ECE 459/559
Secure & Trustworthy Computer Hardware Design

PUF Metrics & Applications

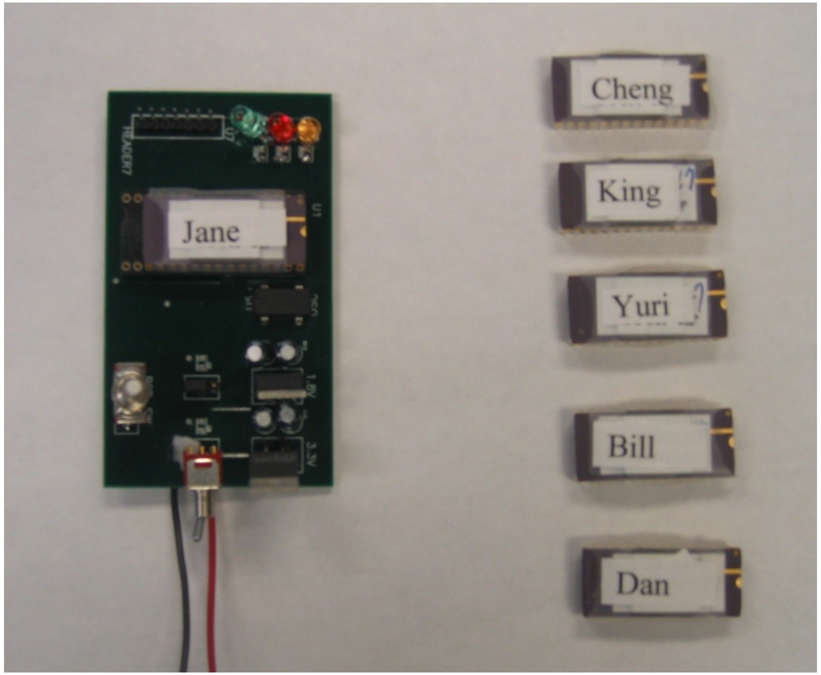
Garrett S. Rose

Spring 2017

THE UNIVERSITY OF TENNESSEE KNOXVILLE

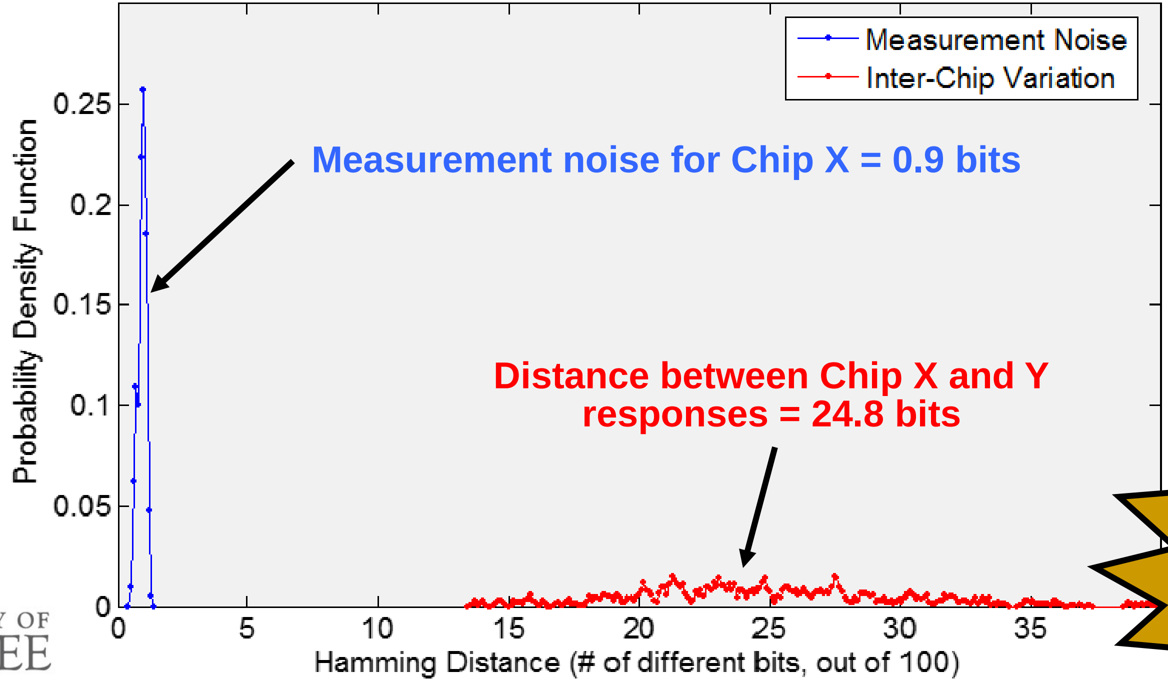
PUF Experiment Example

- Fabricated 200 “identical” chips with arbiter PUFs using TSMC 0.18µ technology on 5 different wafer runs
- Security
  - What is probability that challenge produces different responses on different PUFs?
- Reliability
  - What is probability that PUF output for specific challenge changes with temperature?
  - With voltage fluctuations?



Inter-Chip Distance (Uniqueness)

- Apply random challenges and observe many response bits
- Determine Hamming Distance between responses of different chips – Ideal: 50%



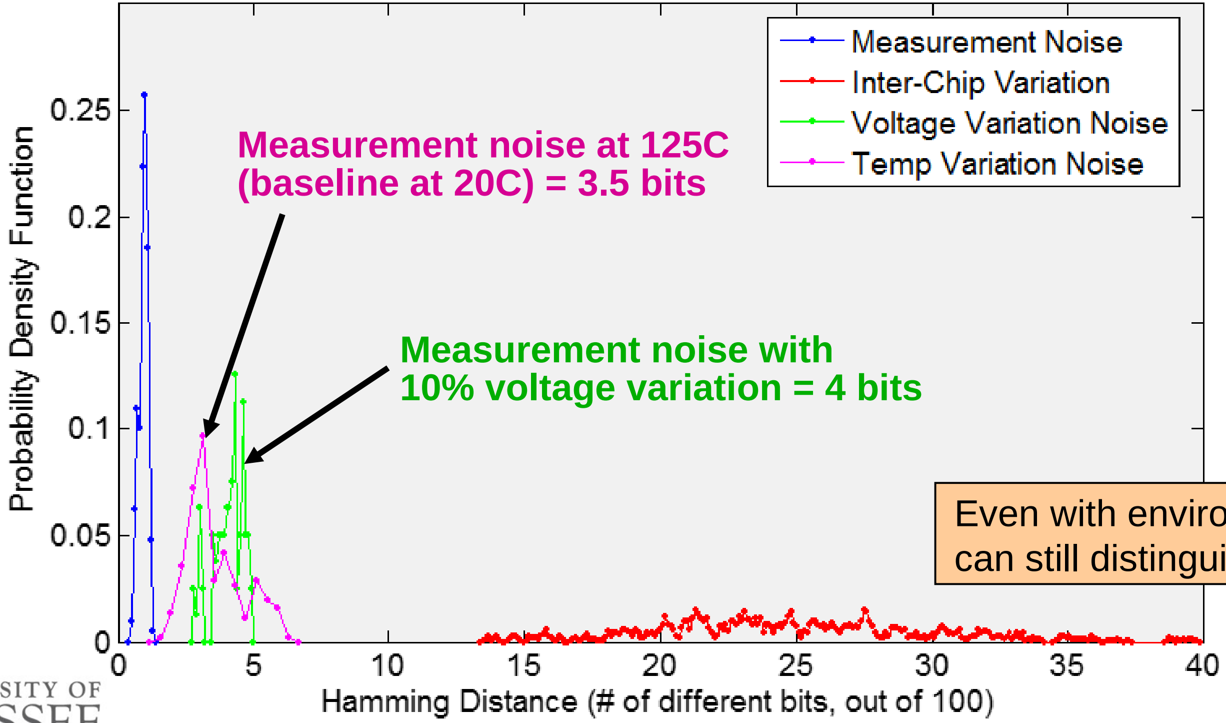
Measurement noise for Chip X = 0.9 bits

Distance between Chip X and Y responses = 24.8 bits

Can identify individual ICs

Environmental Variations

- What happens when we change the voltage and temperature?



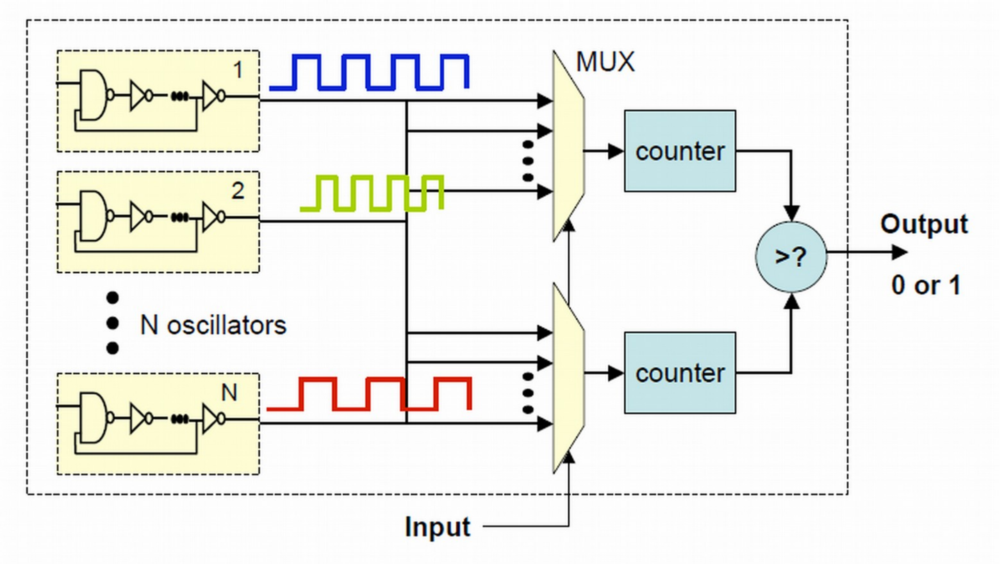
Measurement noise at 125C (baseline at 20C) = 3.5 bits

Measurement noise with 10% voltage variation = 4 bits

Even with environmental variation, we can still distinguish two different PUFs

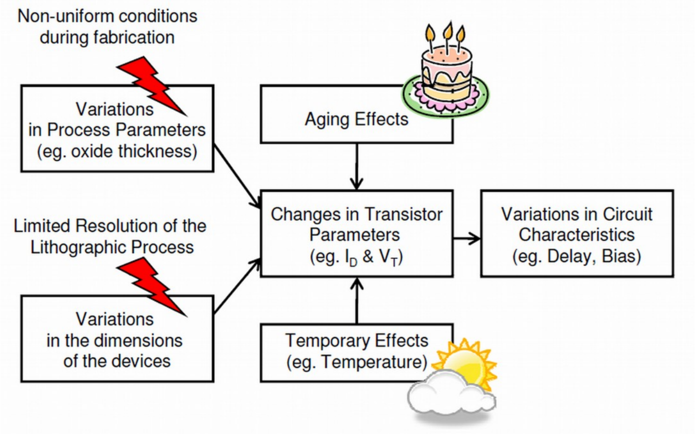
Ring Oscillator (RO) PUF

- Structure relies on delay loops and counters instead of MUX-based switches and flop-based arbiters
- Better results on FPGA – more stable than APUF



Suh et al., “PUFs for Device Authentication & Secret Key Generation,” DAC 2007.

Reliability of RO PUFs

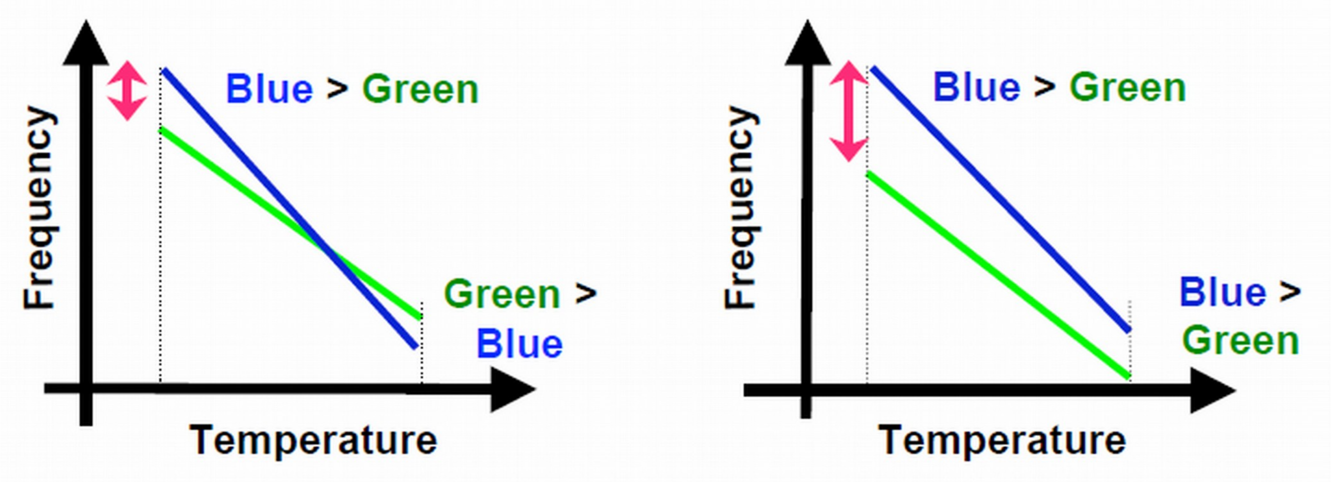

Non-uniform conditions during fabrication
Variations in Process Parameters (eg. oxide thickness)
Aging Effects
Limited Resolution of the Lithographic Process
Changes in Transistor Parameters (eg. I_D & V_T)
Variations in Circuit Characteristics (eg. Delay, Bias)
Variations in the dimensions of the devices
Temporary Effects (eg. Temperature)

- Aging:
  - Negative Bias Temperature Instability (NBTI)
  - Hot Carrier Injection (HCI)
  - Temperature Dependent Dielectric Breakdown
  - Interconnect Failure
- Temperature:
  - Slows down the device

Ganta et al., “Highly Stable Leakage-Based Silicon PUFs,” VLSID 2011.

Reliability Enhancement

- Environmental changes have a large impact on frequency (even relative frequencies)



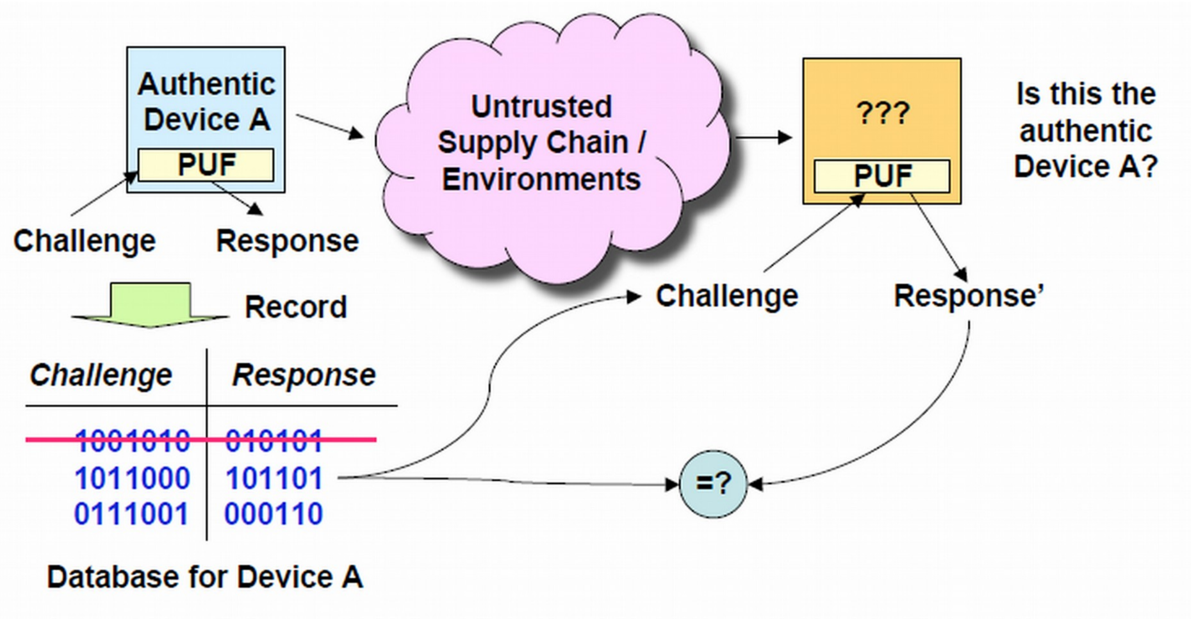
Suh et al., “PUFs for Device Authentication & Secret Key Generation,” DAC 2007.

Thoughts about RO PUF

- ROs whose frequencies are far apart are more stable than ones with closer frequencies
- Possible advantage: do not use all pairs, only stable ones
- Easy to watch distance in the counter and pick ROs with far apart frequencies
  - Can be done during enrollment
- RO PUF allows easier implementation for both ASIC & FPGA
- APUF good in resource constrained platforms, e.g. RFIDs
- RO PUF better for FPGAs and in secure processor design

PUF Application – Authentication

- Same challenges should not be used to prevent man-in-the-middle attacks



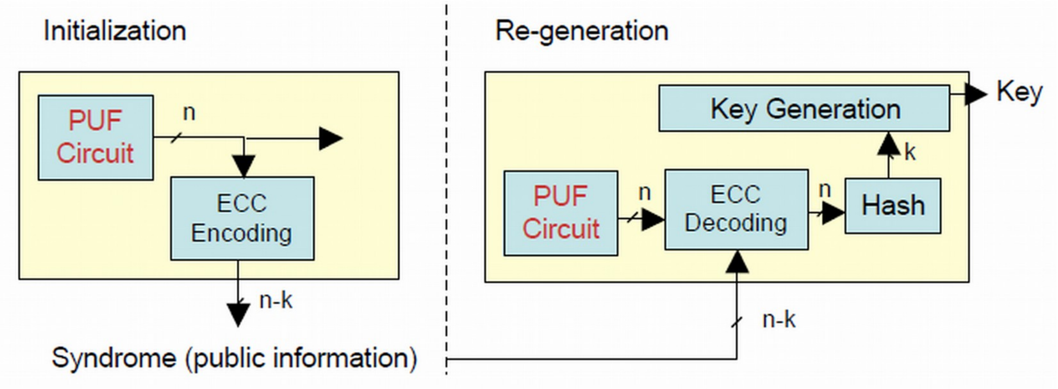
Challenge	*Response*
~~1001010~~	~~010101~~
1011000	101101
0111001	000110

Database for Device A

Suh et al., “PUFs for Device Authentication & Secret Key Generation,” DAC 2007.

PUF Application – Key Generation

- Instability (lack of reliability) is a problem
- Many crypto protocols require specific mathematical properties not found in PUF generated numbers
- How can we use PUFs to generate crypto keys?
  - Error correction process: initialization and regeneration
  - Need one-way function to generate key from PUF output

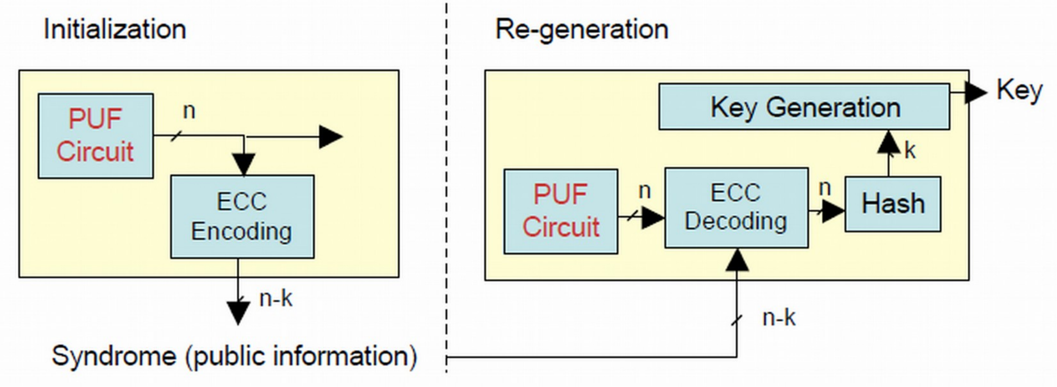


THE UNIVERSITY OF TENNESSEE KNOXVILLE

Suh et al., “PUFs for Device Authentication & Secret Key Generation,” DAC 2007.

Crypto Key Generation

- Initialization: PUF responses generated and error correcting code (e.g., BCH) computes a syndrome (public info)
- Regeneration: PUF uses syndrome from initial phase to correct changes in the responses
- Clearly, syndrome reveals information about the circuit and introduces security vulnerabilities



Suh et al., “PUFs for Device Authentication & Secret Key Generation,” DAC 2007.

Experiments with RO PUFs

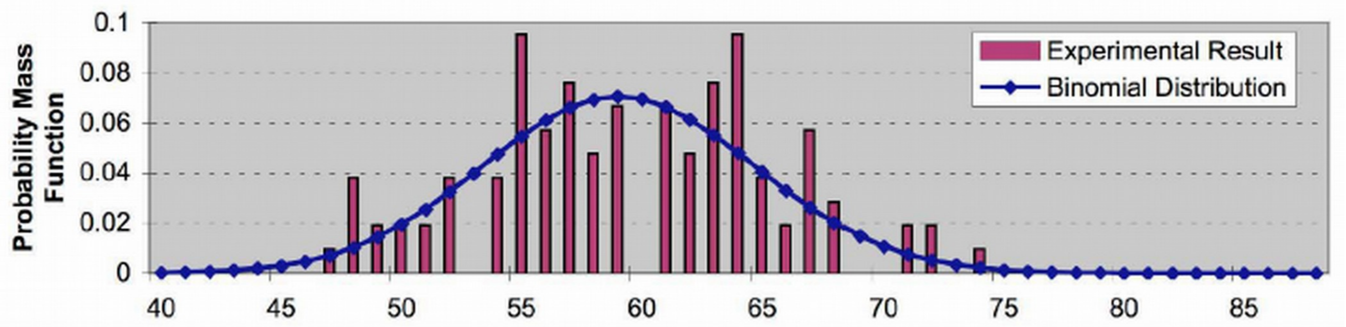
- Experiments done on 15 Xilinx Virtex4 LX25 FPGAs (90nm)
- Placed 1024 ROs in each FPGA as a 16-by-64 array
- Each RO consisted of 5 INVs and 1 AND, implemented using look-up tables
- Goal is to know if PUF responses are unique (for security) and reproducible (for reliability and security)

Primary PUF Security Metrics

- Inter-chip distance
  - How many PUF output bits are different between PUF A and PUF B?
  - Measure of uniqueness
  - If PUF produces uniformly distributed, independent random bits, inter-chip distance should be 50%
- Intra-chip distance
  - How many PUF response bits change when re-generated again from one PUF with or without environmental variation?
  - Indicates the reproducibility or reliability of the PUF
  - Ideally, intra-chip distance should be 0%

Probability Distribution for Inter-Chip Distance

- 128 bits produces from each PUF
- X-axis: number of PUF response bit differences for 2 FPGAs
- Y-axis: probability
- Purple bars show results from 105 pair-wise comparisons
- Blue line shows binomial distribution with fitted parameters (n=128, p=0.4615)
- Average inter-chip distance 0.4615 ~ 0.5

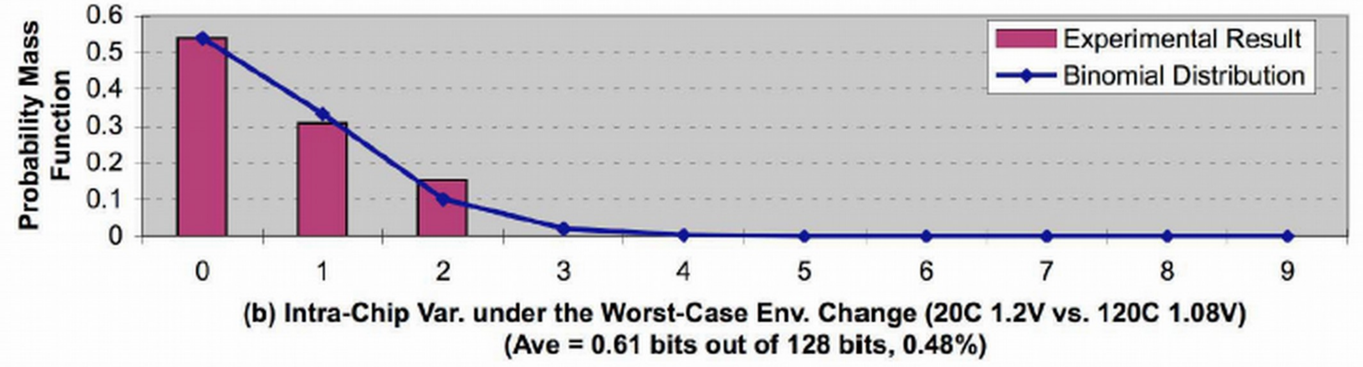


(a) Inter-Chip Variation (Ave = 59.1 bits out of 128 bits, 46.15%)

Suh et al., “PUFs for Device Authentication & Secret Key Generation,” DAC 2007.

Probability Distribution for Intra-Chip Distance

- PUF responses generated at 2 different environmental conditions
- Change temperature from 20C to 120C and core voltage from 1.2V to 1.08V altered PUF responses by ~0.6 bits (0.48%)
- Intra-chip distance is much lower than inter-chip – PUF responses did not change much from small to moderate



Suh et al., “PUFs for Device Authentication & Secret Key Generation,” DAC 2007.

Configurable Ring Oscillator PUF

- Pair which has maximum difference in frequency is selected

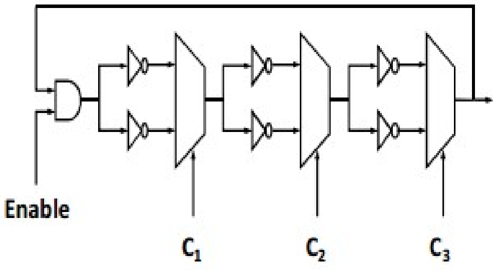


Fig. 3(a)

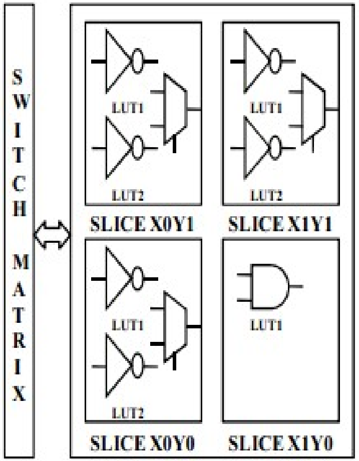


Fig. 3(b)

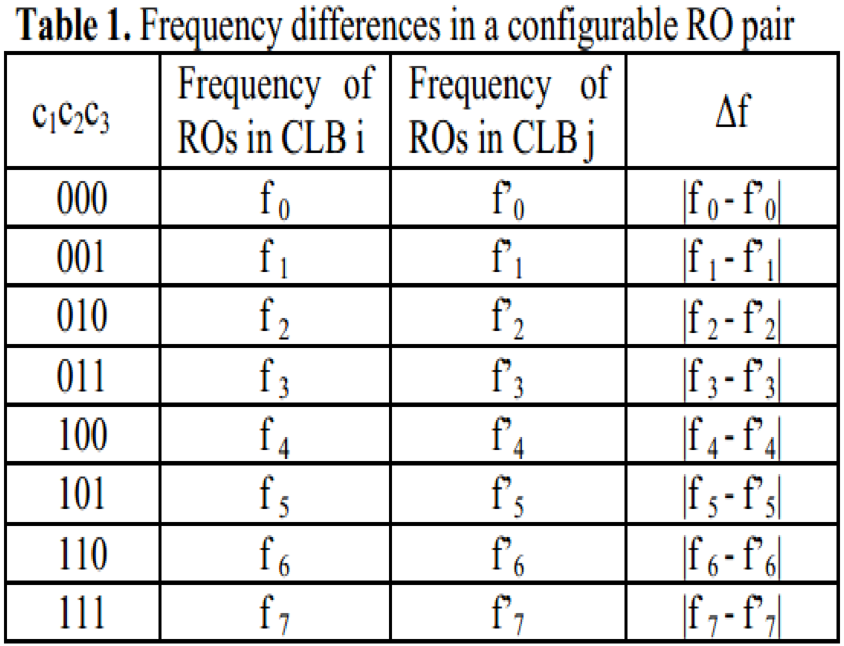


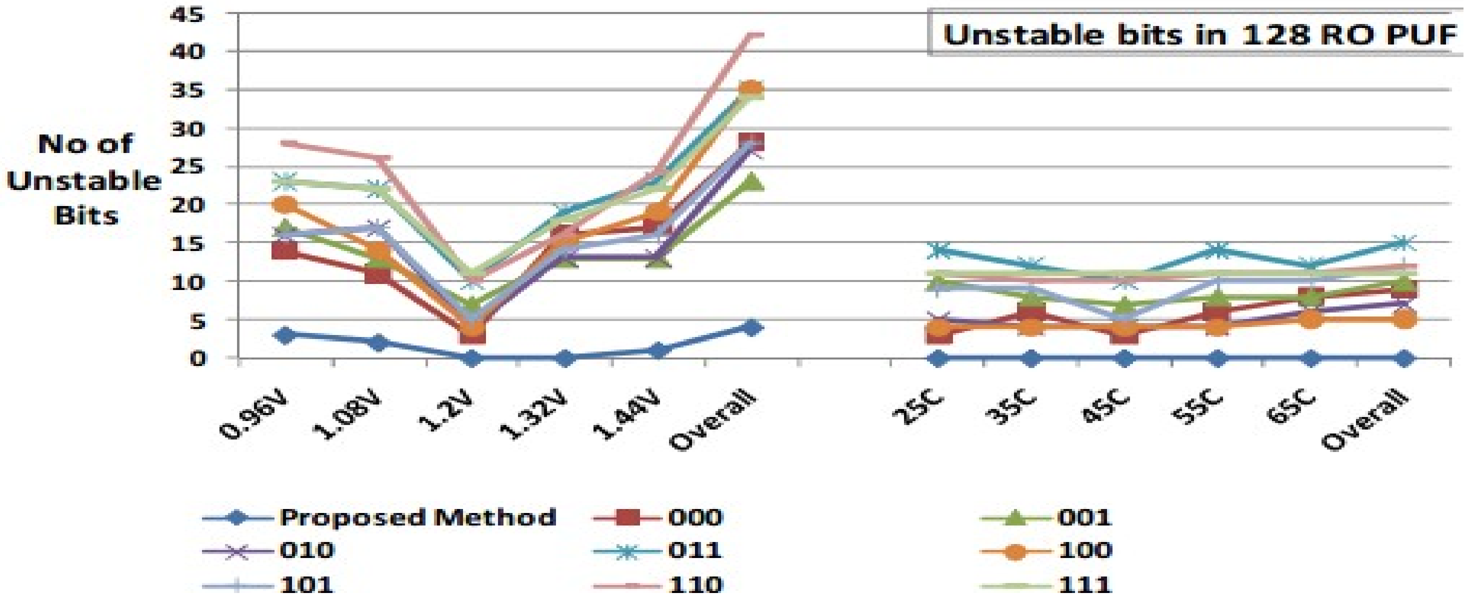
Table 1. Frequency differences in a configurable RO pair

$c_1c_2c_3$	Frequency of ROs in CLB i	Frequency of ROs in CLB j	Δf
000	f_0	f'_0	$\|f_0 - f'_0\|$
001	f_1	f'_1	$\|f_1 - f'_1\|$
010	f_2	f'_2	$\|f_2 - f'_2\|$
011	f_3	f'_3	$\|f_3 - f'_3\|$
100	f_4	f'_4	$\|f_4 - f'_4\|$
101	f_5	f'_5	$\|f_5 - f'_5\|$
110	f_6	f'_6	$\|f_6 - f'_6\|$
111	f_7	f'_7	$\|f_7 - f'_7\|$

Suh et al., “PUFs for Device Authentication & Secret Key Generation,” DAC 2007.

Configurable Ring Oscillator PUF

- A higher difference in frequency leads to higher reliability
- Also adds redundancy… always good thing for computer systems



Suh et al., “PUFs for Device Authentication & Secret Key Generation,” DAC 2007.

Summary

- Two key metrics for physical unclonable functions:
  - Inter-chip distance (a.k.a. uniqueness)
  - Intra-chip distance (a.k.a. reliability)
- Ring oscillator PUF is good for FPGA implementations
- Configurable RO PUF designed to help improve reliability