清華大學

Tsinghua University

ASU

A Highly Reliable and Tamper-Resistant RRAM PUF: Design and Experimental Validation

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/

5/27/16

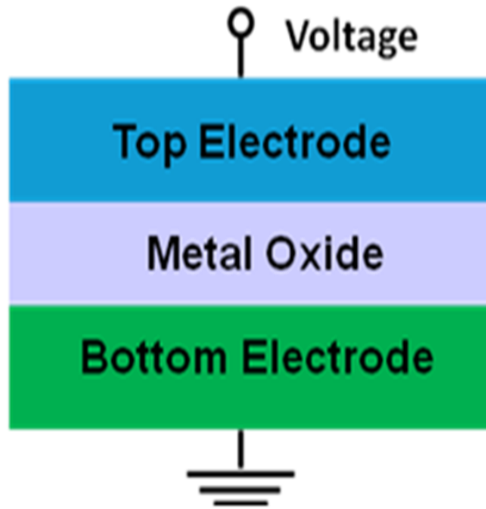
Outline

- **Introduction of RRAM**
- **RRAM PUF Architecture for Key Generation**
- **Performance Evaluation on 1kb RRAM arrays**
- **Strategies to Improve Performance and Reliability**
- **Area Cost and Performance Overhead Analysis**
- **Conclusion**

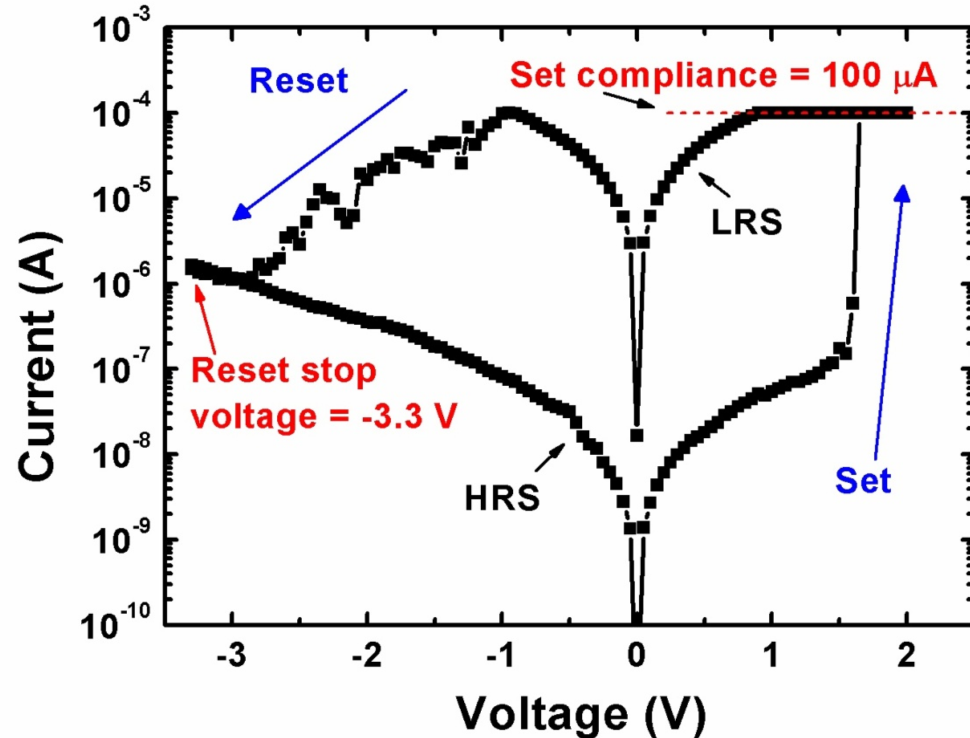
Outline

- **Introduction of RRAM**
- **RRAM PUF Architecture for Key Generation**
- **Performance Evaluation on 1kb RRAM arrays**
- **Strategies to Improve Performance and Reliability**
- **Area Cost and Performance Overhead Analysis**
- **Conclusion**

Oxide RRAM Basics

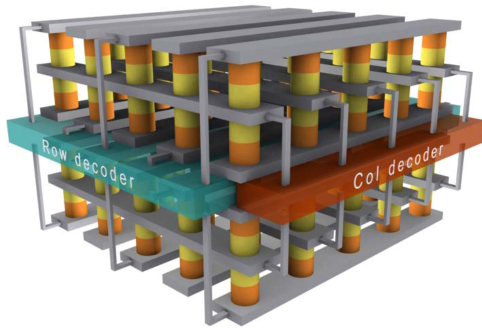


Typical Bipolar I-V Curve

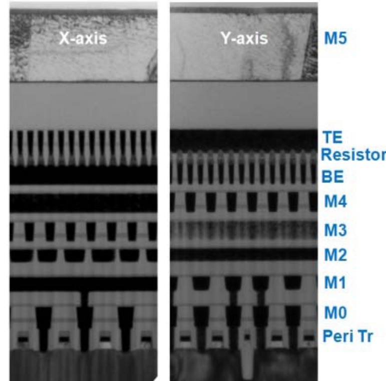


- "0" : High Resistance State (HRS)
- "1" : Low Resistance State (LRS)
- HRS→LRS: SET
- LRS→HRS: RESET

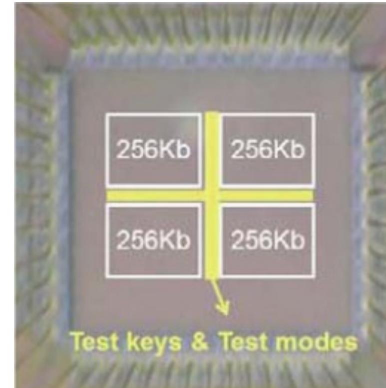
RRAM's Industry R&D



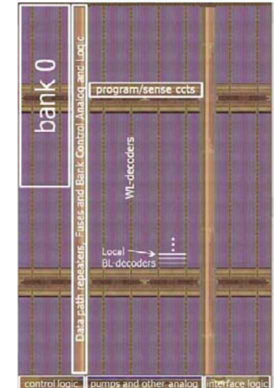
Samsung



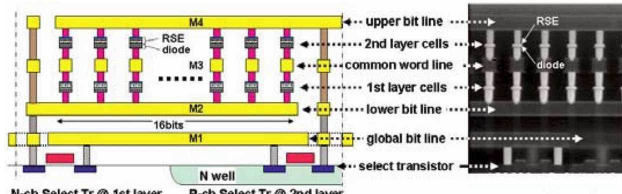
HP & Hynix

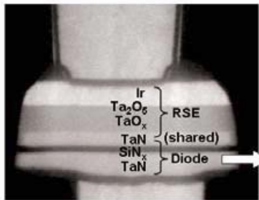


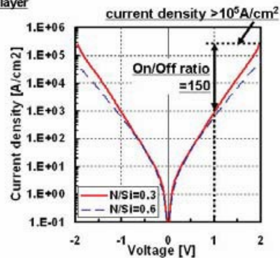
TSMC



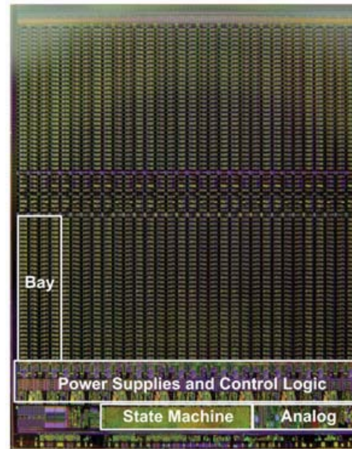
Micron & Sony





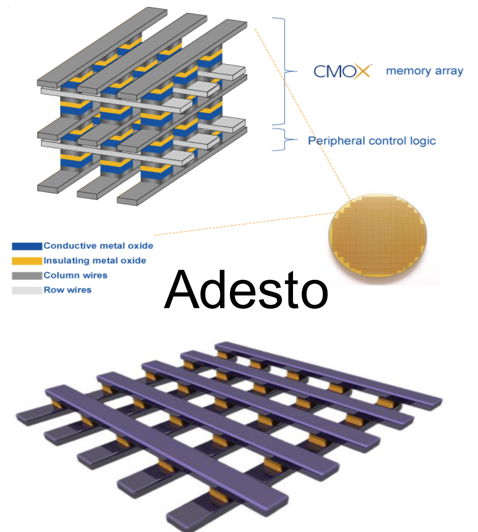


Panasonic



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

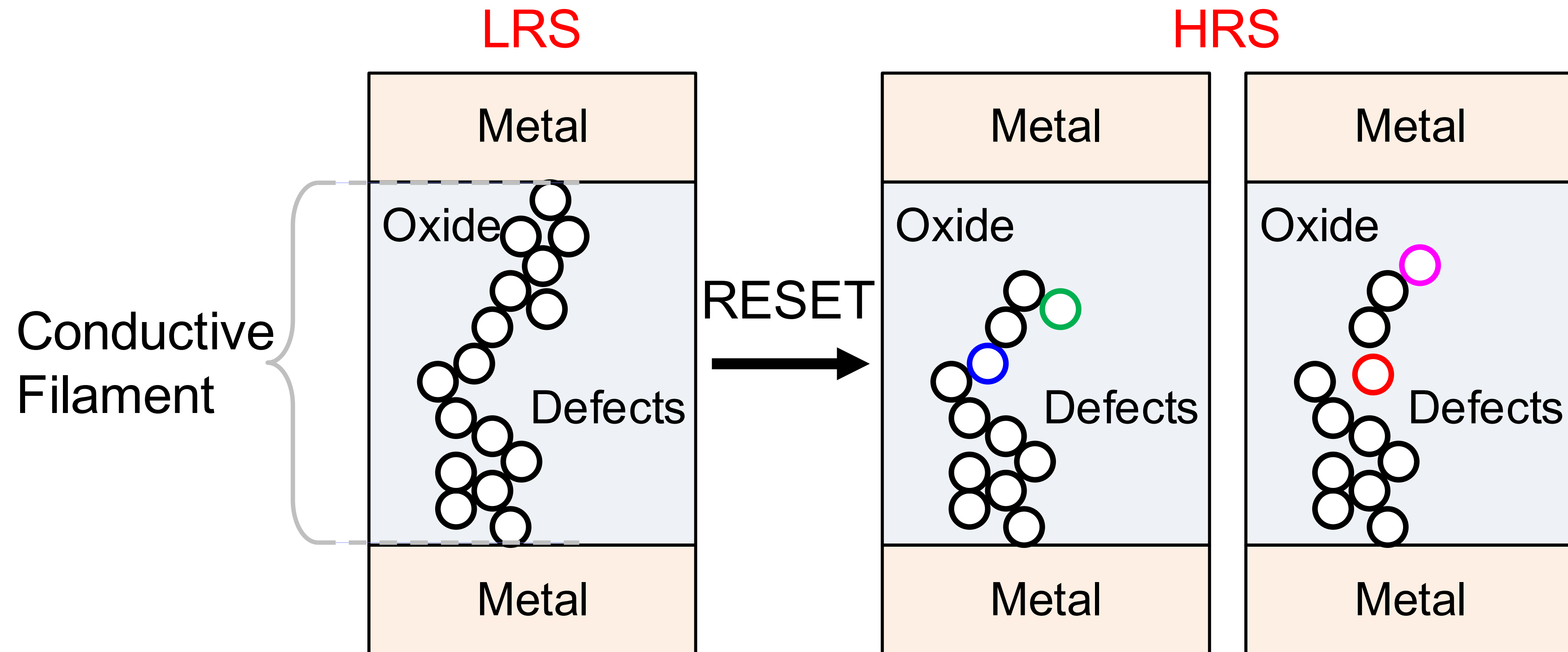
Toshiba & Sandisk



Adesto

The Randomness in RRAM PUF

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

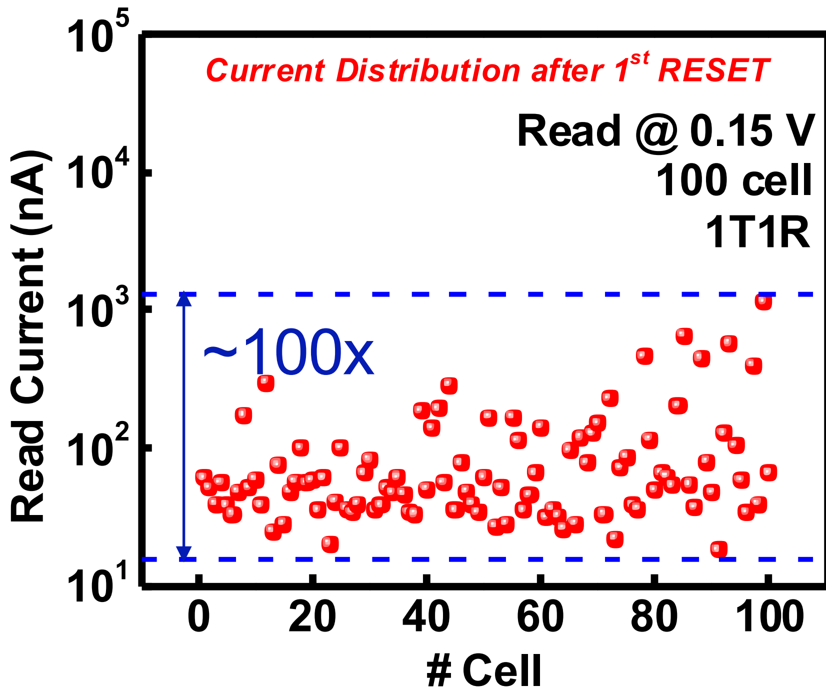


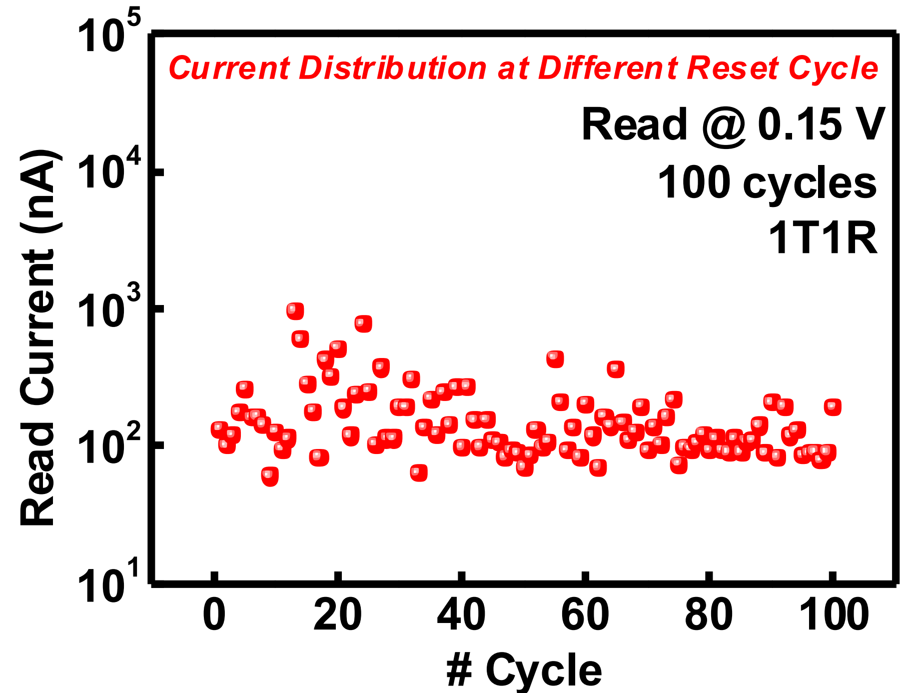
RRAM Device Characteristics from Experimental Data

RRAM device: $TiN/TaOx/HfO_2/TiN$

Cell to Cell | **Cycle to Cycle**

RESET Pulse: 3V, 50ns



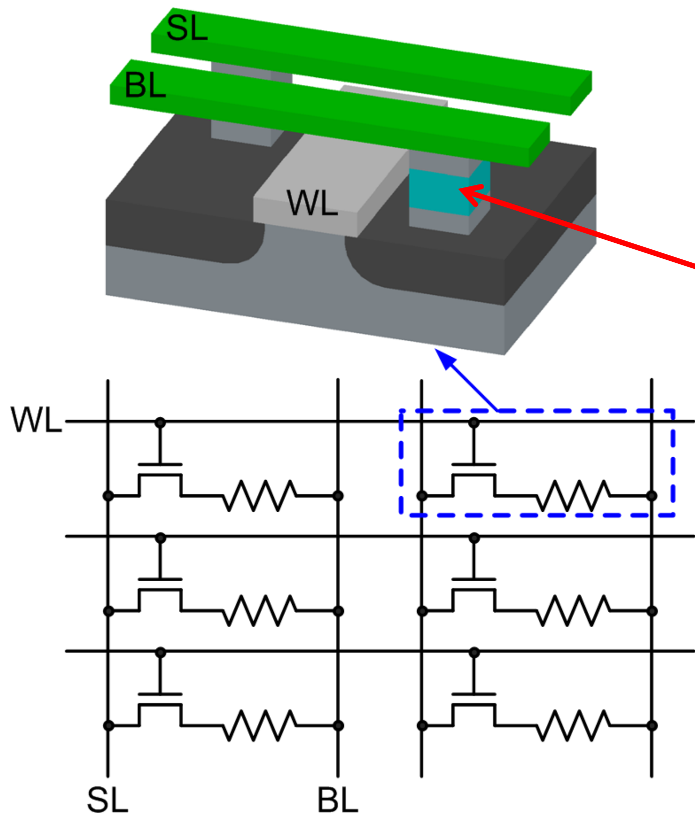


Outline

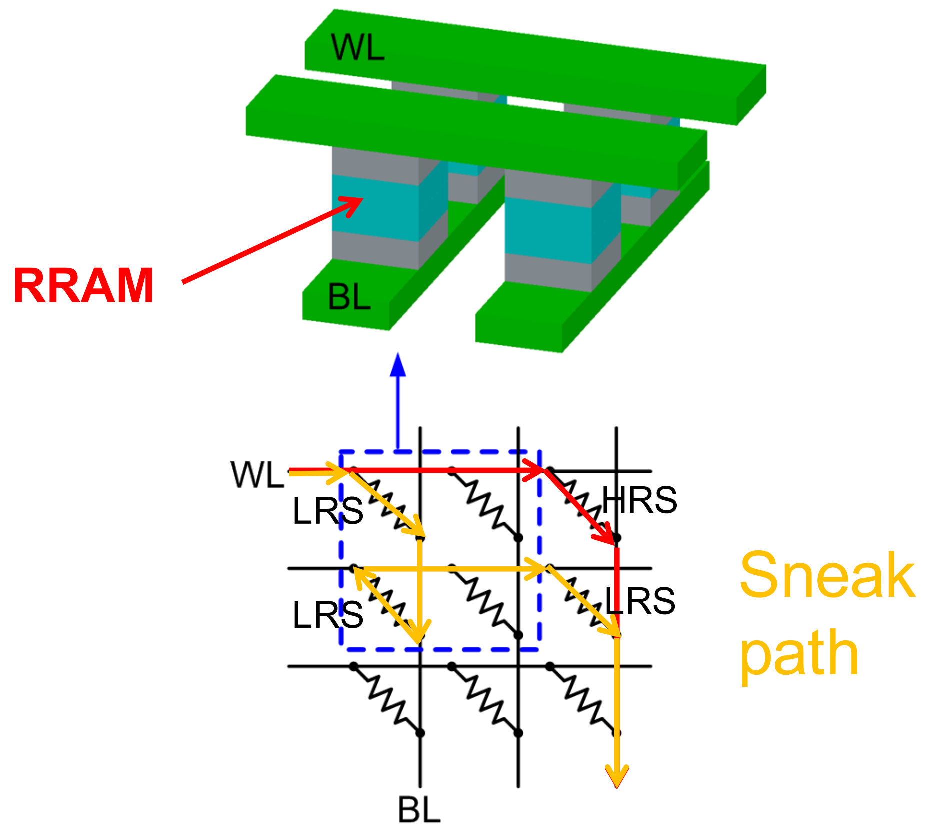
- Introduction of RRAM
- **RRAM PUF Architecture for Key Generation**
- Performance Evaluation on 1kb RRAM arrays
- Strategies to Improve Performance and Reliability
- Area Cost and Performance Overhead Analysis
- Conclusion

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

1T1R architecture



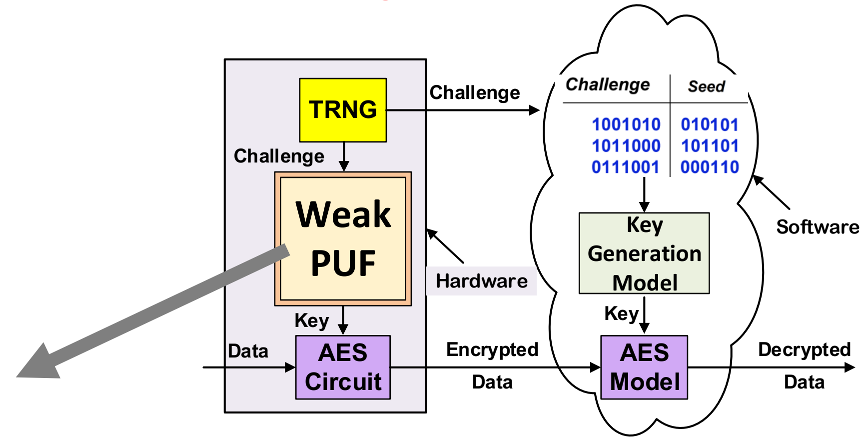
Crossbar architecture



RRAM PUF Architecture for Key Generation

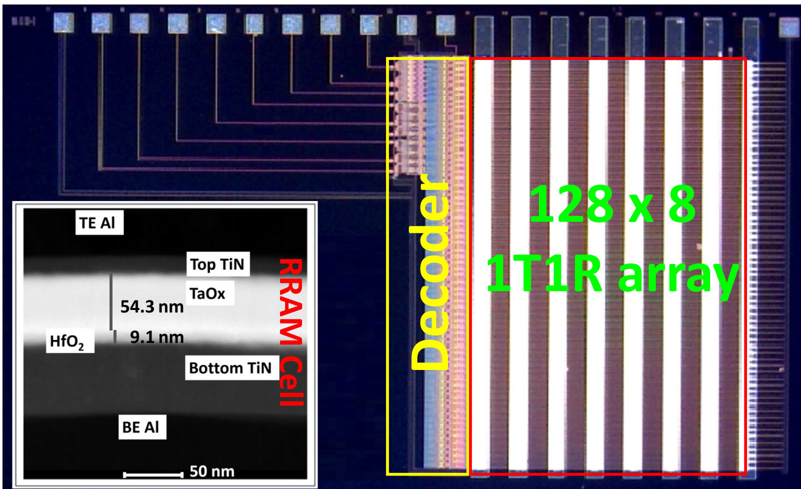
EN
Split SA
Control Logic
SL/BL address
SL/BL Mux
WL Decoder
1T1R Array
WL<0>
WL<n-1>
RRAM
SL<0>
BL<0>
SL<n-1>
BL<n-1>
Challenge → WL address
EN
SA
SA
Response →
R<0>
R<n-1>

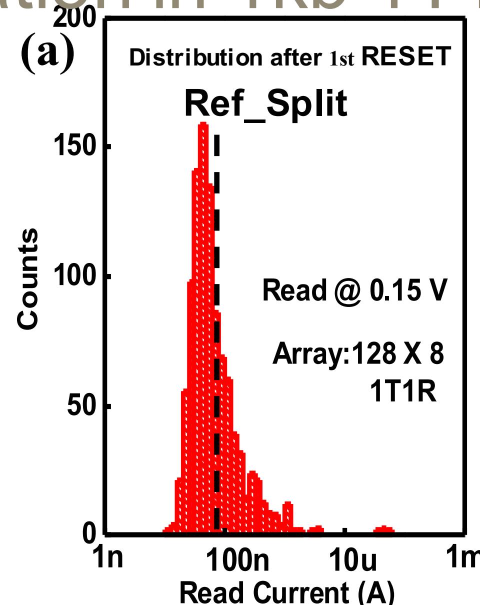
Key Generation

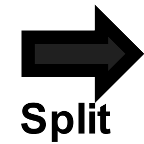


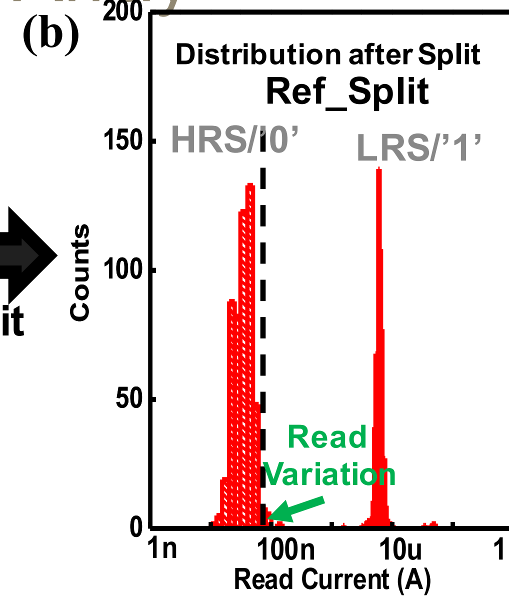
- The red parts are designed only for construction phase (preparation phase)
- The green part is designed only for operation phase (evaluation phase)

RRAM PUF Implementation in 1kb 1T1R Array

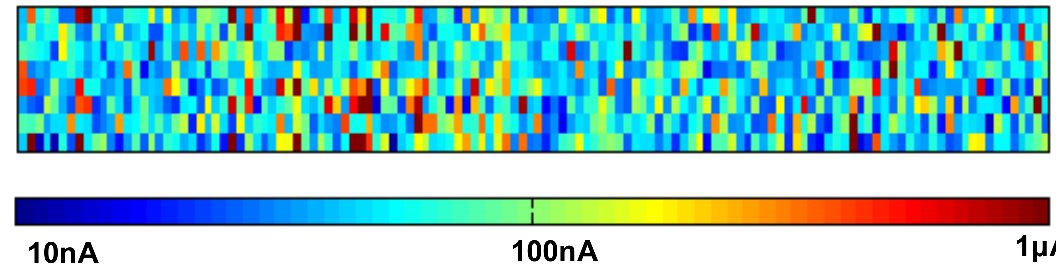


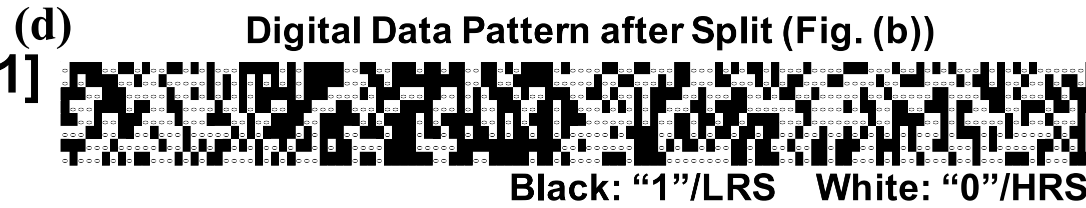






1) **form all the cells to LRS**
2) **RESET all the cells to HRS (entropy source)**
3) **Read out the current**
4) **Find a split reference within the read current distribution**
5) **Digitize the randomness according to the reference [1]**





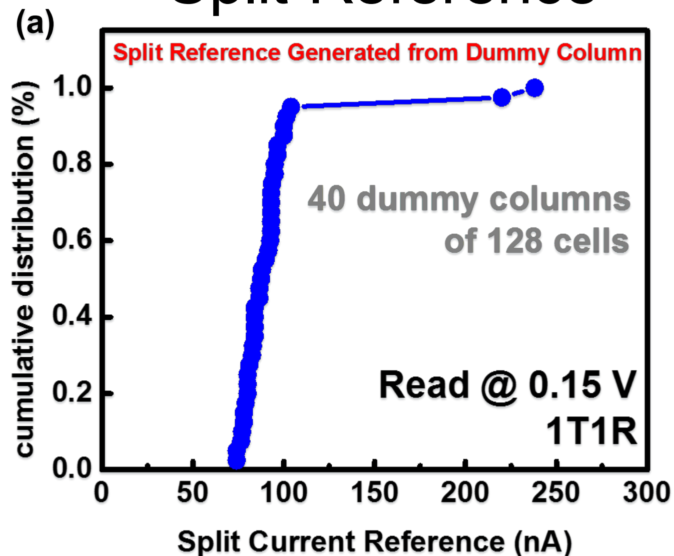
[1] W. Chen, et al, *ICCAD*, 2014

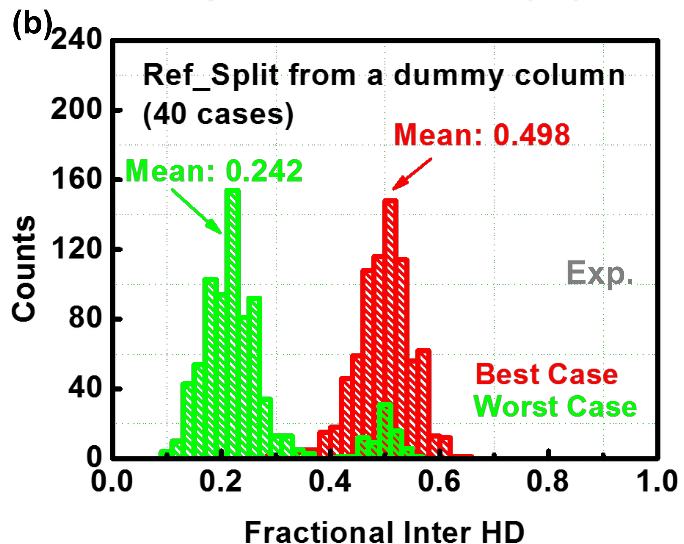
Outline

- Introduction of RRAM
- RRAM PUF Architecture for Key Generation
- **Performance Evaluation on 1kb RRAM arrays**
- Strategies to Improve Performance and Reliability
- Area Cost and Performance Overhead Analysis
- Conclusion

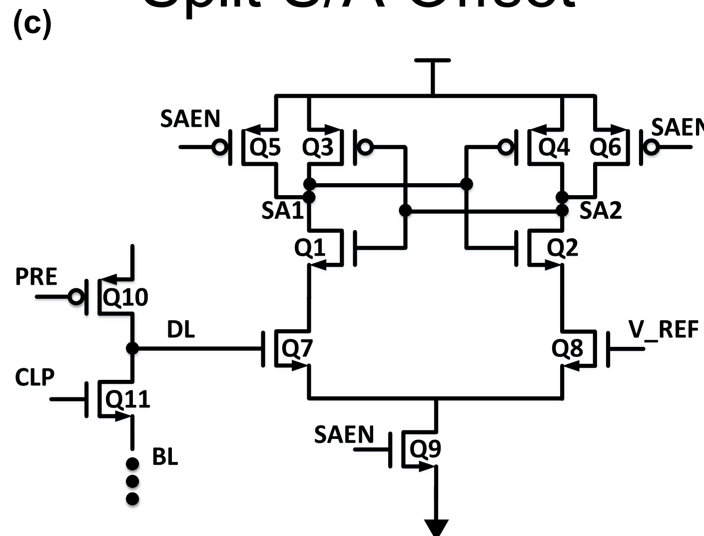
Impacts on Uniqueness

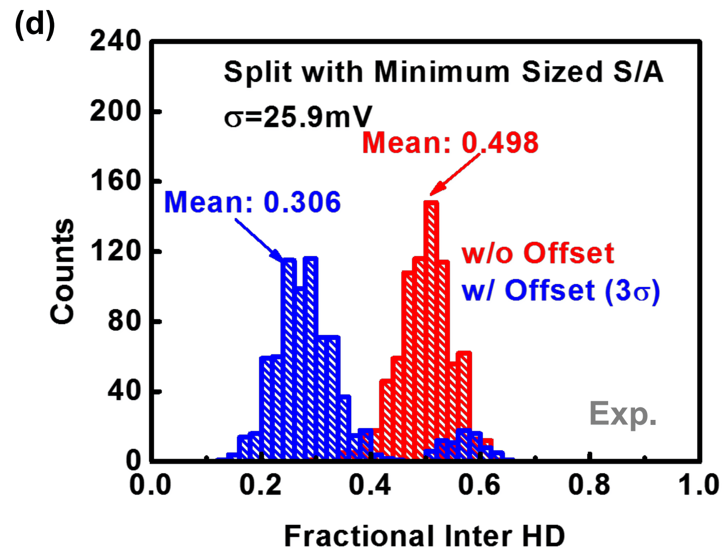
Split Reference





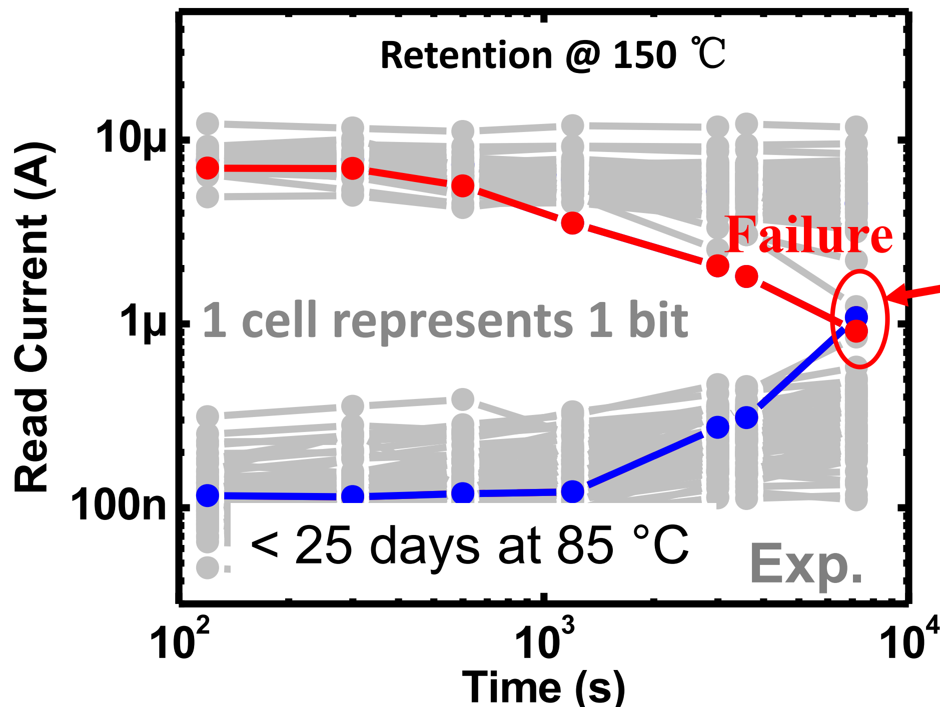
Split S/A Offset





Reliability

- **RRAM device: resistance drifts over time but very slow**
- **High temperature is used to accelerate the failure**
- **Reliability of RRAM PUF requires an excellent data retention even at elevated temperature conditions**



Some response bits flipped. The generated key is not reliable.

Outline

- Introduction of RRAM
- RRAM PUF Architecture for Key Generation
- Performance Evaluation on 1kb RRAM arrays
- **Strategies to Improve Performance and Reliability**
- Area Cost and Performance Overhead Analysis
- Conclusion

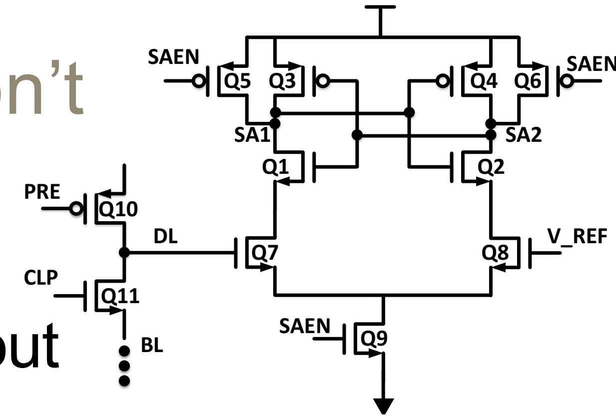
Strategies to Improve Uniqueness

- **Dummy array (1024 cells) is used to generate split reference**

Uniqueness	Ref_Split generated from Array No.				
	1st	2nd	3rd	4th	5th
μ(%)[a]	49.48	48.97	49.79	47.77	49.80
σ(%)[b]	4.90	5.06	4.87	5.56	4.86

- **Dummy array is designed adjacent to the real array on-chip (resulting in larger area overhead on chip)**
- **Dummy array off-chip calibrated with the same batch fabricated with the real array (no area overhead on chip)**

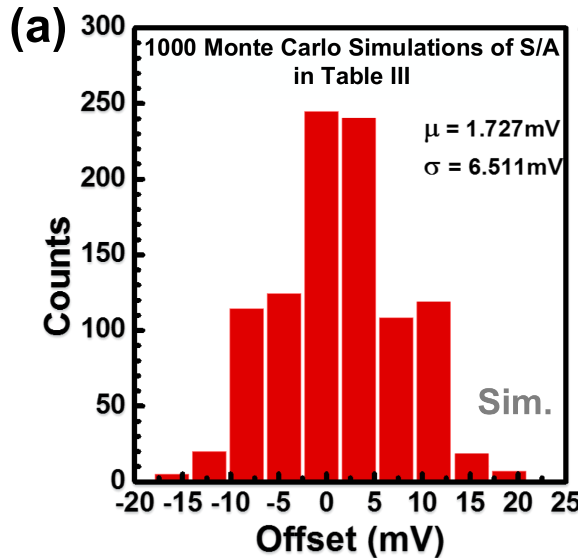
Strategies to Improve Uniqueness Con't

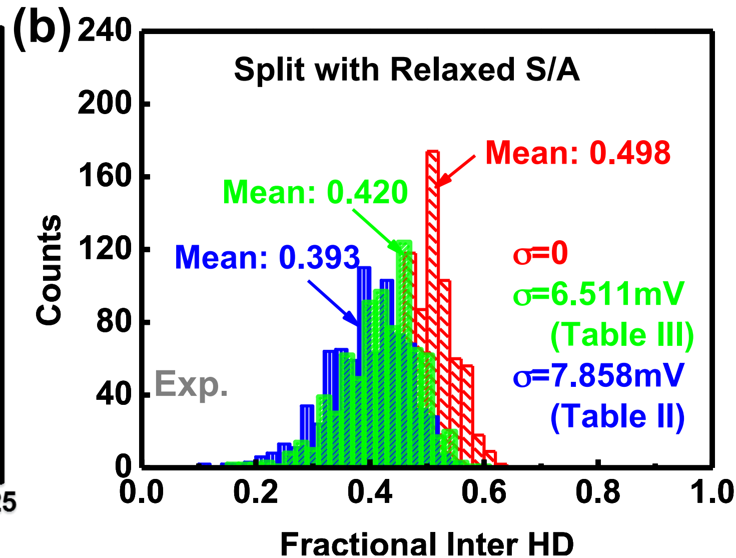


- **Minimizing Split S/A Offset**

1) Symmetrical and common centroid layout design

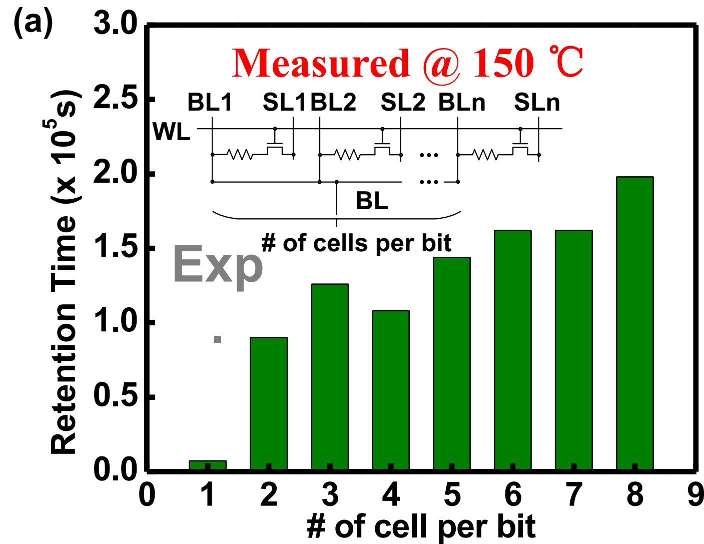
2) Increasing the size the critical transistors, especially the differential input pair

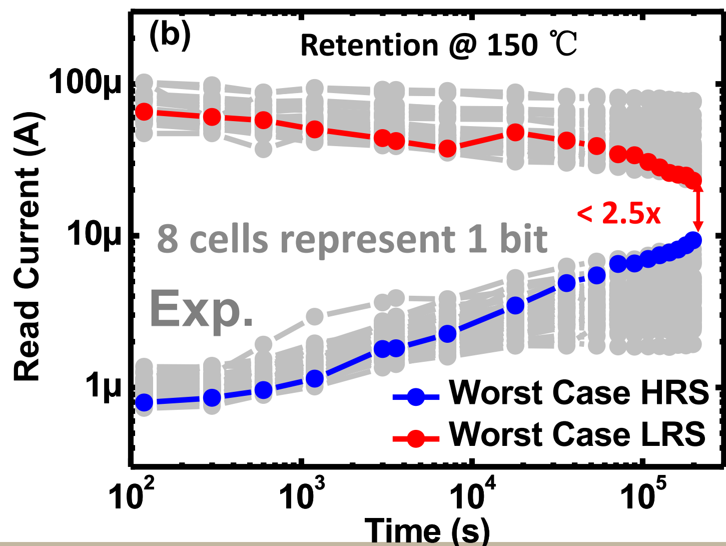


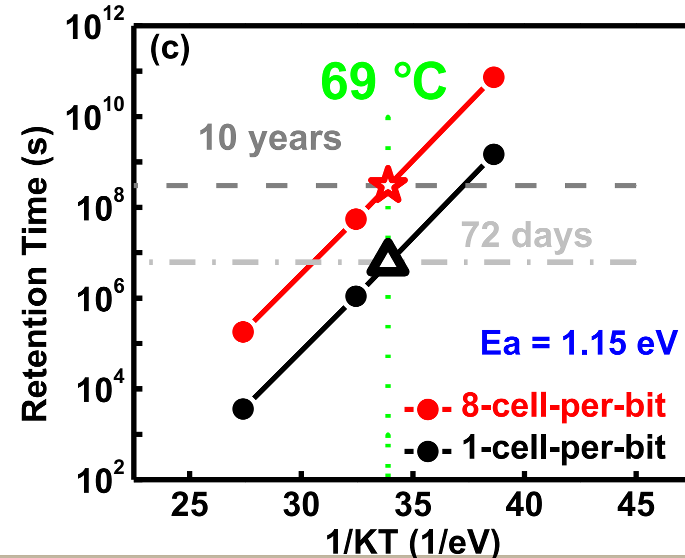


Multi-Cell-Per-Bit to Improve Reliability

- **Redundancy cells are employed to minimize the probability of early lifetime failure due to cell to cell variation.**



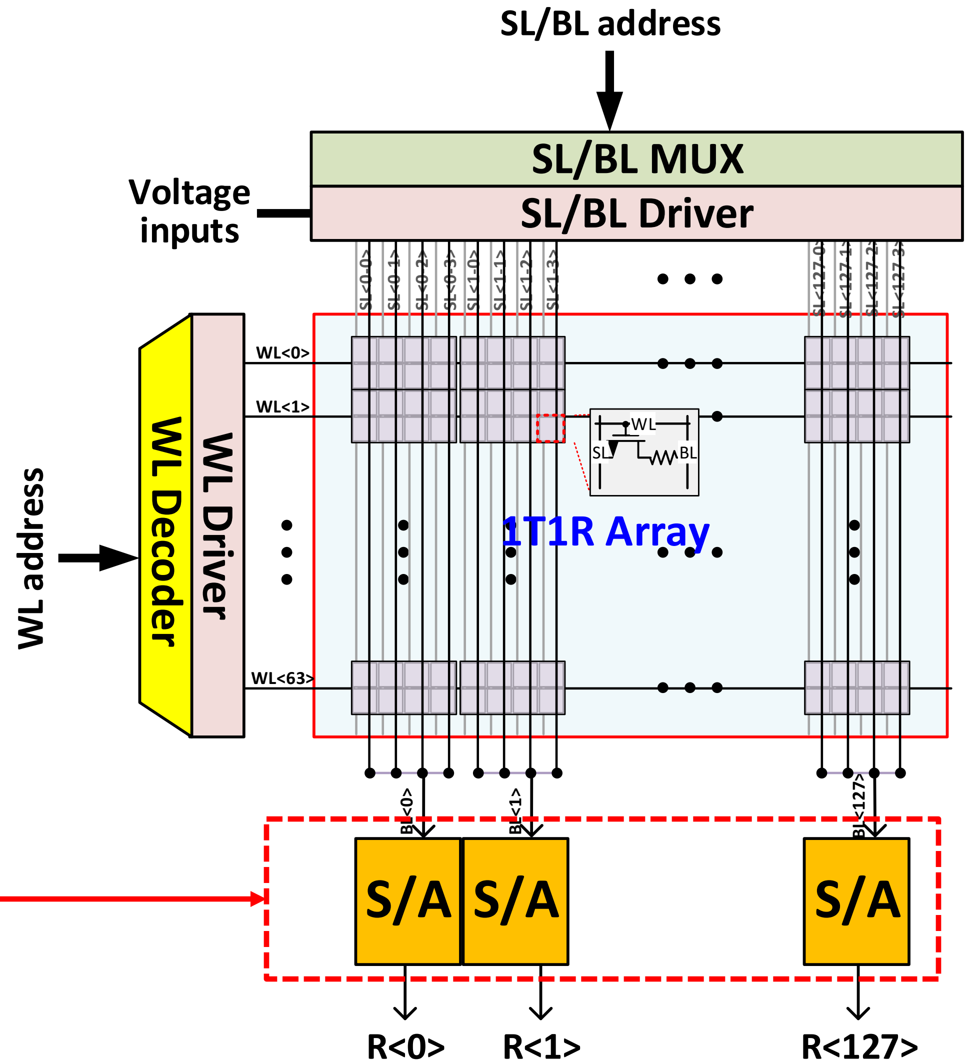




Layout Obfuscation for Tamper Resistance

- **Potential security issue**

An adversary might be able to microprobe the S/A



Layout Obfuscation for Tamper Resistance

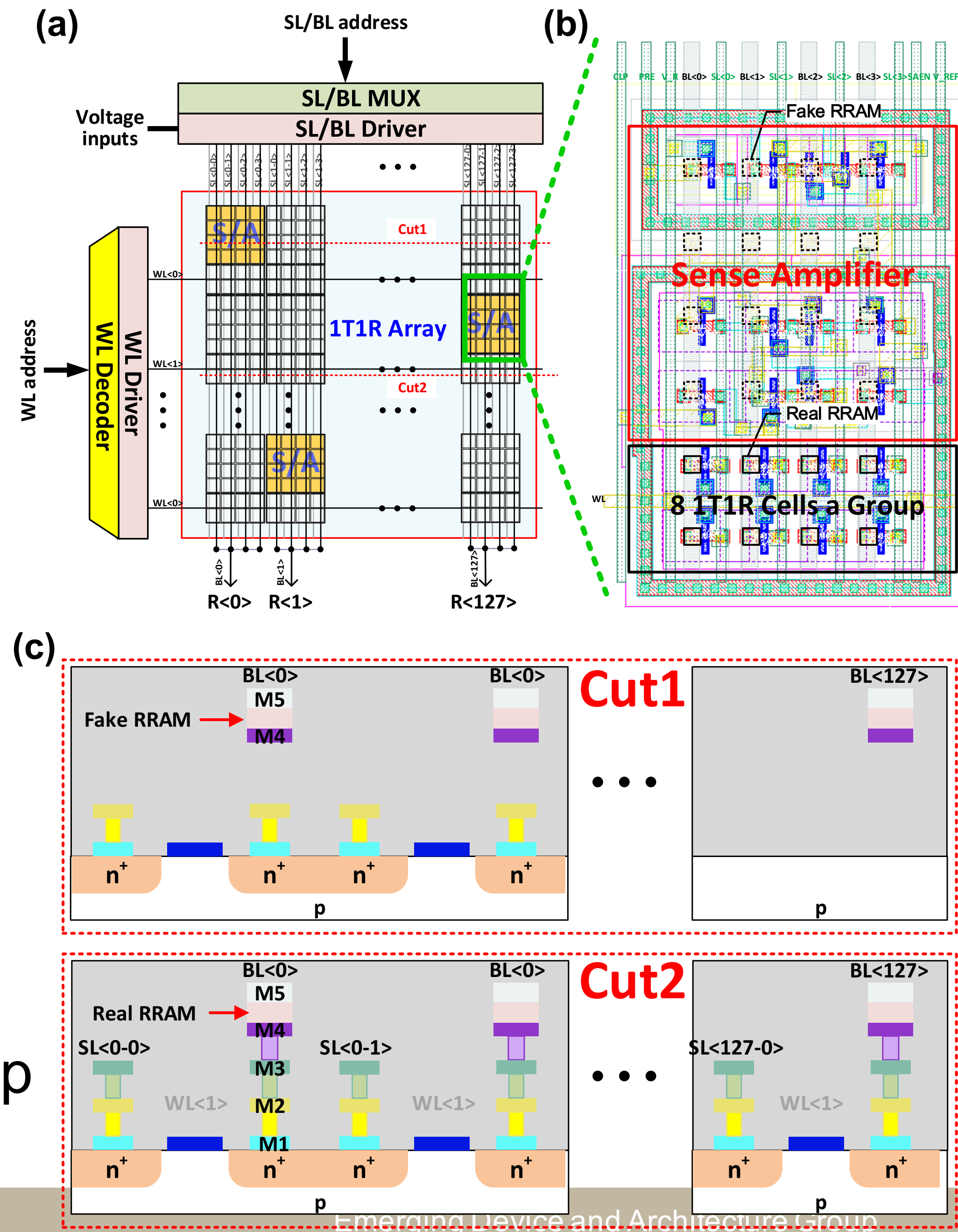
- **Potential security issue**

An adversary might be able to microprobe the S/A

- **Layout Obfuscation**

Hide S/A within 1T1R array and randomize the locations

Fake and real RRAM cells uniformly fabricated on the top



Outline

- Introduction of RRAM
- RRAM PUF Architecture for Key Generation
- Performance Evaluation on 1kb RRAM arrays
- Strategies to Improve Performance and Reliability
- **Area Cost and Performance Overhead Analysis**
- Conclusion

Area Cost and Performance Overhead Analysis Using Cadence and HSPICE

- **Array size: 64x128(1024)**
- **Circuit technology node: TSMC 65 nm**

Architecture	S/A hiding (w/ or w/o)	Latency (ns)	Energy (pJ)	Area (mm^2) *
1-cell-per-bit	w/o	4.24	9.59	0.0083
8-cell-per-bit	w/o	6.46	14.87	0.0390
	w/	16.45	17.69	0.2036

*Including the peripheral circuits (e.g. row decoder, COL MUX, write driver and S/A)

Outline

- Introduction of RRAM
- RRAM PUF Architecture for Key Generation
- Performance Evaluation on 1kb RRAM arrays
- Strategies to Improve Performance and Reliability
- Area Cost and Performance Overhead Analysis
- **Conclusion**

Conclusion

- **Large variability of RRAM resistance in HRS was leveraged as a source of entropy for weak PUF application**
- **The performance and reliability of RRAM weak PUF were evaluated experimentally on the 1kb 1T1R arrays**
- **The factors that affect the RRAM weak PUF metrics were discussed and strategies were proposed to improve the performance and reliability**
- **The potential security problem was discussed and layout obfuscation was proposed for tamper resistance**

Backup

S/A sizing

S/A TRANSISTORS' SIZE TO REDUCE OFFSET σ TO 7.858 MV

Transistor	Q1/Q2	Q3/Q4	Q5/Q6	Q7/Q8	Q9	Q10/Q11
Gate Length (nm)	60	60	60	180	60	60
Width (nm)	240	240	120	900	120	120

S/A TRANSISTORS' SIZE TO REDUCE OFFSET σ TO 6.511 MV

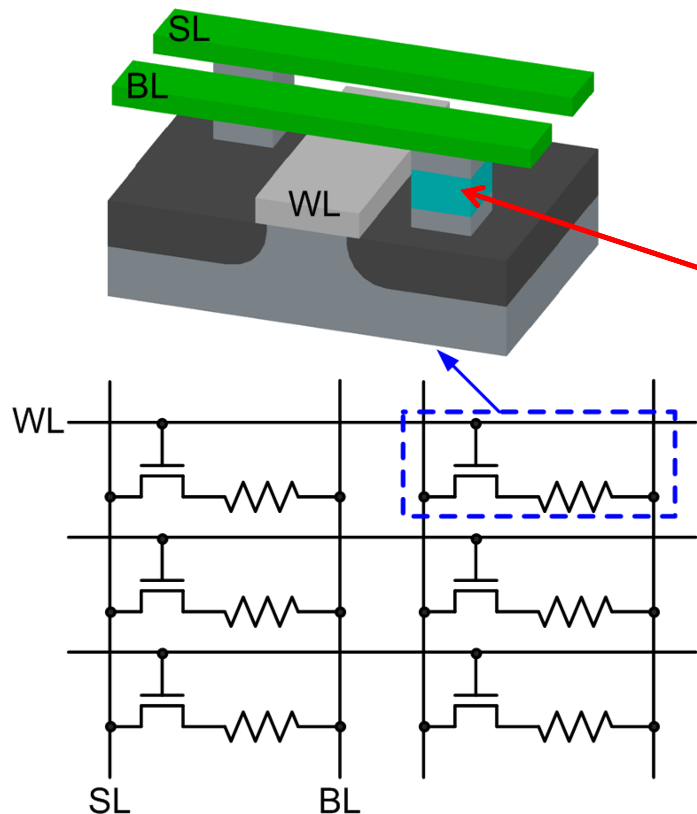
Transistor	Q1/Q2	Q3/Q4	Q5/Q6	Q7/Q8	Q9	Q10/Q11
Gate Length (nm)	60	60	60	180	60	60
Width (nm)	240	240	120	1800	240	120

Brief Comparison of Silicon PUFs

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

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

1T1R architecture



Crossbar architecture