Initial SRAM state as a Fingerprint and Source of True Random Numbers for RFID Tags

Dan Holcomb[1], Wayne P. Burleson[1], Kevin Fu[2]

[1]Electrical and Computer Engineering

[2]Computer Science

UNIVERSITY OF Massachusetts Amherst

RFIDSec July 2007, Malaga, Spain

Motivation

- Passive RFID circuits give rise to a need for low cost ID and RNG

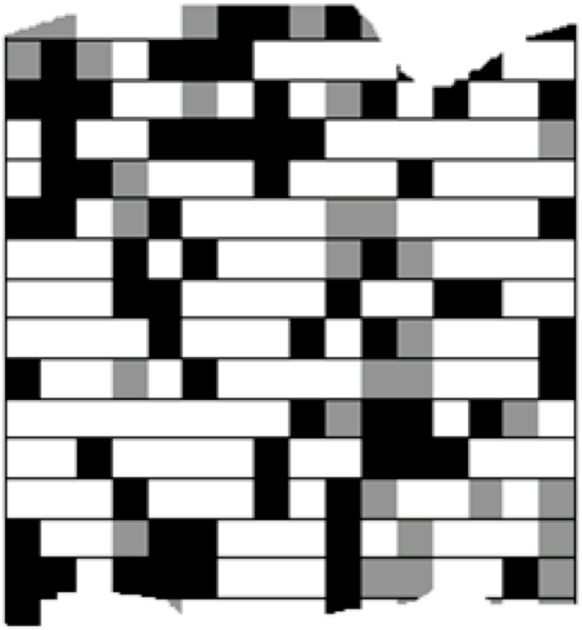
  Many circuits have identifying characteristics
  - Threshold voltages [Loftstrom00, Su07]
  - Path Delays [Gassend02]

  Many circuits have randomness
  - Delay [Suh05]
  - Jitter [Sunar07]
  - Metastability [Kinnimet02, Tokunaga07]

- Set out to explore whether ID and RNG can be accomplished **without dedicated circuitry**

Fingerprint Extraction and Random Numbers from SRAM (FERNS)

- Initial SRAM state is a physical fingerprint
  - A function of process variation and noise
- Fingerprint provides identification
  - Process variation is time invariant
- Fingerprint provides randomness
  - Noise is time variant
- Exploratory work
  - Your results may vary…



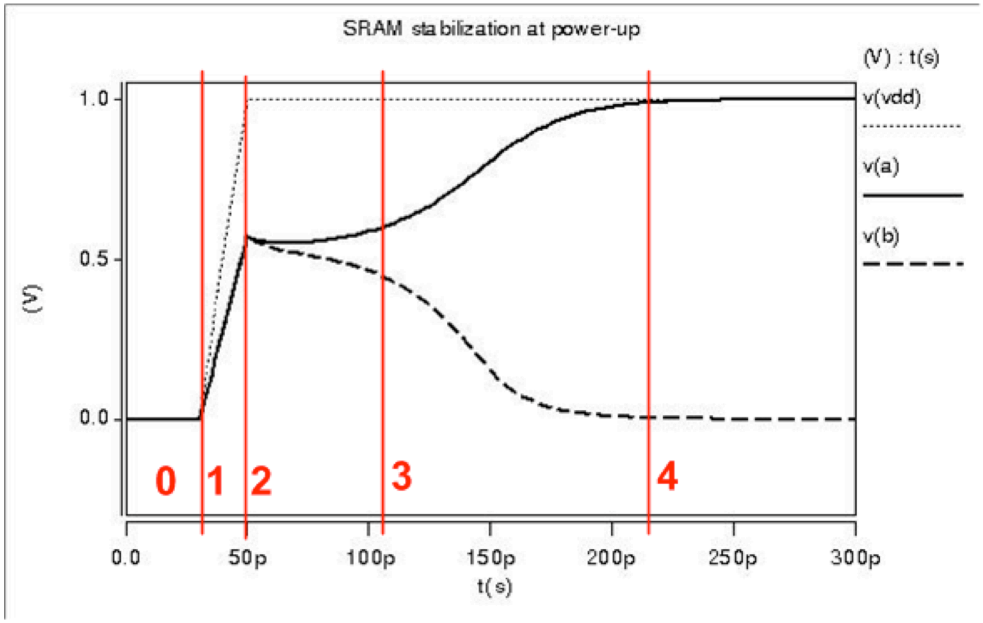
Why FERNS for RFID?

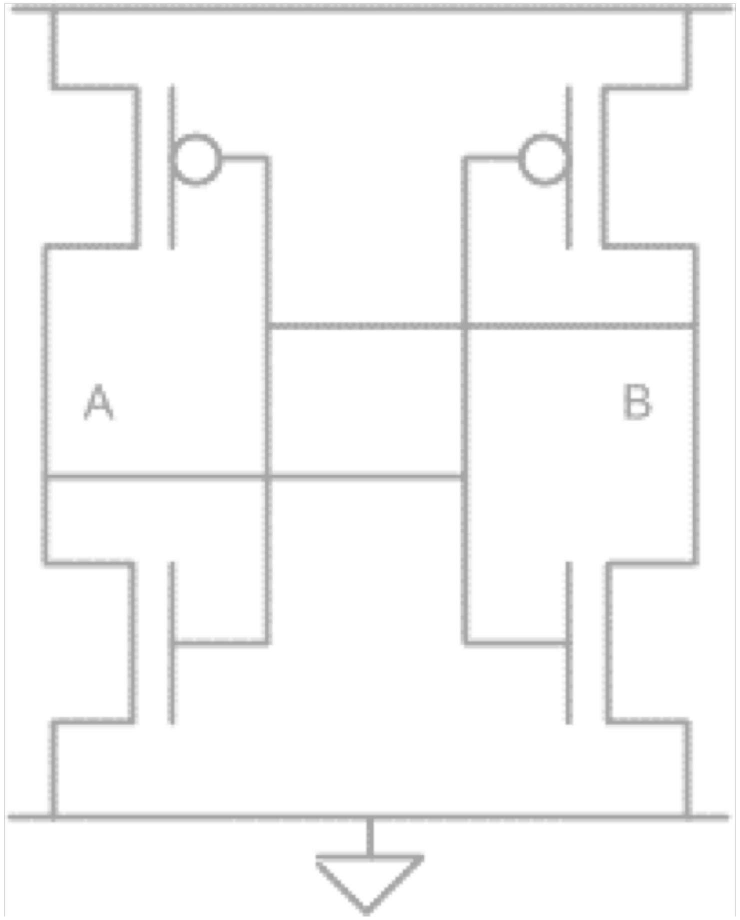
- Could help meet extreme cost constraints
  - Simple Process
    - No NVM technology – Simple CMOS
    - No programming
  - Existing hardware
    - RNG and ID circuit is “repurposed” as memory
- Matches passive tag usage model
  - ID an idle tag
    - ID is “reset” at end of session
  - Generate a single random number
    - Fixed computation model

Overview

- **Principle of Operation**
- Experimental Platforms
- Fingerprint Extraction
- Random Number Generation

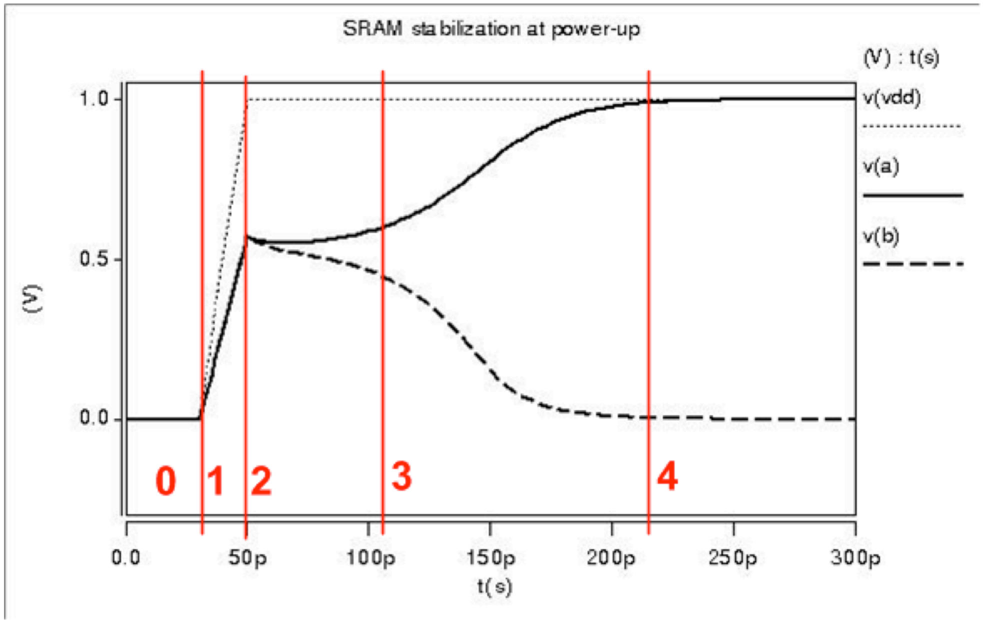
Power-up of Standard 6T CMOS SRAM cell

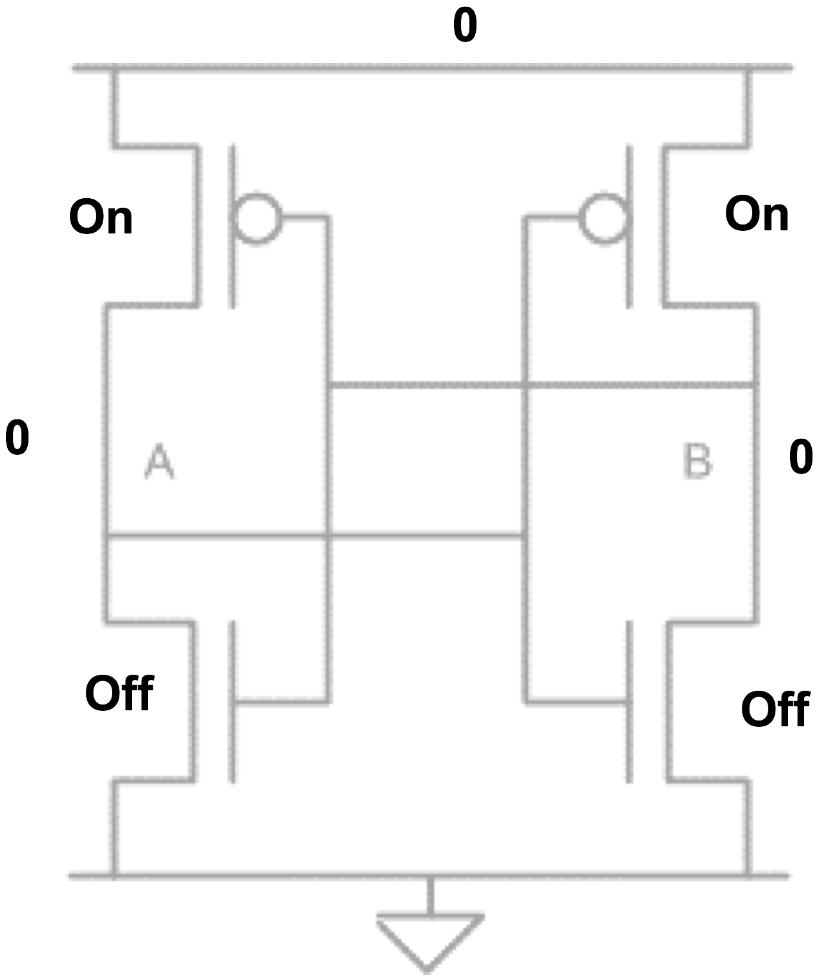




Power-up of Standard 6T CMOS SRAM cell

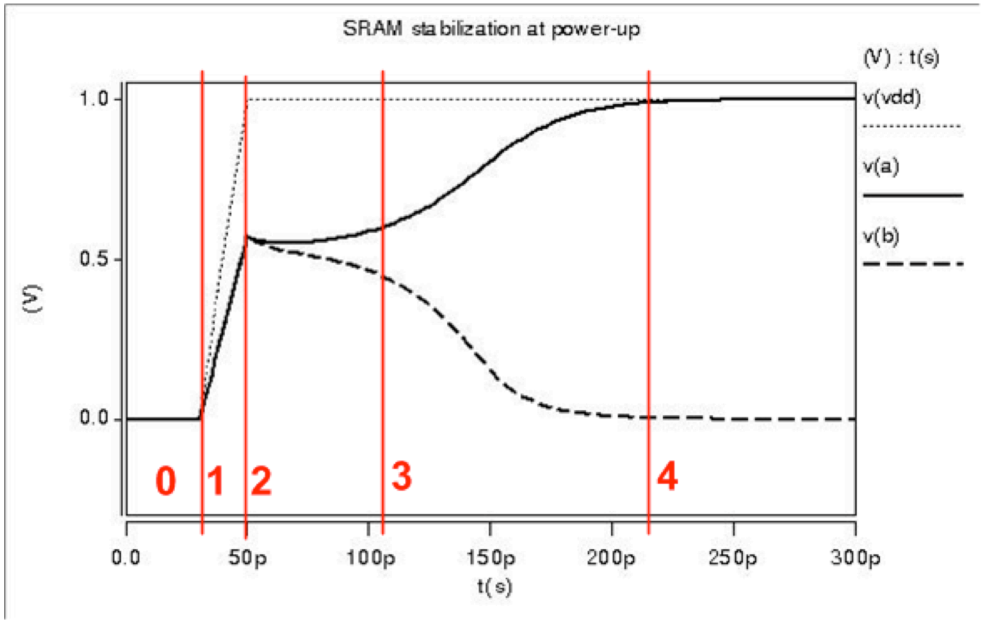
(0) Initial Condition

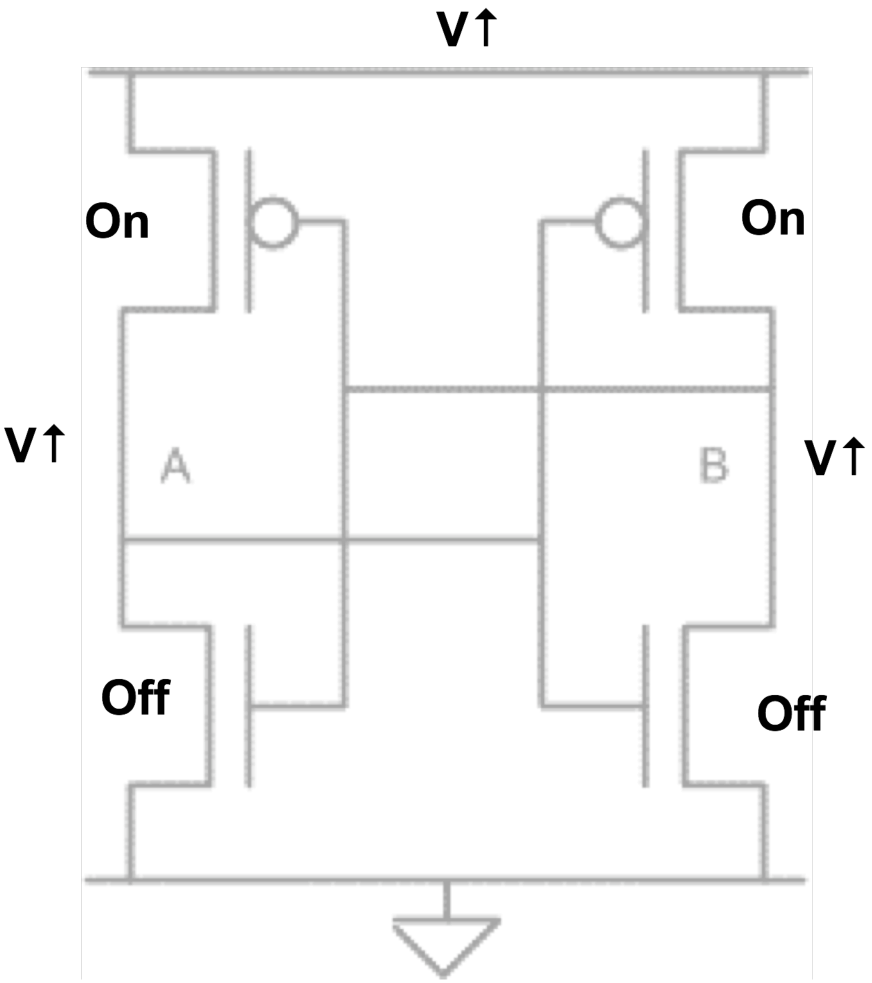




Power-up of Standard 6T CMOS SRAM cell

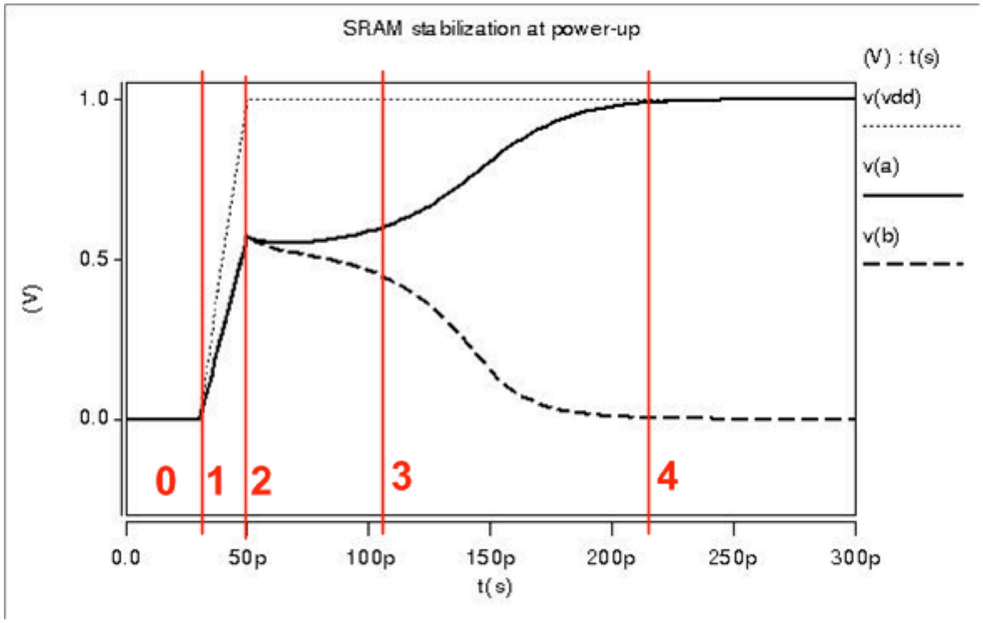
(1) Chip is powered on

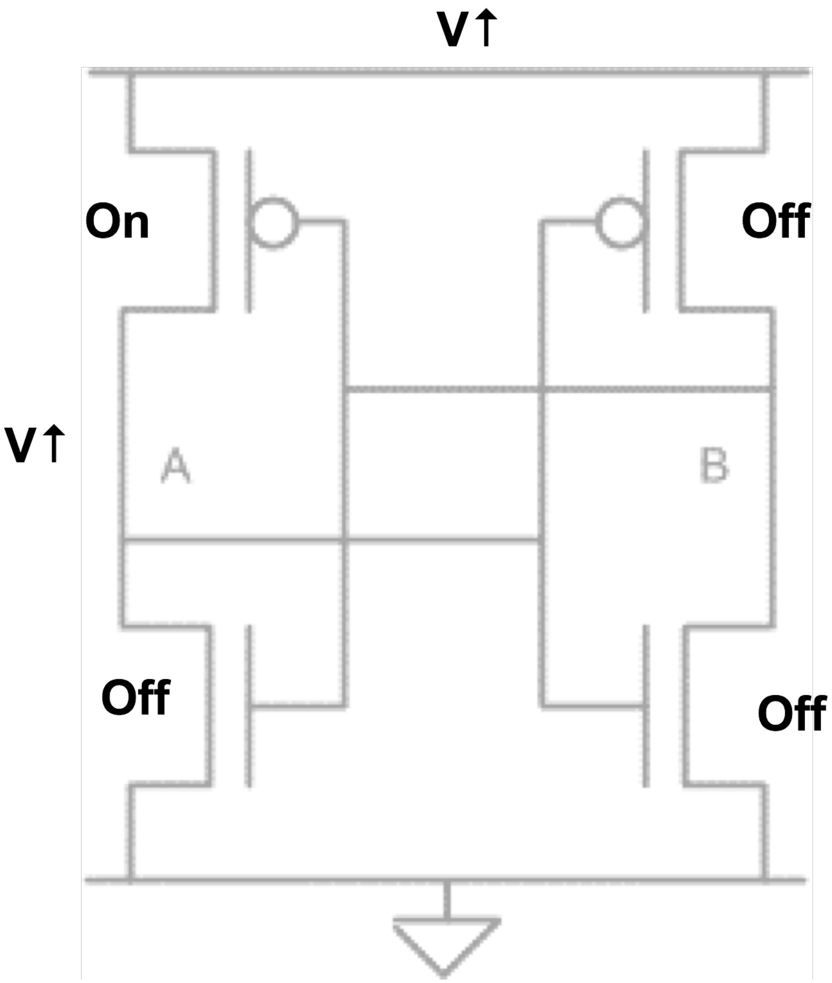




Power-up of Standard 6T CMOS SRAM cell

(2) PMOS Threshold Reached





V↑

V↑

On

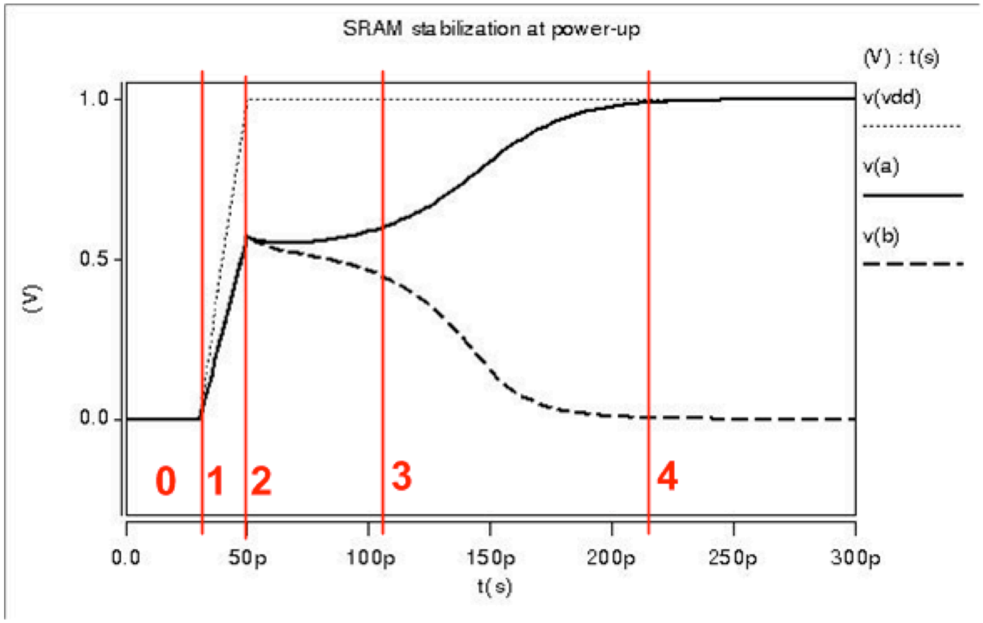
Off

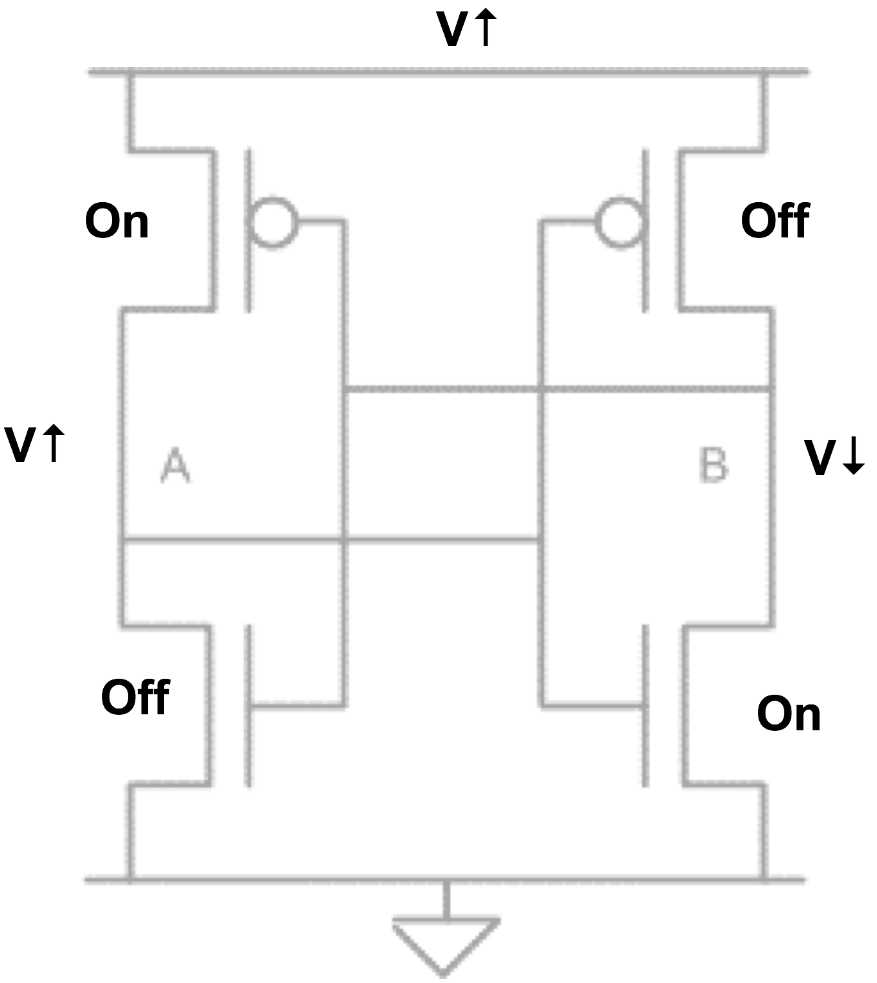
Off

Off

Power-up of Standard 6T CMOS SRAM cell

(3) NMOS Threshold Reached





V↑

On

Off

V↑

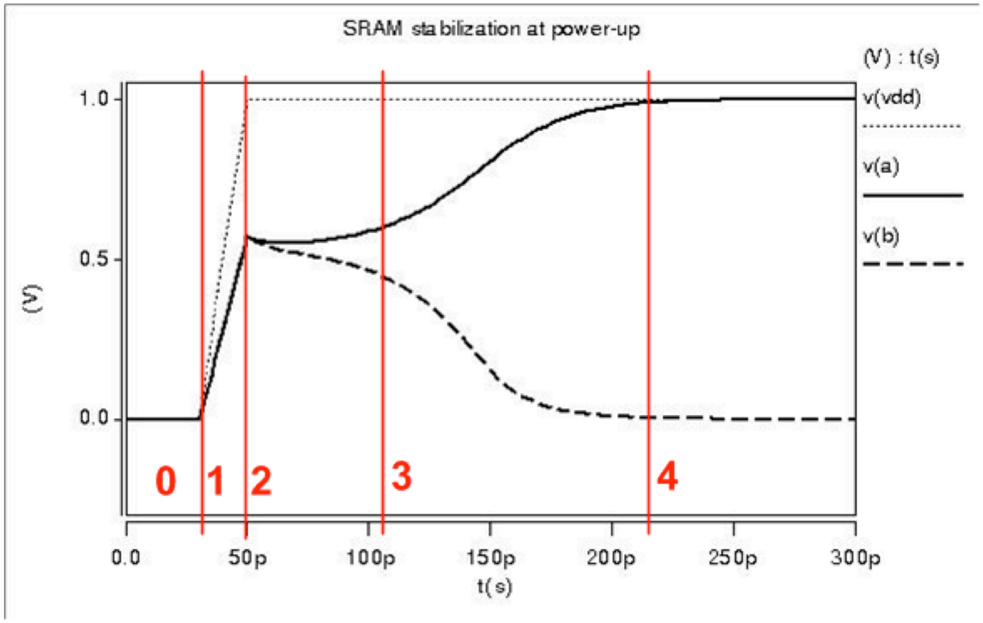
V↓

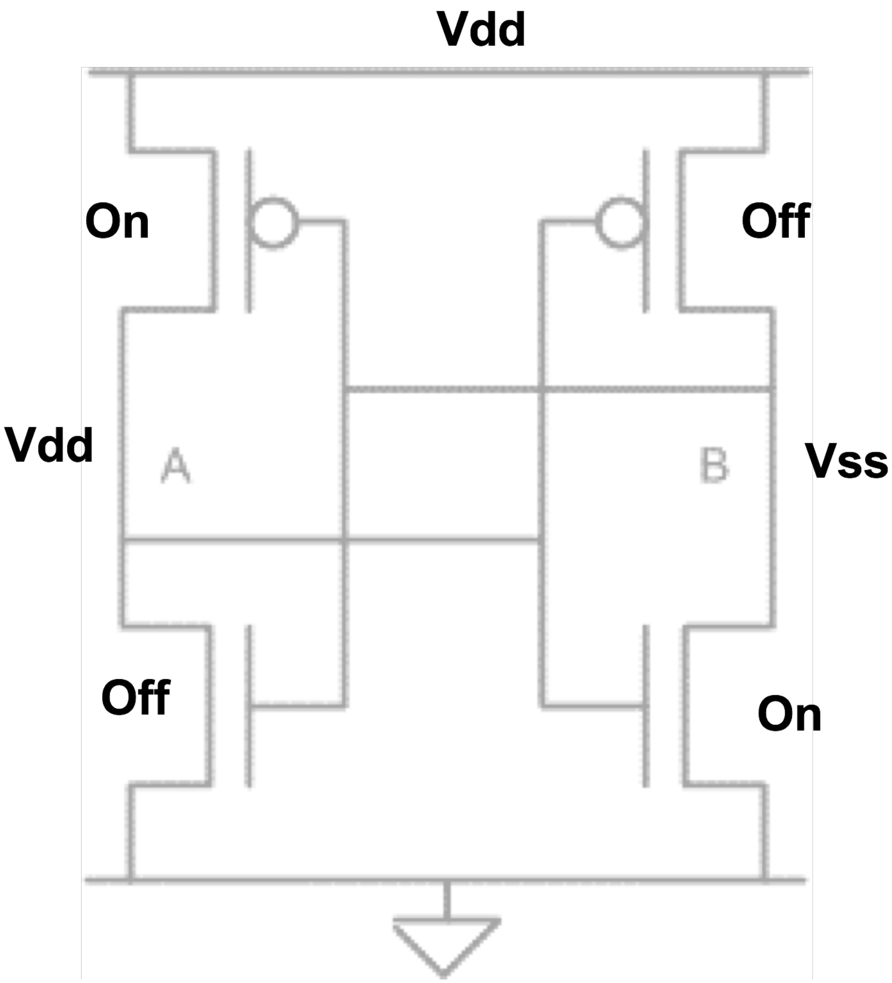
Off

On

Power-up of Standard 6T CMOS SRAM cell

(4) Stable State





Vdd

On

Off

Vdd

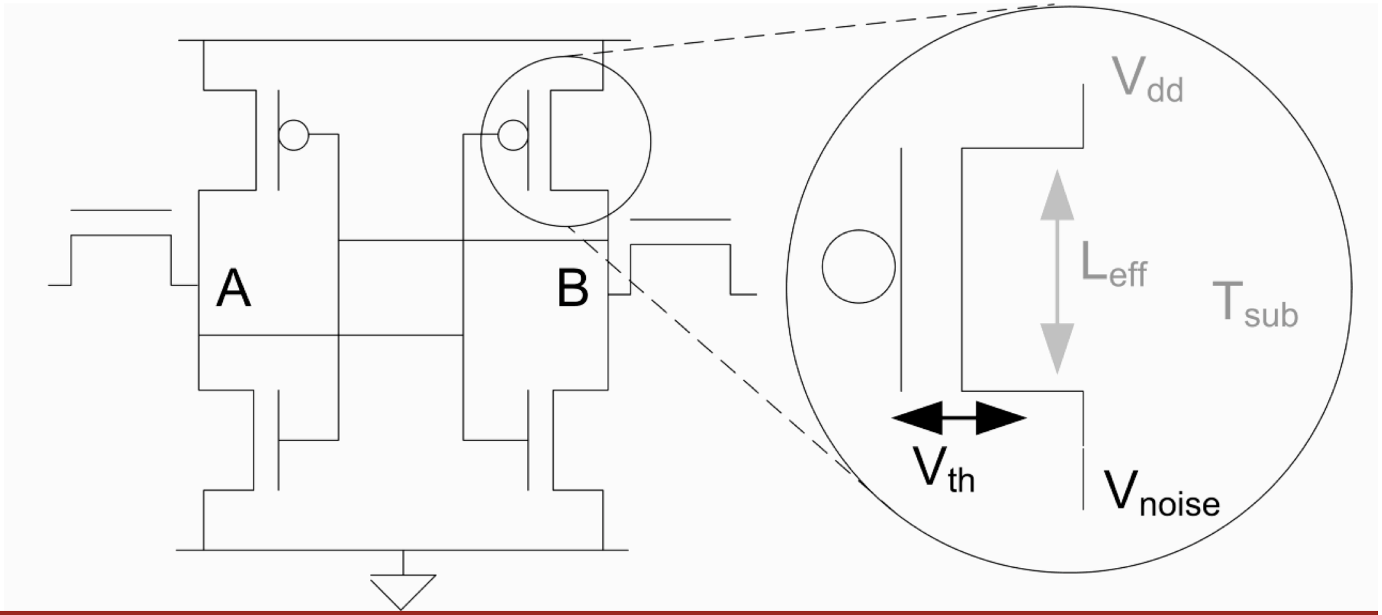
Vss

Off

On

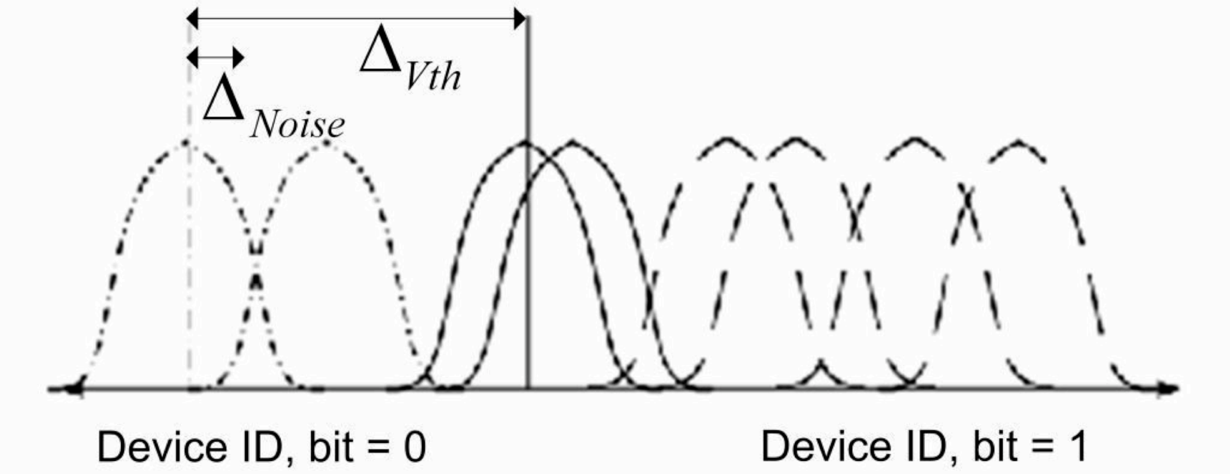
Impact of Variation

- Randomness imparted in manufacture
- Impacts fight between cross-coupled inverters
  - Only local mismatch
  - Primarily V_{th} – random dopant concentrations [Tang97]
  - Also L_{eff} [Friedberg2005]



Impact of Noise

- Time varying sources of randomness influence cell outcomes
  - Thermal noise
  - Shot noise
- Other noise sources likely to be common mode
  - Supply noise
  - Temperature

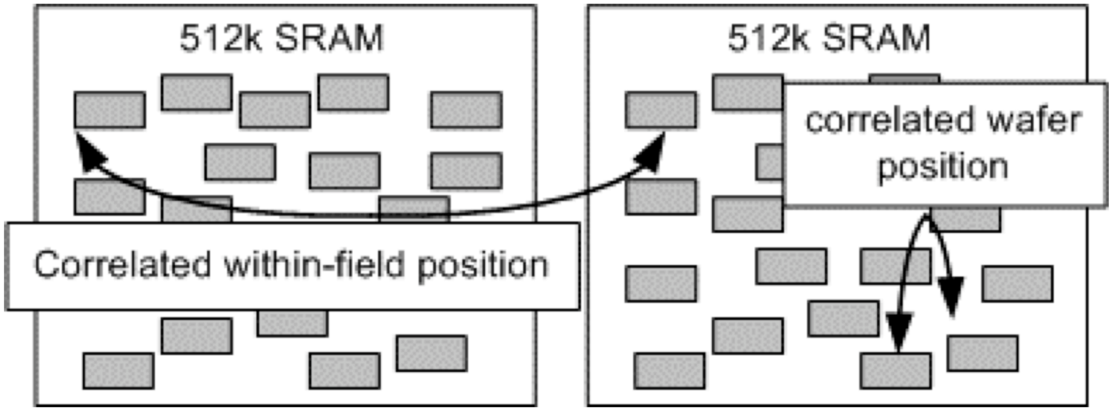


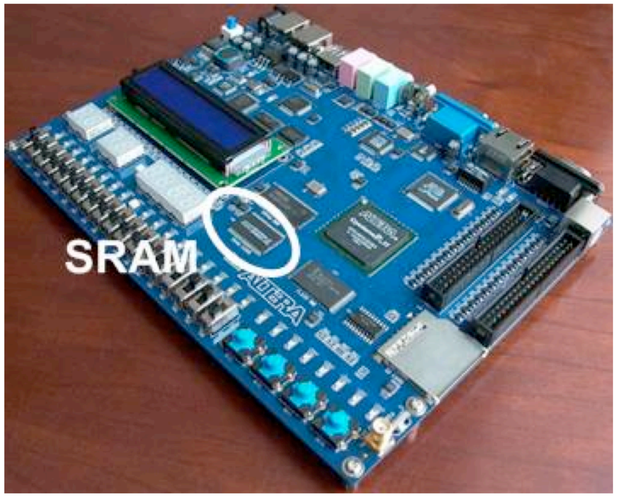
Overview

- Principle of Operation
- **Experimental Platforms**
- Fingerprint Extraction
- Random Number Generation

160 Virtual Tags

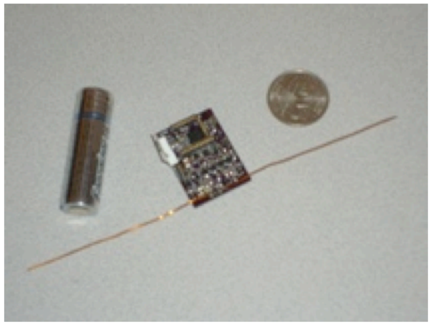
- 256 byte blocks of memory
  - Located across 8 instances of a 512K SRAM
  - 20 virtual tags on each
    - Same addresses on each chip
  - Comparison of potentially correlated cases





Ultra-Low-Power Microcontrollers

- Wirelessly-Powered Platform for Sensing and Computation* [Smith06]
  - Passive UHF device using TI MSP430
  - EPC gen 1 - 64 bit packets
  - 15 qty of 64 bit IDs (across 3 chips)



- 10 TI MSP430 chips
  - 256 byte SRAM memory (.1uA)
  - read out via JTAG debugger

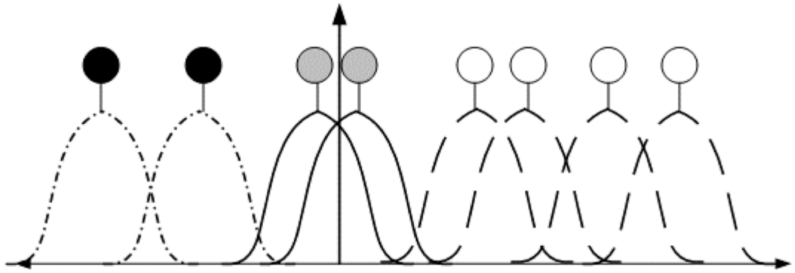
*Intel Research Seattle

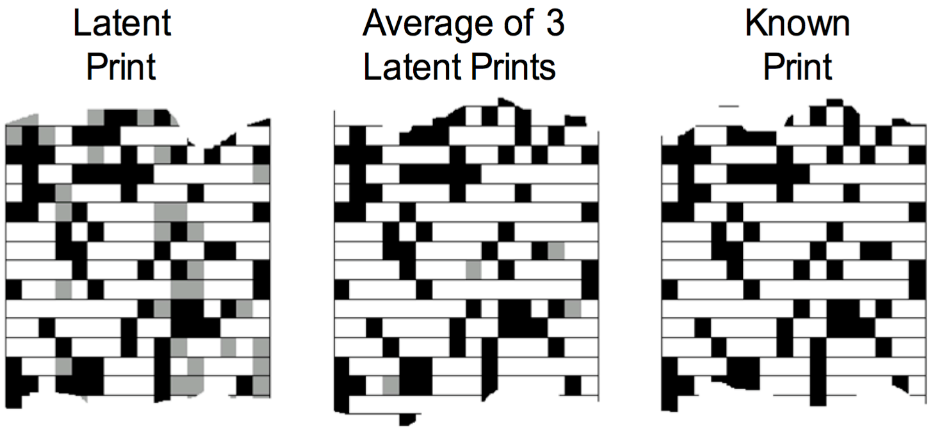
Overview

- Principle of Operation
- Experimental Platforms
- **Fingerprint Extraction**
- Random Number Generation

Fingerprint Identification

- *Latent print* is a single print
  - Influenced by noise
- *Known print* is bitwise mean of latent prints
  - Removes noise

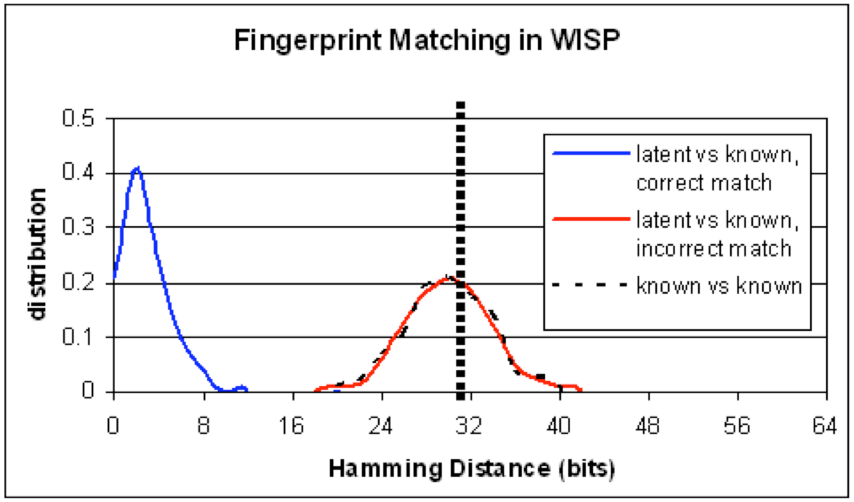


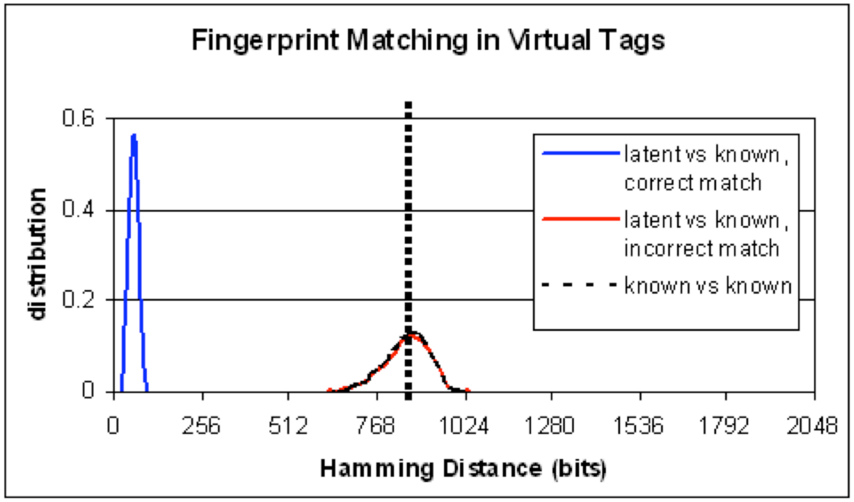


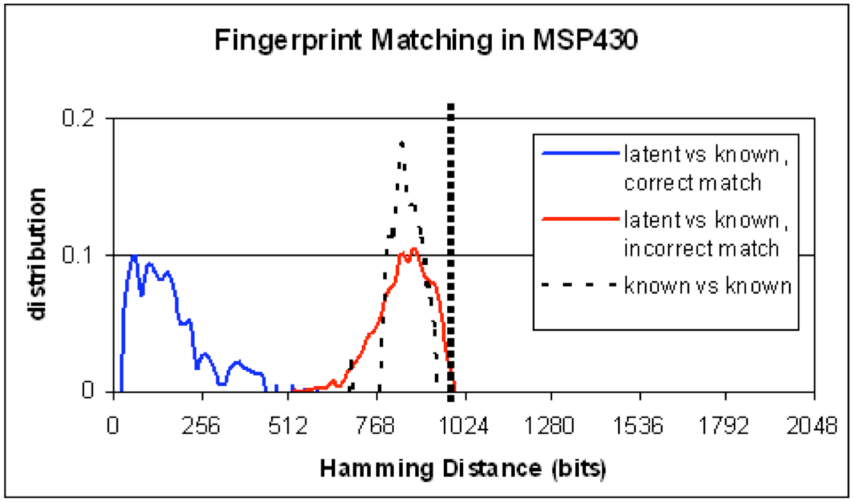
- Identification requires latent prints be similar to known print of same circuit, but different from other circuits
- Hamming distance used for comparison

Fingerprint Matching

- Measured over varied scenarios
- MSP430 shows more noise
  - Possible noise from local circuitry
  - High performance vs. low leakage
- JTAG debugger induces correlation
  - Passive power does not





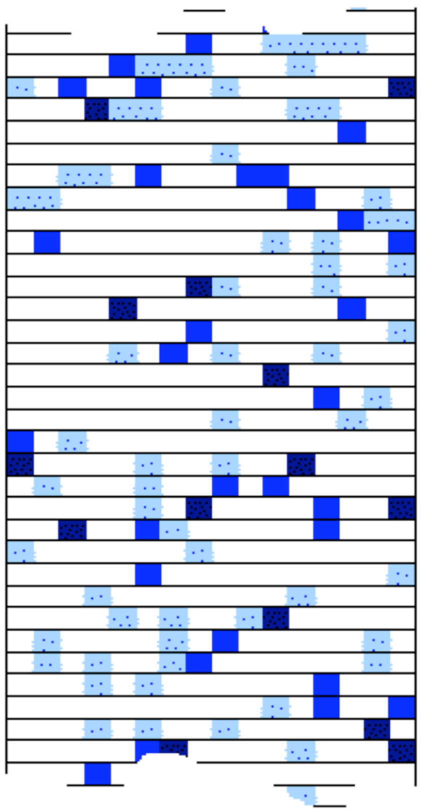


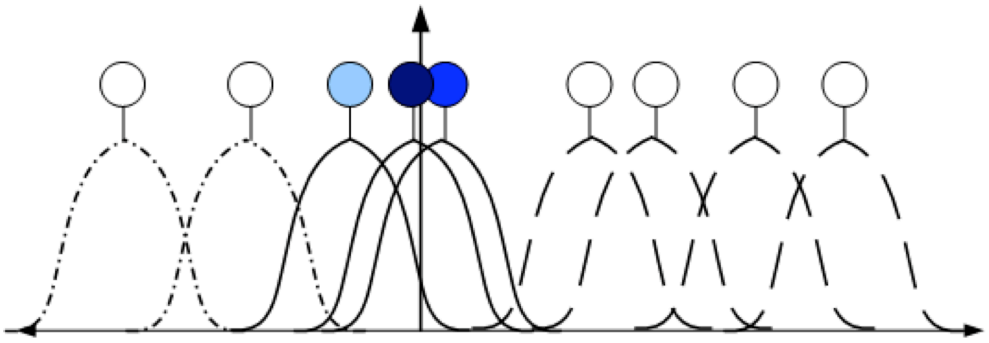
Overview

- Principle of Operation
- Experimental Platforms
- Fingerprint Extraction
- **Random Number Generation**

Random Number Generation

- Randomness comes from SRAM cells that are well matched
  - Per bit of virtual tag:
    - .050 bits of min entropy
    - .093 bits of Shannon entropy
  - Distributed across memory array
    - Possible tolerance to attack
    - Locations vary from chip to chip





KEY			
▩	0.333 < P(x=1) < 0.666		
🟦	0.166 < P(x=1) < 0.333	or	0.666 < P(x=1) < 0.833
░	0 < P(x=1) < 0.1666	or	0.833 < P(x=1) < 1

Entropy Extraction

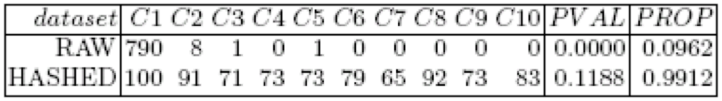
- Use universal hashing to extract 128 random bits from 2048 bits of fingerprint
  - NH Polynomial (PH) hashing algorithm [Yüksel04]
    - Hashing performed in software

$$PH_K(M) = \sum_{i=1}^{8} (m_{2i-1} + k_{2i-1})(m_{2i} + k_{2i})$$

$$M = (m_1, \dots, m_{16}) \qquad K = (k_1, \dots, k_{16})$$

$$m_i, k_i \in P_{64} \text{ polynomials over GF(2)}$$

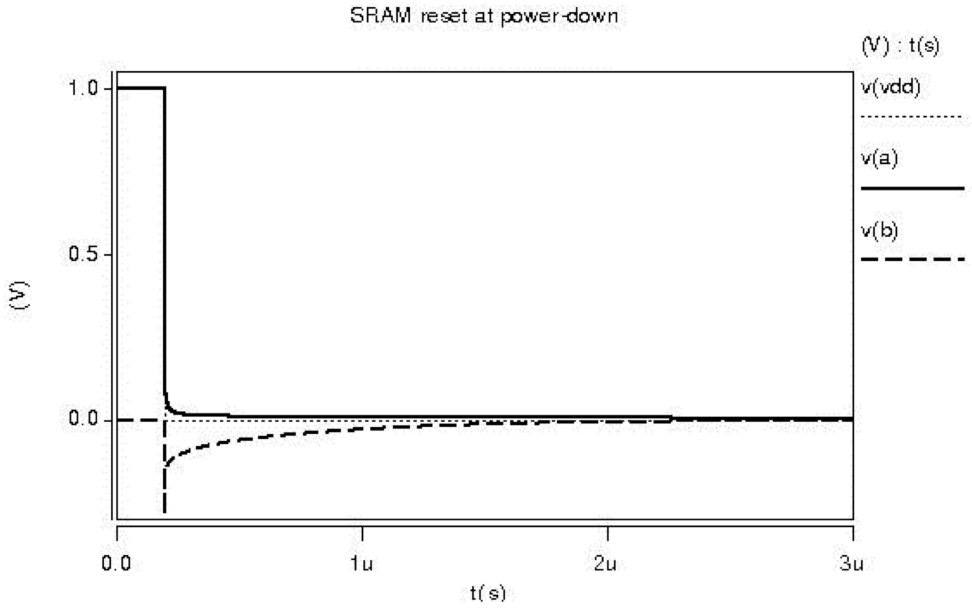
  - Passes NIST approximate entropy test



dataset	*C1*	*C2*	*C3*	*C4*	*C5*	*C6*	*C7*	*C8*	*C9*	*C10*	*PVAL*	*PROP*
RAW	790	8	1	0	1	0	0	0	0	0	0.0000	0.0962
HASHED	100	91	71	73	73	79	65	92	73	83	0.1188	0.9912

Future Work

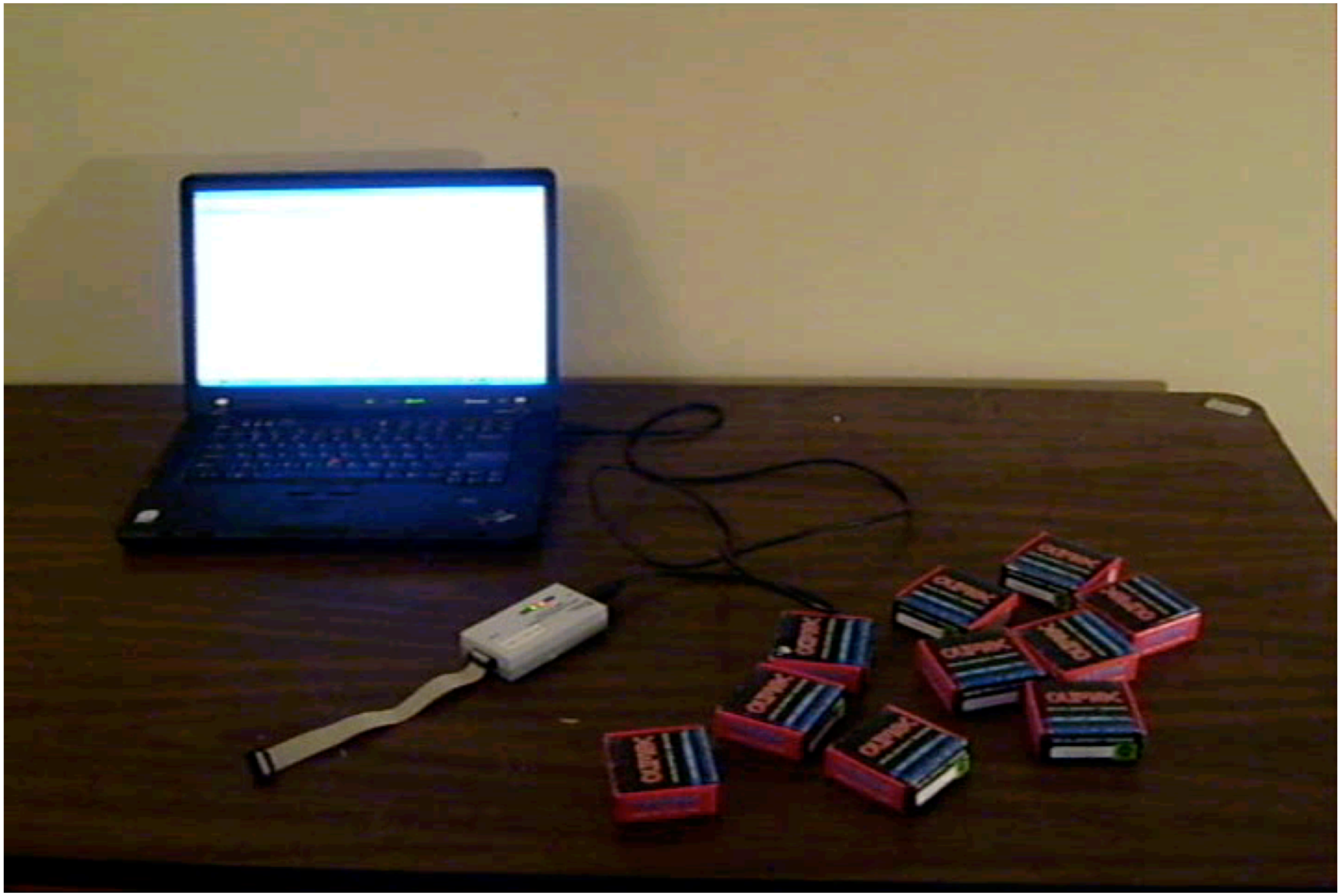
- Further development of RNG
  - Improve and analyze extraction
- Explore vulnerability to side channel attacks
- Effects of aging on threshold voltages
- Make better use of RAM cells
  - More reliable ID



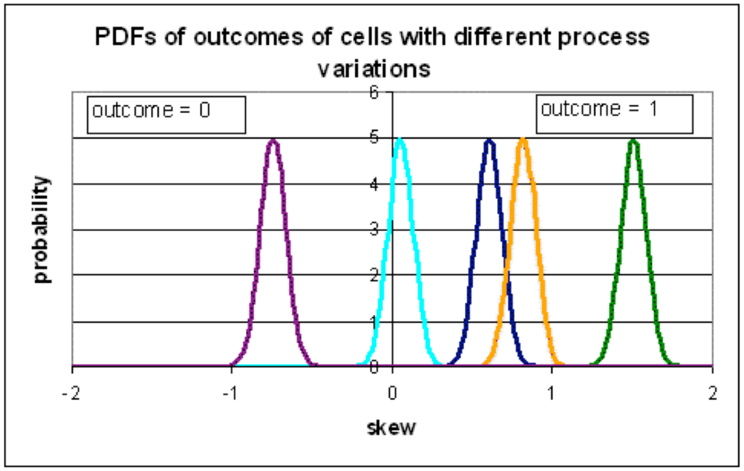
Conclusions

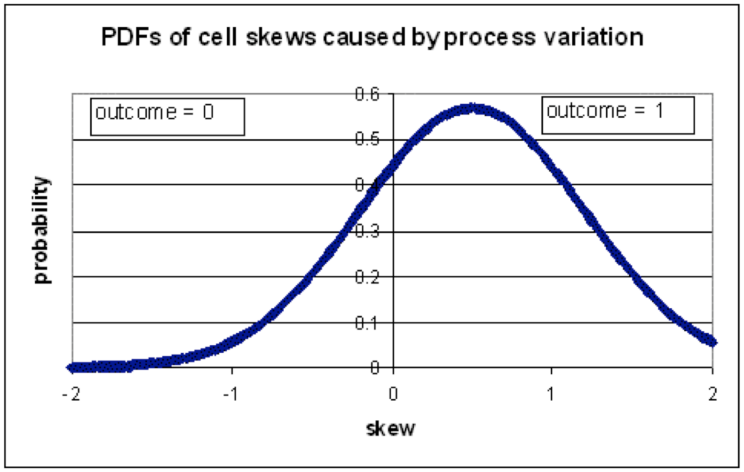
- SRAM power-up generates usable fingerprints
  - SRAM chips and microcontroller memory
  - Passive and active power
- Large differences across chips provide identification
- Smaller differences across trials can be used for Random Number Generation
- Potentially a good match for RFID
- Preliminary work
  - To be explored further

Backup - Fingerprint Matching Demonstration

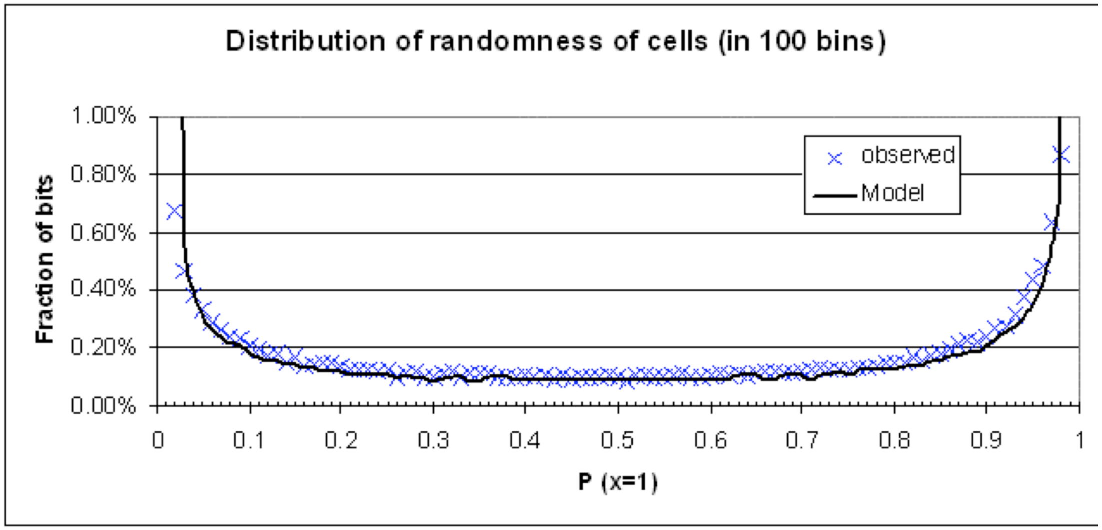


Backup – Virtual Tags Model vs Experiment


PDFs of outcomes of cells with different process variations

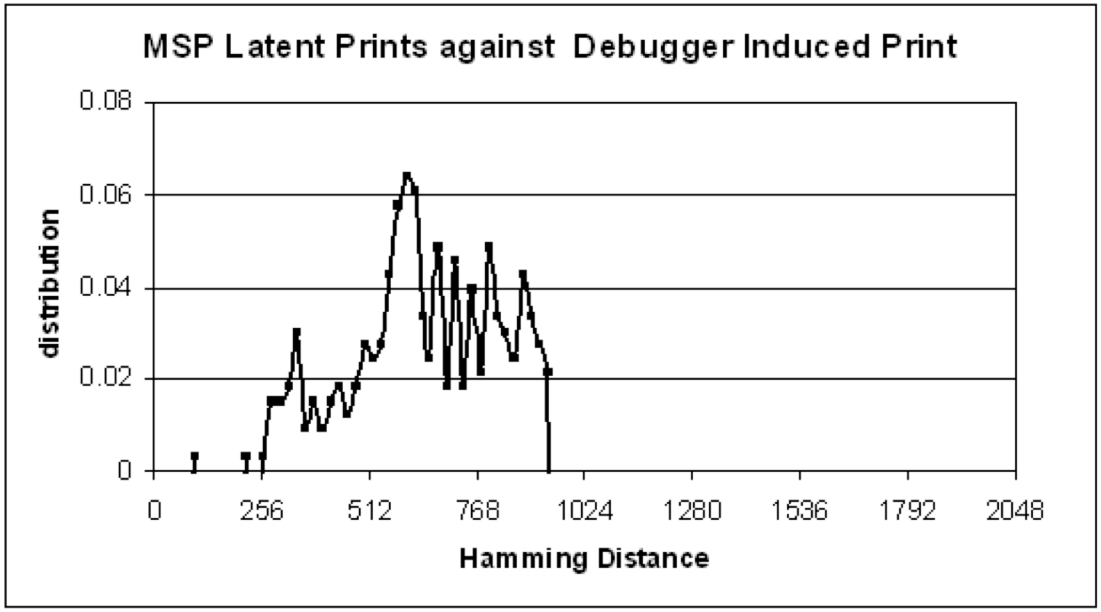

PDFs of cell skews caused by process variation

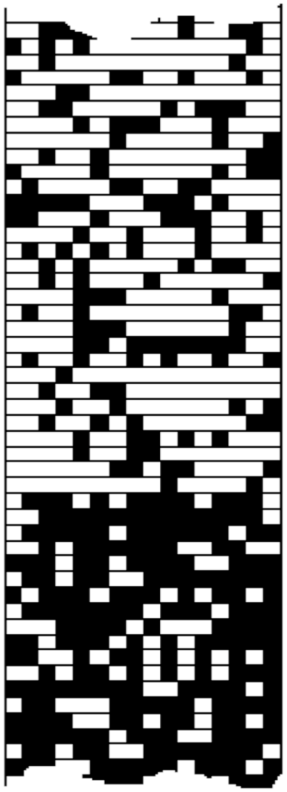
0.40 <P(x=1) < 0.60	2.16%
0.30 <P(x=1) < 0.70	4.25%
0.20 <P(x=1) < 0.80	6.77%
0.10 <P(x=1) < 0.90	10.28%
0.01 <P(x=1) < 0.99	19.77%
P(x=1) =0.00	**16.44%**
P(x=1) =1.00	**63.79%**


Distribution of randomness of cells (in 100 bins)

Backup – JTAG induced Correlation

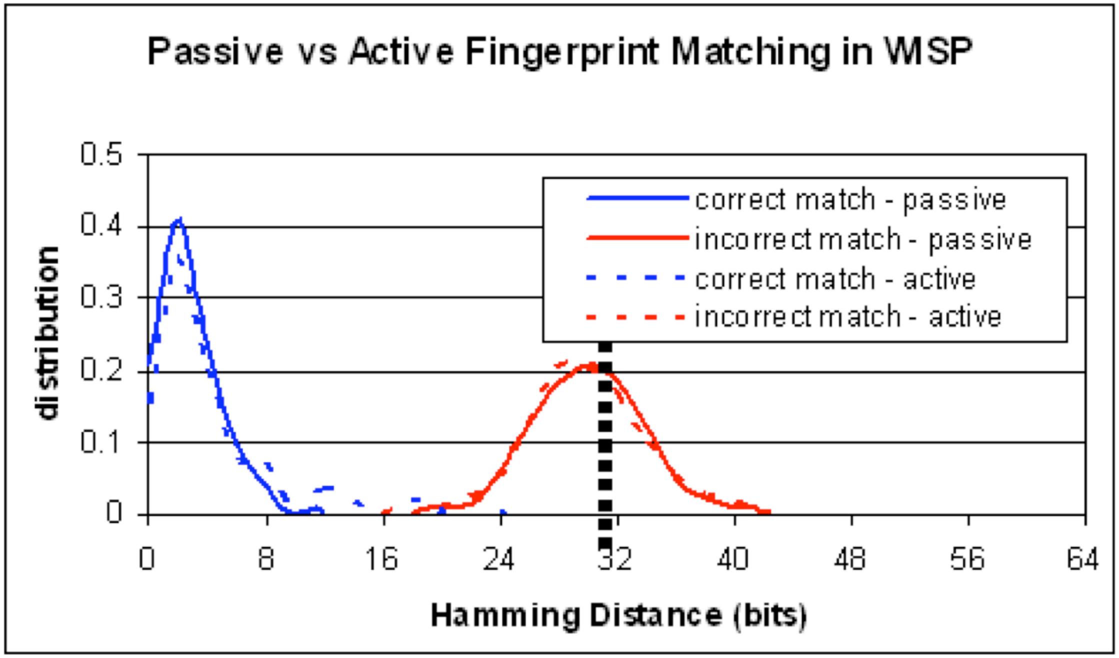
- Using JTAG causes all devices to tend towards same initial state
  - Only on MSP430
  - Doesn't occur with passive power
  - Cause unknown
  - Negatively Impacts fingerprint matching





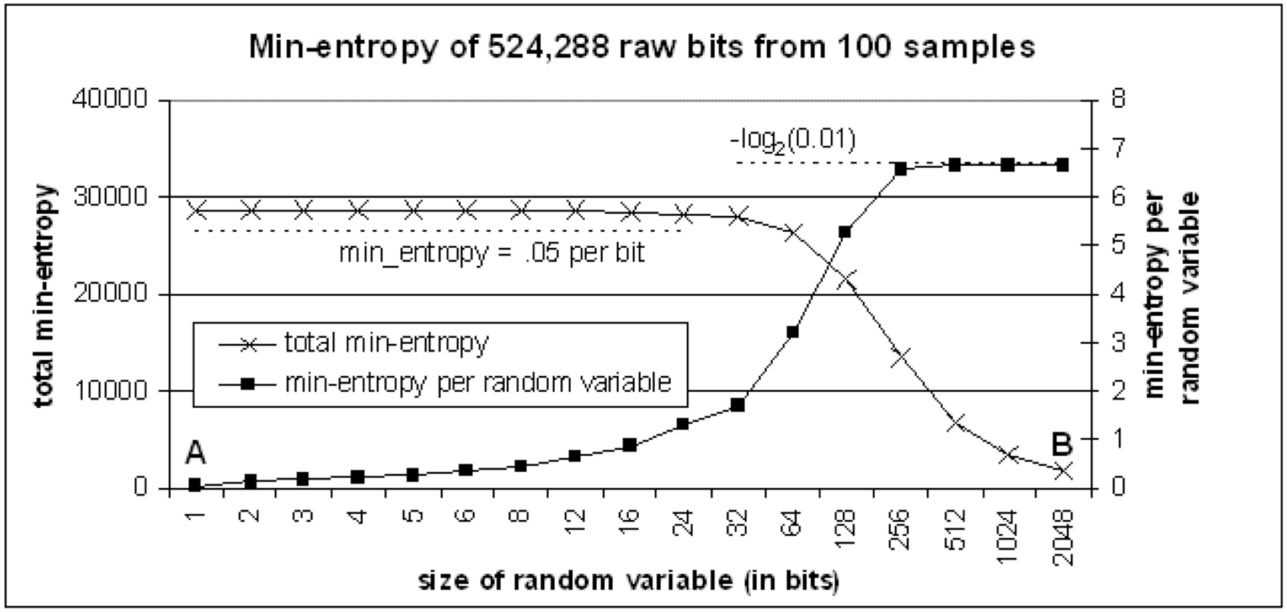
Backup – Passive vs Active power

- Same devices, same bits of memory
  - Powered through JTAG vs passively powered
  - Shows debugger induced correlation



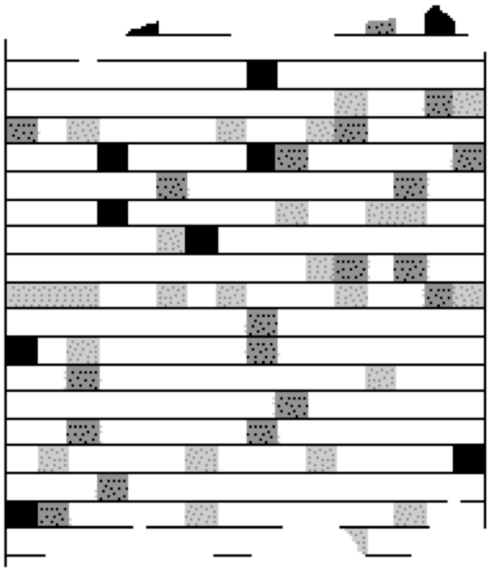
Backup – Min Entropy

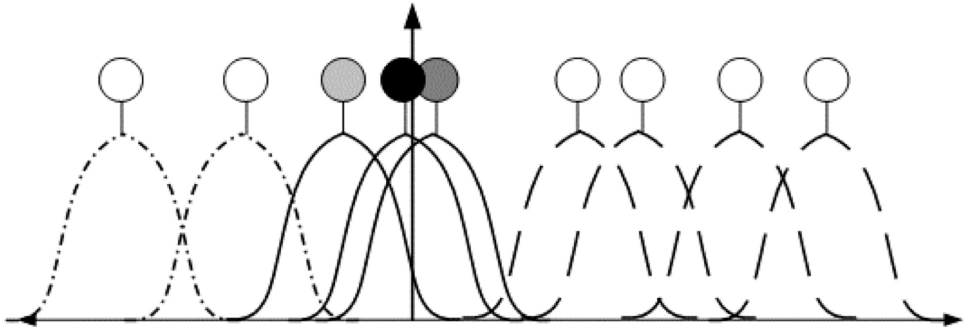
- Per bit of Virtual Tag SRAM:
  - 0.050 bits of min entropy $$H_\infty(x) = -\log_2(\max_i p_i)$$
  - 0.093 bits of Shannon entropy $$H(x) = -\sum_i p_i \log_2(p_i)$$



Random Number Generation

- Randomness comes from SRAM cells that are well matched
  - Per bit of virtual tag:
    - .050 bits of min entropy
    - .093 bits of Shannon entropy
  - Distributed across memory array
    - Possible tolerance to attack
    - Locations vary from chip to chip





KEY			
■	0.333 < P(x=1) < 0.666		
▩	0.166 < P(x=1) < 0.333	or	0.666 < P(x=1) < 0.833
░	0 < P(x=1) < 0.1666	or	0.833 < P(x=1) < 1