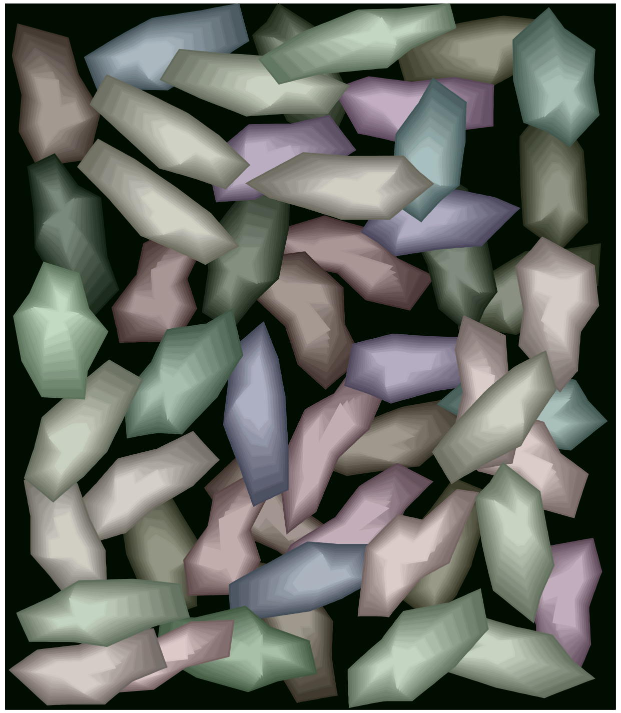
Feature: Process Variation

- Do we expect process variation (length, widths, oxide thickness) in circuit and system?
  - Impact circuit performance
  - Functional failure
  - Major obstacle to the continued scaling of integrated-circuit technology in the sub-45 nm regime
- Process variations can be turned into a feature rather than a problem?
  - Each IC has unique properties

Solution

Extract key information from a complex physical system.

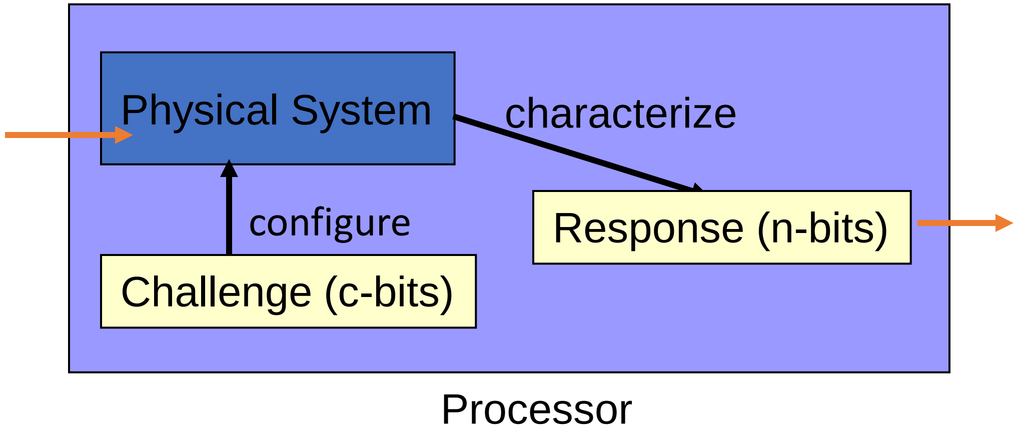


Devadas, et. al, DAC02

Physical Unclonable/Random Functions (PUFs)

- Generate keys from a complex physical system

Hard to fully characterize or predict



Use as a secret

Can generate many secrets by changing the challenge

- Security Advantage
  - Keys are generated on demand → No non-volatile secrets
  - No need to program the secret
  - Can generate multiple master keys
- What can be hard to predict, but easy to measure?

Definition

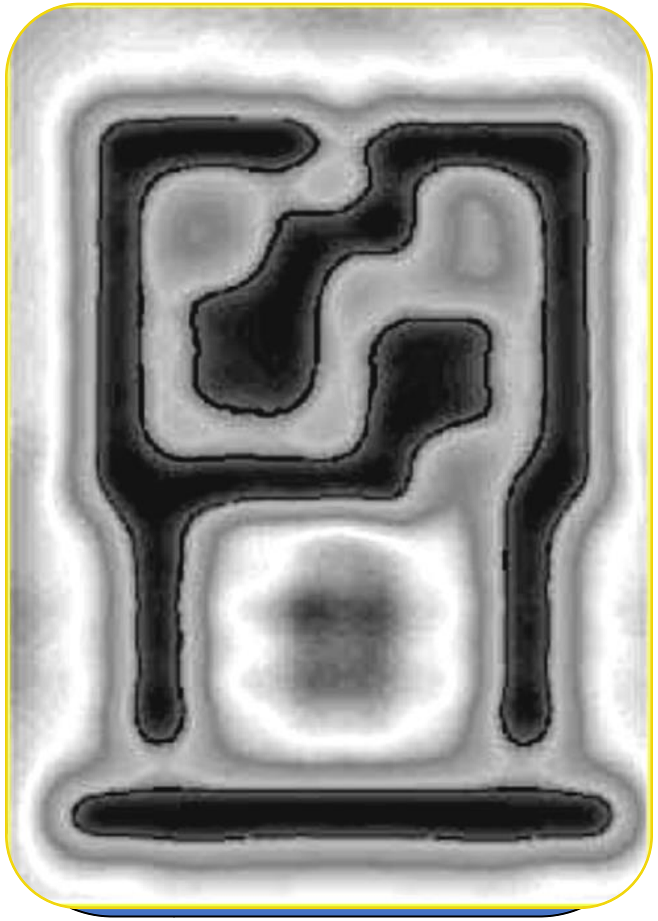
A Physical Random Function or Physical Unclonable Function (PUF) is a function that is:

- Based on a physical system
- Easy to evaluate (using the physical system)
- Its output looks like a random function
- Unpredictable even for an attacker with physical access

WYSINWYG

Sub-Wavelength WYSINWYG

What You See Is Not What You Get

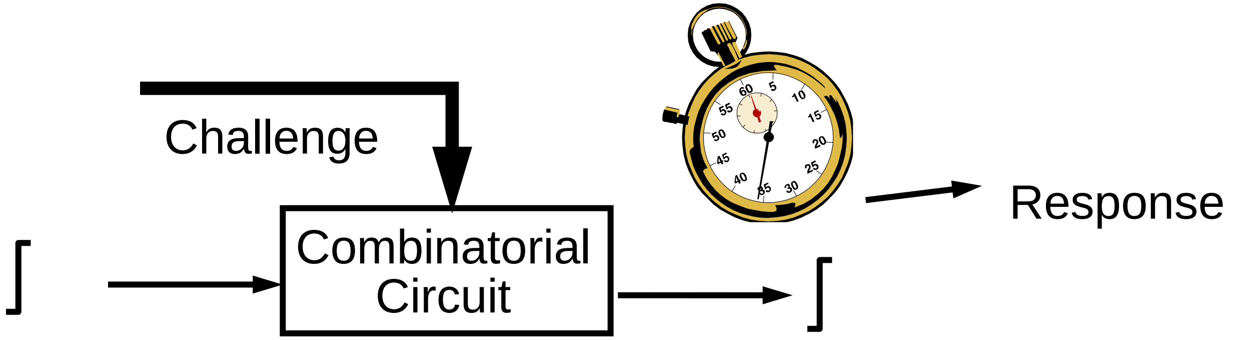


Process variations

No two transistors have the same parameters

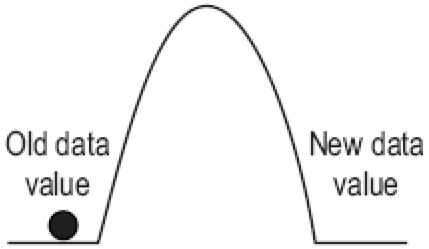
Silicon PUF – Proof of Concept

- Because of process variations, no two Integrated Circuits are identical
- Experiments in which *identical circuits with identical layouts* were placed on different FPGAs show that path delays vary enough across ICs to use them for identification.



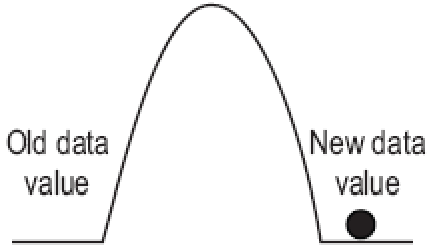
Metastability – Three Timing Conditions

Too Late



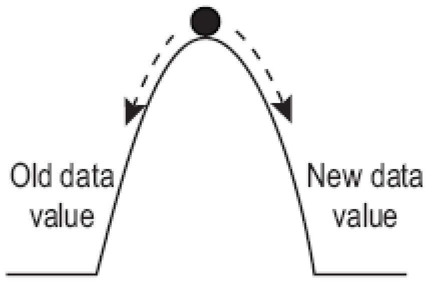
Signal transition occurs after clock edge and minimum t_H: Ball lands on the old data side.

Just Right

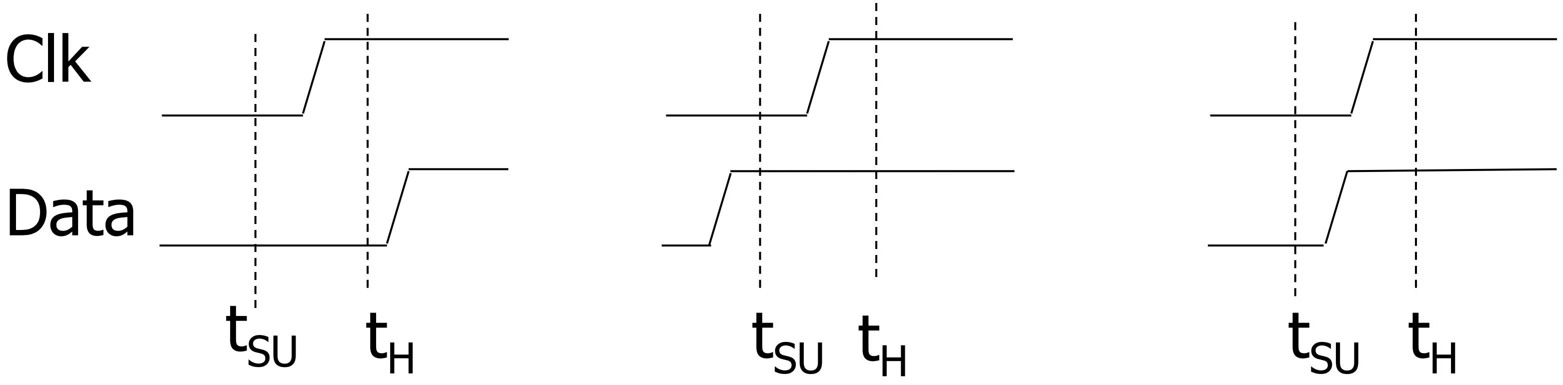


Signal transition meets register t_{SU} and t_H: Ball lands on the new data side.

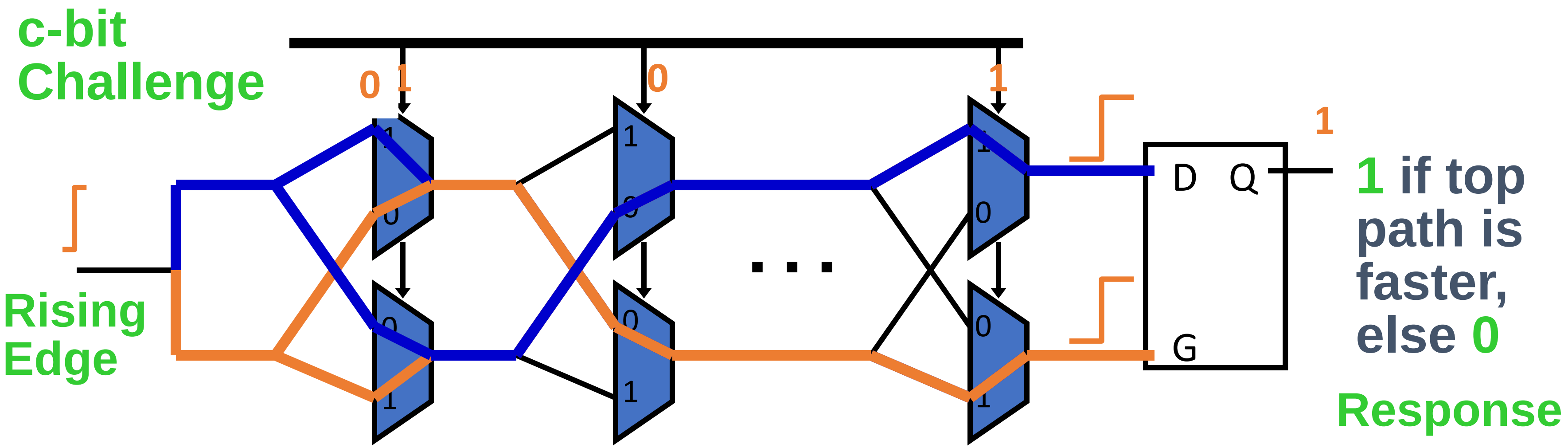
Too Early



Signal violates register t_{SU} or t_H: Ball balances at top of hill or takes too long to reach the bottom. Output is metastable and violates t_{CO}.



A Candidate: Silicon PUF



- Compare two paths with an identical delay in design
  - Random process variation determines which path is faster
  - An arbiter outputs 1-bit digital response
- **Path delays in an IC are statistically distributed due to random manufacturing variations**

Experiments

- Fabricated candidate PUF on multiple ICs, 0.18um TSMC
- Apply 100 random challenges and observe responses

**Distance between Chip X and Y
responses = 24**

- Two chips are different because of process variations.
- If the distance between chip X and chip Y are higher then it is good to detect ICs.
- Temperature adds some noise as a result it might give different results at different temperatures.
- There is also measurement noise.

Measurement Attacks and Software Attacks

Can an adversary create a *software clone* of a given PUF chip?

- A software clone of PUF is impossible. Experiment shows that best model for chip X has 10 errors which is almost equal to 50%.

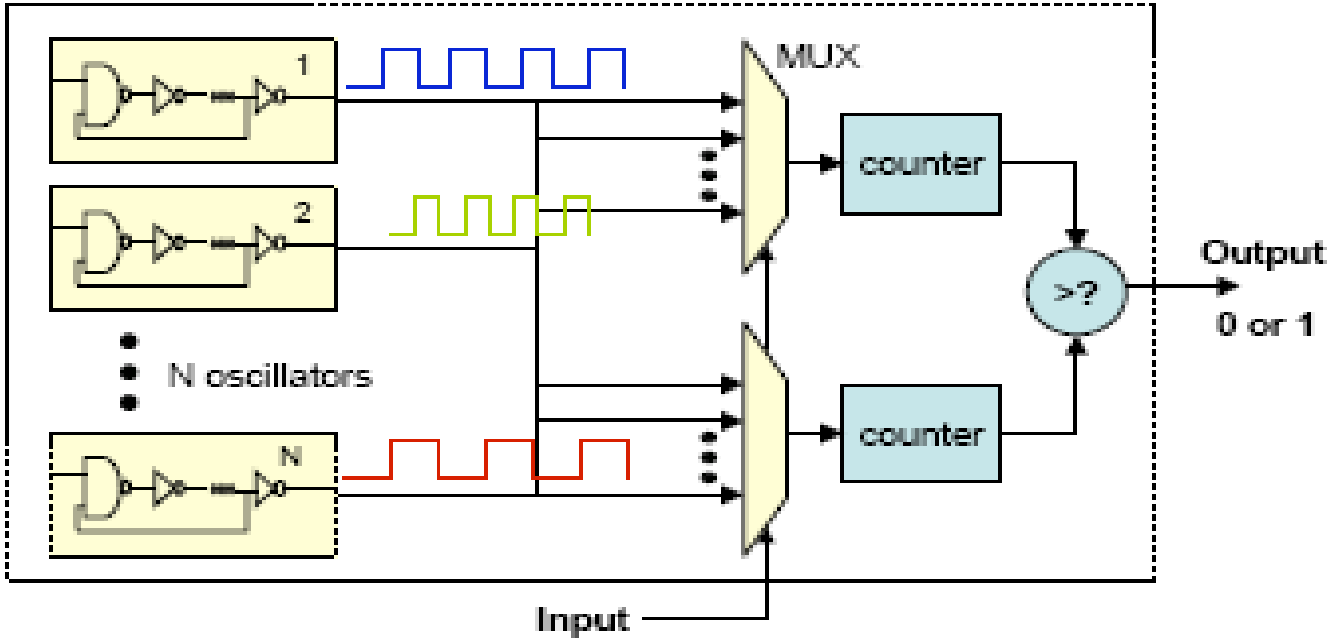
“Best” model for Chip X has error = 10

Physical Attacks

- Make PUF delays depend on overlaid metal layers and package
- Invasive attack (e.g., package removal) changes PUF delays and destroys PUF
- Non-invasive attacks are still possible
  - To find wire delays one needs to find precise relative timing of transient signals as opposed to looking for 0’s and 1’s
  - Wire delay is not a number but a function of challenge bits and adjacent wire voltages and capacitances

Ring-Oscillator (RO) PUF

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

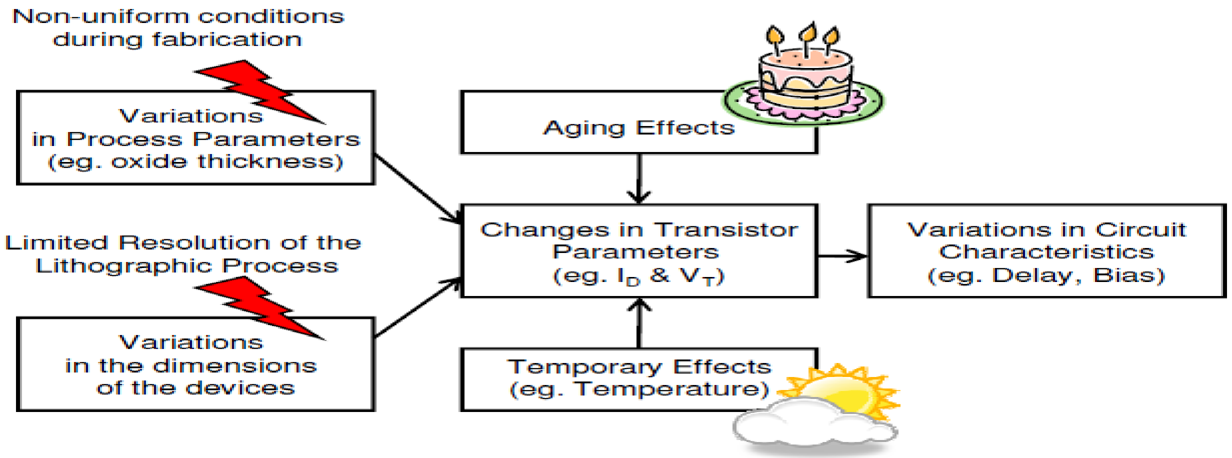


RO PUFs (cont'd)

- 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.

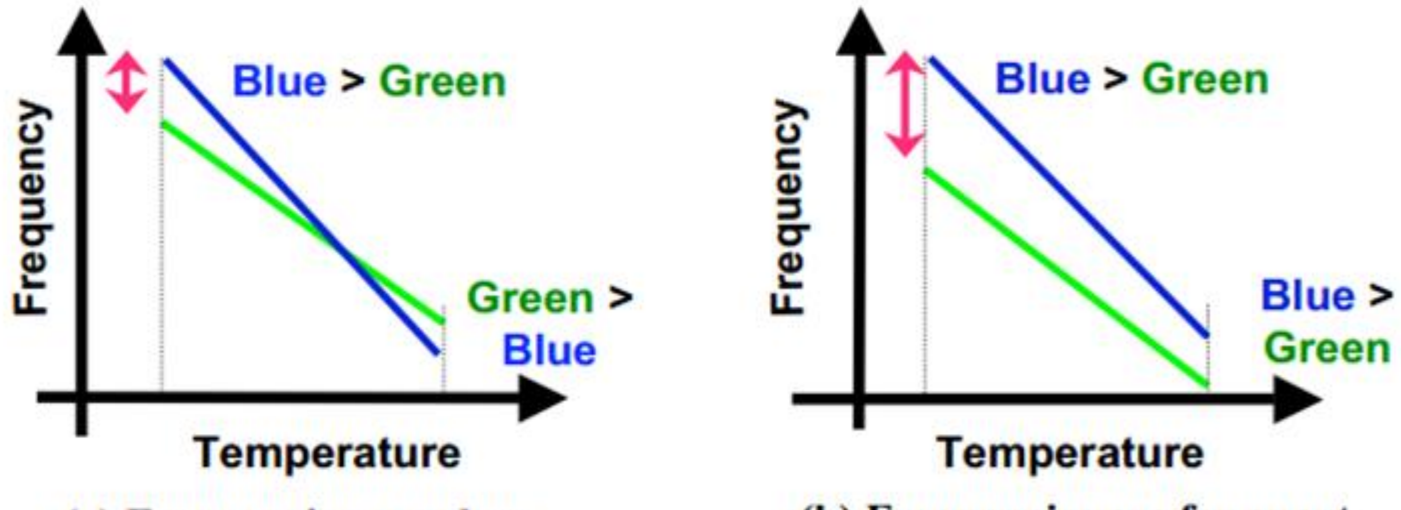
Reliability of RO PUFS


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

- 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

RO PUFs

- 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.