DRV-Fingerprinting: Using Data Retention Voltage of SRAM Cells for Chip Identification

Daniel E. Holcomb, UC Berkeley
Amir Rahmati, UMass Amherst
Mastooreh Salajegheh, UMass Amherst
Wayne P. Burleson, UMass Amherst
Kevin Fu, UMass Amherst/Univ. Michigan

http://spqr.cs.umass.edu/

RFIDsec12, Nijmegen, The Netherlands, July 3, 2012

Motivation

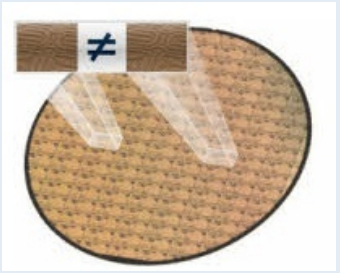
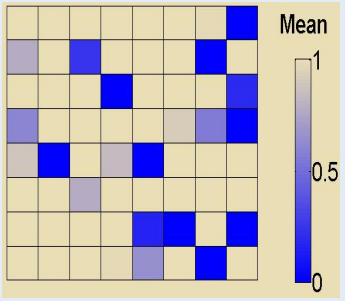


Image from www.verayo.cor

- PUFs enable authentication of RFID devices
  - Low cost and physically random
  - Need uniqueness, reliability, security and efficiency
  - Numerous recent designs (RFIDSec, CHES, HOST, SECSI, DAC,…)
- Background:
  - Can we leverage intrinsic properties of circuit?
  - SRAM provides a convenient read-out mechanism
  - SRAM cells are increasingly variable in advanced CMOS
  - SRAM cells power-up to 1 or 0 fairly reliably on each chip.



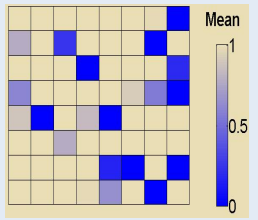
- Problem: Can we improve success rate of chip ID based on SRAM variations?
- Idea: Rather than just observing power-up state, observe the voltage at which the decision occurs!

A Brief History of PUFs

- Physical one-way functions,
  - Optical scattering [Pappu et al. Science 02]
- Physical unclonable functions in CMOS
  - Arbiter PUF [Gassend et al. CCS 02]
    - Additive model attacks [Lim MIT MS Thesis 03]
    - Improved Arbiter PUFs [Majzoobi et al. ICCAD 08]
      - Evolutionary algorithms [Ruhrmair et al. CCS 10]
    - Prevent modeling attacks by hiding CRPs
  - Errors must be corrected before any hashing
    - Helper data for error correction [Maes et al. CHES 09]
    - Index-based syndrome code for arbiter PUFs [Yu et al. D&T 10]
      - Adapted for SRAM PUFs [Hiller et al. HOST 12]
  - Physically obfuscated Keys (weak PUFs)
- Complete Survey [Maes and Verbauwhede, 2010]

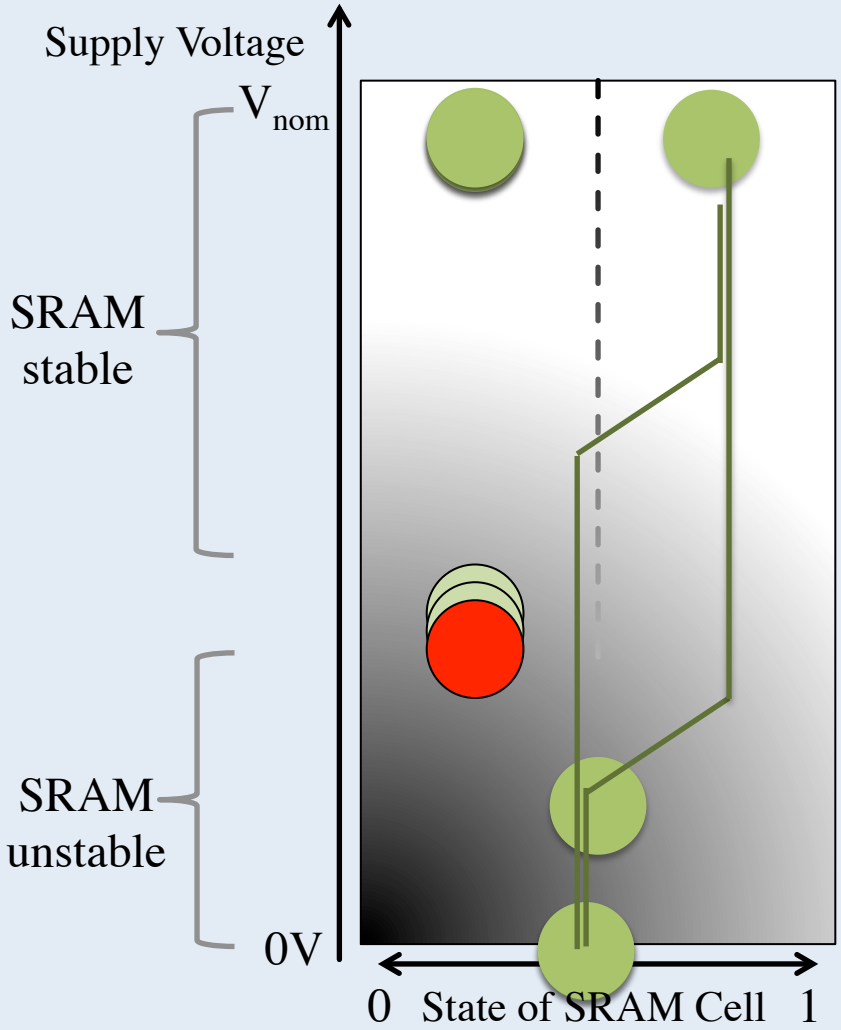
SRAM Characterization

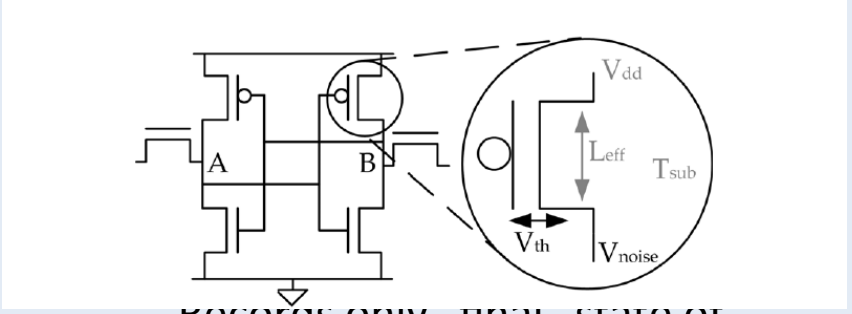
- SRAM power-up fingerprint
  - Patented for characterizing circuits [Layman et al. 02]
  - Security applications proposed later
    - ID and TRNG [Holcomb et al. RFIDSec 07, TrComp 09]
    - Physically Obfuscated Key [Guajardo et al. CHES 07], Intrinsic ID



- Data Retention Voltage (DRV)
  - SRAM cells can not reliably retain state below a certain voltage (typically 200-300mV)
  - Optimal operation is at low voltage, but DRV failures prohibit ultra-low voltages [Qin et al. ISQED 04]
- Our contribution: **DRV fingerprinting**

SRAM Fingerprints – Power-up and DRV

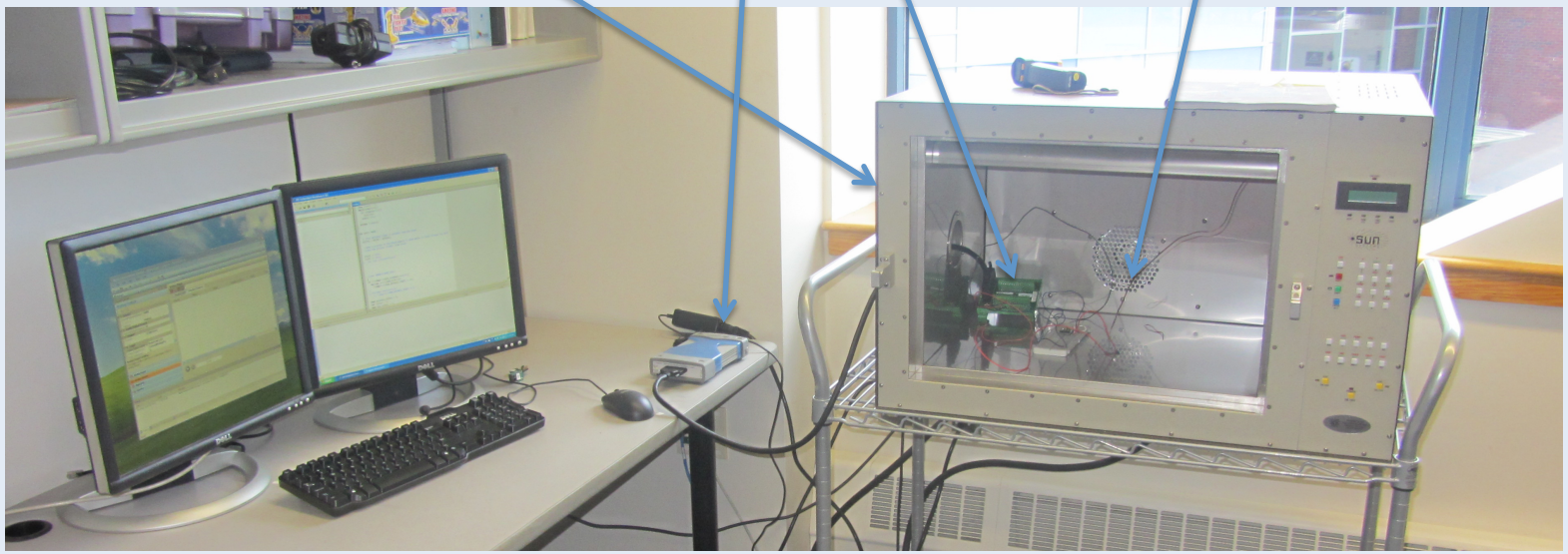




  - Records only "final" state of power-up
  - No knowledge of behavior as function of voltage
- DRV fingerprint
  - Record *highest* voltage v_c of flip after each written state
    - Approximated using discrete test voltages (~10mV)
  - How long to remain at each voltage v_c? (~2ms?)
    - Probably a function of temperature

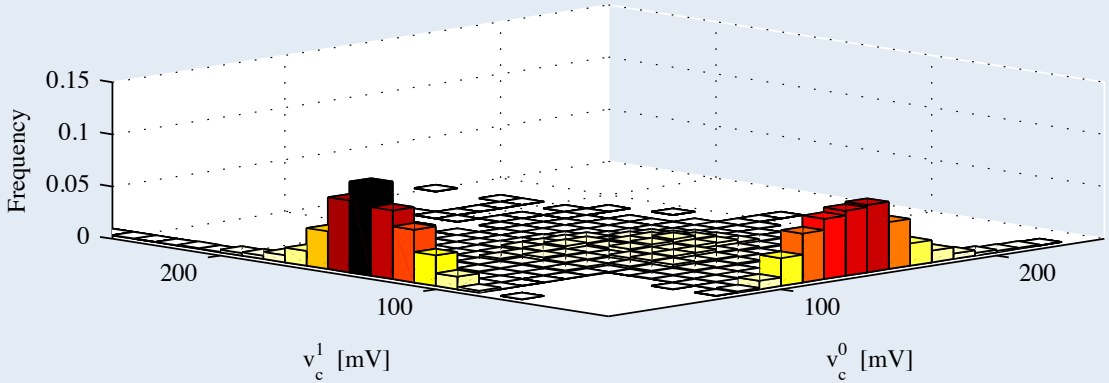
Experimental Set up

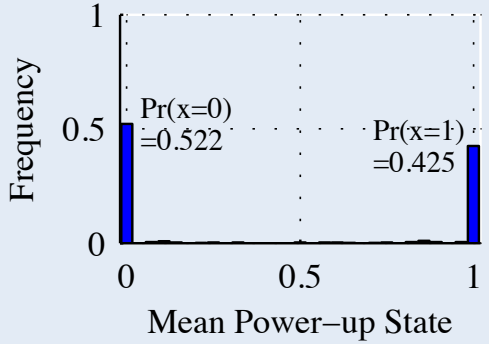
- Texas Instruments MSP430F2131 microcontroller (same family used in Umass Moo…)
  - 256 Bytes of SRAM (240 Bytes usable)
- Agilent U2541A-series data acquisition (DAQ)
- Thermal chamber and temperature sensor



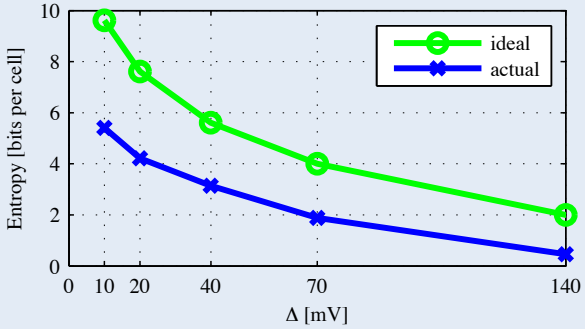
DRV is More Informative than Power-up

- Consider outcomes for test voltages $v_c^{0,1}$ with step Δ = 10mV
  - 28 test voltages per written state, 28^2 = 784 total outcomes per cell
  - vs. N+1 outcomes for N power-up trials



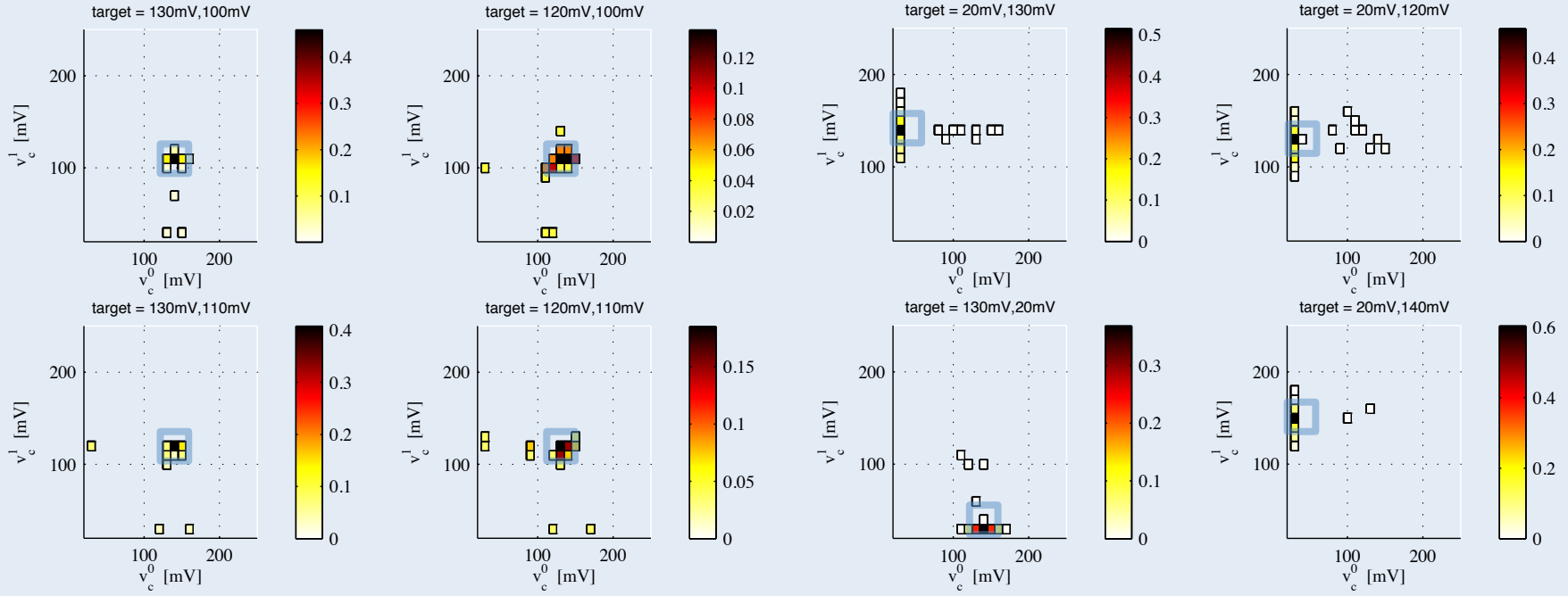


- DRV entropy depends on step size
  - 5.12 bits at 10mV
  - Usefulness will depend on repeatability
  - Too small a voltage step just captures noise
    - Increases characterization time



Repeatability of common DRVs

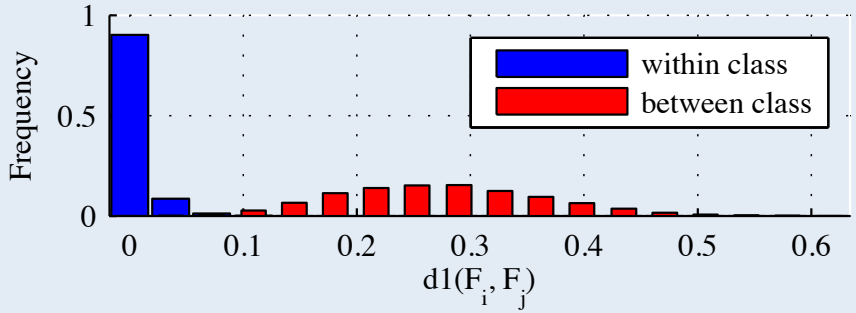
- If a cell produces some given DRV, what will a 2nd DRV from same cell produce?
  - 2nd DRV sometimes matches target exactly (10mV step size)
  - Generally within small distance

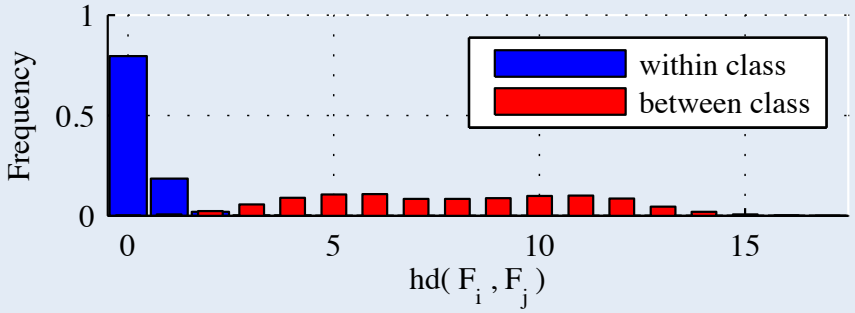


16-bit Fingerprints

- 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 $hd(F_i, F_j) = \sum_{n=0}^{k-1} p_{i+n} \oplus p_{j+n}$

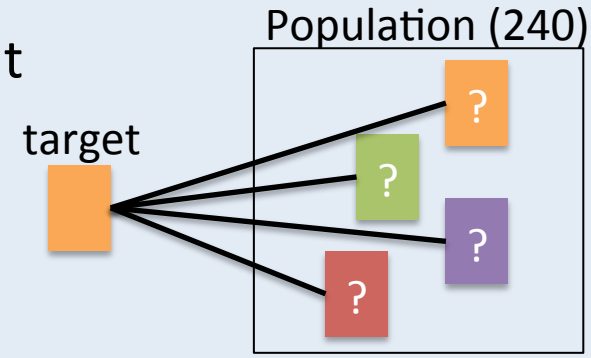
- Within class pairings are largely distinguishable from between class pairings



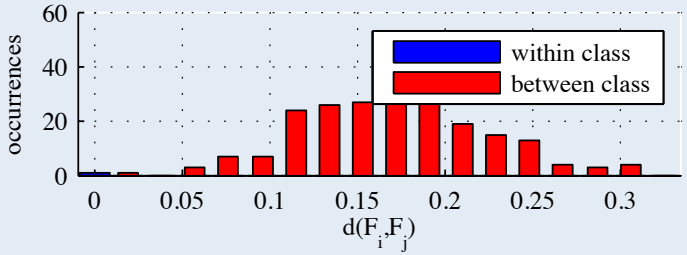


Top Match Experiment

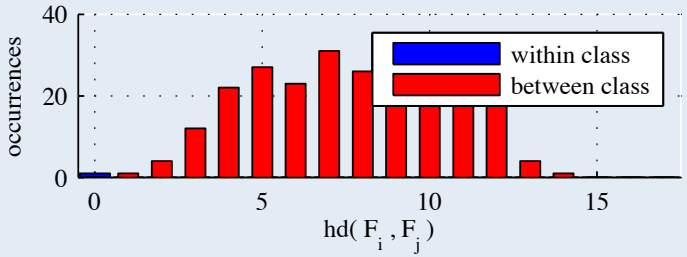
- Find top match in Population of 240 16-bit fingerprints
  - 1 from target, 239 from other cells
  - Collected at room temperature



- DRV fingerprint:
  - 99.7% : top match is target
  - 0.3% : top match is not target



- Power-up fingerprint:
  - 71.7% : Closest distance is unique and is target
  - 24.7% : Multiple closest, including target
  - 3.6% : Target not closest distance



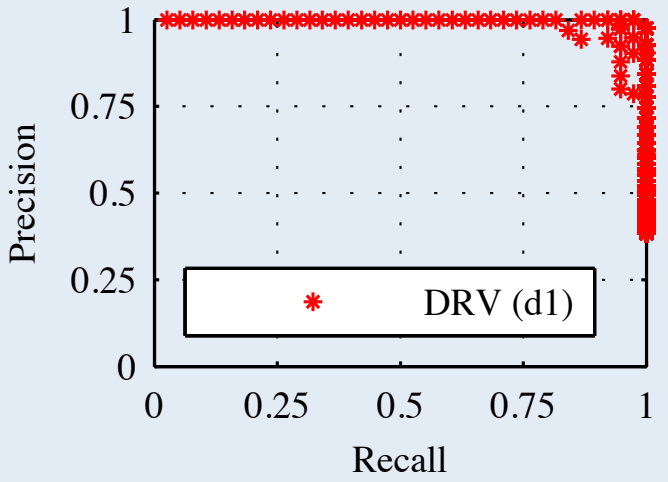
Precision and Recall

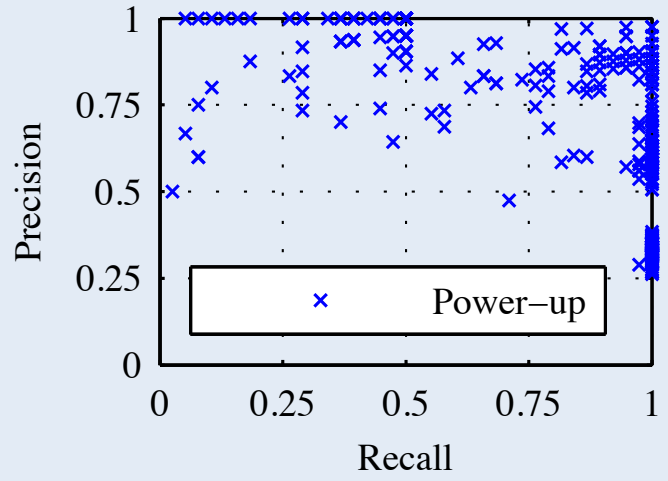
- Distance threshold *d* selects pairings
  - Guess that f_1, f_2 are same device if $D(f_1,f_2)<d$
- As *d* increases, precision drops and recall increases
  - Sweep *d* for achievable precision/recall points

$$Precision(d) = \frac{D(f_1, f_2) < d \quad \cap \quad f_1 == f_2}{D(f_1, f_2) < d}$$

$$Recall(d) = \frac{D(f_1, f_2) < d \quad \cap \quad f_1 == f_2}{f_1 == f_2}$$

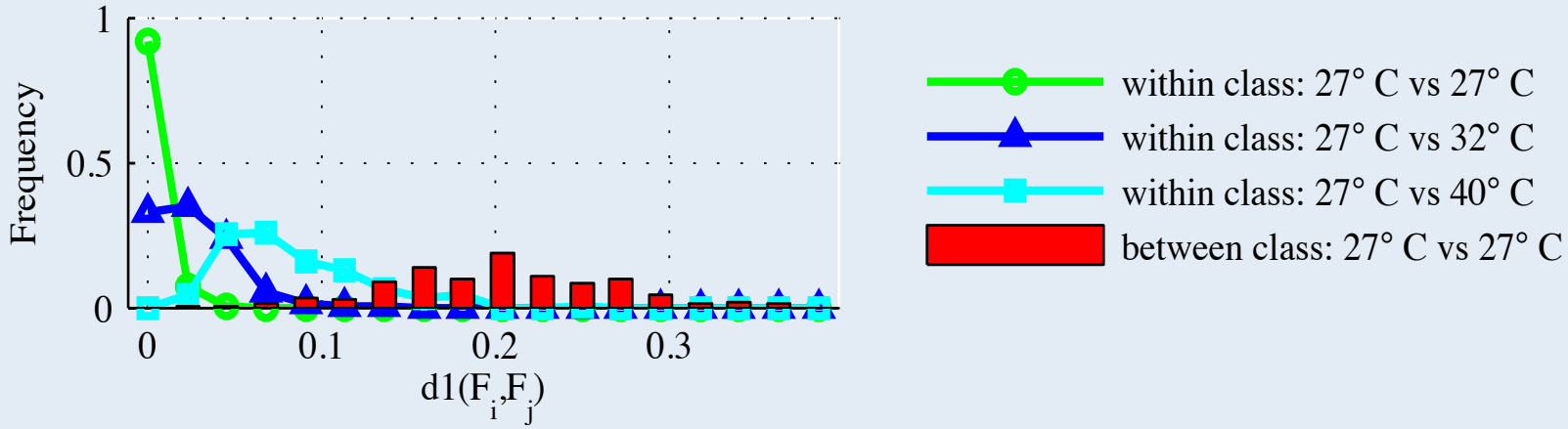
- Population of 1019 16-bit fingerprints
  - 19 match target, 1000 do not match
  - Sweep *d* for each random population





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

Practical Issues

- Characterization procedure requires:
  - Test voltage generation v_c = [Vdd, 20 mV], $\Delta = 10$ mV
    - On-chip voltage generation, increasingly used in modern processors… but not at fine granularity
      - Techniques exist, with costs associated
    - Generate test voltages off-chip for smart cards
    - *Leverage natural decay of voltage in RFID tags…*
  - State that is persistent across test voltages
    - Write to Flash or other non-volatile memory
    - Or power DRV SRAM using separate power supply

Reliability Considerations

- Want to minimize characterization time, without sacrificing reliability
  - Time spent at each voltage contributes to runtime
  - But must wait long enough for failures to surface
  - Conservatively allowed 5 seconds per test voltage
  - Literature hints that 2ms sufficient [Nourivand et al. TVLSI 12]
- Reliability of matching with temperature
  - Quantify whether DRV shifts are common-mode
  - Better matching algorithms or error correction
- Persistence of DRV fingerprints over lifetime of chip

Discussion

- Can we generalize this to ANY arbitrary characterization procedure?
  - How to "Challenge" each chip?
    - Supply voltage
    - Temperature
    - Digital challenges
  - How to observe "Response"
    - SRAM readout
    - Arbiter result
    - Other?
  - Metrics: uniqueness, reliability, security, efficiency

Conclusions

- A new SRAM mechanism for ID or Physically obfuscated key
- ✔ Identification with fewer SRAM cells
- ✔ Softer distance measure
  - Could lead to improved matching algorithm
  - Lower-cost error correction
- ✘ Voltage generation
- ✘ Runtime to take fingerprint