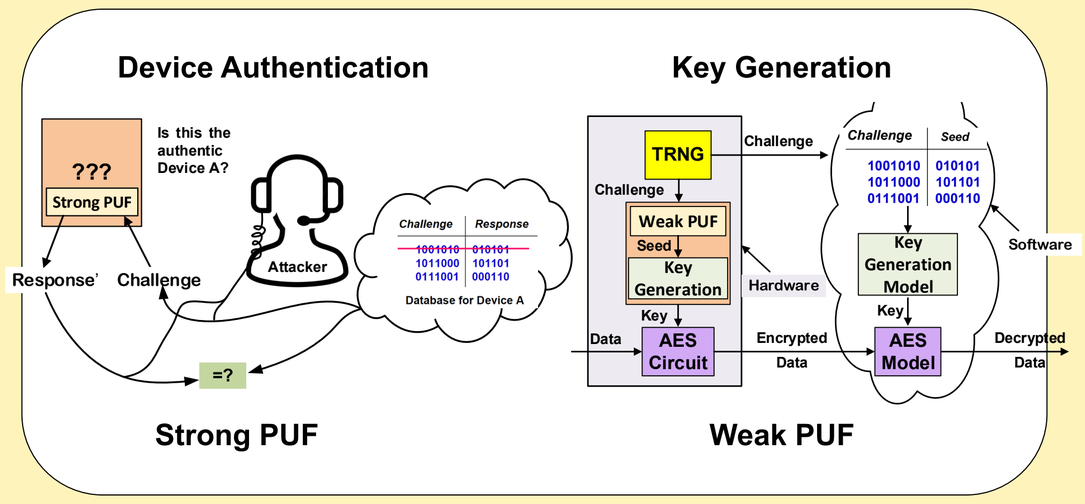
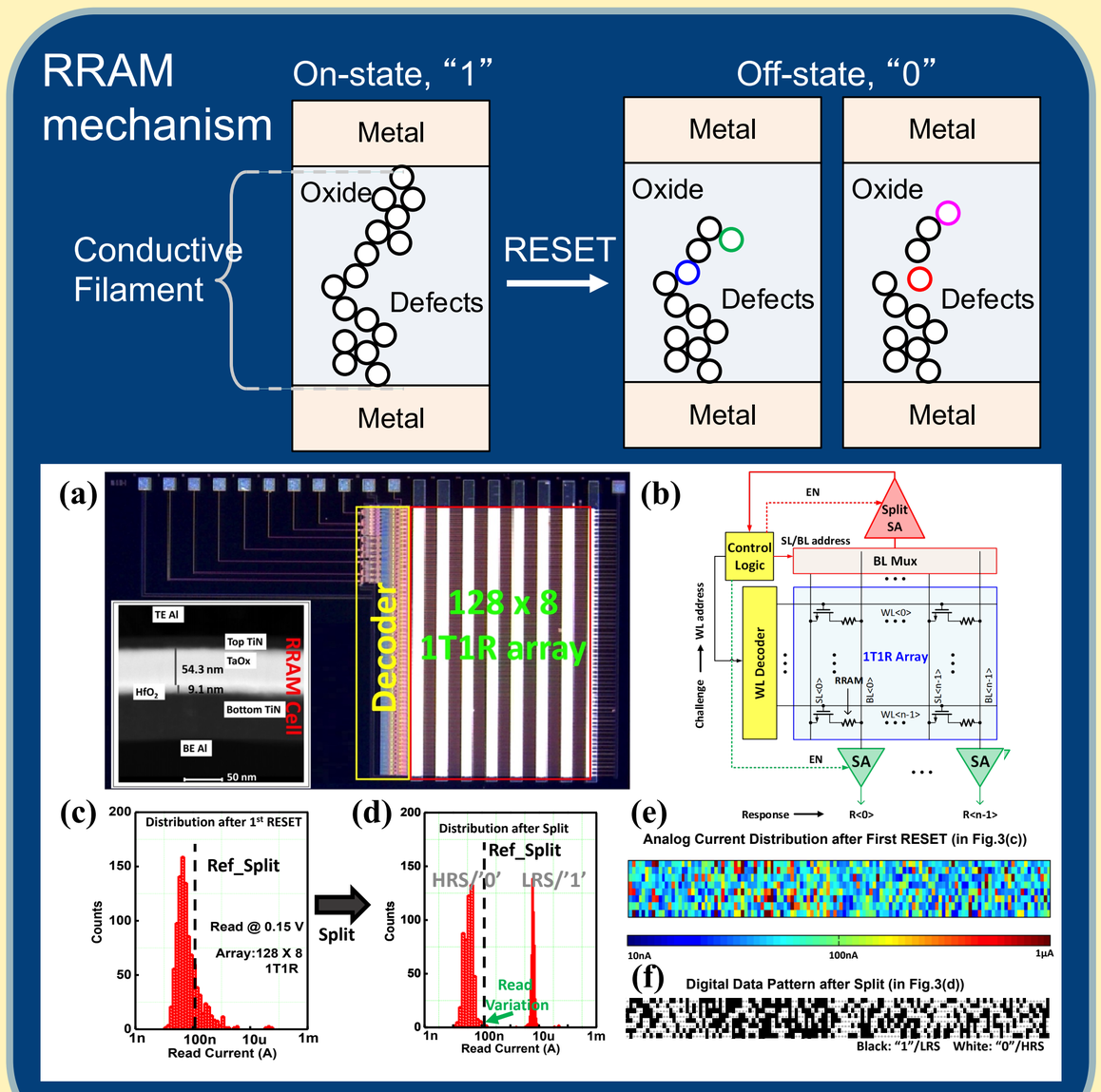
Design of RRAM based Hardware Security Primitives

PI: Shimeng Yu, Co-PI: Chaitali Chakrabarti, Arizona State University
http://faculty.engineering.asu.edu/shimengyu/

The objective of this project is to experimentally design and fabricate RRAM based hardware security primitives for device authentication and key generation.

- Each Internet of Things (IoT) devices should be equipped with a unique device signature that can be used for authentication by cloud
- The data transfer between IoT devices and cloud should be encrypted using device-specific cryptographic key
- These new demands require a design of *compact* and *low-power* security primitives
- Resistive random access memory (RRAM) provides variability and entropy source for implementing physical unclonable function (PUF) and true random number generation (TRNG)





Implementation of RRAM based PUF

Approach

Design

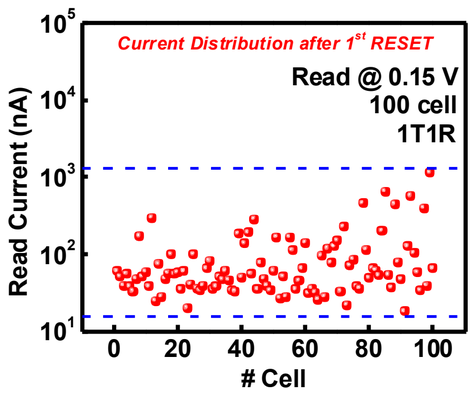
- Leverage RRAM's variability to design PUF and RRAM's random telegraph noise to design TRNG
- The design targets are small chip area, low power, high reliability and strong security
- Techniques such as layout obfuscation, redundancy and error correction will be used

Fabrication and Measurement

- Experimentally tape-out the RRAM based PUF and TRNG through PI's custom fabrication channel, as RRAM foundry is not commercially available
- The realistic data measured from the test chips will be used to develop more practical security protocols

Variability of RRAM Characterized

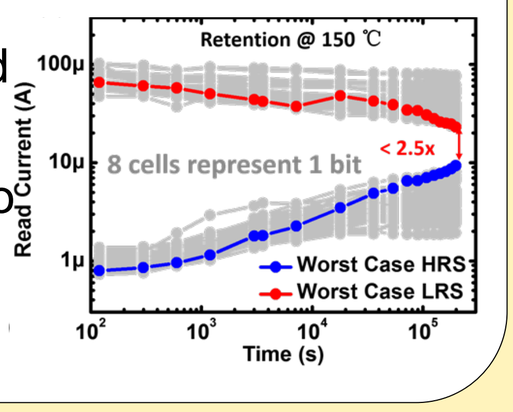
Device-to-device variability is measured on 1kb 1-transistor-1-resistor (1T1R) HfO_x RRAM array



RRAM Weak PUF Implemented in 1T1R Array

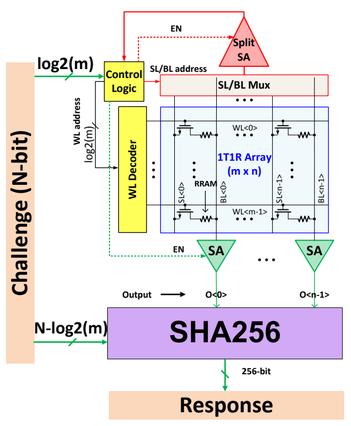
Uniqueness characterized to be close to 50%.

Reliability characterized to be >10 years at 69 °C by extrapolation



RRAM Strong PUF (1T1R Array + SHA)

To enhance challenge-response pair (CRP) space, part of the 256 challenge bits are fed into SHA for hashing



RRAM PUF+AES Chip for Tape-out

RRAM PUF (1T1R Array) is used as key generation (with ECC) for AES encryption.

Design is done and sent out for tape-out at 130 nm node

References:
[1] R. Liu, H. Wu, Y. Pang, H. Qian, S. Yu, "A highly reliable and tamper-resistant RRAM PUF: design and experimental validation," IEEE HOST 2016
[2] P.-Y. Chen, R. Fang, R. Liu, C. Chakrabarti, Y. Cao, S. Yu, "Exploiting resistive cross-point array for compact design of physical unclonable function," IEEE HOST 2015

NSF Secure and Trustworthy Cyberspace Biennial Principal Investigator Meeting
Jan. 9 -11th 2017
Arlington, VA