STARSS: Small: Design of Light-weight RRAM based Hardware Security Primitives for IoT Devices

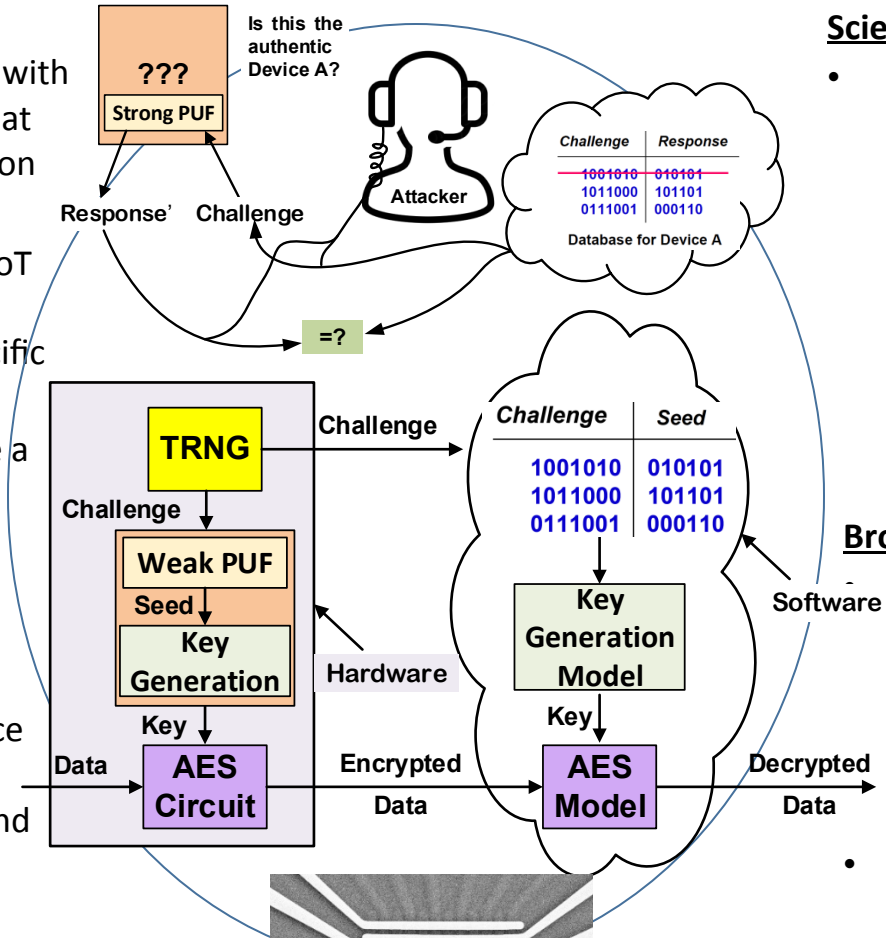
PI: Shimeng Yu, Co-PI: Chaitali Chakrabarti

Challenge:

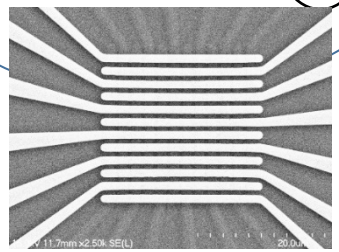
- Each Internet of Things (IoT) devices should be equipped with a unique device signature that can be used for authentication by cloud
- The data transfer between IoT devices and cloud should be encrypted using device-specific cryptographic key
- These new demands require a design of compact and low-power security primitives

Solution:

- Resistive random access memory (RRAM) provides variability and entropy source for implementing physical unclonable function (PUF) and true random number generation (TRNG)



RRAM technology



RRAM security primitives

Scientific Impact:

- Experimentally tape-out the RRAM based PUF and TRNG through PI's custom fabrication channel. The realistic data measured from the test chips will be valuable for system designers to develop more practical protocols using RRAM security primitives.

Broader Impact:

If successful, billions of IoT devices could be protected by integration of RRAM based security primitives with conventional silicon circuits.

- Will train graduate, undergraduate and K-12 students with knowledge and skills in emerging device technologies and hardware security

NSF-CNS-1615774 and SRC Contract 2016-TS-2691

Arizona State University
Email: shimeng.yu@asu.edu