Physical Unclonable Functions

Shabnam Larimian

Department of Electrical and Computer Engineering
University of California, Santa Barbara

CS 293G, Spring 2018

Outline

- Motivation
- Hardware Cryptographic Technique
- Physical Unclonable Function (PUF)
  - PUF Features
  - PUF Responses vs. Classical Secret Keys
- CMOS-Based PUF
  - Delayed-Based PUF
  - Ring Oscillator PUF
  - SRAM PUF
- CMOS-Based PUF: Pros and Cons
- Nanoscale PUFs
- Methods of Attacking a PUF
- Summary

Motivation

The beginning of information technology led to expansion of interconnected devices.

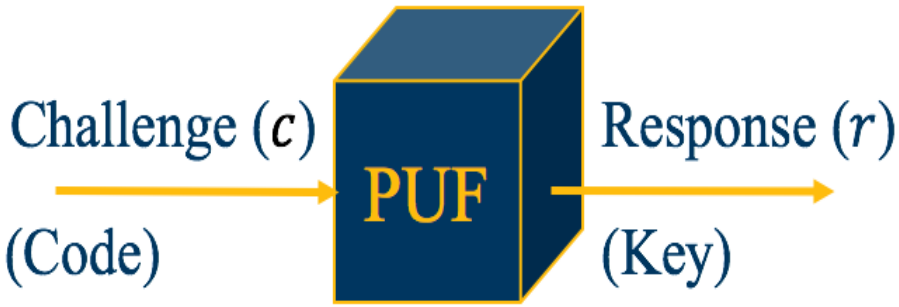
Motivation (Cont.)

Adversary can access and attack interconnected devices due to their inherent mobility.

Hardware Cryptographic Technique

- The most common cryptography technique is storing secret keys in non-volatile memory (NVM).
  - This needs hardware cryptographic operations such as digital signatures or encryption which are expensive in terms of design area and power consumption
  - Storing secret keys in NVM makes them vulnerable to invasive attacks. Therefore, active detection and prevention circuitry is required which must be continually powered.
- Because of the mentioned issues, researchers are looking for other solutions.
  - PUF is among new promising solutions that can be a great replacement for conventional method.

PUF



PUF is like a black box. It gets challenge or code as input and generates the response or key.

PUF (Cont.)

- PUF maps intrinsic properties of hardware devices (e.g. process variability) into unique digital information.
- PUF derives keys from physical properties instead of storing secret keys in digital memory.
- PUF has hardware randomness, thus it is hard to copy and reverse engineer.
- PUFs can be used in different applications such as authentication, identification, and key generation.

PUF Features

- PUF has three features:
  - Uniqueness:
    - The mapping function of PUF must be unique for each PUF instance.
  - Security:
    - The mapping function must be hard to infer or model.
  - Reliability:
    - The response must be repeatable over time for a particular PUF instance.

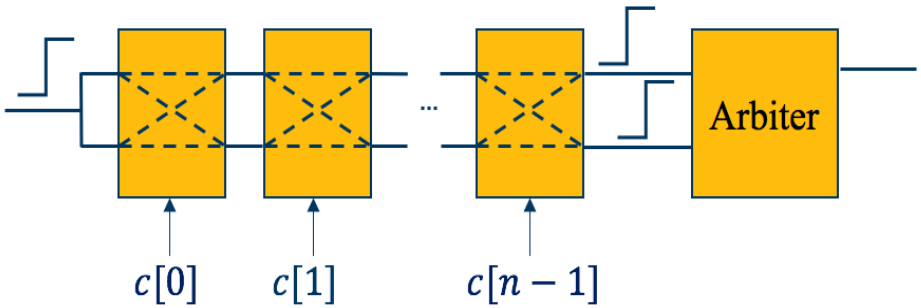
PUF Responses vs. Classical Secret Keys

- Pros:
  - Unclonable
    - Reason: PUFs are based on uncontrollable and unpredictable device manufacturing variations.
  - Simpler fabrication and low cost
    - Reason: PUFs need no memory to store secret keys.
  - Not vulnerable to many of physical attacks
    - Reason 1: PUFs generate output only when powered.
    - Reason 2: PUFs have complex behavior.
- Cons:
  - PUFs could have high bit error rate.

CMOS-Based PUF

- Different technologies can be used to build PUF primitives. Because CMOS has a well-established fabrication infrastructure, it is used as base of many PUF instances.
- Delay-based PUF, ring oscillator PUF, and SRAM PUF are three famous CMOS-based PUFs.

Delay-based PUF

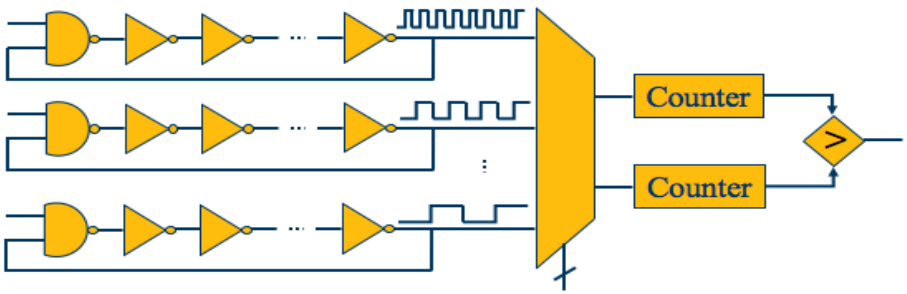


- Each stage is constructed from two multiplexers (MUXes).
- Based on the input of MUXes, the input signal will go through one of the designed paths.

Delay-based PUF (Cont.)

- Even if we try to build identical 2-input MUXes in each stage, the paths will have different delays because of process variation.
- In other words, unique variations in propagation delays through interconnects and logic cause one path to have less delay than the other.
- This type of PUF is based on the race along two signal paths of nearly equal delay.

Ring Oscillator PUF

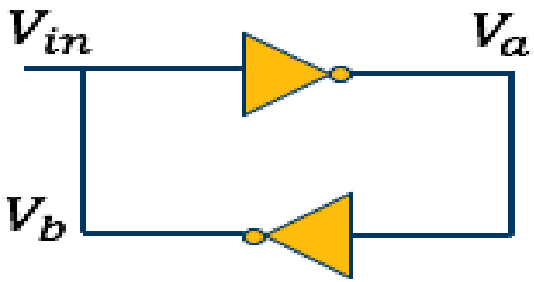


- Ring oscillator PUF consists of many delay loops that oscillate with a particular frequency.
- The number of logic cycles of each RO is counted by its respective counters.

Ring Oscillator PUF (Cont.)

- Even if the ring oscillators are laid out identically, the manufacturing variations results in different frequency for each loop.
- The counters counts the number of edges over a fixed period of time.
- The output response bit is generated by comparing the oscillation frequencies of ring oscillator loops.

SRAM PUF



- SRAM memory consists of SRAM cells.
- Each SRAM cell is composed of two cross-coupled inverters that are built from p-MOS and n-MOS transistors.

SRAM PUF (Cont.)

- When SRAM cell is powered on, its logical state is determined by the threshold voltages of the p-MOS transistors.
- The transistor that starts conducting first determines the logical value of the SRAM Cell.
- Each SRAM cell has its own preferred state.
- The preference of each SRAM cell is independent of the location of the cell on chip or wafer.
- As a result of these features, the power-on value of SRAM cell can be used as a base of PUF primitive.

CMOS-Based PUF: Pros and Cons

- Pros:
  - CMOS has a well-established fabrication infrastructure.
- Cons:
  - CMOS-based PUFs have reliability issues and are susceptible to modeling attacks .
  - CMOS-based PUFs have relatively large area comparing to nanoscale devices which has negative effects on:
    - cost
    - energy
    - throughput per area

Nanoscale PUFs

- Because of the issues that CMOS-based PUFs have, researchers are looking for other types of PUFs including nanoscale PUFs.
- Among the nanoscale devices memristors are great candidate because:
  - Although they are so far immature technology, they are compatible with CMOS fabrication standards.
  - They are sensitive to process variation.
  - They are nanoscale devices which makes them:
    - dense
    - energy efficient
    - fast

Methods of Attacking a PUF

- Ideally, we are looking for PUFs that are secure against attacks, so we cannot clone and predict them.
- In order to evaluate PUF's security, its behavior should be investigated against different attacks.
- Attacks can be categorized in different groups such as invasive, non-invasive, and hybrid attacks.

Methods of Attacking a PUF (Cont.)

- Invasive:
  - This type of attack alters the system or its environment.
- Non-invasive:
  - Side-channel attacks:
    - power side-channel attacks
    - timing side-channel attacks
    - electromagnetic attacks
  - Numerical attacks:
    - mathematical attacks
    - algorithm attacks
  - Machine learning attacks
- Hybrid:
  - This type of attack is a combination of multiple attacks.

Summary

- Current solution of for hardware security of secret keys is storing them in non-volatile memories.
- Because of the issues that this method has, new methods are under study. Among them, PUFs are great candidates.
- There are different CMOS-based PUFs. To reduce their issues, nanoscale devices are considered as a replacement for base element of PUFs.
- In order to analyze PUF, its resilience against different attacks should be studied.