DRV-Fingerprinting

Using Data Retention Voltage of SRAM Cells for Chip Identification

Dan Holcomb[1], **Amir Rahmati**, Mastooreh Salajegheh, Wayne Burleson, Kevin Fu

1 UC Berkeley

Presented in RFIDSec'12

The Problem

How can we identify/authenticate a chip?

Use Physical Characteristics

Store Identification Data

The Problem

How can we identify/authenticate a chip?

- ✓ Immutable
- ✓ Resistant to Cloning
- ✓ Resistant to Tampering

Use Physical Characteristics

Physical Unclonable Functions

- SRAM Power-up State (Holcomb'07)
- Flash Memory (Prabhu'11)
- Statistical Delay Variations of Wires and Transistors (Lee'04)

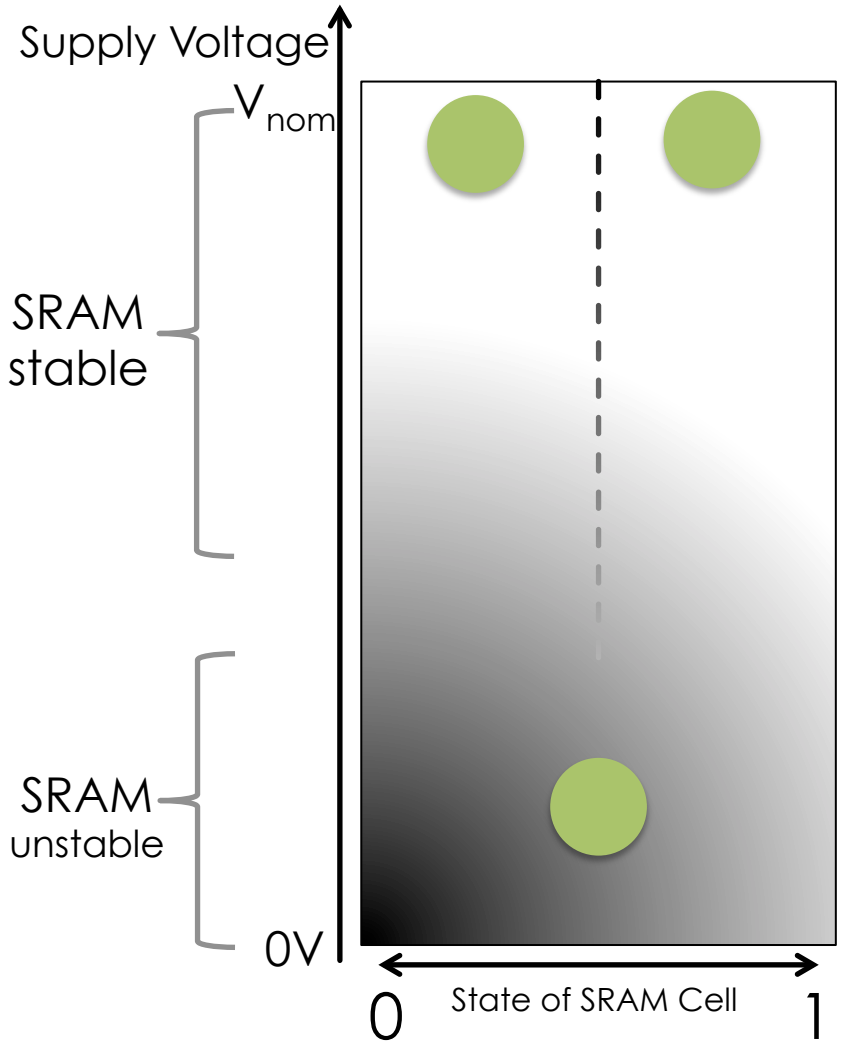
SRAM Power-up State

- ✓ Widely available
- ✓ Low cost and physically random
- ✗ Need large sample size
- ✗ Unreliable precision on small samples

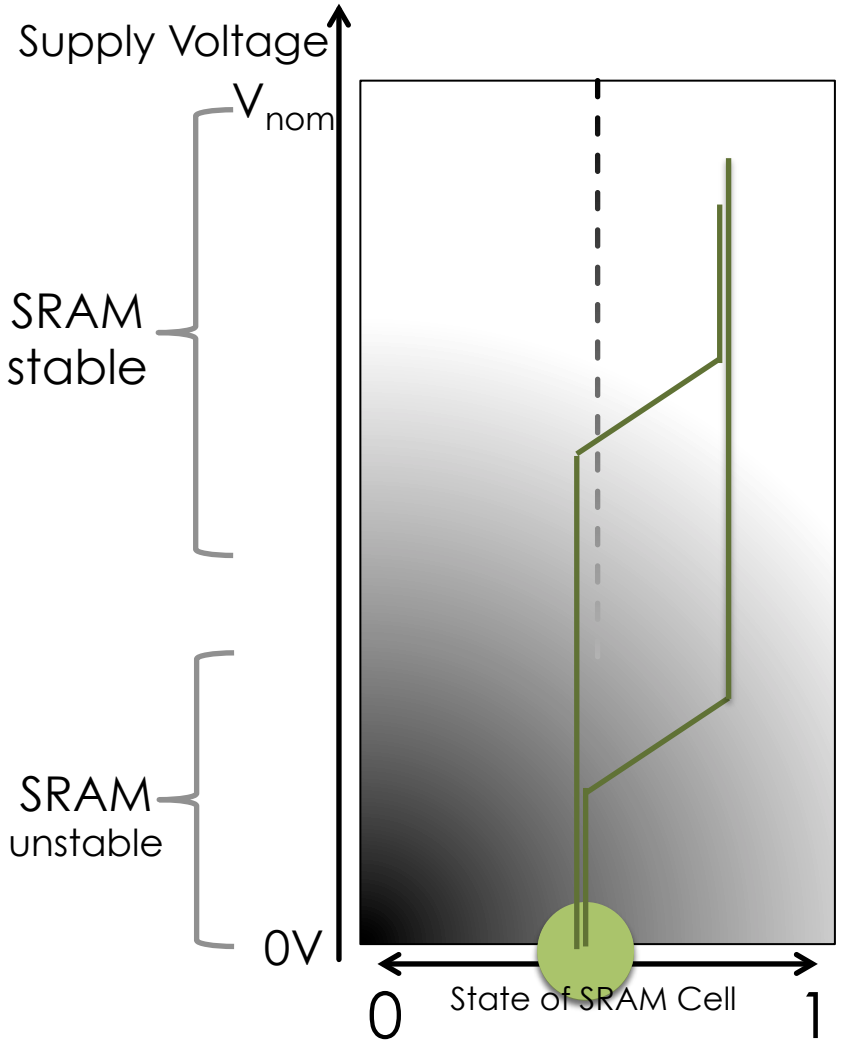
Our Solution

a new method for chip fingerprinting that uses Data Retention Voltage (DRV) in SRAM as the identifier

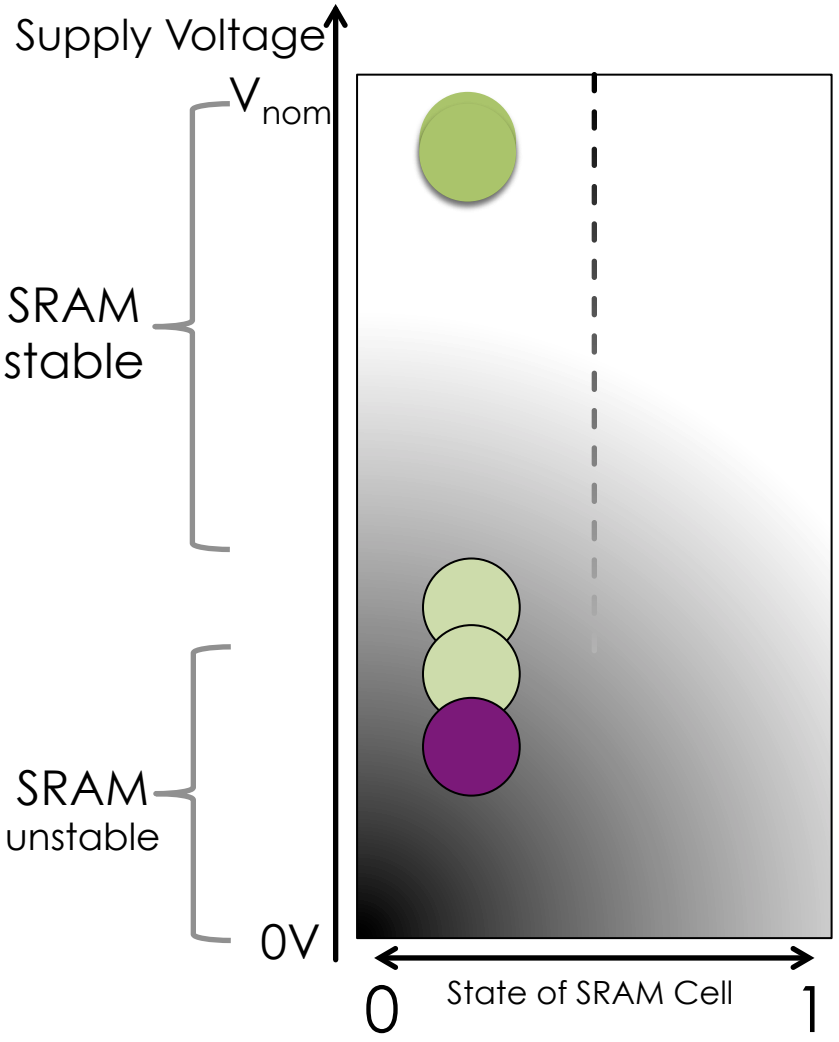
SRAM Behavior



Power-up Fingerprint



DRV Fingerprints



Our Algorithm

① Initialize SRAM to 1

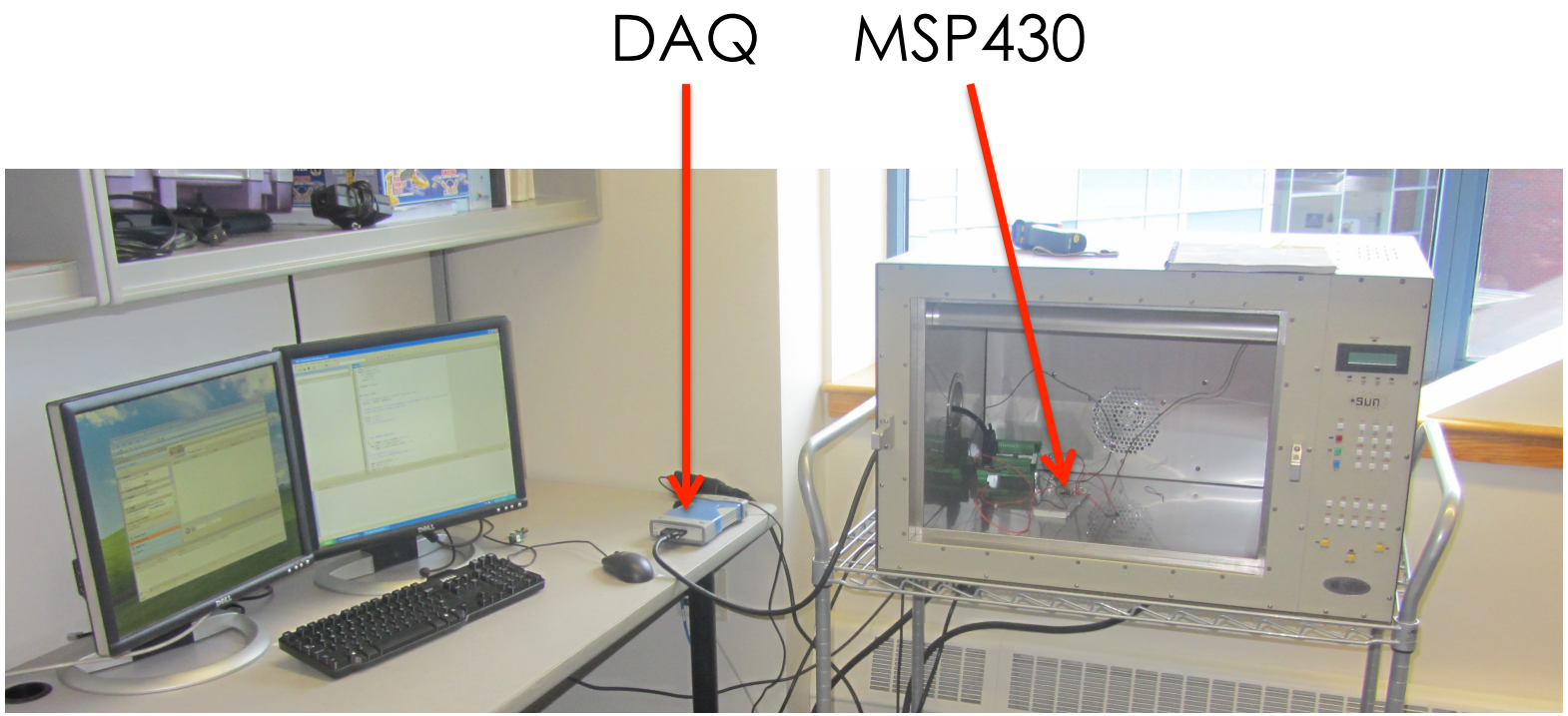
② Reduce voltage to 300mv

③ Increase voltage and check for bit flips

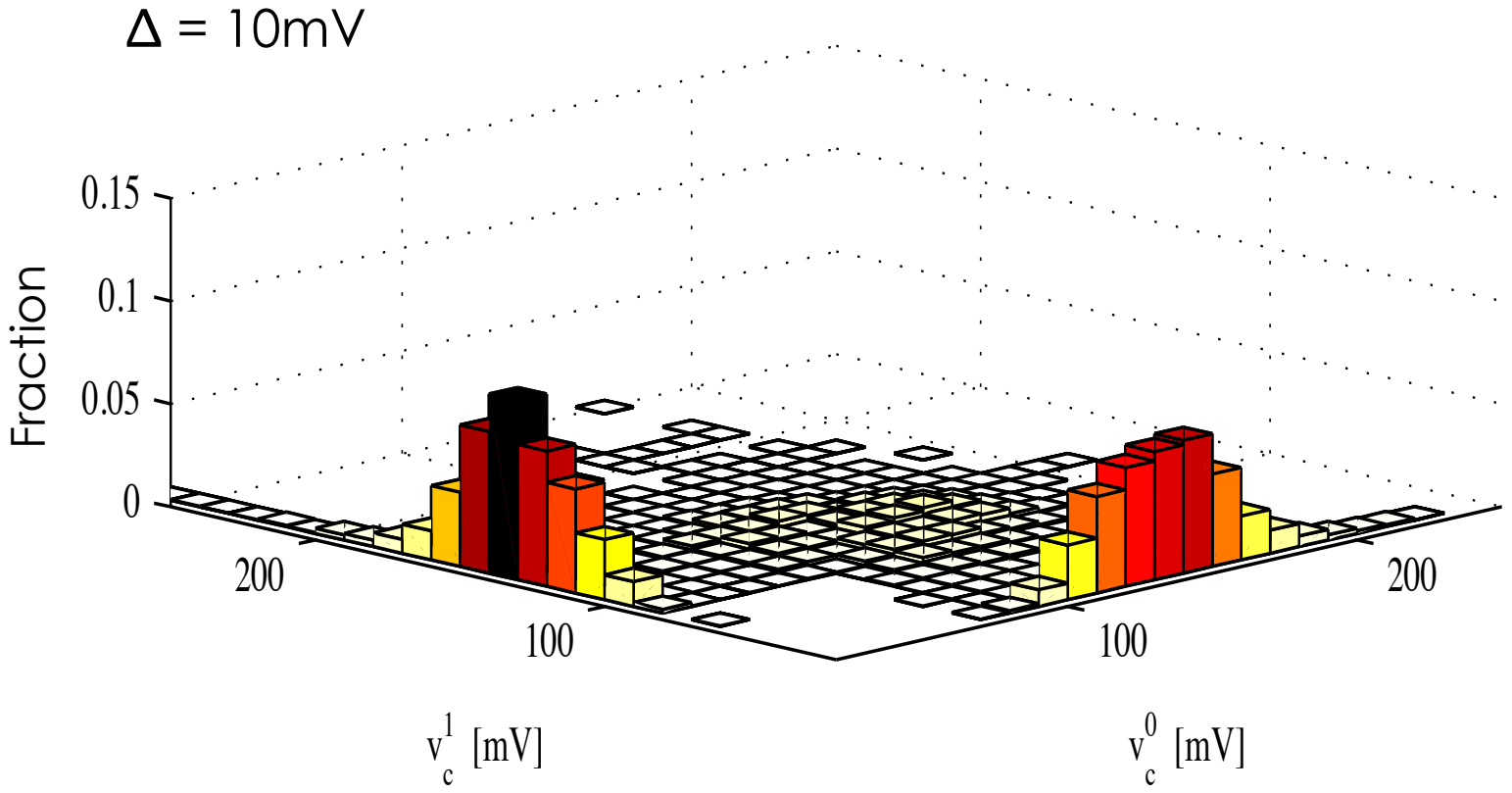
④ Repeat for voltages 290 – 10

⑤ Repeat for 0 initialization

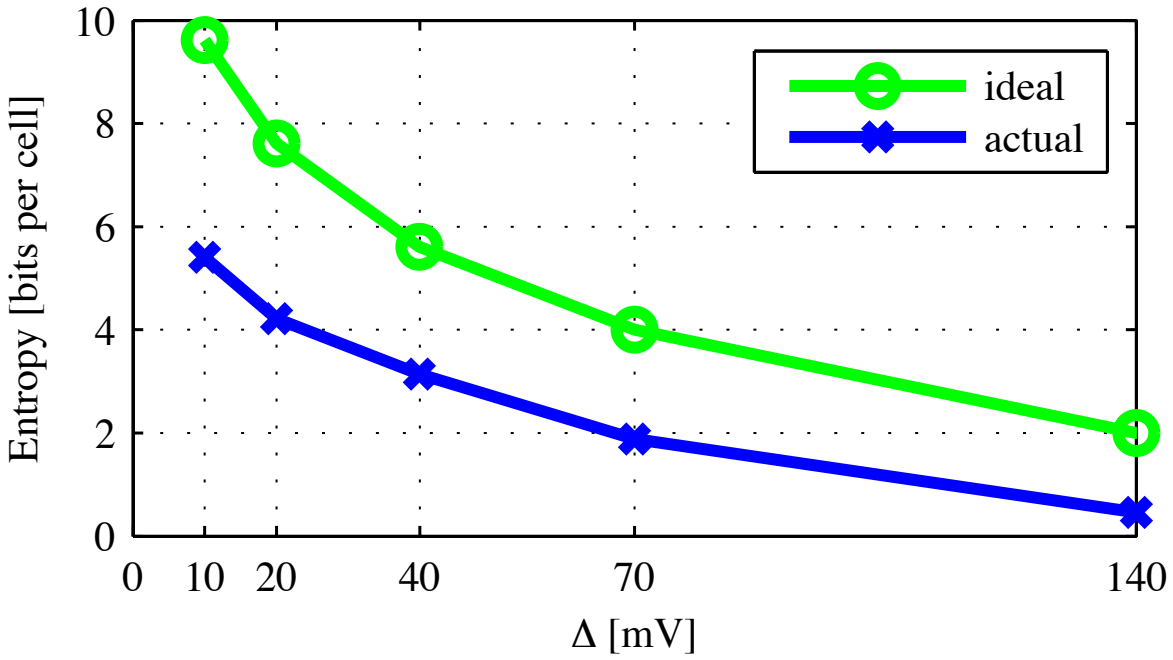
Experimental Setup



DRV vs. Power-up: Info Density



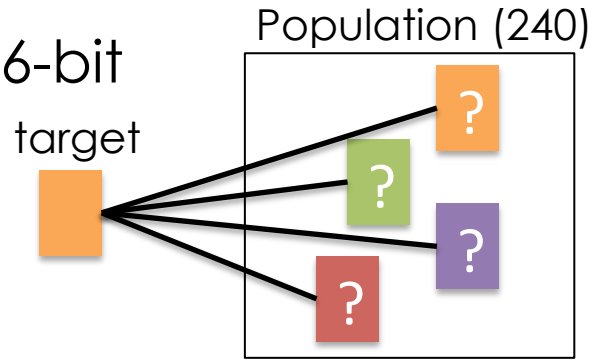
DRV vs. Power-up: Info Density



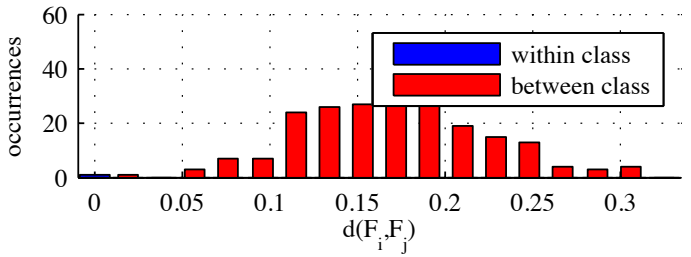
SRAM Power-up	Entropy (bits per cell)
Ideal	1
Actual	0.06 [Holcomb'07]

Accuracy
DRV vs. Power-up

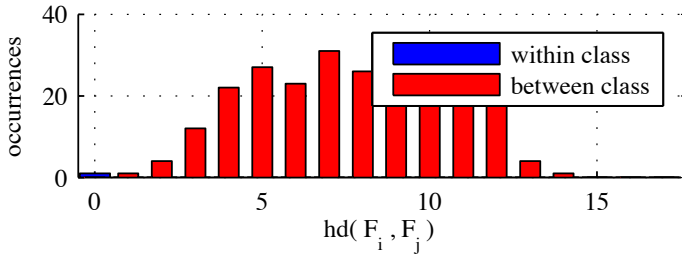
- Find top match in Population of 240 16-bit fingerprints
  - 1 from target, 239 from other cells
  - Collected at room temperature
  - More than 300 trials



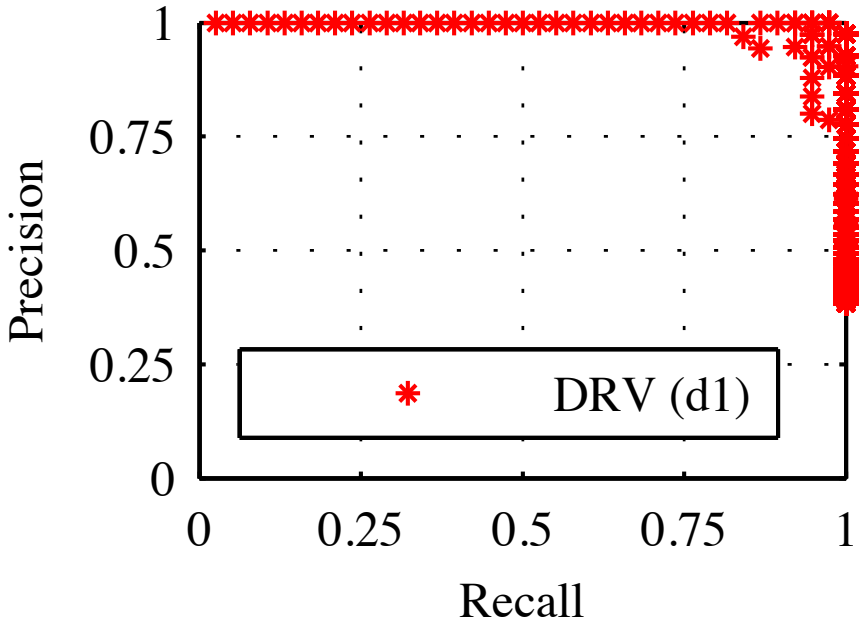
- DRV fingerprint:
  - 99.7% Correct Match
  - 0.3% Incorrect Match

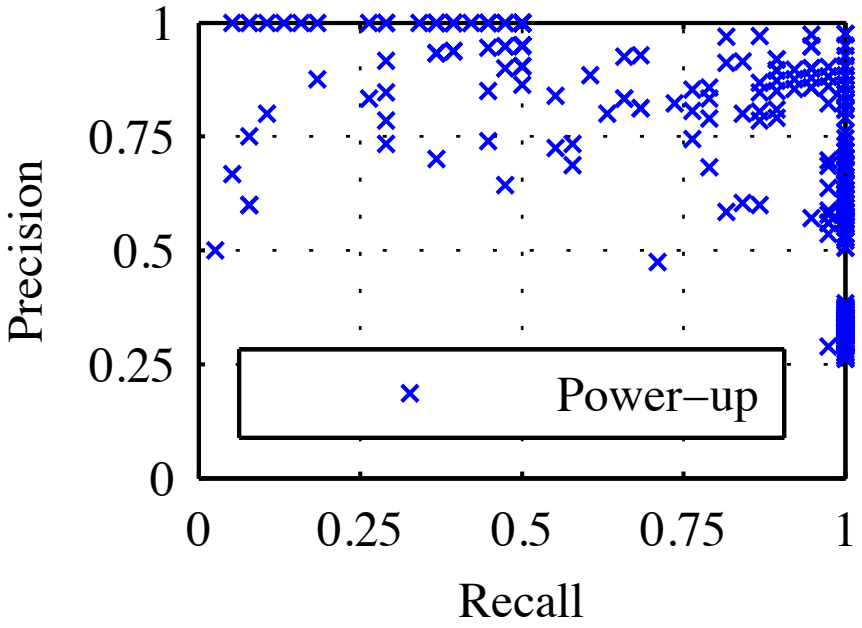


- Power-up fingerprint:
  - 71.7% Correct Match
  - 24.7% Multiple Matches
  - 3.6% Incorrect Match



Precision and Recall





Conclusion

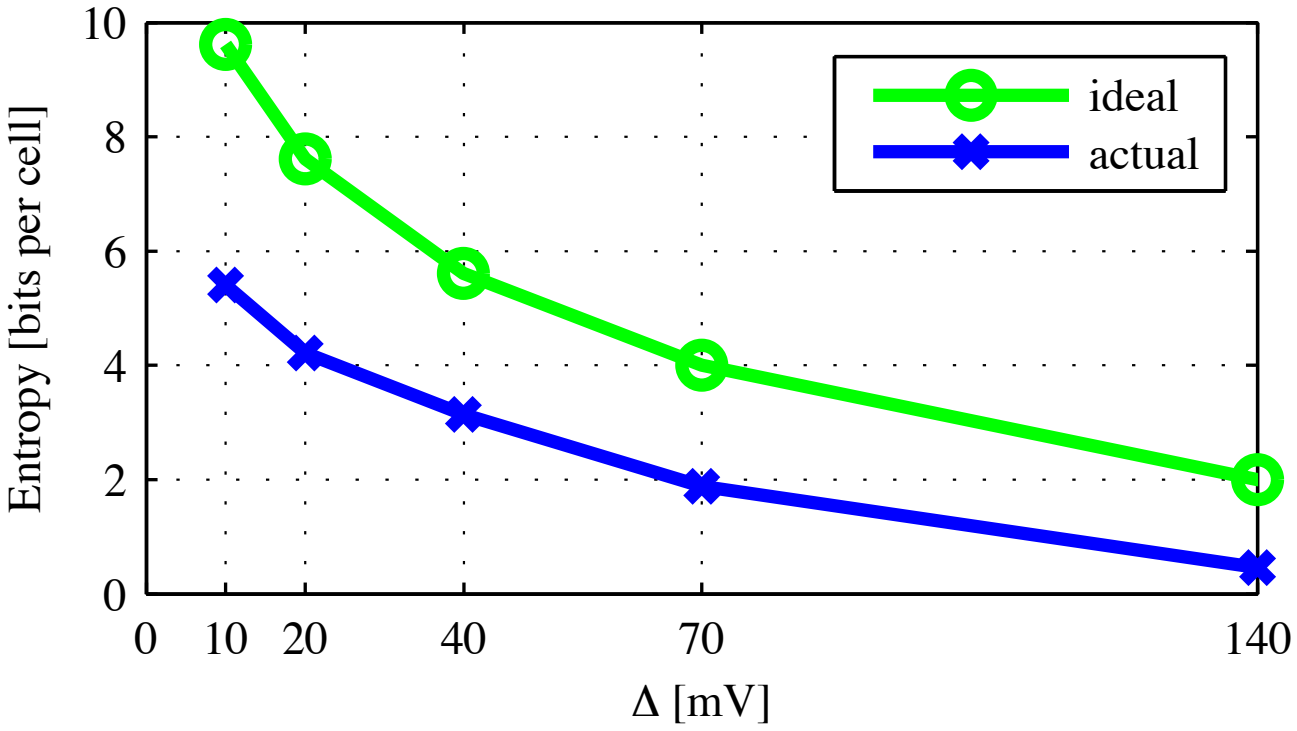
Data Retention Voltage as a new identification method

- ✓ Better Precision
- ✓ Smaller Sample Size
- ✗ Harder to implement

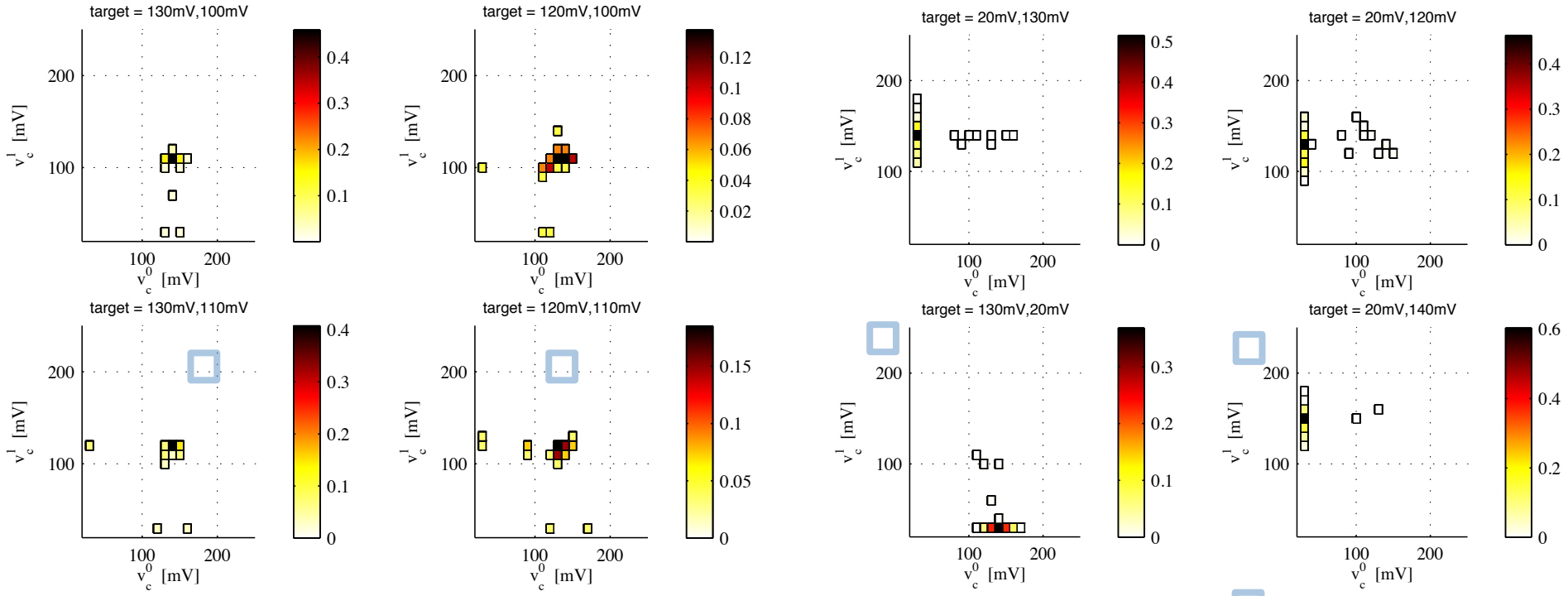
SPQR LABORATORY

Presented in RFIDSec 2012
https://spqr.cs.umass.edu

DRV entropy vs. Step size



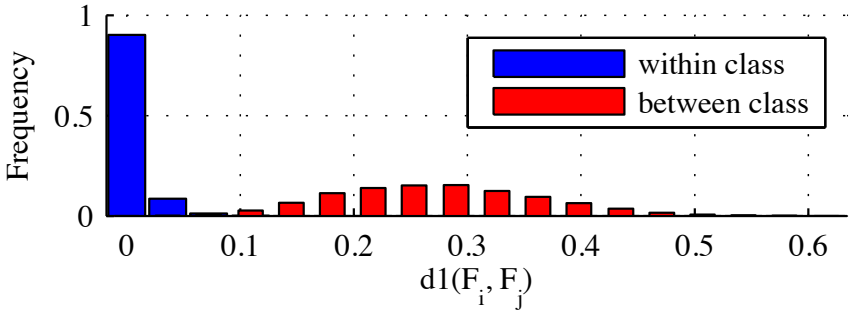
Repeatability of common DRVs

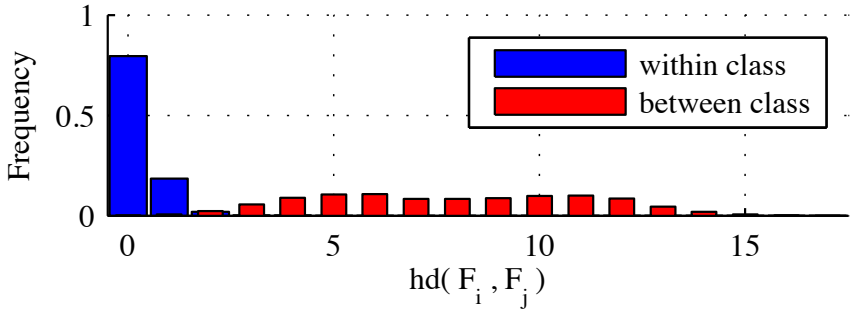


Fingerprinting Model

- Distance metrics
  - DRV : use $d1(F_i, F_j) = \sum_{n=0}^{k-1} \left(v_{i+n}^0 - v_{j+n}^0\right)^2 + \left(v_{i+n}^1 - v_{j+n}^1\right)^2$
  - Power-up : use $hd(F_i, F_j) = \sum_{n=0}^{k-1} p_{i+n} \oplus p_{j+n}$

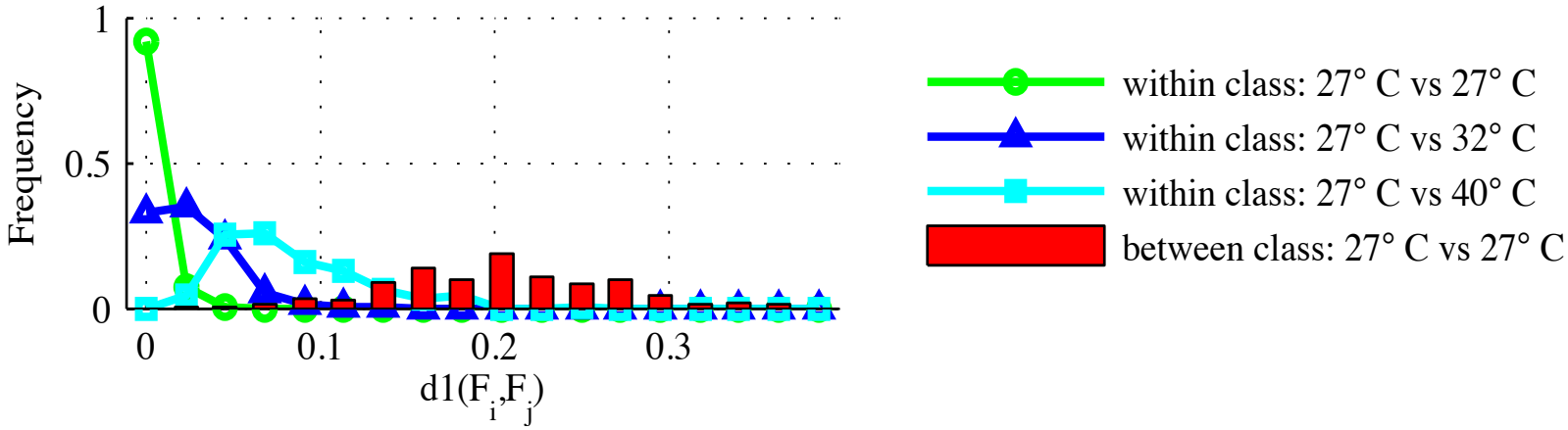
- Within class pairings are largely distinguishable from between class pairings





Impact of Temperature

- Within class pairings taken at different temperatures
- Temperature increases distances of within class pairings
  - Can mitigate by increasing fingerprint size



- If shift is predictable, can modify the distance metric for better matching
  - Not yet well-understood