Silicon Physical Random Functions

Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas

Presented by: Jose Rodrigo Sanchez Vicarte

Table of Contents

Motivation

- Identification And Authentication Of Individual ICs
- Tamper Resistant IC Characterization
- Devices Are Already Inherently Unique

Previous Solution - Unique Identifier

- Enables Identification, Not Authentication
- Vulnerable To Invasive And Non-invasive Attacks
- Tamper Resistance Is Expensive And Difficult

Physical Unclonable Function - Definition

- Maps Challenges to Responses
- Embodied by a Physical Device
- Easily Evaluates The Function In A Short Amount Of Time
- Hard To Characterize

Physical Unclonable Function

- Enough variation already exists in ICs for individual authentication, due to statistical delay variation for equivalent wires and devices across different ICs
- Can Be Made Tolerant To Environmental Variance And Aging
- Create A Single Unique Response For Each Manufactured IC
- Transient response is nonlinear and non-monotonic; gives only indirect information on the delays of wires and devices

Physical Unclonable Function

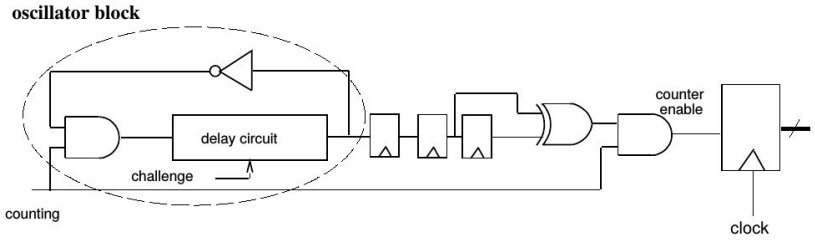


Figure 1: Self-Oscillating Loop Circuit.

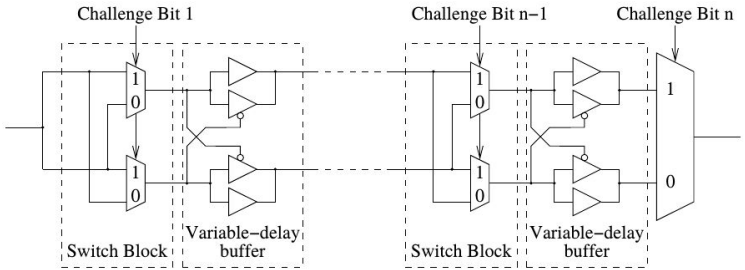


Figure 2: Non-Monotonic Delay Circuit.

Manufacturer Resistant

- Technically Impossible To Produce Two Identical PUFs
- Database of challenges and responses, however, is provided by the manufacturer

Authentication: Challenge-Response Pairs

Use Multiple Challenge Response Pairs

- Very difficult for two ICs to have the same response to a combination of challenges, even if they have the same response to one or more of the challenges; use a combination of challenges to generate a many-bit response
- Challenge-response pair cannot be reused, as an attacker may build a database with the revealed challenge-response pairs

Controlled PUF - Definition

- Only accessible by a physically linked algorithm, which is made inseparable from the system by intertwining it with the PUF in a very fine grained way
- Restricts Challenges To Which It Will Respond
- Limits The Information About Responses Given

Controlled PUF - Random Function

- Pre-Compose the PUF with a random function, making it impossible for the adversary to choose the challenge being presented to the PUF
- Post-Compose by hashing the output

Controlled PUF - Personalities

- Owner of the PUF has a controllable parameter so different facets of the PUF are presented to different applications; hash the challenge with a user selected personality number

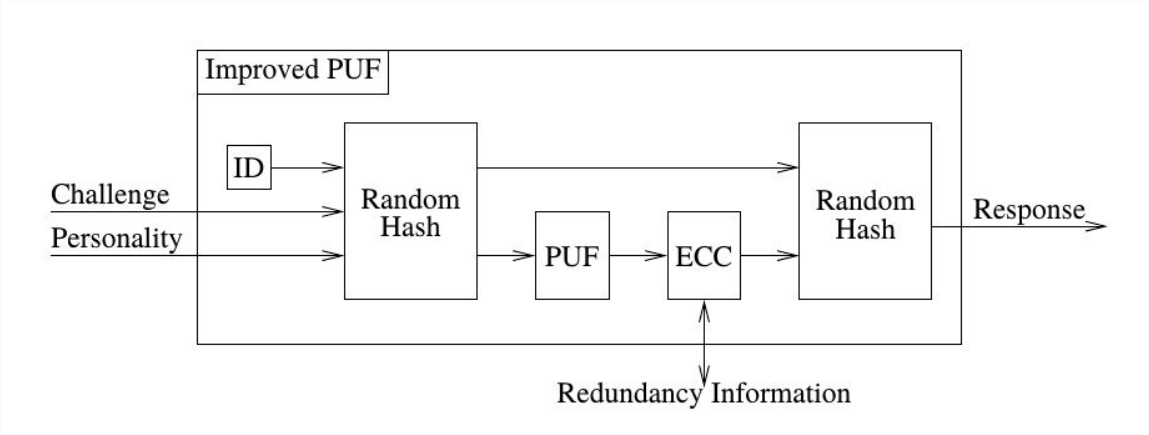
Controlled PUF - Error Correction

- Account for slight variations from one run to another; make the PUF’s output identical each time a challenge is reused
- Requires redundant information be created when the challenge-response pair is created

Controlled PUF - Unique Identifier

- Guarantee a difference in PUFs across many ICs by incorporating a unique ID into the IC and using it to hash the challenge

Controlled PUF - Definition



Environmental Variations

- Temperature
- Voltage Supply
- Aging

Environmental Variations

- ~~Temperature~~ Use relative measurement of delays
- ~~Voltage Supply~~ Same as temperature
- ~~Aging~~ Minimal, compared to temperature and voltage supply

Alternatively, expect different responses, based on environmental characteristics

Attacks

- Identical, Counterfeit, IC
  - Prohibitively Expensive
- Direct Measurement
  - Changes Timing Characteristics
- Model the PUF
  - Most Realistic Attack
  - Measure the response of a polynomial number of adaptively-chosen challenges
- Attack the Control Algorithm
  - Wire the IC so an adversary has to change the timing characteristics in order to reach the control circuit

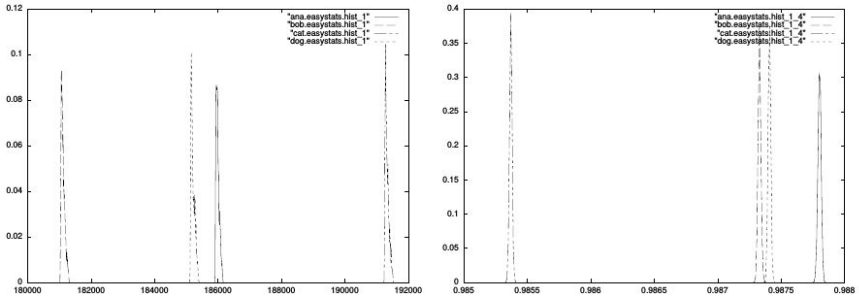
Applications

- Authenticated Identification
- Proof of Execution on a Specific Processor

Experiments

- Consecutive Measurements of the Same Delay
- Interference Between Loops
- Environmental Variation

Experiments



(a) Uncompensated

(b) Compensated

Figure 6: These histograms show the relation between measurement error (width of a peak) and inter-FPGA variation (each peak is for a different FPGA), with and without compensation. Clearly information about the FPGA's identity can be extracted from these measurements.

Future Work

- Measuring physical characteristics of the chip directly; omit the self-oscillating circuits
- Differential power analysis on a controlled PUF to reveal challenges
- Aging