PUFs

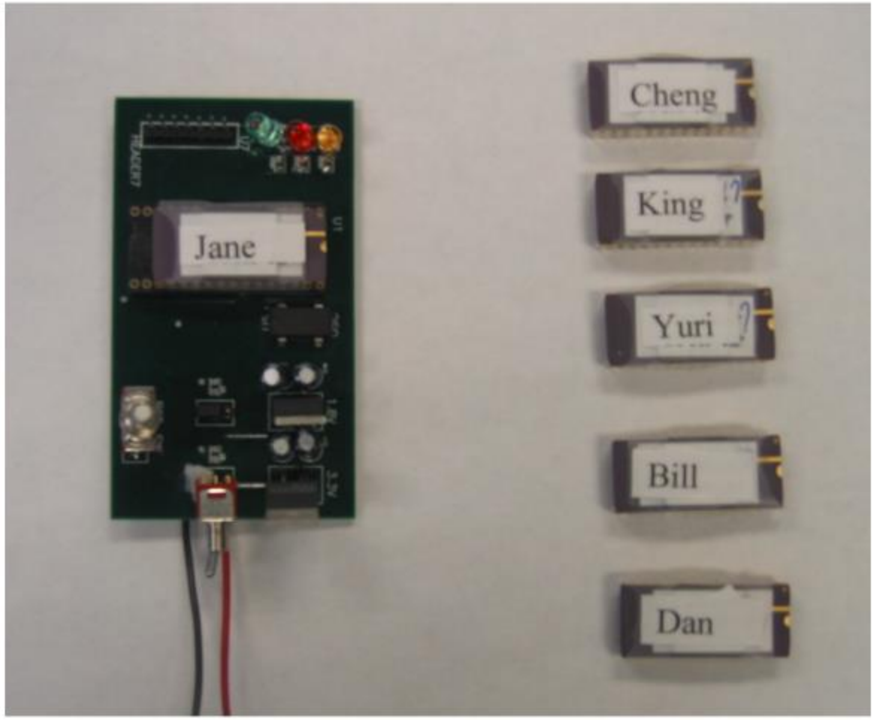
Yu Bi

ELE594 – Special Topic on Hardware Security & Trust

University of Rhode Island

PUF Experiments

- Fabricated 200 “identical” chips with PUFs in TSMC 0.18μ on 5 different wafer runs



Security

– What is the probability that a challenge produces different responses on two different PUFs?

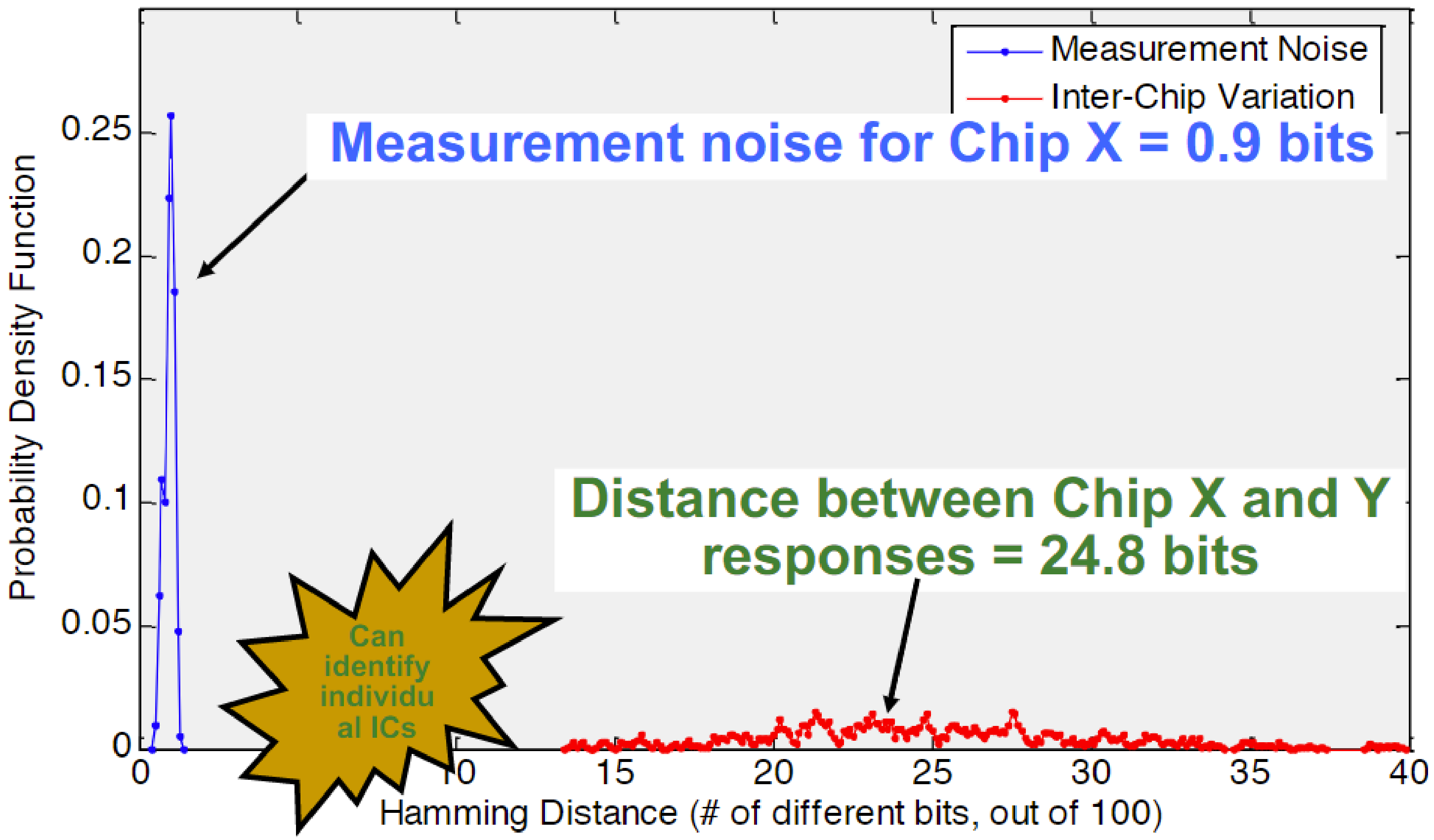
Reliability

– What is the probability that a PUF output for a challenge changes with temperature?

– With voltage variation?

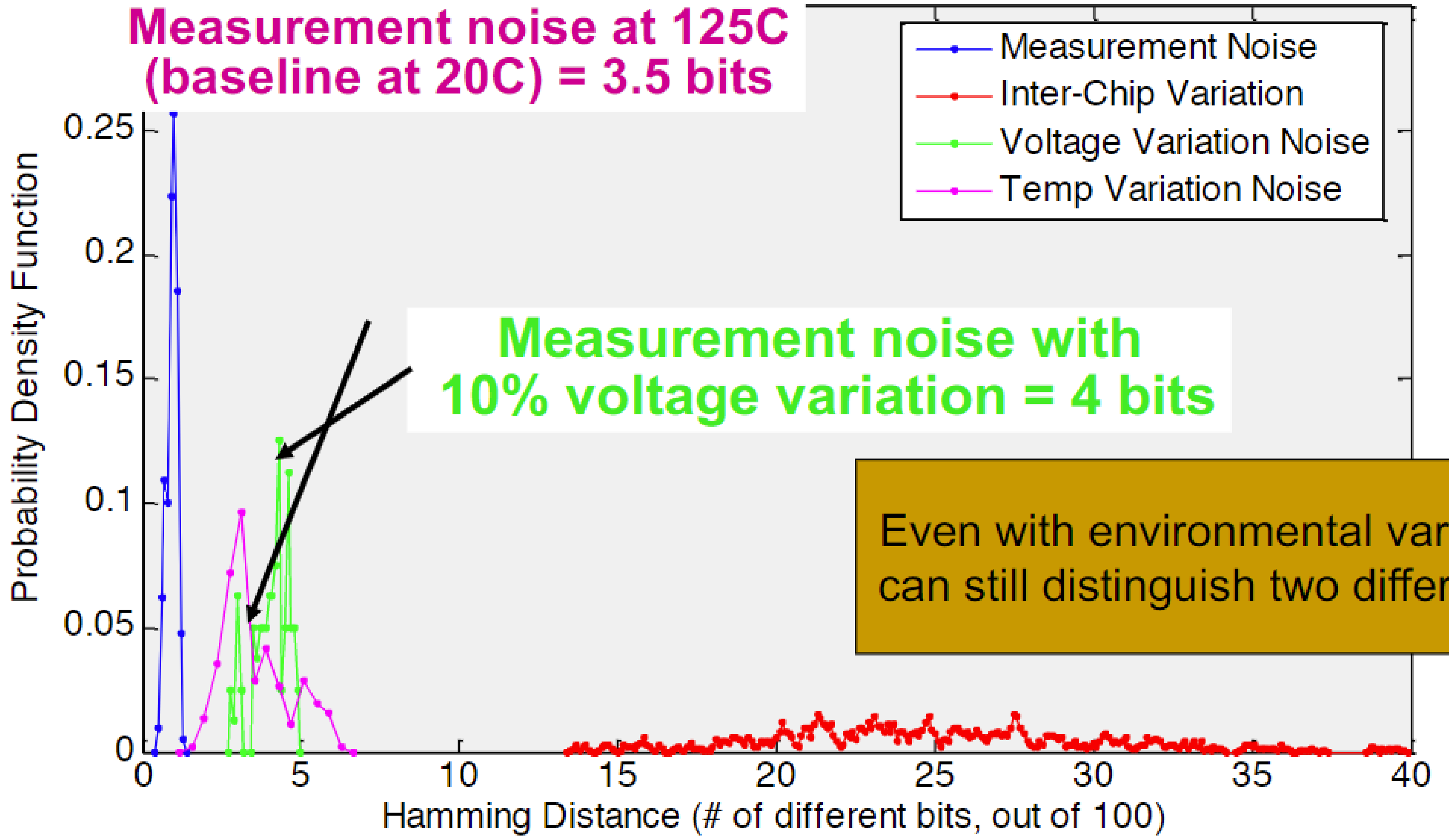
Inter-Chip Variation

- Apply random challenges and observe 100 response bits



Environmental Variations

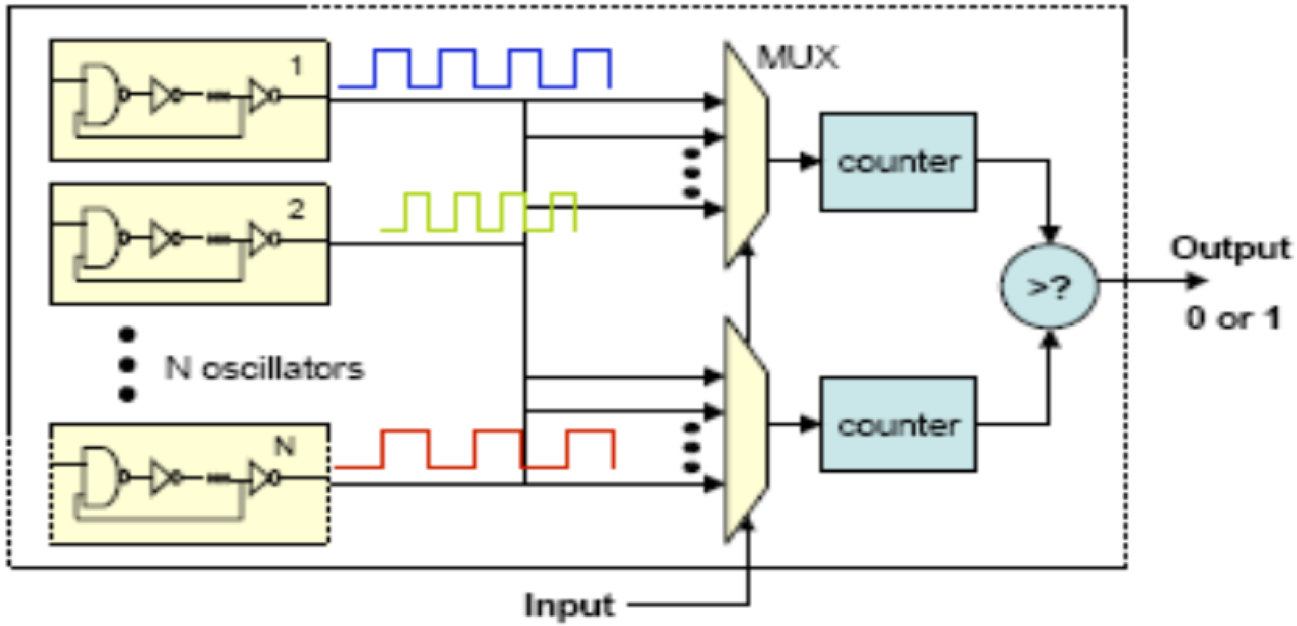
- What happens if we change voltage and temperature?



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

Ring-Oscillator (RO) PUF

- The structure relies on delay loops and counters instead of MUX and arbiters
- Better results on FPGA – more stable

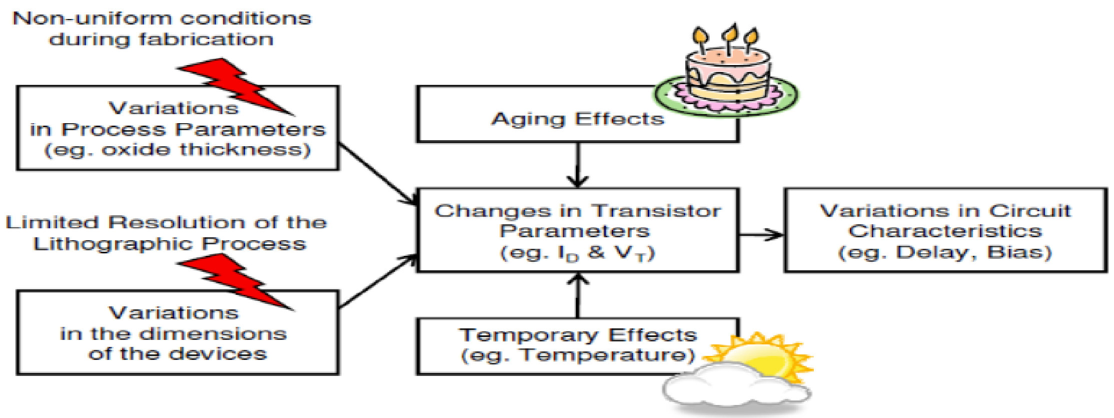


Ring-Oscillator (RO) PUF

- Easy to duplicate a ring oscillator and make sure the oscillators are identical
  - Much easier than ensuring the racing paths with equal path segments
- How many bits can we generate from the scheme in the previous page?
  - There are N(N-1)/2 distinct pairs, but the entropy is significantly smaller: $\log_2(N!)$
  - E.g., 35 ROs can produce 133 bits, 128 ROs can produce 716, and 1024 ROs can produce 8769

Consider the following minimal example, given three ROs: $RO_A.f < RO_B.f$ and $RO_B.f < RO_C.f$ implicates $RO_A.f < RO_C.f$. The total PUF entropy is only $log_2(N!)$ bit as there are *N!* ways to sort the frequency values.

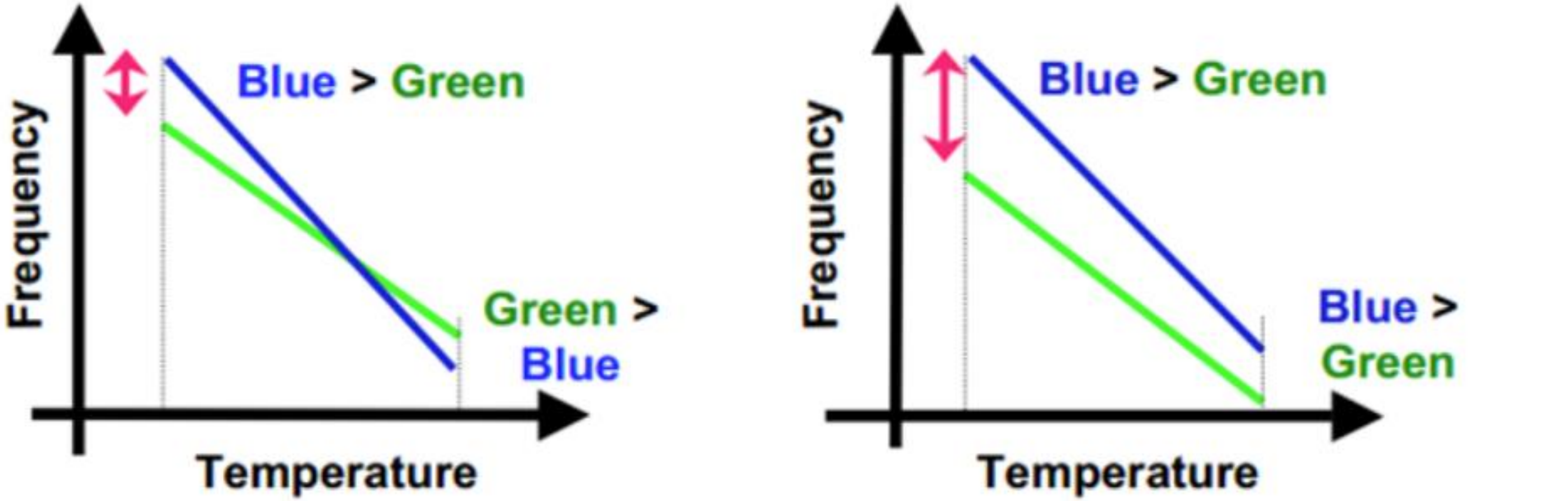
Ring-Oscillator (RO) PUF



- Two types of reliability issues:
- Aging:
  - Negative Bias Temperature Instability
  - Hot Carrier Injection (HCI)
  - Temp Dependent Dielectric Breakdown
  - Interconnect Failure
- Temperature
  - Slows down the device

Reliability Enhancement

- Environmental changes have a large impact on the freq. (and even relative ones)



(a) Frequencies are close

(b) Frequencies are far apart

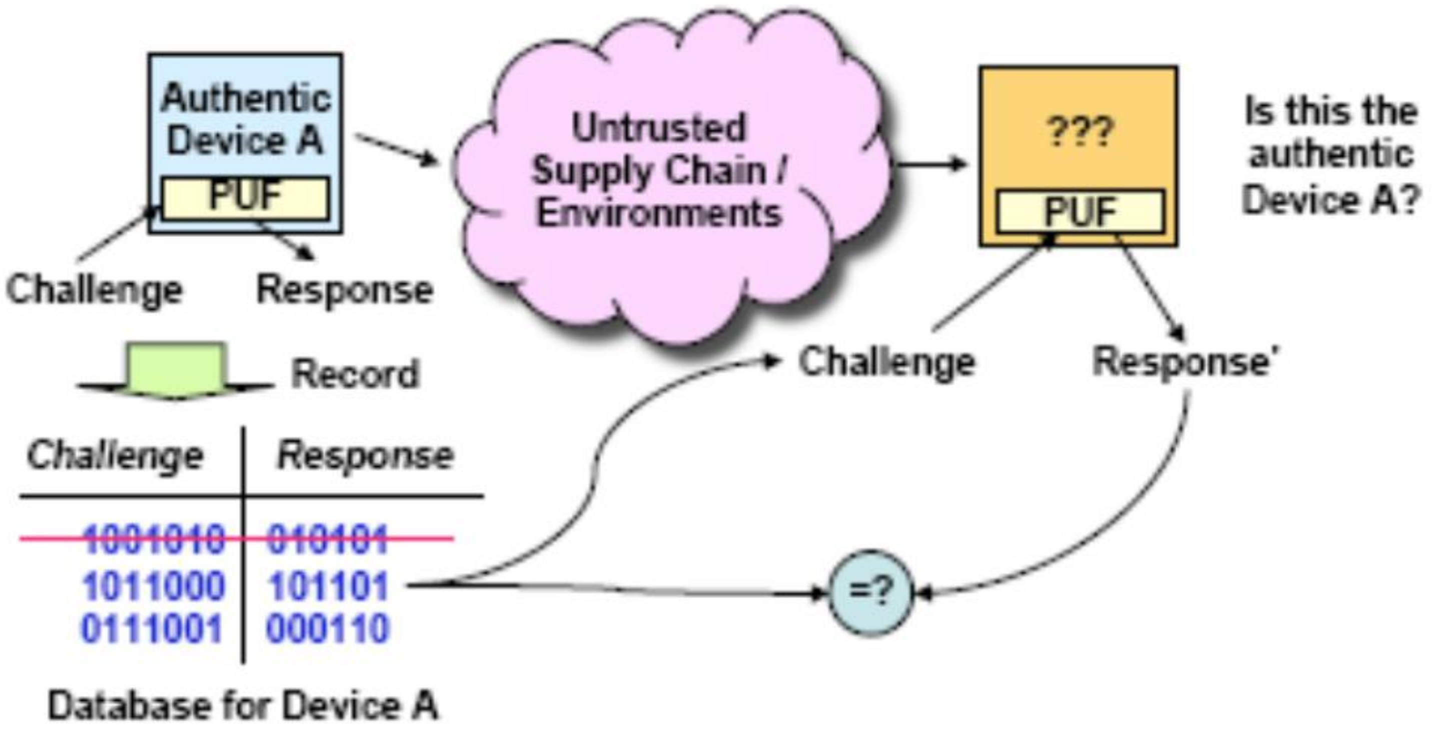
Ring-Oscillator (RO) PUF

- ROs whose frequencies are far are more stable than the ones with closer frequencies
  - Possible advantage: do not use all pairs, but only the stable ones
  - It is easy to watch the distance in the counter and pick the very different ones.
    - Can be done during enrollment

- RO PUF allows an easier implementation for both ASICs and FPGAs.
- The **Arbiter** PUF is appropriate for resource constrained platforms such as RFIDs and the **RO PUF** is better for use in FPGAs and in secure processor design.

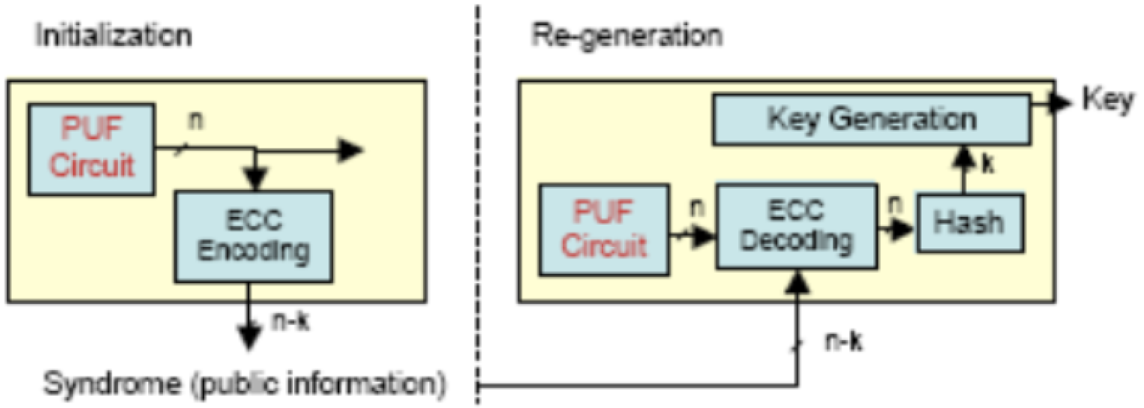
Authentication

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



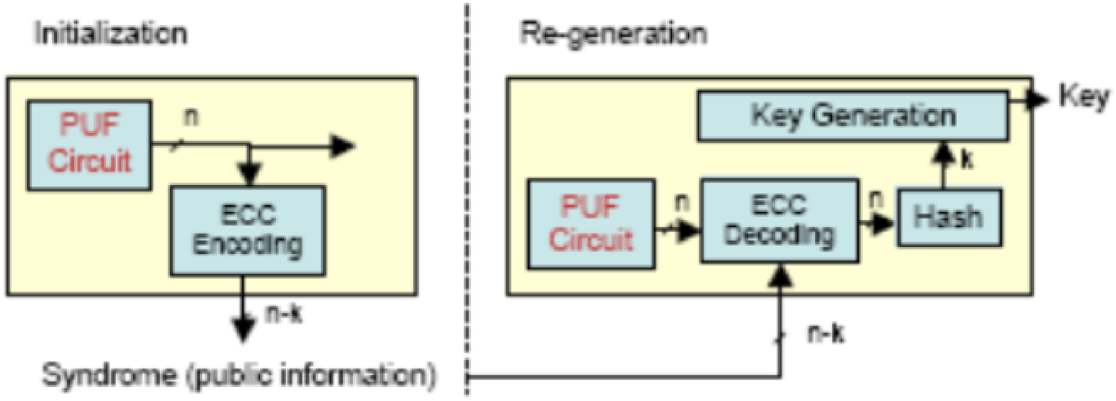
Key Generation

- The unstability is a problem
- Some crypto protocols (e.g., RSA) require specific mathematical properties that random numbers generated by PUFs do not have
- How can we use PUFs to generate crypto keys?
  - Error correction process: initialization and regeneration
  - There should be a one-way function that can generate the key from the PUF output



Key Generation

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



Experiments with RO PUFs

- Experiments done on 15 Xilinx Virtex4 LX25 FPGA (90nm)
- They 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
- The goal is to know if the PUF outputs are unique (for security) and reproducible (for reliability and security)

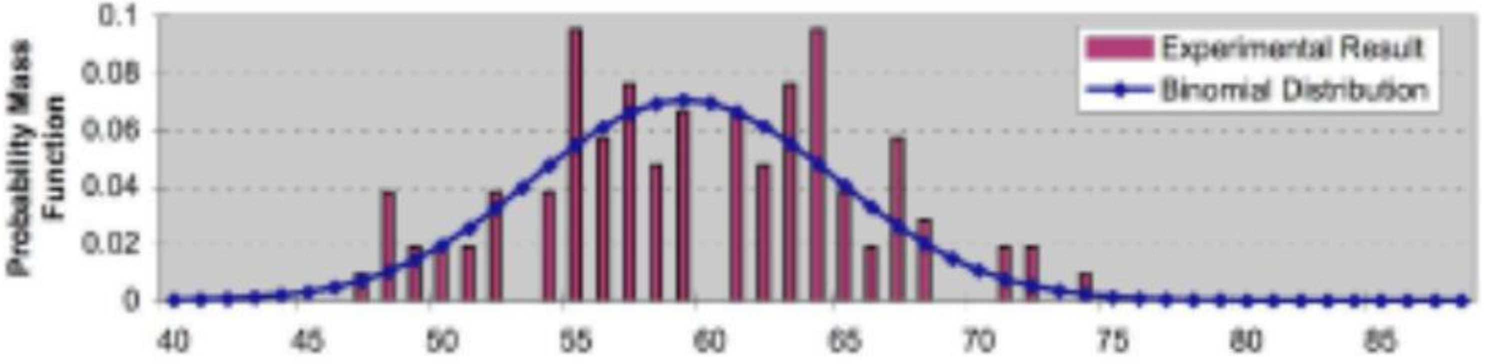
Metrics

- *Inter-chip variation*: How many PUF output bits are different between PUF A and PUF B? This is a measure of uniqueness. If the PUF produces uniformly distributed independent random bits, the inter-chip variation should be 50% on average.

- *Intra-chip (environmental) variation*: How many PUF output bits change when re-generated again from a single PUF with or without environmental changes? This indicates the *reproducibility* of the PUF outputs. Ideally, the intra-chip variation should be 0%.

Distribution

- 128 bits are produced from each PUF
- x-axis: number of PUF o/p bits different b/w two FPGAs; y-axis: probability
- Purple bars show the results from 105 pair-wise comparisons
- Blue lines show a binomial distribution with fitted parameters (n=128, p =0.4615)
- Average inter-chip variations 0.4615 ~ 0.5



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

Other PUFs

- SRAM PUF
- Bistable Ring PUF
- DRAM PUF
- Magnetic PUF
- Emerging Memory PUF (e.g. ReRAM)
- Optical PUF
- …….