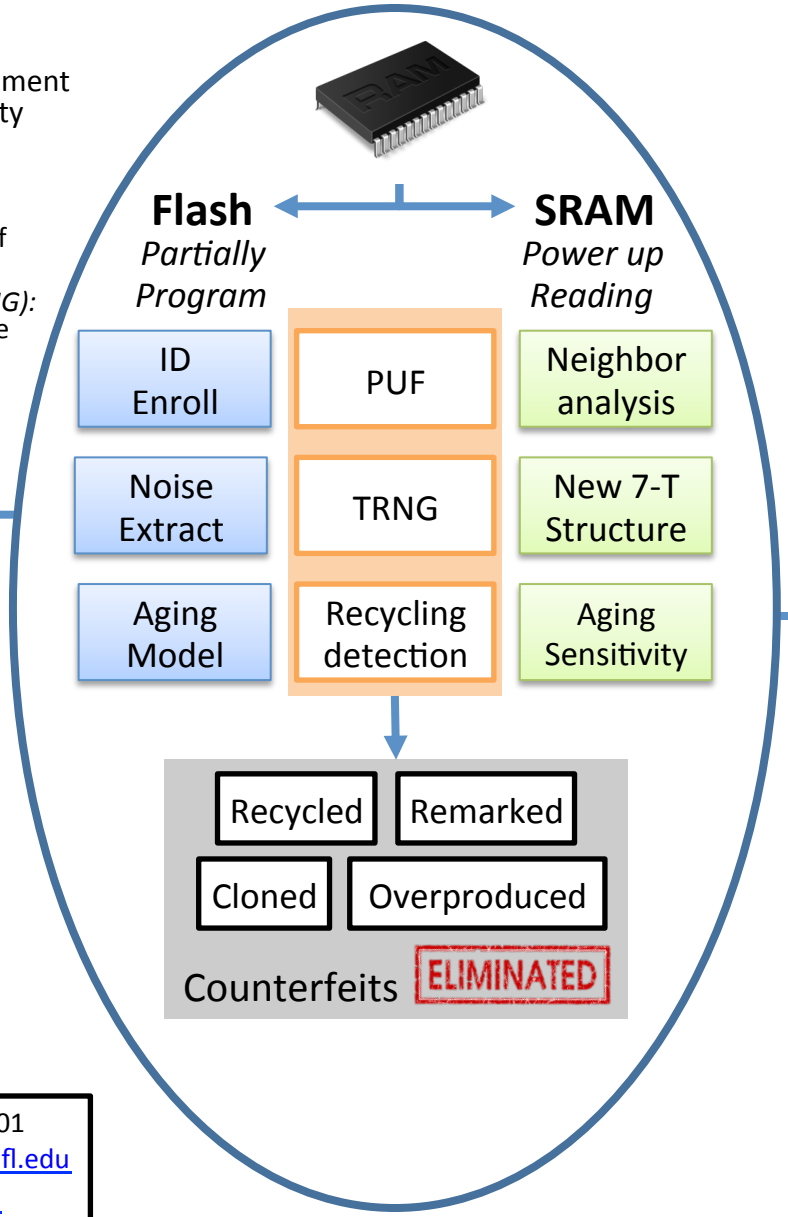
SaTC: STARSS: Design of Low-Cost Memory-Based Security Primitives and Techniques for High-Volume Products

Challenges: High overhead and enrollment costs when addressing security/reliability concerns, especially when multiple primitives are needed for

- *Physical Unclonable Function (PUF):* Uniqueness and reliability in the face of environmental conditions and aging
- *True Random Number Generation (TRNG):* Entropy requirements, especially in the face of environmental manipulation
- *Anti-Counterfeit (AC) Detection:* Few methods that are not only accurate but intrinsic/embedded (i.e., without need for additional sensors)

Solutions: Security primitives based on embedded and standalone memories (near zero overhead)

- Identification of unique properties, 'best' roles, and complementary roles of SRAM, DRAM, and Flash based on (i) volatility, density, and endurance; (ii) reliability, and randomness; (iii) sensitivity of power up behavior, latency, discharge, and partial programming to variations
- *First* memory-based detecting recycled (used) counterfeit memories and SoCs.
- All theory supported by experimental results from memories of different technology nodes and vendors.



Scientific Impacts:

- *SRAM*: (i) Optimal cell selection for PUF-based secret key and random number generation that removes the need for insecure and expensive post processing; (ii) SRAM-inspired circuit design for TRNG;. (iii) Aging sensitive bit prediction for recycled IC detection.
- *Flash:* Partially programming for (i) device ID generation and (ii) recycled IC detection.
- *DRAM:* Work-in-progress

Broader Impacts:

- Anti-counterfeit focus with impacts on economic innovation and growth of semiconductor and electronic industry, IP rights holders, and safety risks for critical and commercial systems
- Security primitives based on embedded memory which is abundantly available in microprocessors, DSPs, MCUs, etc., that benefit healthcare, automotive, military and intelligence, etc. systems
- This project has involved several undergraduate students and students from underrepresented groups.

NSF Project #1561023 / SRC Task #2648.001
PI: Mark Tehranipoor, tehranipoor@ece.ufl.edu
Co-PI: Domenic Forte, dforte@ece.ufl.edu