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

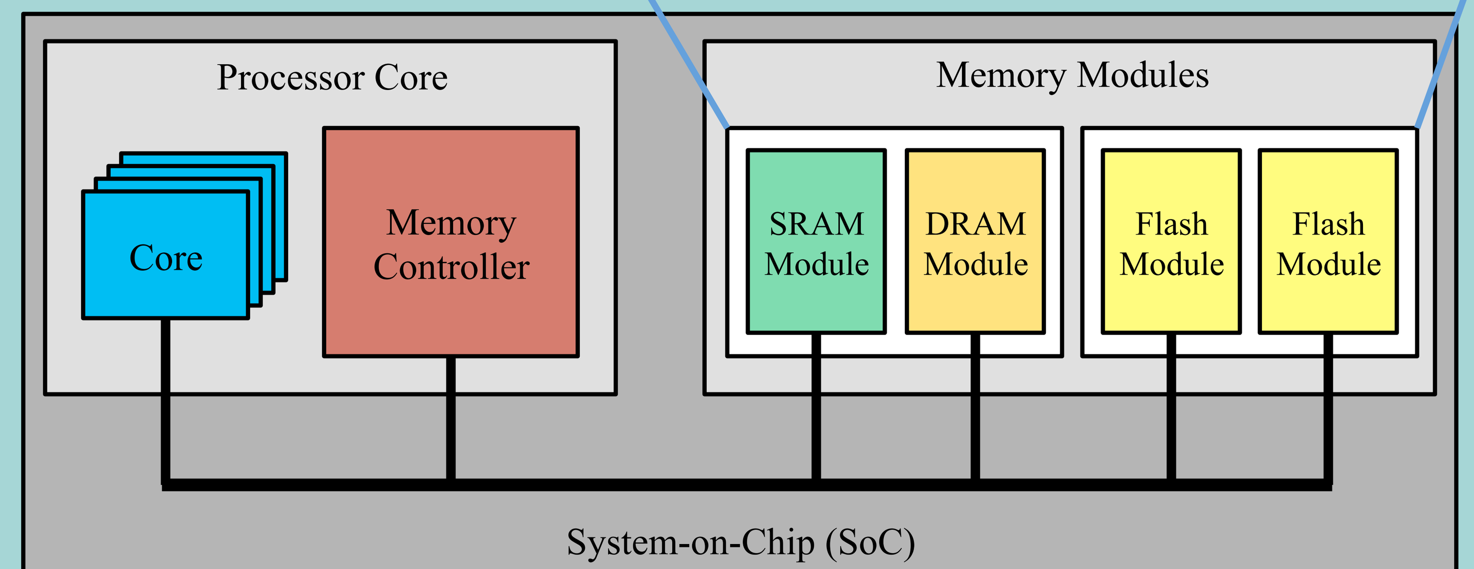
PI: Mark Tehranipoor, University of Florida, tehranipoor@ece.ufl.edu
Co-PI: Domenic Forte, University of Florida, dforte@ece.ufl.edu

Overview

- High overhead and enrollment costs especially when addressing security/reliability concerns that demand multiple primitives
- **Solution:** Security primitives based on embedded memories which are abundantly available in DSPs, MCUs, etc.
- **Goals**
  - Selection of "best" M-PUF and M-TRNG cells with low-cost tests suitable for high volume products
  - Determine "best" role for each region of memory hierarchy (SRAM, DRAM, Flash)
  - First memory based anti-counterfeit (M-AC) for recycling detection

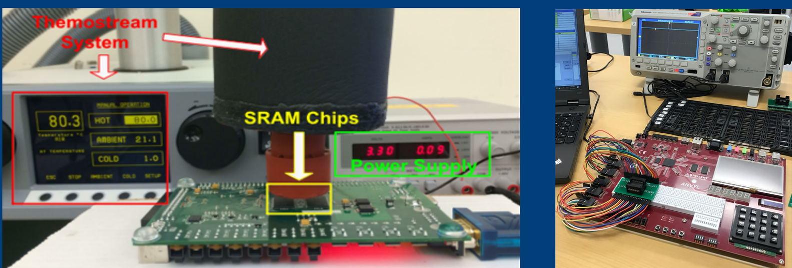
1. Physical Unclonable Functions (PUFs)
2. True Random Number Generators (TRNGs)
3. Anti-Counterfeit (AC) Technology*

* To our knowledge, this will be the first work to use memory for anti-recycling

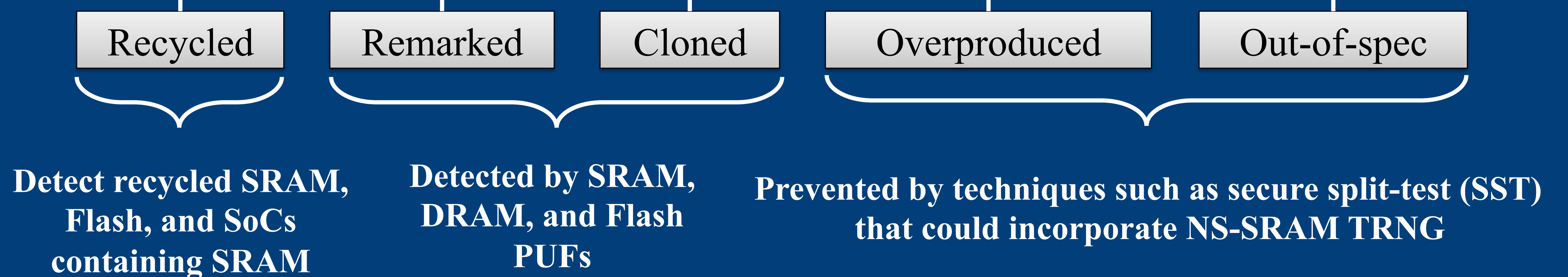


Silicon Experiment Stations

- The results for this project (shown in poster) are collected from real SRAM and Flash



Detection Coverage of Counterfeits Types by Proposed Techniques



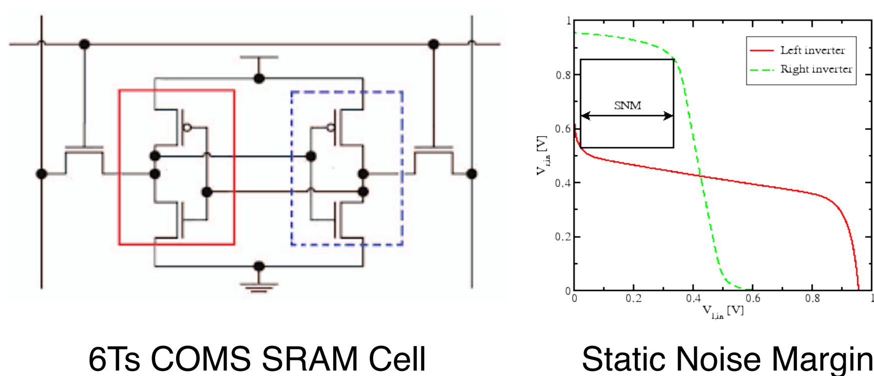
Detect recycled SRAM, Flash, and SoCs containing SRAM

Detected by SRAM, DRAM, and Flash PUFs

Prevented by techniques such as secure split-test (SST) that could incorporate NS-SRAM TRNG

SRAM Startup Behavior

- Cells favoring 0 or 1 at startup → ideal for PUF based keys and IDs

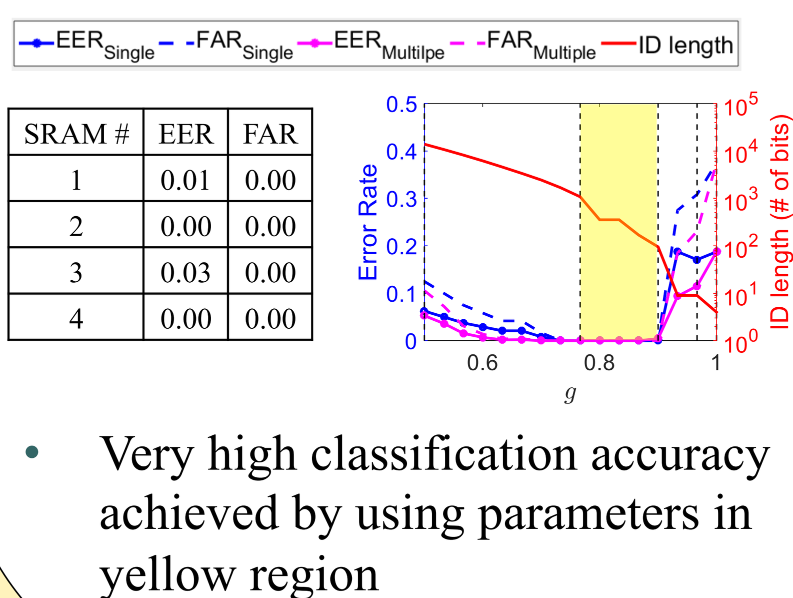


6Ts COMS SRAM Cell — Static Noise Margin

Neighborhood-based Bit Selection Metrics/Algorithms

- **Observation:** Stability of SRAM start-up behavior influenced by neighboring cells
- **Objective:** Metrics that identify SRAM cells ideal for PUF with low cost enrollment based on neighbors
  - **Total Neighborhood Analysis**: (i) identifies optimal number of stable cells around a PUF target cell; (ii) identifies aging sensitive bit (ASB) locations
  - **Neighborhood Pairs Analysis**: identifies location of physically adjacent neighbors based on stability
  - **Enrollment Condition Analysis:** (i) identifies best voltage-temperature corners for enrolling SRAM PUF
- **Results:** ~99.999% SRAM PUF against environmental variations and aging.

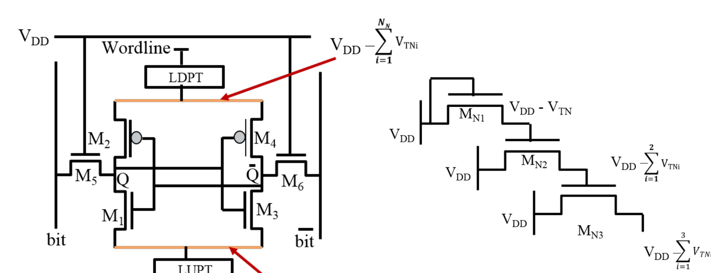
Recycling Detection for Standalone and Embedded SRAM



SRAM #	EER	FAR
1	0.01	0.00
2	0.00	0.00
3	0.03	0.00
4	0.00	0.00

- Very high classification accuracy achieved by using parameters in yellow region

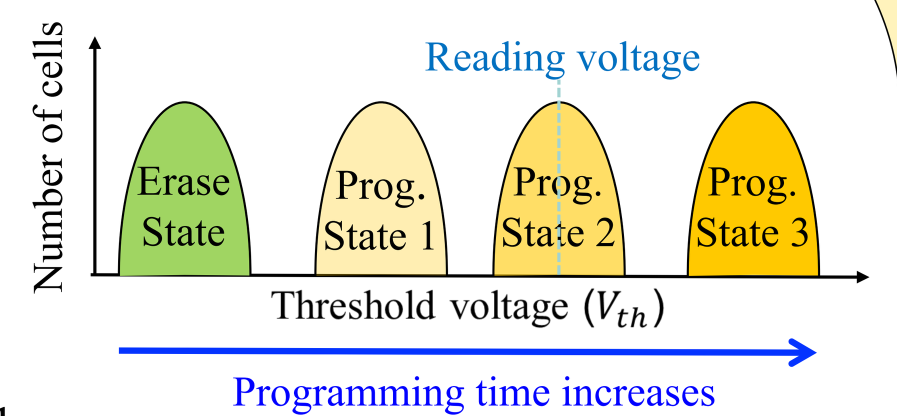
Noise-sensitive (NS) SRAM-based TRNG



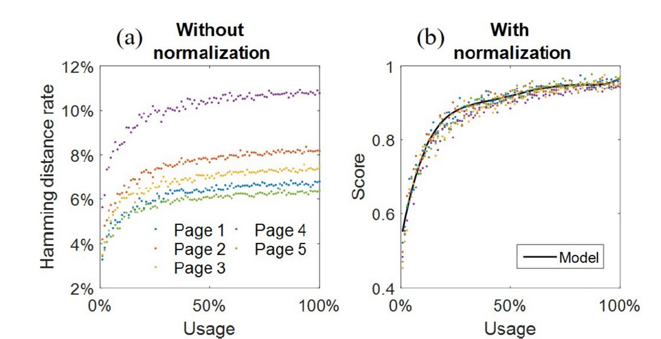
- **NS-SRAM Cell:** designed with reduced noise margins to improve TRNG entropy
- **Results:** ~25X more random than standard 6T-TRNG

Flash Partial Programming

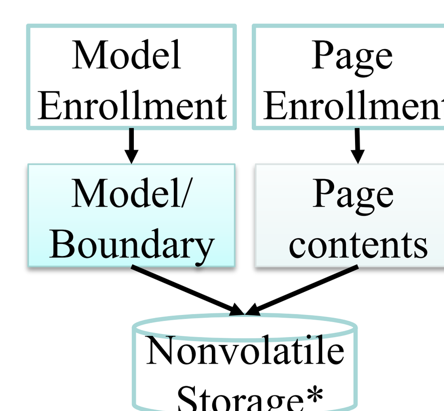
- Interrupt programming operation results in random write errors



- **Observations:**
  1) Rate of errors follows well-defined model with aging/use
  2) Locations w/ and w/out errors become intrinsic w/ aging/use
  3) Negligible variation in errors across voltage and temperature



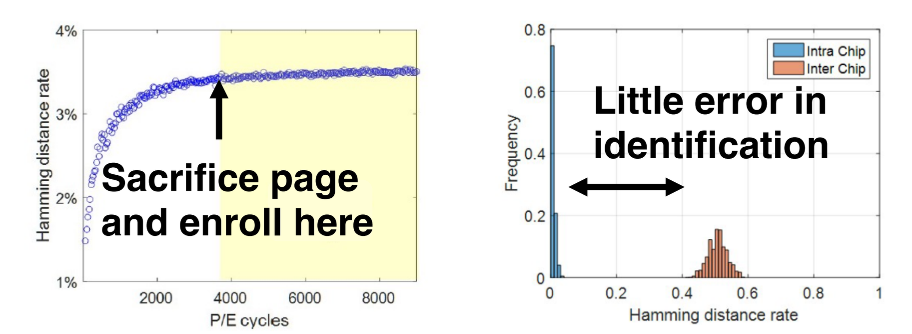
Enrollment



* Intrinsic to Flash

PUF/ID Generation

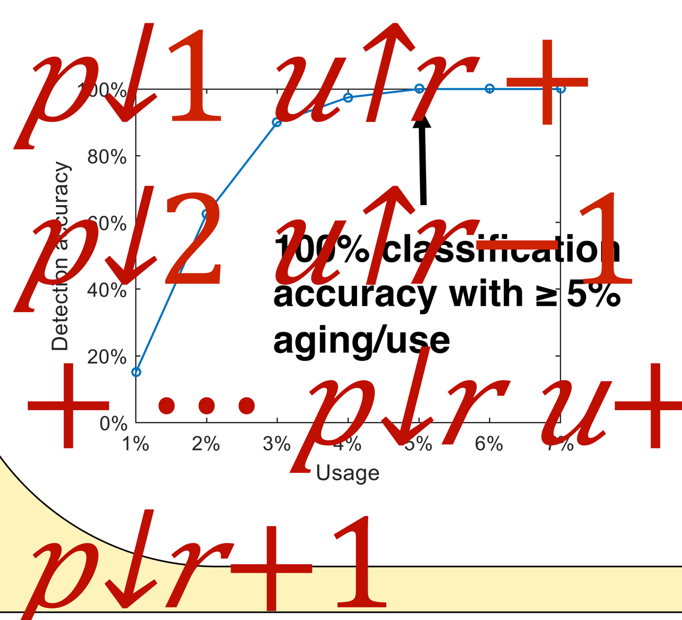
- Exploiting observations 1 and 3
- Storing locations w/ and w/out errors for ID



Recycled Flash Detection

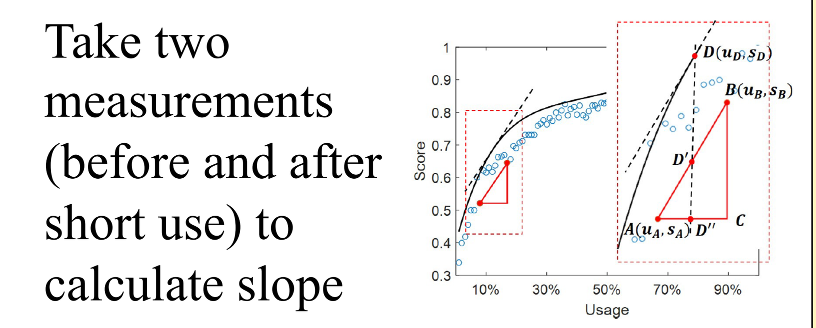
- Exploiting observation 1
- **Rough Usage Estimation:** Enroll coefficients of model and later predict amount of use

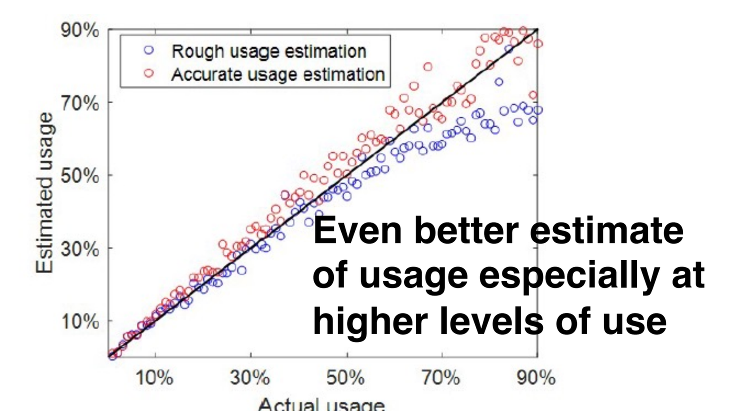
$p_1 u^r + p_2 u^{r-1} + \dots p_r u + p_{r+1}$



Accurate Usage Estimation

- Take two measurements (before and after short use) to calculate slope





Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN