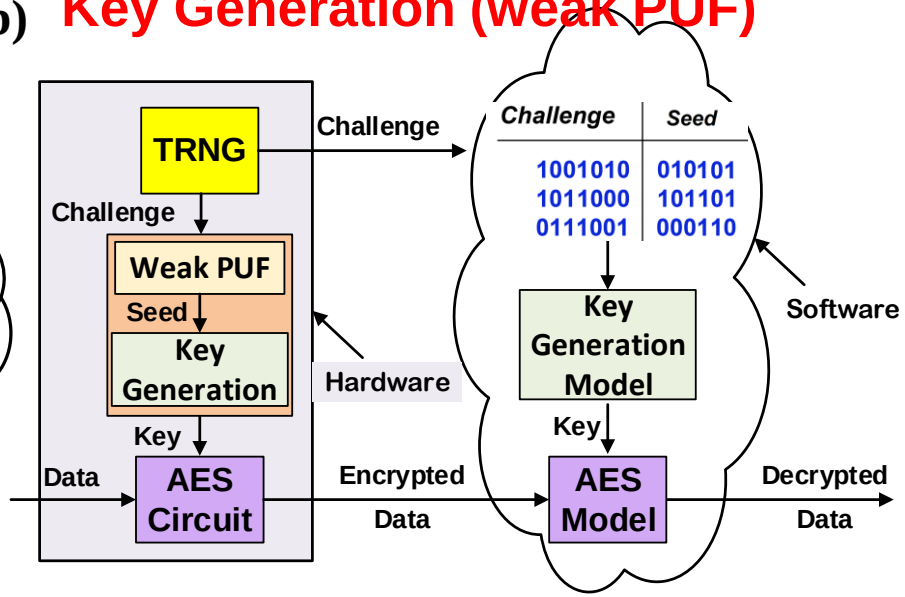


Application:

(a) Authentication (strong PUF)



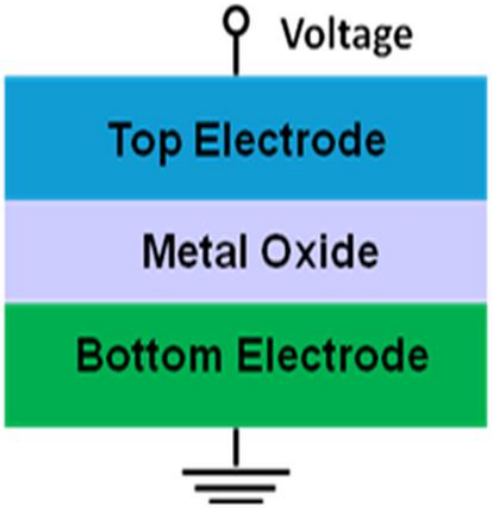
(b) Key Generation (weak PUF)



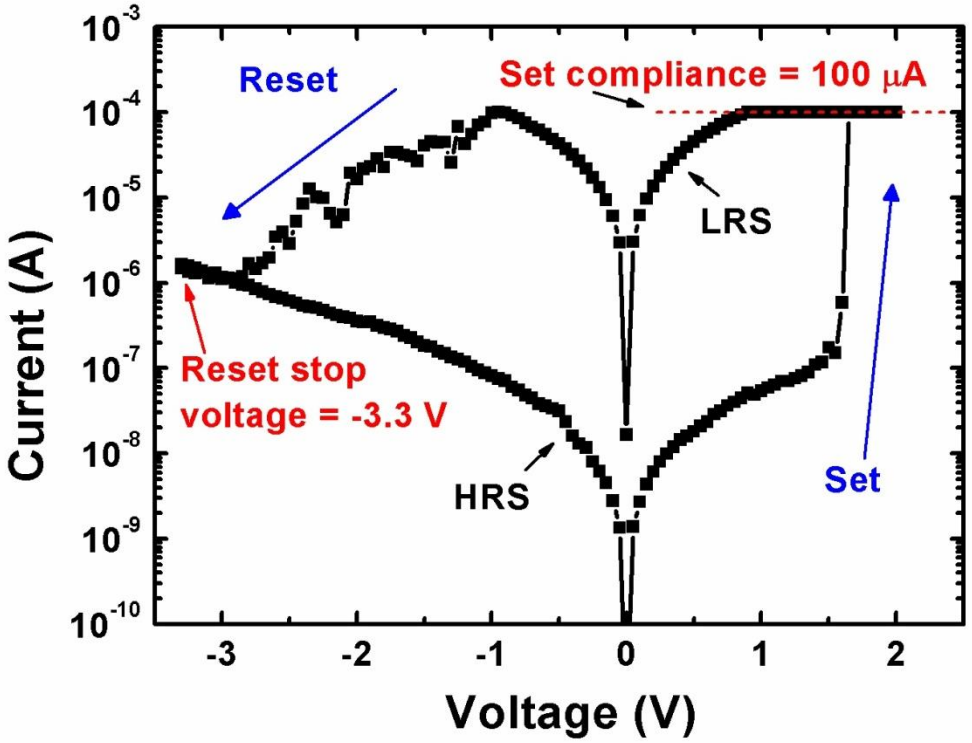
PUF Implementations

- Complex physical systems (non-electronic or analog)
  - Optical PUF: Complex interaction of light with scatter particles
  - Coating PUF: Random capacitance of dielectric coating on IC
  - Power distribution PUF: resistance variation in chip power-grid
- Digital IC PUFs (utilize manufacturing variability)
  - Based on signal delay variability
    - Arbiter PUF: signal delay difference determined by an arbiter
    - Feed-forward arbiter PUF: add nonlinearity in arbiter PUF
    - Ring oscillator PUF: variability in RO frequencies
  - Based on unstable states in cross-coupled gates
    - SRAM PUF: startup state of SRAM during power-up
    - Butterfly PUF: cross-coupled latches in "clear/preset"
    - Latch PUF: cross-coupled NOR gates in "reset"
    - Flip-flop PUF: power-up behavior of flip-flops
- Nonvolatile Memory (NVM) PUFs (variability in manufacturing and mechanisms; potentially reconfigurable)
  - Phase change memory (PCM)
  - Spin-transfer-torque random-access-memory (STTRAM)
  - Resistive random-access-memory (RRAM)

Oxide RRAM Basics

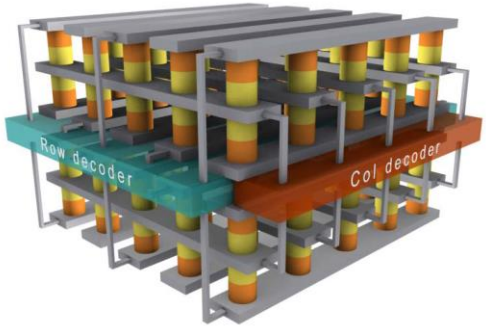


Typical Bipolar I-V Curve

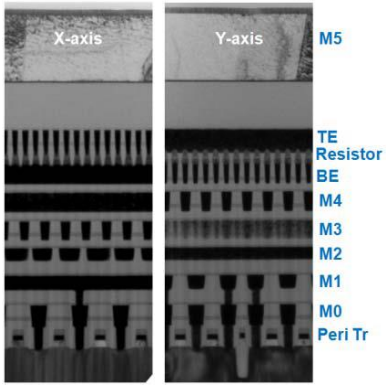


- ❑ **“0” : High Resistance State (HRS)**
- ❑ **“1” : Low Resistance State (LRS)**
- ❑ **HRS→LRS: SET**
- ❑ **LRS→HRS: RESET**

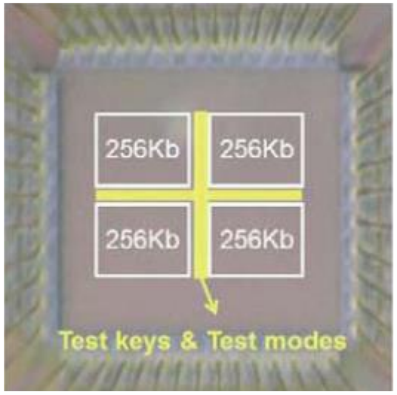
RRAM's Industry R&D



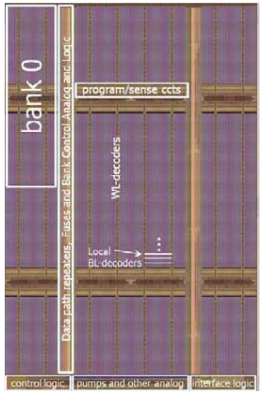
Samsung



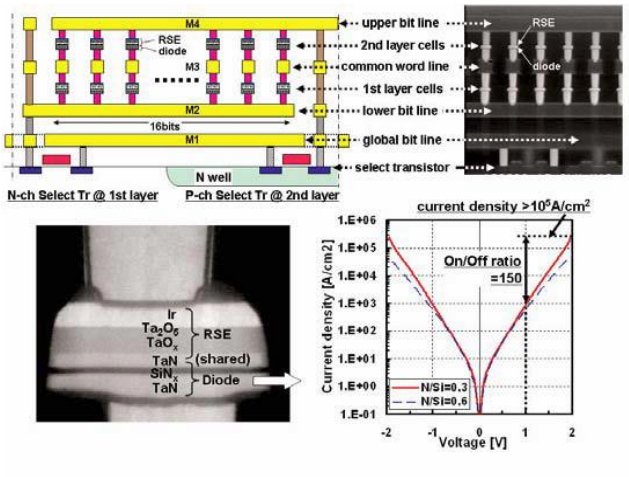
HP & Hynix



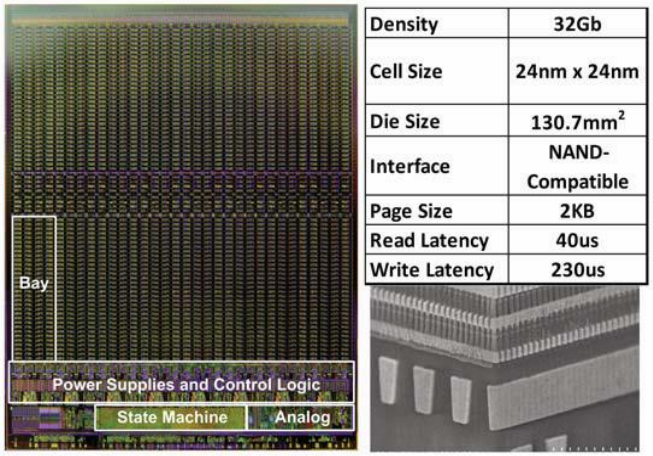
TSMC



Micron & Sony

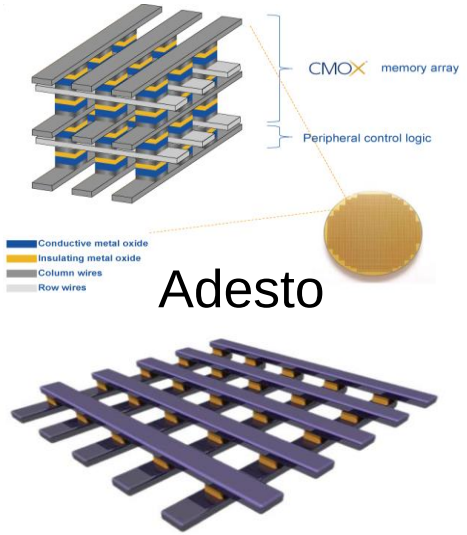


Panasonic



Density	32Gb
Cell Size	24nm x 24nm
Die Size	130.7mm^2
Interface	NAND-Compatible
Page Size	2KB
Read Latency	40us
Write Latency	230us

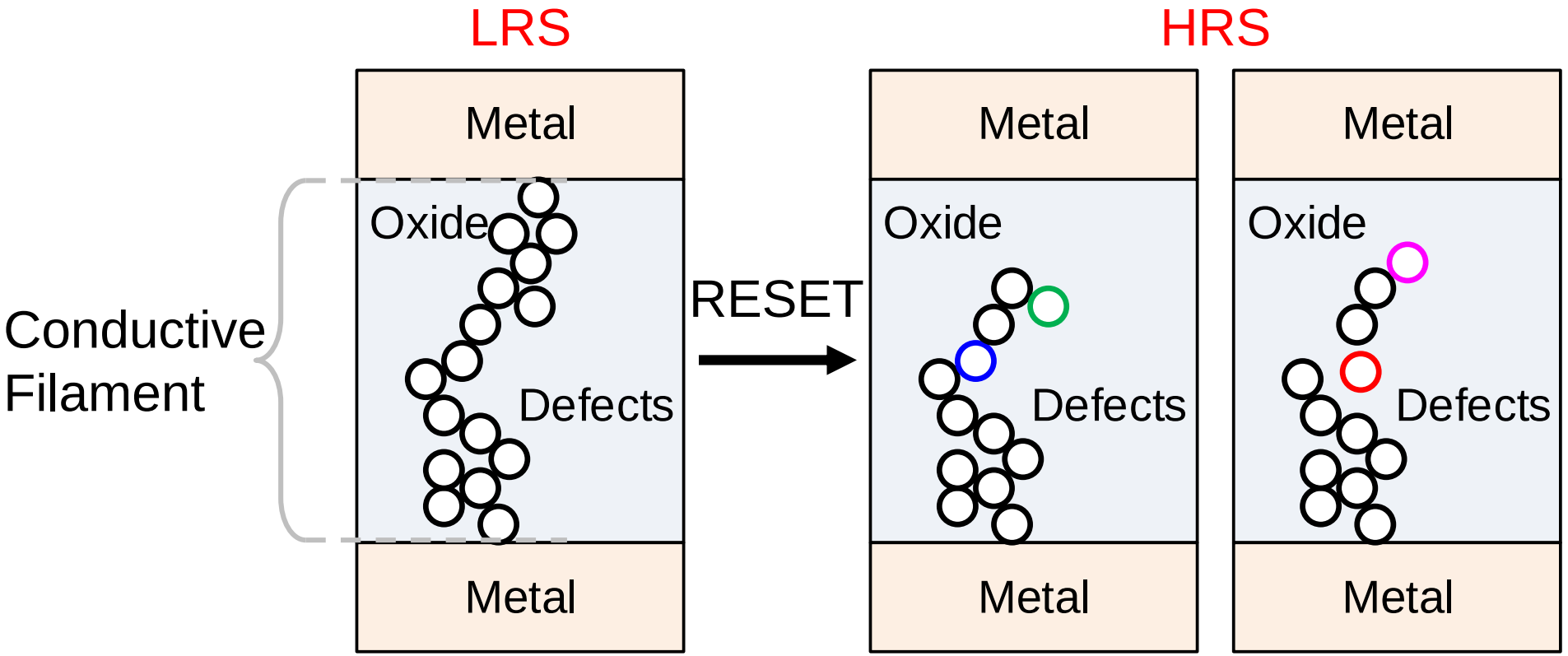
Toshiba & Sandisk



Adesto

The Randomness in RRAM

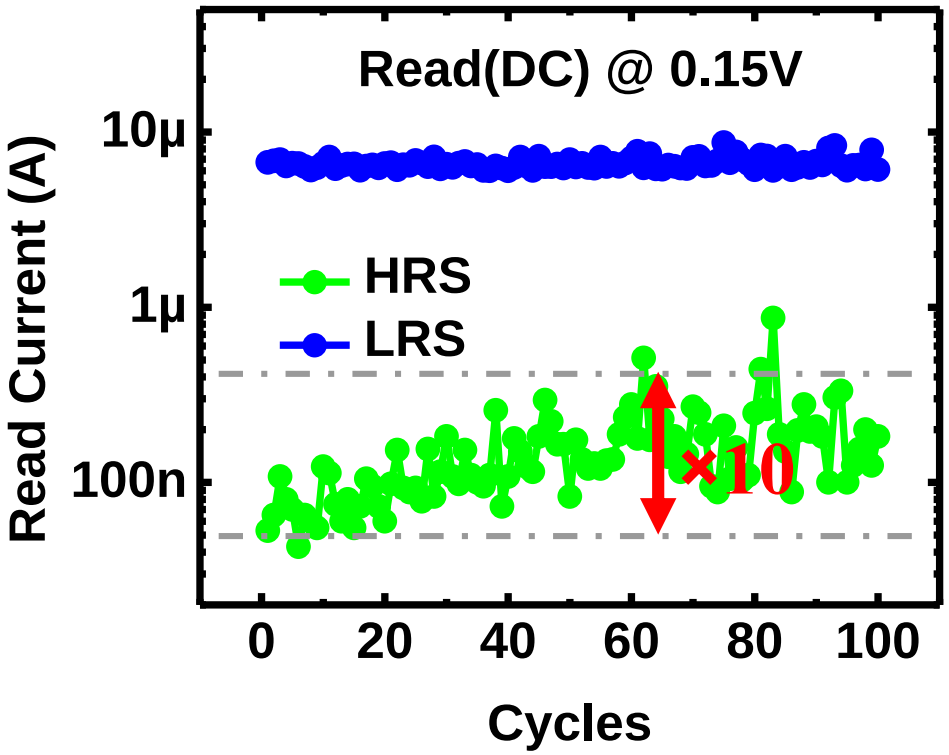
- **A small change in defect location significantly changes the resistance due to electron tunneling mechanism in HRS**



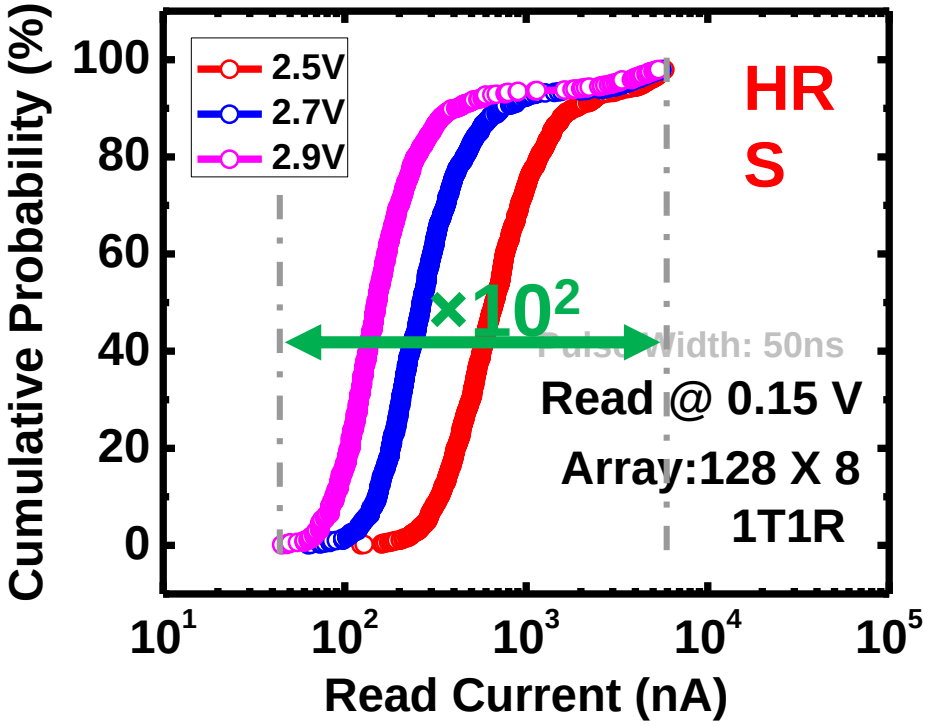
RRAM Variability

RRAM device: TiN/TaOx/HfO_2/TiN

Cycle 2 Cycle (Configurable)



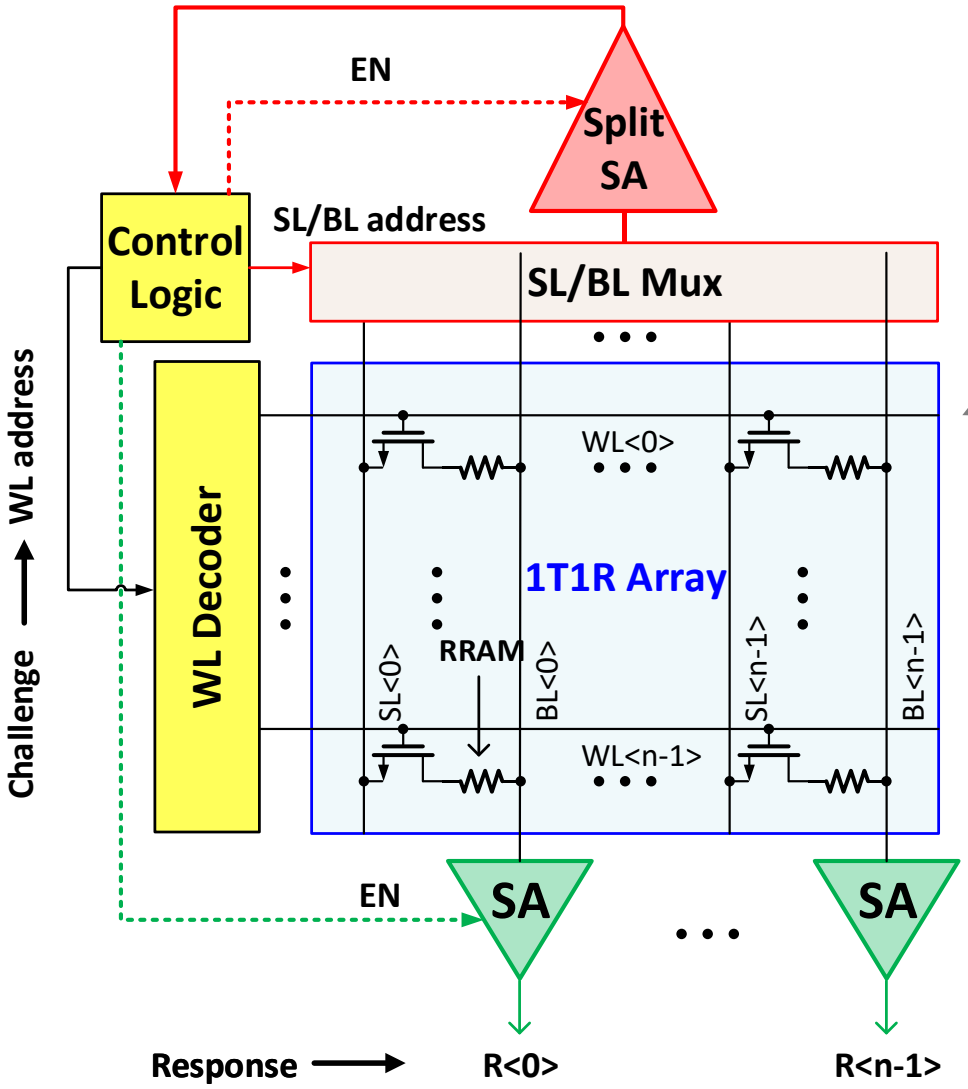
Device 2 Device



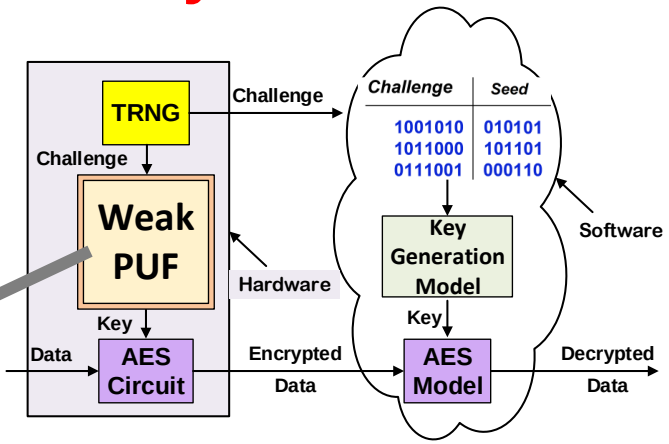
Outline

- **Introduction**
  - Physical Unclonable Function
  - RRAM
- **RRAM PUF Architecture for Authentication**
  - RRAM strong PUF architecture
  - Implementation strategy for PUF
- **Performance Evaluation on 1kb RRAM arrays**
  - PUF Performance Metric
  - Uniqueness, Uniformity, Diffuseness and Reproducibility
- **Machine Learning Attack Evaluation**
- **Conclusion**

RRAM weak PUF Architecture



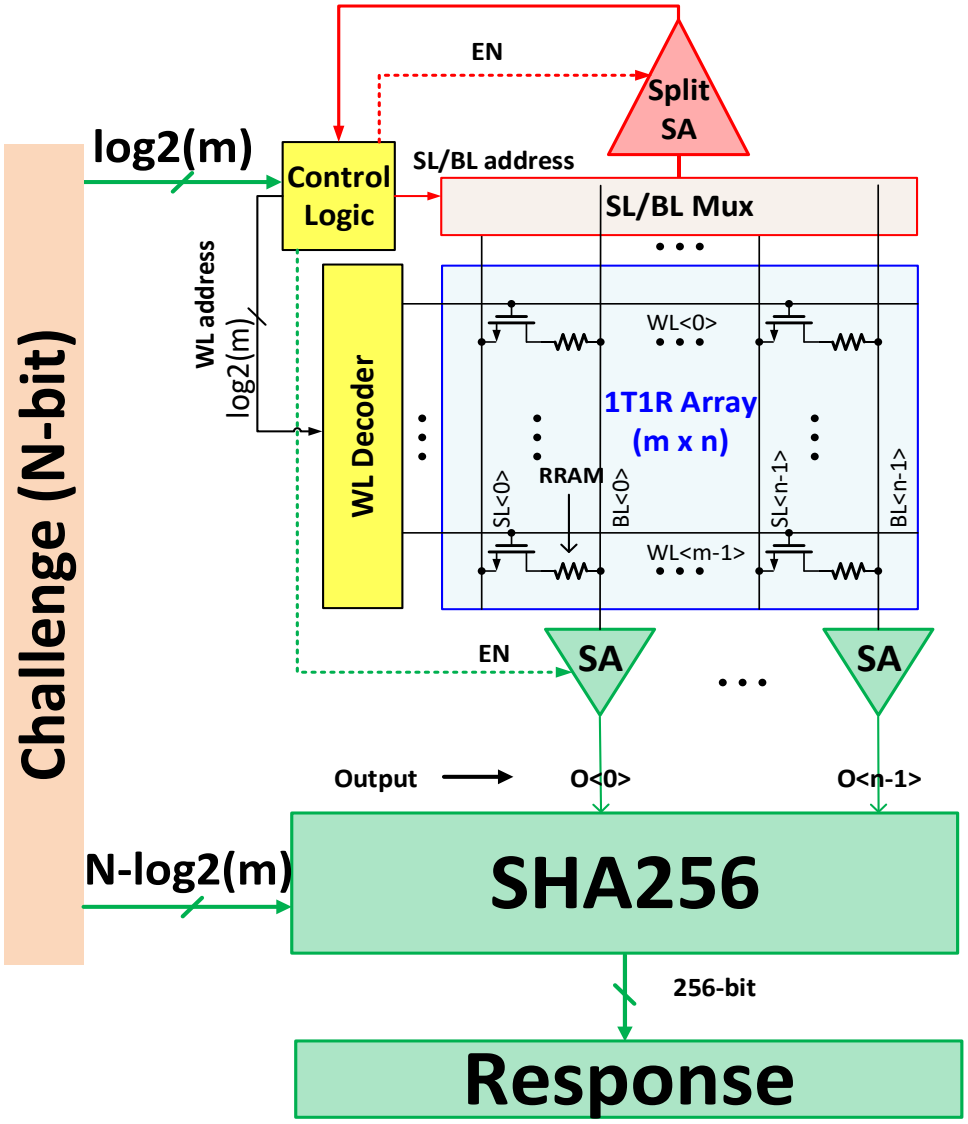
Key Generation



1. Each RRAM cell generates one response bit.
2. CRP space is limited by RRAM capacity.

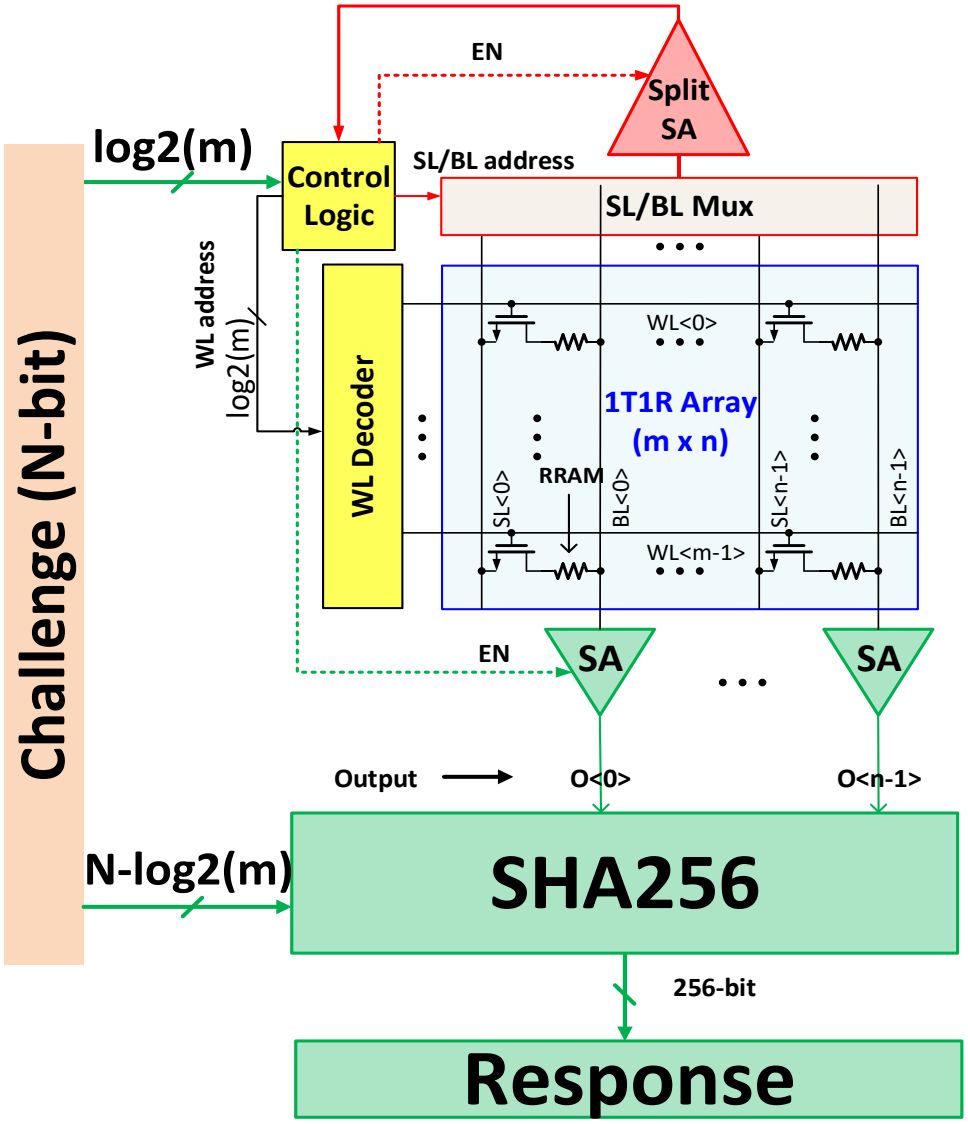
R. Liu *et al*, IEEE EDL 2015

RRAM PUF Architecture for Authentication



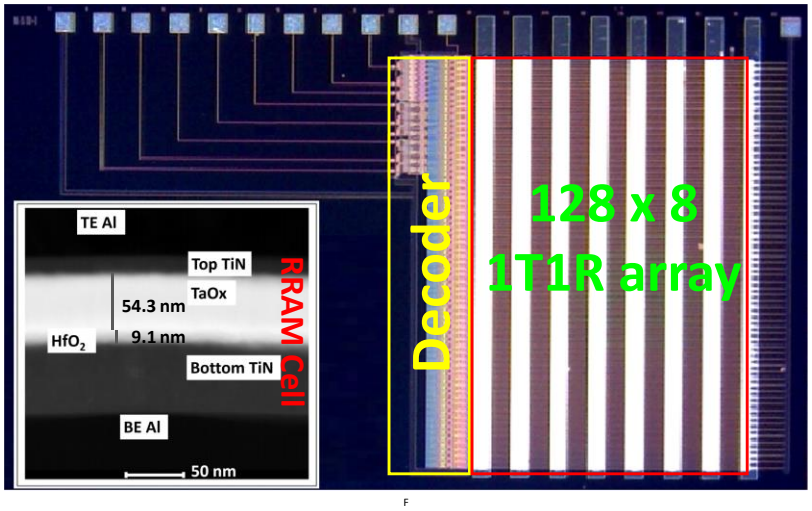
1. Embed the RRAM array with SHA engine to increase the CRP space.
   - RRAM array (entropy source)
   - SHA engine (large CRP)
2. Challenge vector is split into two segments.

RRAM PUF Architecture for Authentication



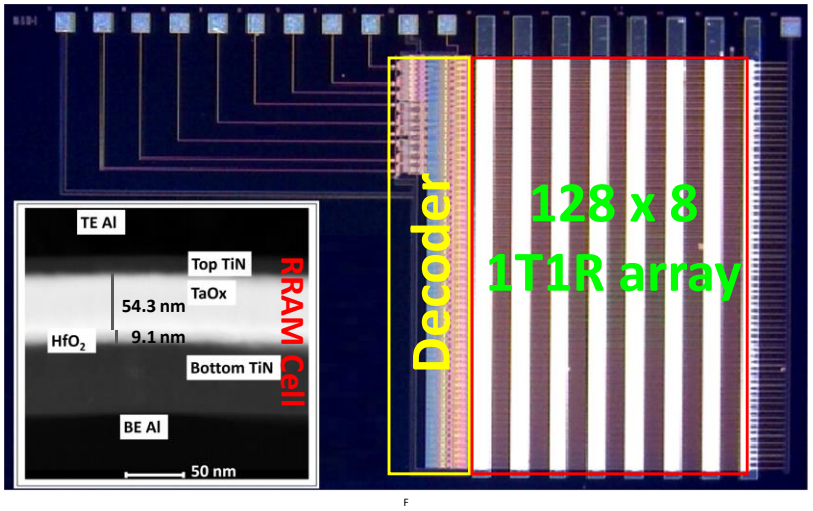
- **The red parts are designed only for construction phase (preparation phase)**
- **The green parts are designed only for operation phase (evaluation phase)**

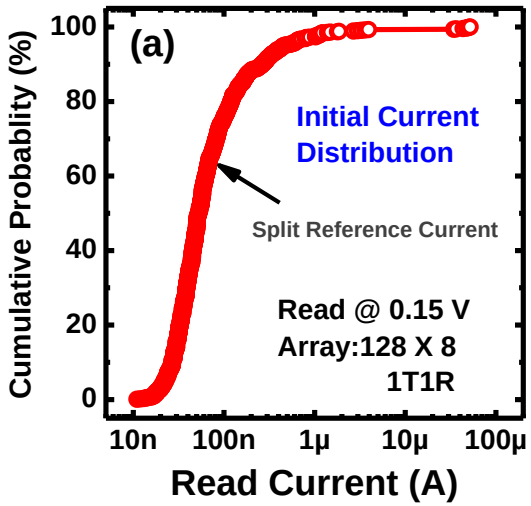
Implementation Strategy for PUF



1) form all the cells to LRS

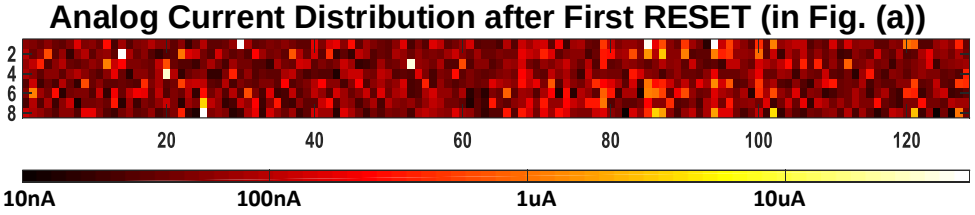
Implementation Strategy for PUF



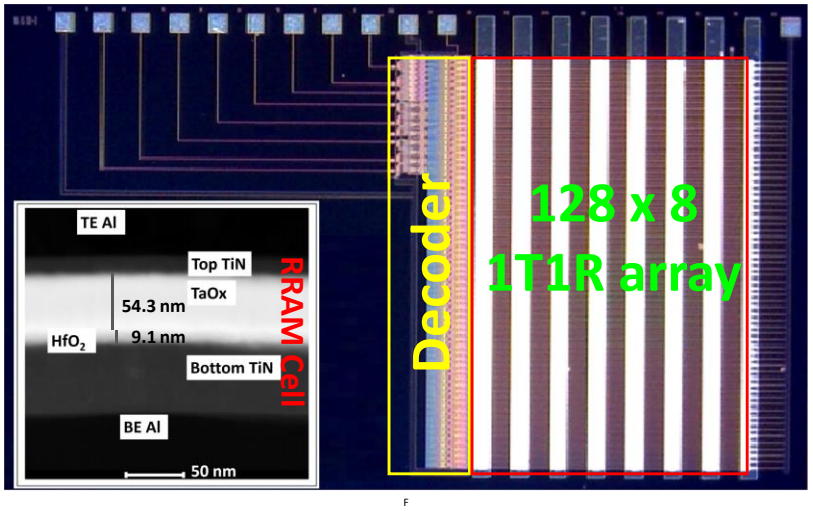


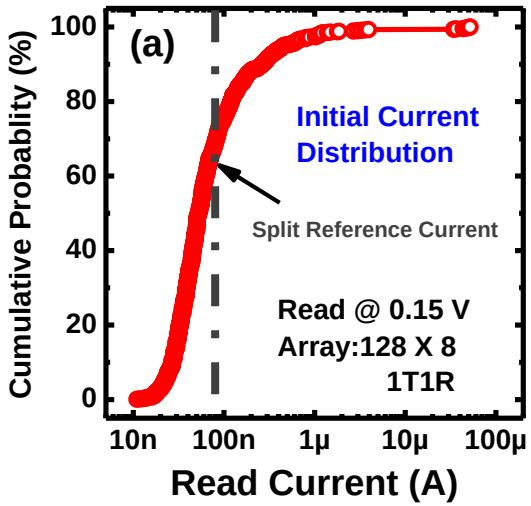
1) form all the cells to LRS
2) RESET all the cells to HRS (entropy source)
3) Read out the current

(c)



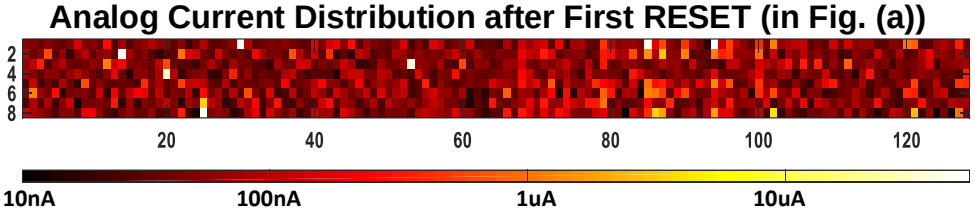
Implementation Strategy for PUF



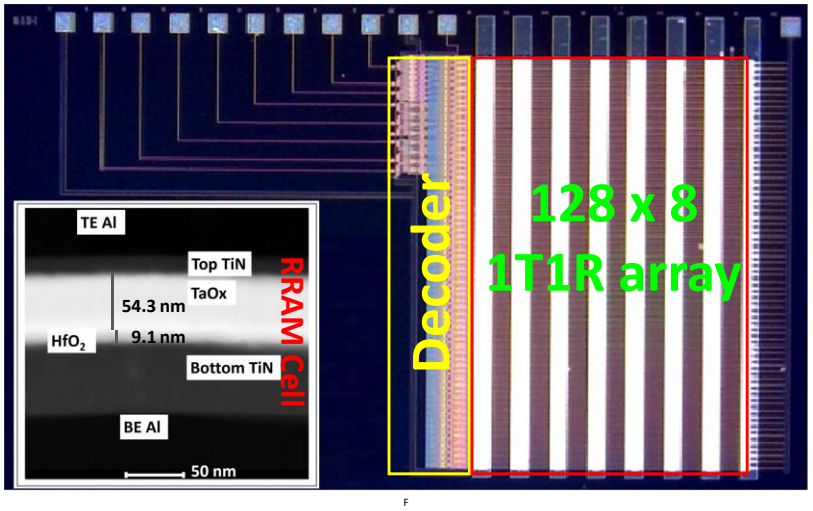


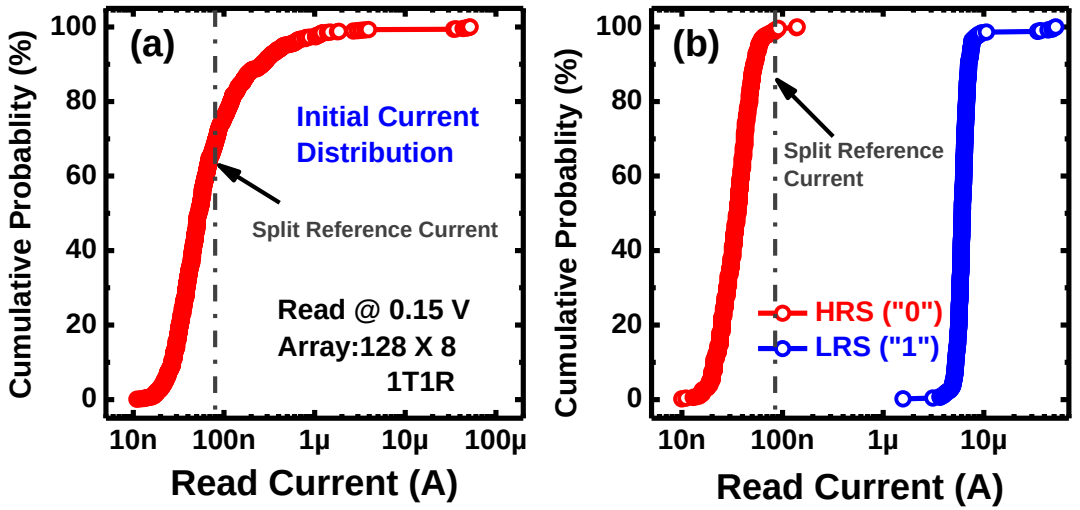
1) form all the cells to LRS
2) RESET all the cells to HRS (entropy source)
3) Read out the current
4) Find a split reference within the read current distribution

(c)

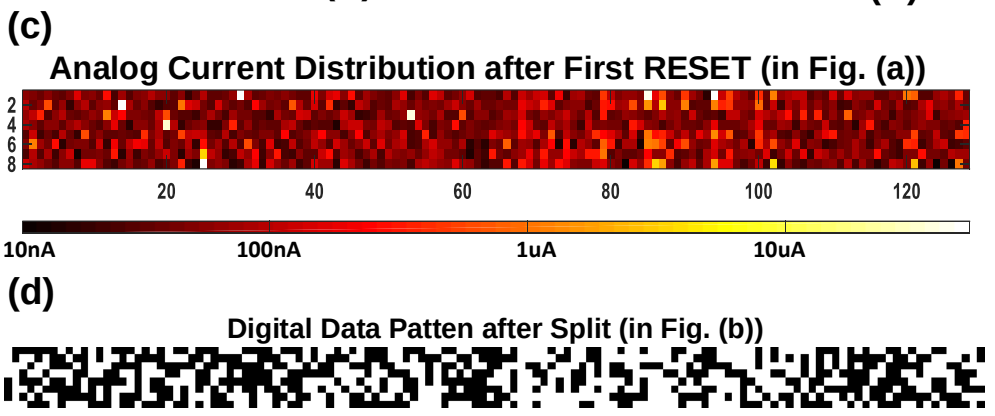


Implementation Strategy for PUF





1) form all the cells to LRS
2) RESET all the cells to HRS (entropy source)
3) Read out the current
4) Find a split reference within the read current distribution
5) Digitize the randomness according to the reference [1]



[1] W. Chen, et al, *ICCAD*, 2014

Outline

- **Introduction**
  - Physical Unclonable Function
  - RRAM
- **RRAM PUF Architecture for Authentication**
  - RRAM strong PUF architecture
  - Implementation strategy for PUF
- **Performance Evaluation on 1kb RRAM arrays**
  - PUF Performance Metric
  - Uniqueness, Uniformity, Diffuseness and Reproducibility
- **Machine Learning Attack Evaluation**
- **Conclusion**

PUF Performance Metrics

Uniqueness means that the responses evaluated from evaluating the same challenge **on different PUF instances** should not be similar (Inter-Hamming Distance, ideally 50%).

A. Chen *et al*, IEEE EDL Feb 2015

PUF Performance Metrics

Uniqueness means that the responses evaluated from evaluating the same challenge **on different PUF instances** should not be similar (Inter-Hamming Distance, ideally 50%).

Uniformity is an indicator of the percentage of ‘1’ and ‘0’ in the response vector (ideally 50%).

A. Chen *et al*, IEEE EDL Feb 2015

PUF Performance Metrics

Uniqueness means that the responses evaluated from evaluating the same challenge **on different PUF instances** should not be similar (Inter-Hamming Distance, ideally 50%).

Uniformity is an indicator of the percentage of '1' and '0' in the response vector (ideally 50%).

Diffuseness means the average hamming distances for all the possible responses generated by the **same PUF instance** for different challenges (ideally 50%).

A. Chen *et al*, IEEE EDL Feb 2015

PUF Performance Metrics

Uniqueness means that the responses evaluated from evaluating the same challenge **on different PUF instances** should not be similar (Inter-Hamming Distance, ideally 50%).

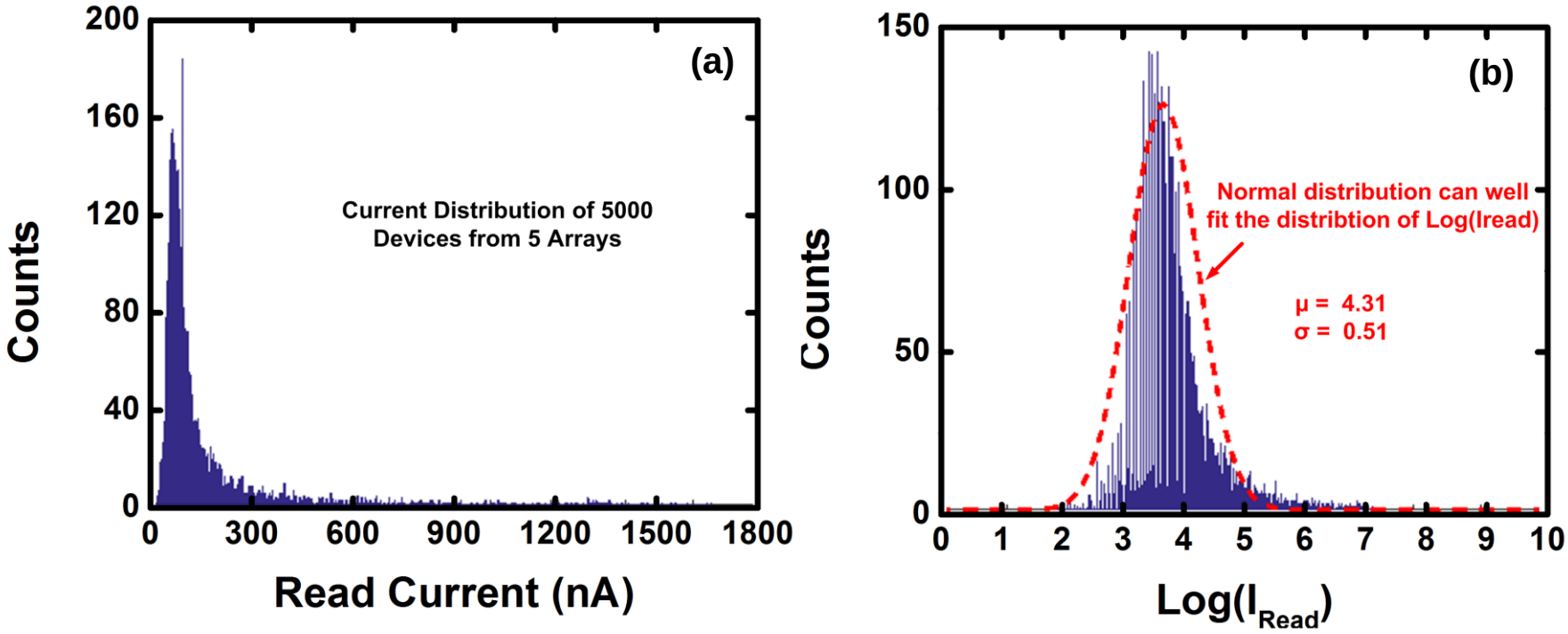
Uniformity is an indicator of the percentage of '1' and '0' in the response vector (ideally 50%).

Diffuseness means the average hamming distances for all the possible responses generated by the **same PUF instance** for different challenges (ideally 50%).

Reliability is a metric to assess the similarity of the responses resulting from evaluating the **same challenge** on the **same PUF instance** under **different circumstances**, (Intra-Hamming Distance, ideally 0%).

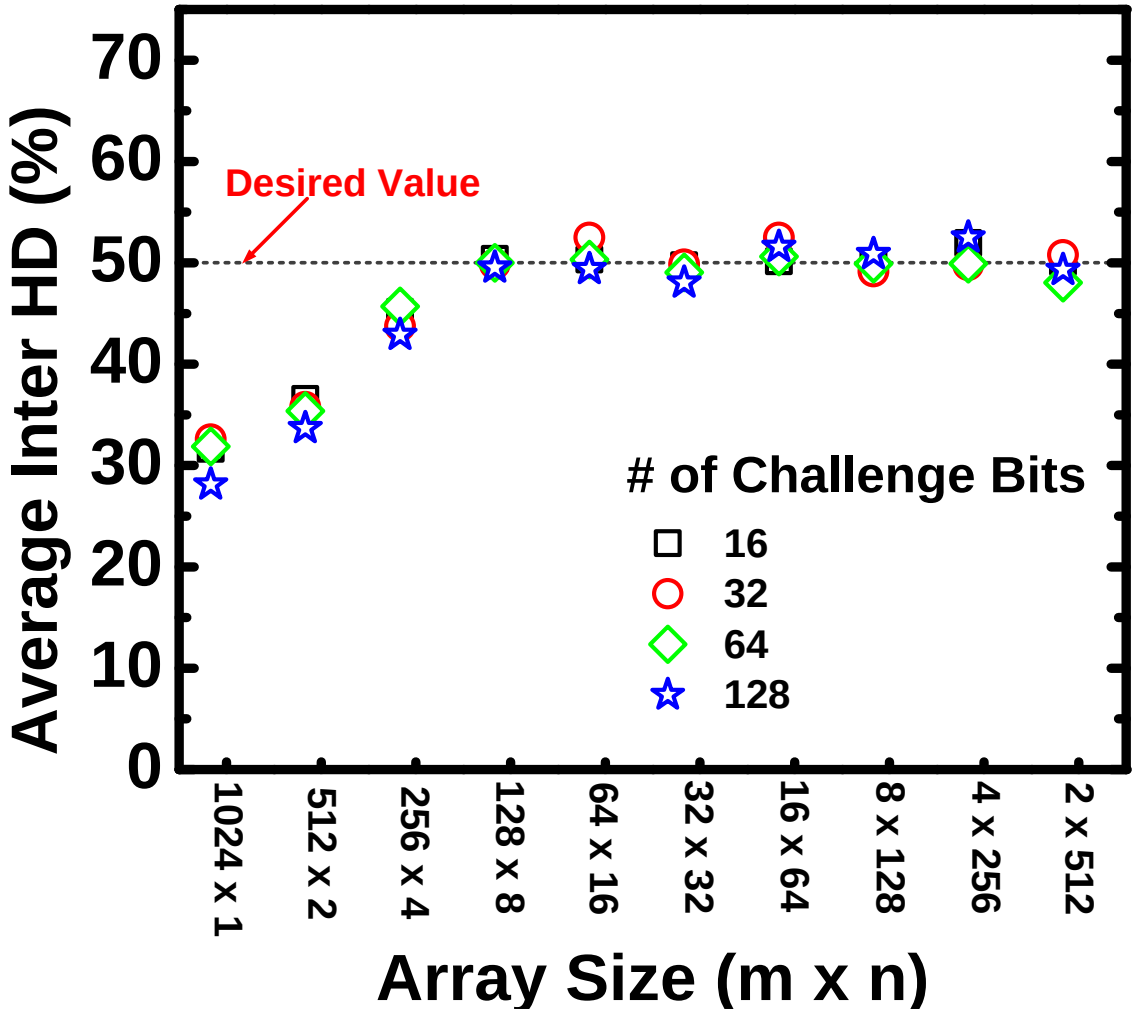
A. Chen *et al*, IEEE EDL Feb 2015

Distribution of Read Current of 5 1kb RRAM Arrays

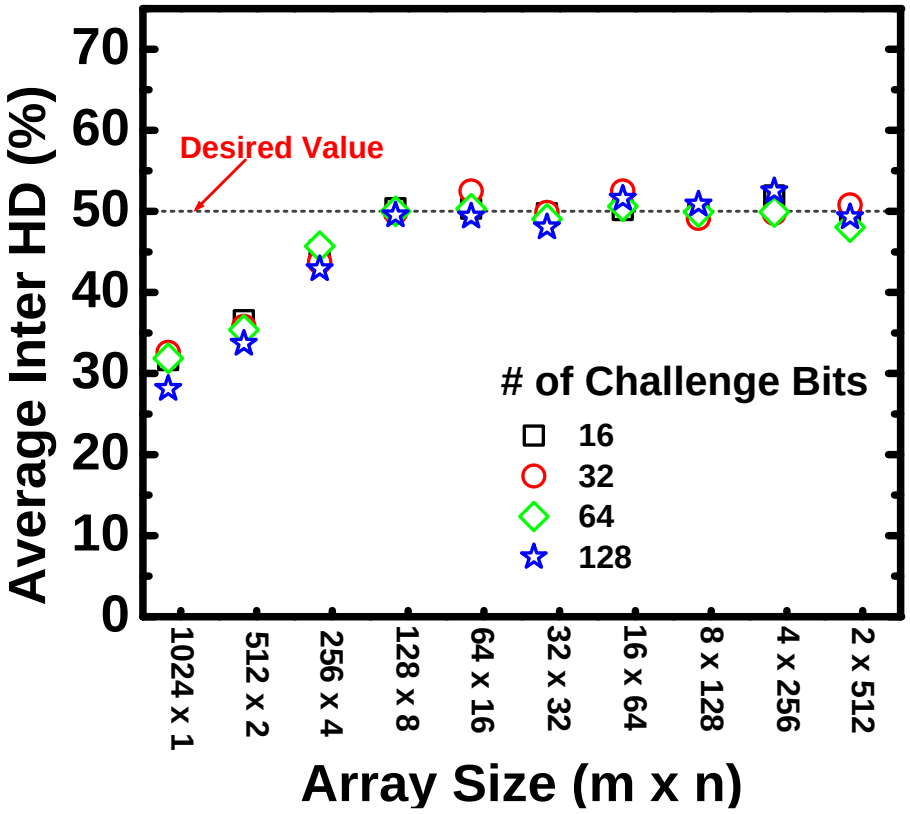


The probability density function (PDF) is used to randomly generate the data pattern of the other 95 1 kb arrays.

Uniqueness

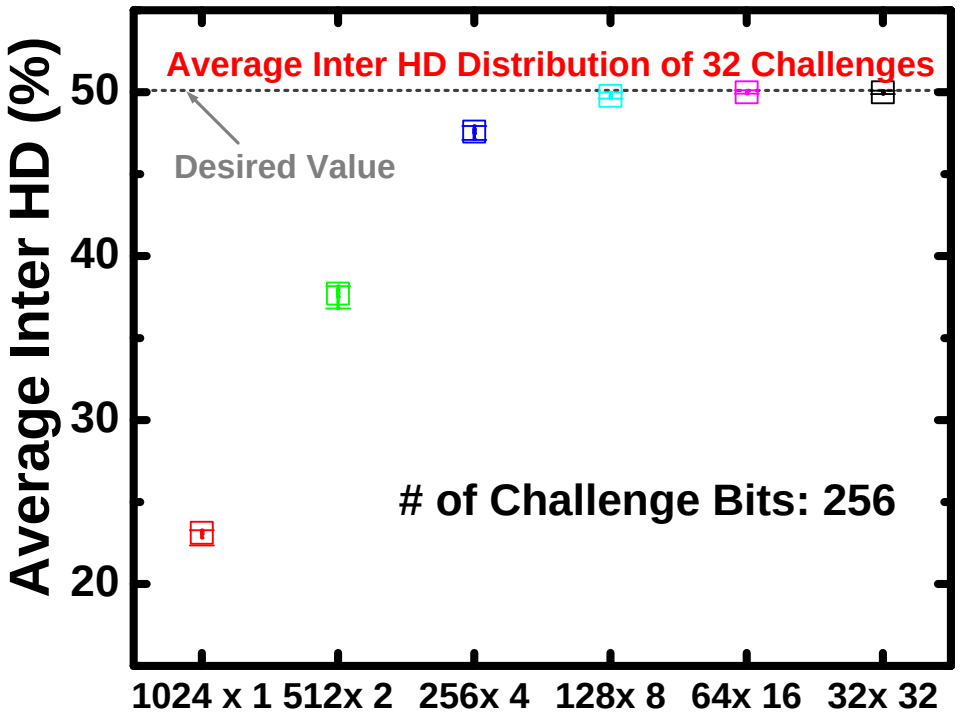

Average Inter HD (%)
70
60
50
40
30
20
10
0
Desired Value
# of Challenge Bits
16
32
64
128
1024 x 1
512 x 2
256 x 4
128 x 8
64 x 16
32 x 32
16 x 64
8 x 128
4 x 256
2 x 512
Array Size (m x n)

Uniqueness



- **To achieve good uniqueness, RRAM outputs > 8 bits**
- **The length of challenge vector shows negligible effect, which means the CRP space can be increased by increasing the length of challenge vector**

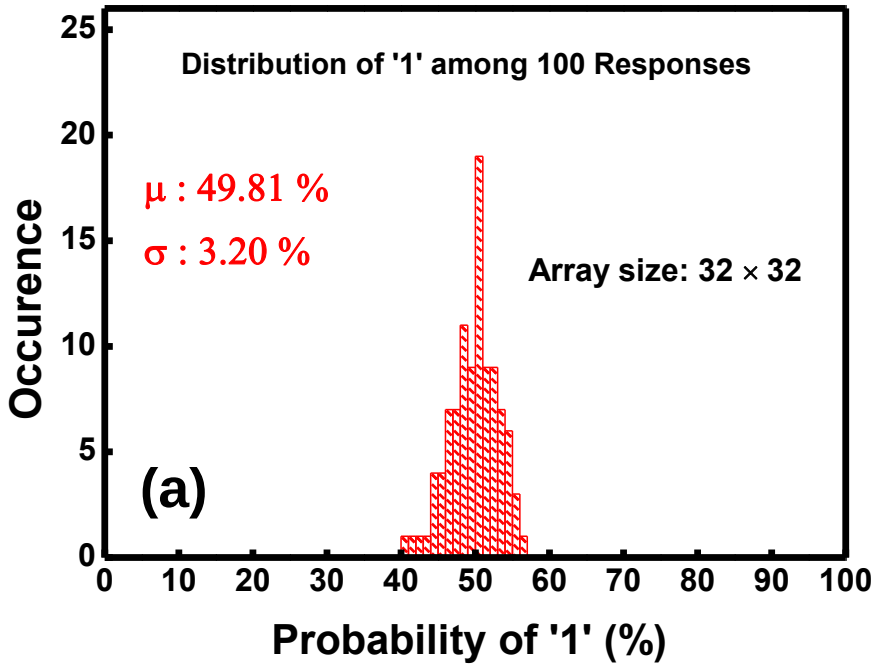
Uniqueness



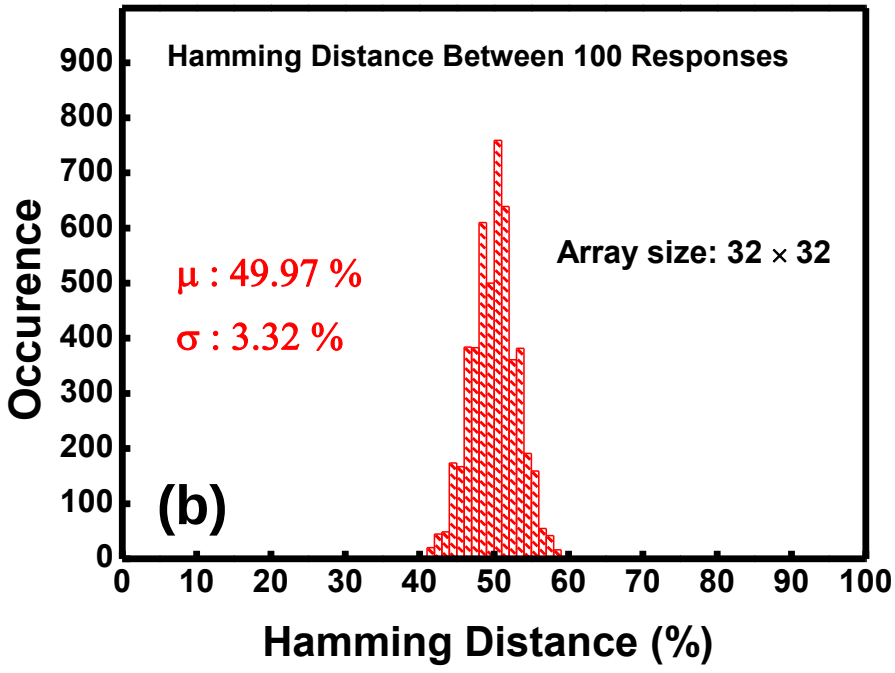
In practical, the attacker may try to obtain the secret bits from RRAM cells with brute-force computing. With more bits from RRAM array,
e.g. if the RRAM outputs is 32-bit, it needs to compute ~1.4 × 10^{11} times to reveal all the RRAM content for a 1kb RRAM.

Uniformity and Diffuseness

Uniformity

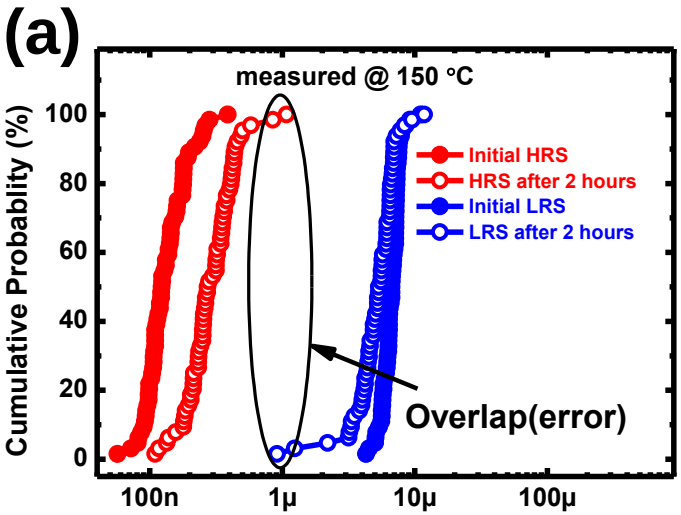


Diffuseness

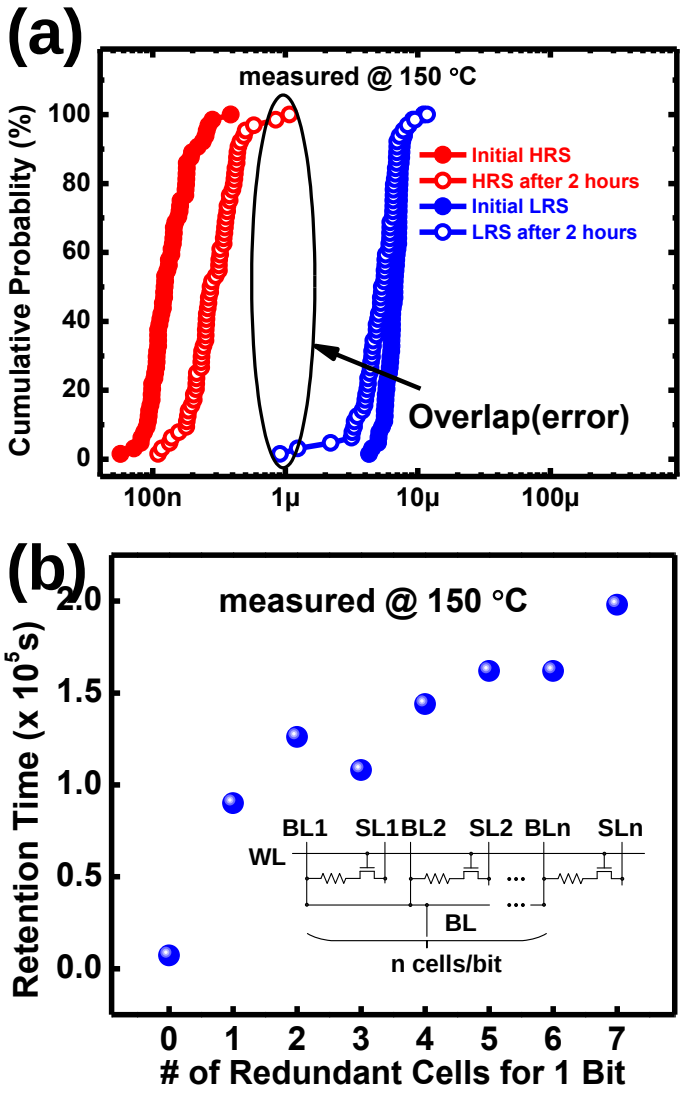


Centered at ~50% with tight distribution

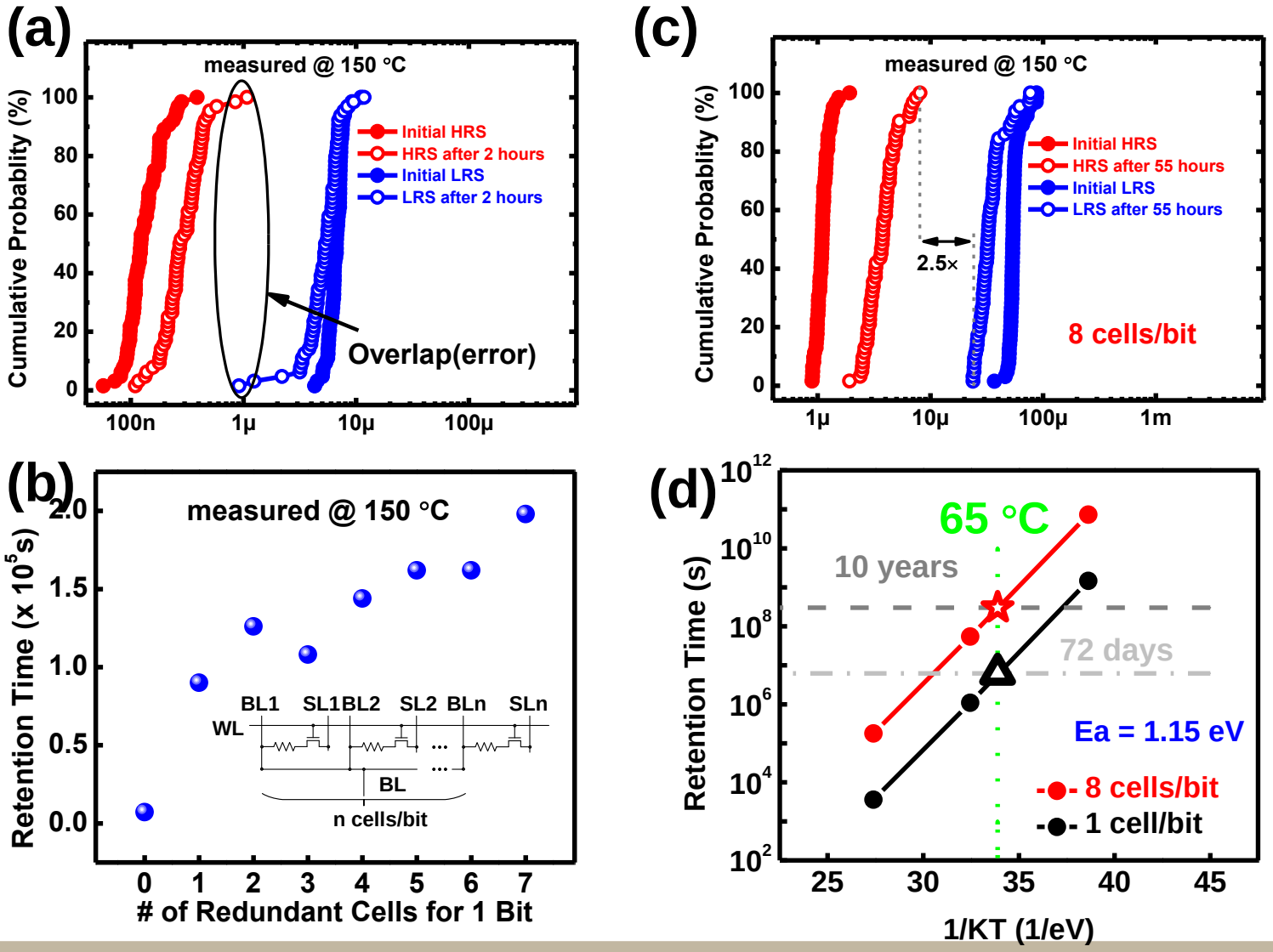
Reproducibility or Reliability



Reproducibility or Reliability



Reproducibility or Reliability



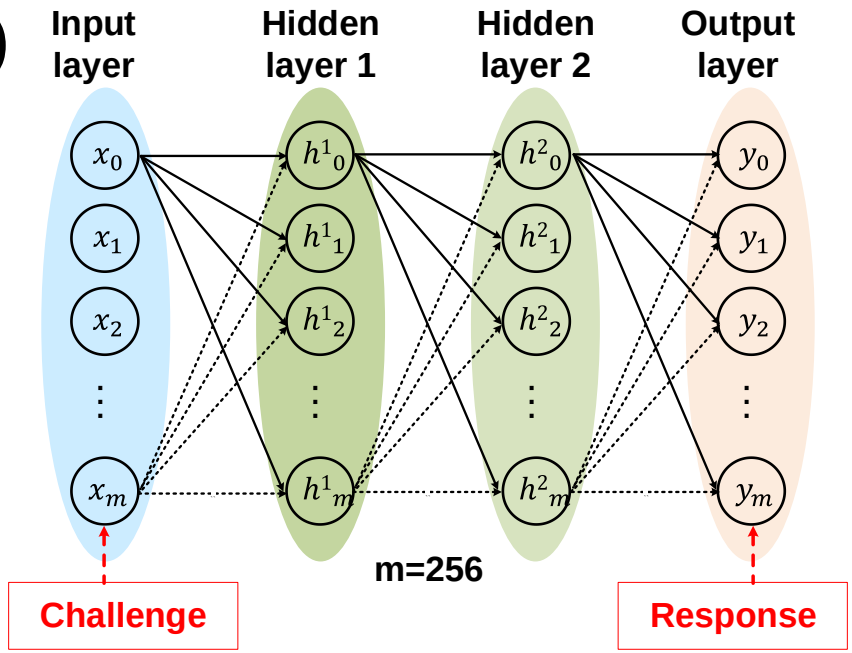
Outline

- **Introduction**
  - Physical Unclonable Function
  - RRAM
- **RRAM PUF Architecture for Authentication**
  - RRAM strong PUF architecture
  - Implementation strategy for PUF
- **Performance Evaluation on 1kb RRAM arrays**
  - PUF Performance Metric
  - Uniqueness, Uniformity, Diffuseness and Reproducibility
- **Machine Learning Attack Evaluation**
- **Conclusion**

Machine Learning Attack

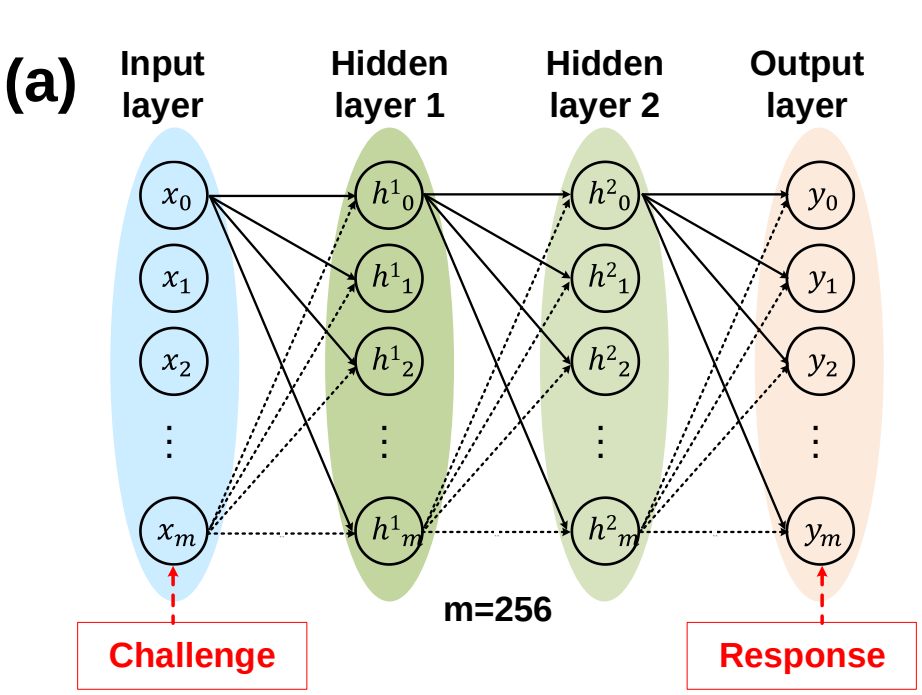
Neural Network Structure

(a)

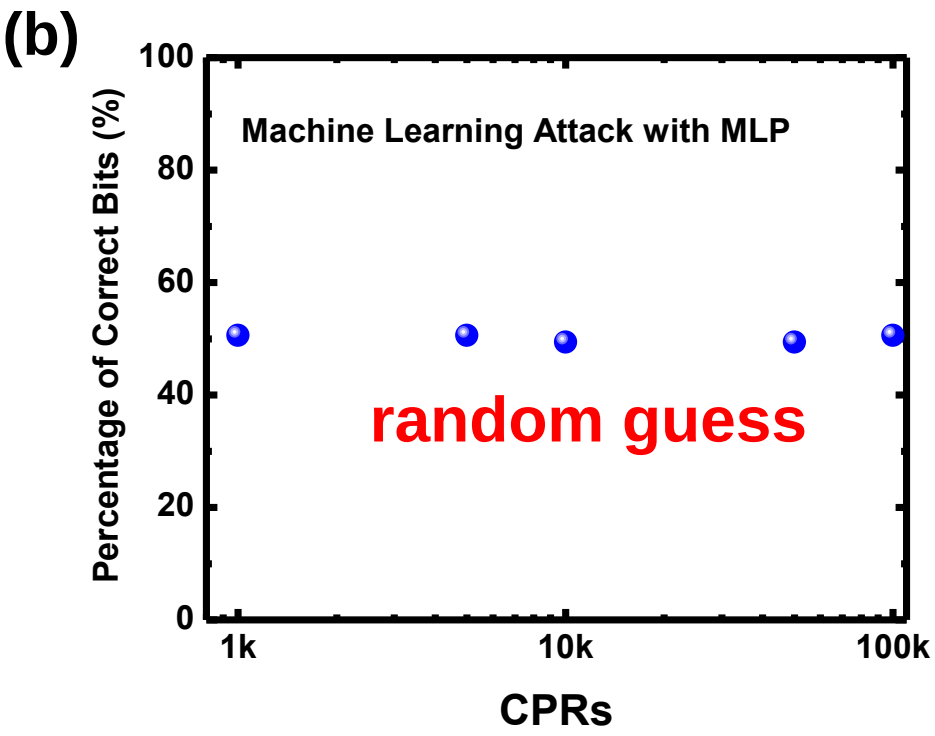


Machine Learning Attack

Neural Network Structure

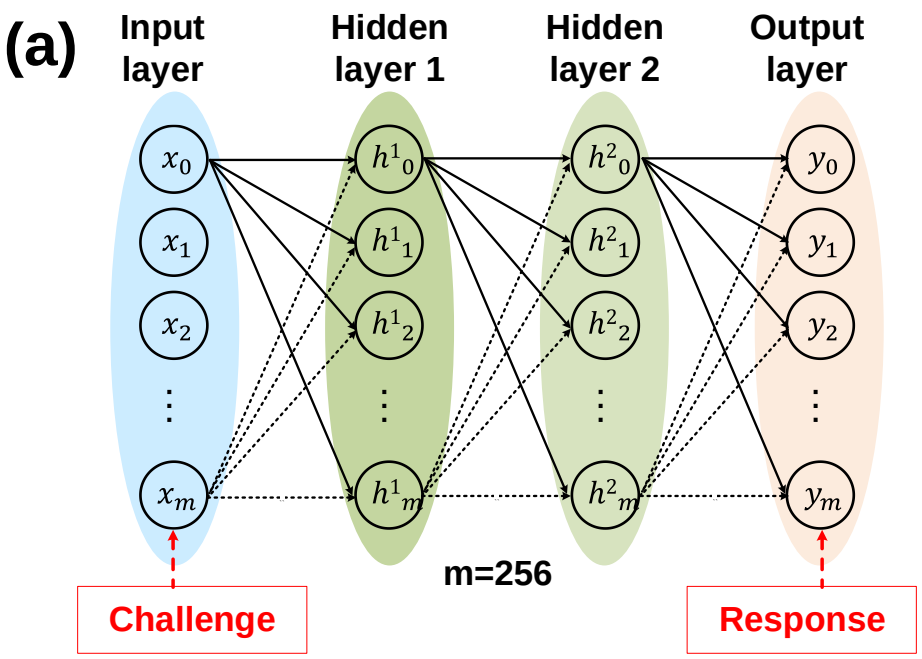


Predication Rate

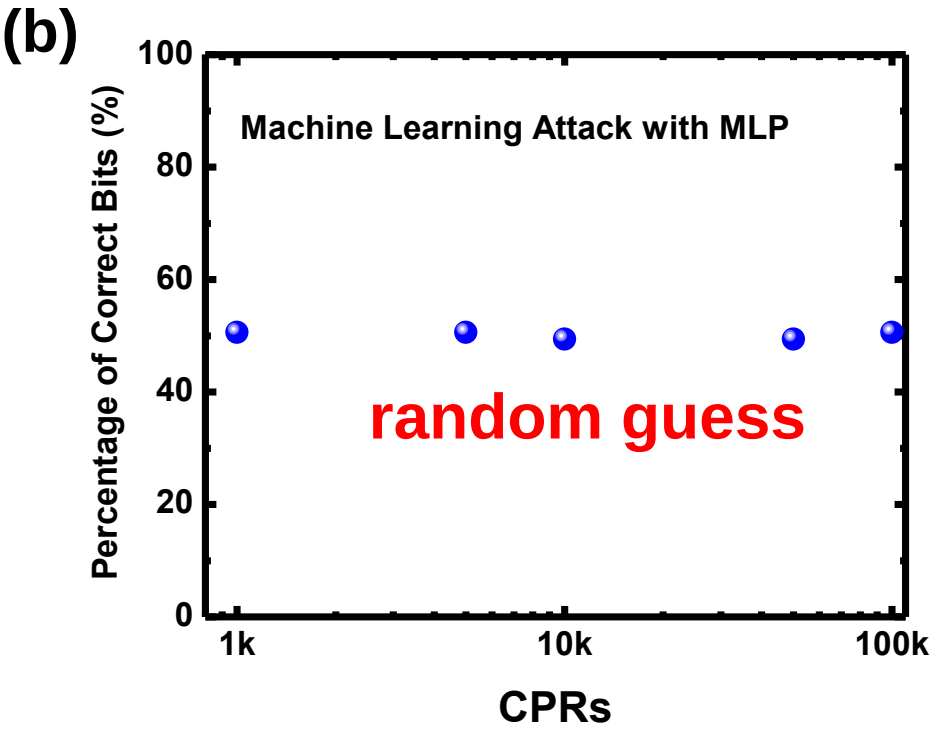


Machine Learning Attack

Neural Network Structure



Predication Rate



RRAM strong PUF offers a high resistance against the ML attack due to the collision resistance of SHA .

Outline

- **Introduction**
  - Physical Unclonable Function
  - RRAM
- **RRAM PUF Architecture for Authentication**
  - RRAM strong PUF architecture
  - Implementation strategy for PUF
- **Performance Evaluation on 1kb RRAM arrays**
  - PUF Performance Metric
  - Uniqueness, Uniformity, Diffuseness and Reproducibility
- **Machine Learning Attack Evaluation**
- **Conclusion**

Conclusion

- **Large variability of RRAM resistance in HRS was leveraged as a source of entropy for PUF application.**
- **RRAM array is embedded with SHA-256 to implement a strong PUF for device authentication.**
- **The performance and reliability of RRAM strong PUF were evaluated on the 1kb 1T1R arrays via simulation.**
  - To achieve good uniqueness and high security, more RRAM outputs should be feed into SHA engine.
  - Redundant RRAM cell is employed to improve RRAM PUF's reliability against resistance drifting over time.
- **The proposed RRAM strong PUF demonstrated to be immune to machine learning attack.**

Acknowledgement

Backup

Brief Comparison of Silicon PUFs

<table>
<tr><th>PUF</th><th>Pros</th><th>Cons</th><th>Vulnerability</th></tr>
<tr><td>Delay based</td><td>• Large # of CRPs
• Mature technology</td><td>Efforts for Place and Route</td><td>Machine learning attack</td></tr>
<tr><td>SRAM</td><td>Mature technology</td><td>Small # of CRPs</td><td>Photon emission attack</td></tr>
<tr><td>STT-RAM</td><td rowspan="3">• Compact
• Low fabrication cost</td><td>• ~2x ON/OFF ratio
• Small variation in resistance</td><td rowspan="3">Invasive probing attack (possible but very hard)</td></tr>
<tr><td>PCRAM</td><td rowspan="2">Retention problem (aging effect)
Severity: PCRAM>RRAM</td></tr>
<tr><td>RRAM</td></tr>
</table>

RRAM Array: 1-transistor-1-resistor (1T1R) vs. Cross-point Architecture

1T1R architecture

Crossbar architecture