Physically “Unclonable” Functions or Physically hard for yoU to clone Functions PUFs Part II

ECE 4156/6156 Hardware-Oriented Security and Trust

Spring 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Book and Website

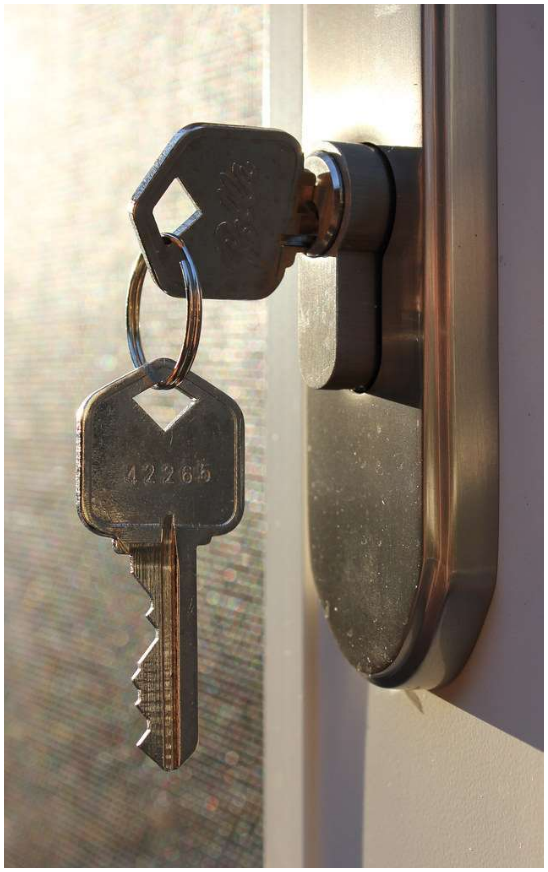
- These notes are based on the following book
  - Physically Unclonable Functions
  - *Constructions, Properties and Applications*
  - by Roel Maes
  - Springer-Verlag
  - 2013
  - ISBN 978-3-642-41394-0
  - ISBN 978-3-642-41395-7 (eBook)
- And these notes are based on research & papers by Professor James Plusquellic of the University of New Mexico
- http://ece-research.unm.edu/jimp/

Reading

- Physically Unclonable Functions, Chapters 1, 2 & 4

PUF Goals

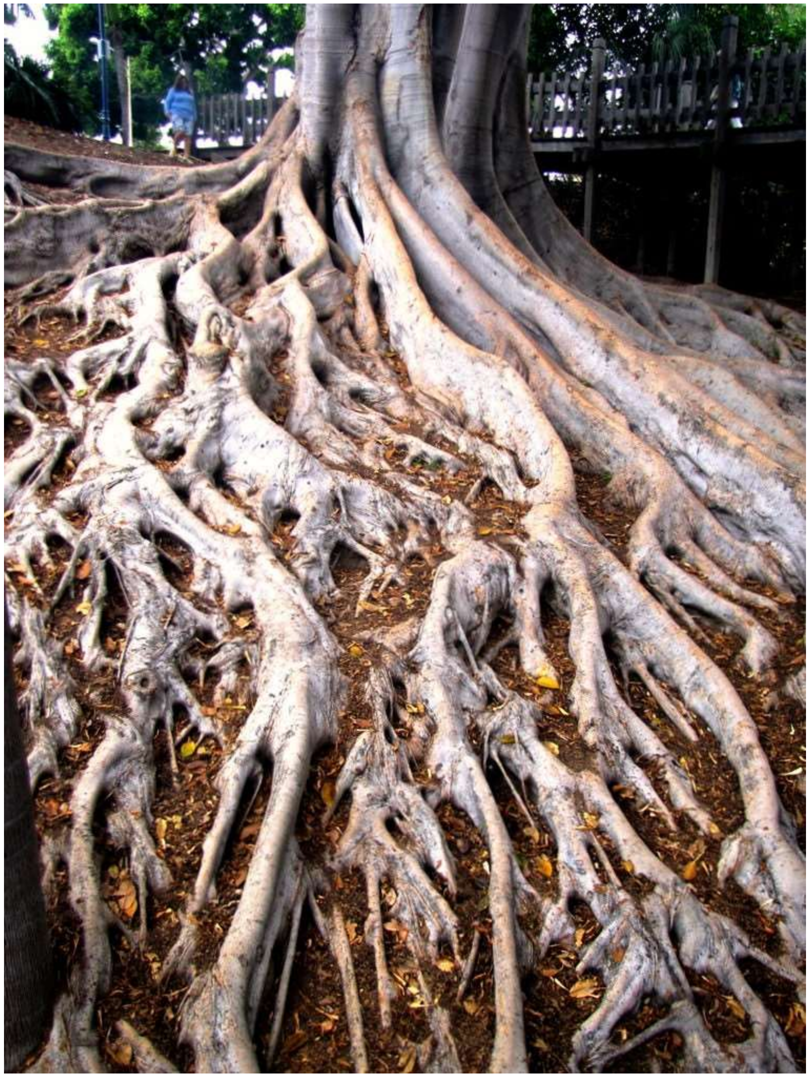
"Fingerprint" by CPOA is licensed with CC BY-ND 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nd/2.0/



"door key" by woodleywonderworks is licensed with CC BY 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by/2.0/

PUF Goals (continued)

- Root-of-Trust (RoT)
- Non-Volatile Memory (NVM) is the main alternative
- NVM is typically considered to be much more vulnerable to attack
  - By definition of “memory,” one can read and write NVM bits
  - PUF technology, on the other hand, typically cannot be written
- “An expression of an inherent and unclonable instance-specific feature of a physical object” (Maes, pg. 6)



"Banyan Tree Roots" by moonjazz is marked under CC PDM 1.0. To view the terms, visit https://creativecommons.org/publicdomain/mark/1.0/

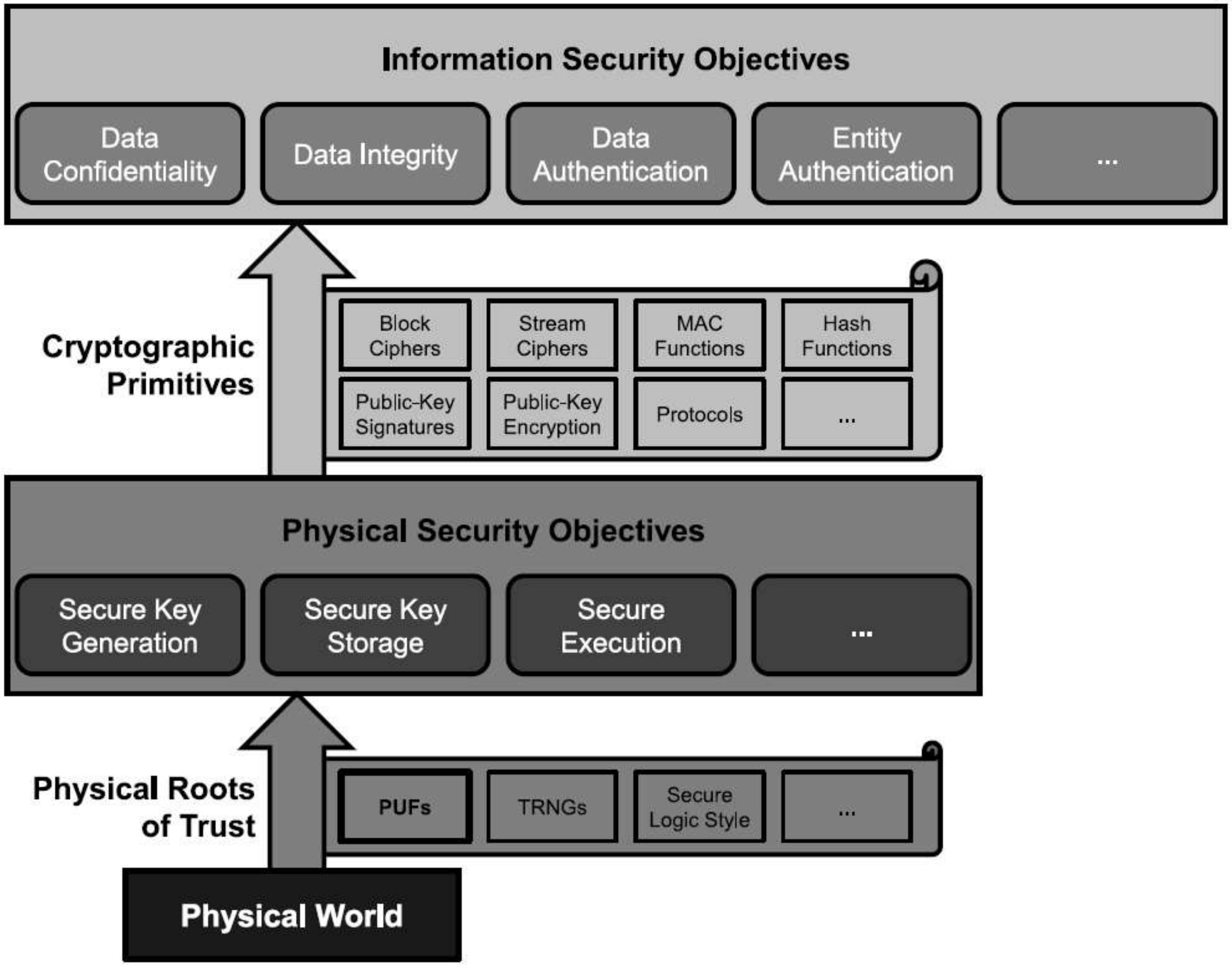


Fig. 1.1 Relations between information security, cryptography, physical security and physical roots of trust

Is a PUF a Function?

- Let *y* = *puf*(*x*).*Eval*
- If by “function” what is meant is a “deterministic function,” the answer for all known silicon PUFs is “No!”
  - The main reason is the variation due to temperature and voltage
- If by “function” what is meant is a “probabilistic function,” the answer is “Yes”

The Billion Dollar PUF Question

- Can the underlying physics of a PUF be harnessed to provide the following
  - An exponentially large (as opposed to polynomial) challenge-response space
  - Statistically reliable responses which can be utilized for cryptography
    - Authentication
    - Encryption
  - Sufficient sizes of “*n*” such that an adversary cannot carry out brute-force attacks successfully

The Million Dollar PUF Question

- Can the underlying physics of a PUF be harnessed to provide the following
  - A large (e.g., polynomial) challenge-response space
  - Statistically reliable responses which can be utilized for cryptography
    - Encryption
  - Hide the challenge
    - e.g., only provide challenge during a secure enrollment process
  - Sufficient physical hiding of the PUF response from side-channel and other physical attacks
  - Use the obscurity of the above to avoid brute-force attacks with other than a negligible probability of success
    - Analogy: use of a small password but lock up after 10 (or less, e.g., seven or three) guesses

PUF Definition

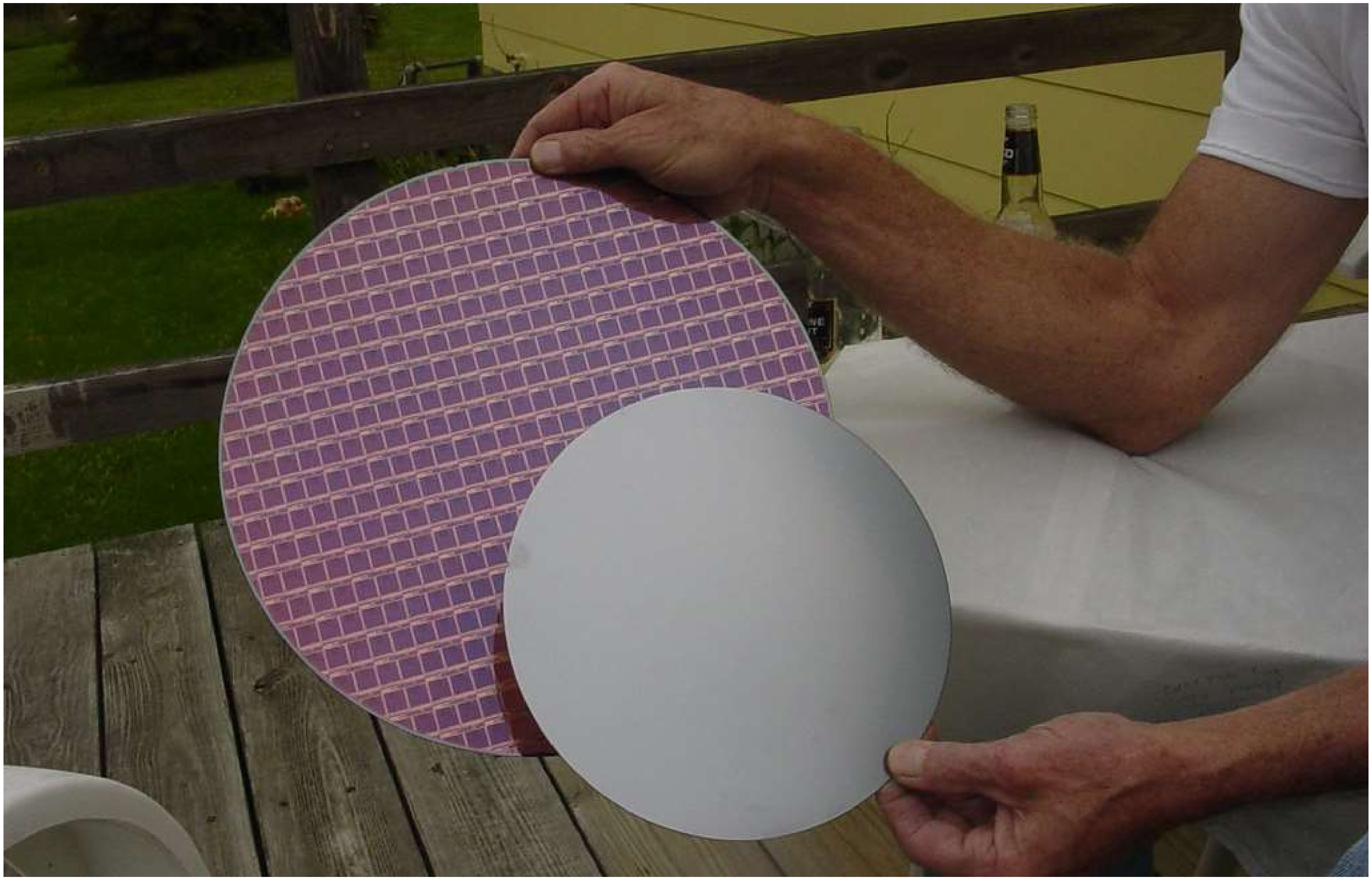
- A PUF is a combination of a physical source and a technique as follows:
  - A physical *source* of randomness (also referred to as *entropy*)
    - This course will focus almost exclusively on silicon based processes
    - There is a very strong relationship with testability of microchip technology
      - In a sense the more testable a process is, the less suitable is that aspect of the process as a source of randomness
  - A technique to *measure* the random physical source and present the result in the form of a number (i.e., a bit pattern)

What is Entropy?

- Second law of thermodynamics
- Molecules in a gas expand randomly to fill the available space

Extrinsic versus Intrinsic PUFs

- An extrinsic PUF has its entropy source and measurement technology distinct
  - Example: optical PUF
  - An optical PUF typically has a fiber optic cable connected to a microchip for measurement
  - Random fluctuations in the material appear to approach the level of randomness of atomic decay
  - Once fabricated, the fiber optic material has repeatable fluctuations
- An intrinsic PUF has its entropy source and measurement in the same physical object
  - This class focuses on intrinsic PUFs in silicon



"Silicon Wafers" by LarimdaME is licensed with CC BY-NC 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc/2.0/

Silicon Fabrication Processes

- No two silicon dice are identical
- Each die has unique characteristics
  - Nanometer variations in atomic composition
  - What is drawn or intended by a designer is never exactly implemented
  - E.g., in the last few planar MOSFET generations, layout was changed by Optical Proximity Correction (OPC) techniques, e.g., corners of a bus wire
- The effects of variations in silicon processes are typically exhibited and measured via electrical characteristics
  - Delay
  - Voltage levels
- Overall goal of fabrication is to eliminate variations either within a die (intra-die) and between different dice (inter-die)

Back to the Goals of PUF Usage

- What if we lack certainty regarding the inability of an adversary to carry out a successful attack on a PUF?
  - Not certain that the search space grows exponentially
  - Not certain that "*n*" can be made large enough to rule out brute force attacks
  - Not sure that an adversary with insider access to one of the supply chain steps cannot glean information sufficient to carry out a successful attack
- A so-called "Weak PUF" is not guaranteed to have an exponential challenge-response space
- Some applications – e.g., part tracking on a manufacturing floor – may benefit from weak PUF technology
- A so-called "Strong PUF" claims to have a negligible probability of being successfully attacked for a given attack surface

Strong PUF Attack Surface

- Adversary has physical possession of the microchip for a limited time
  - E.g., a chip is being mounted on a printed circuit board by an “untrusted” company in a country distinct from the eventual country of usage
  - Initial chip fabrication may occur within the country of usage but by a manufacturing plant owned by an international company
- Adversary can collect a polynomial number of challenge-response pairs and store them
- Adversary can also aim to build a model of the physical PUF
  - Note that this is distinct from traditional cryptanalysis

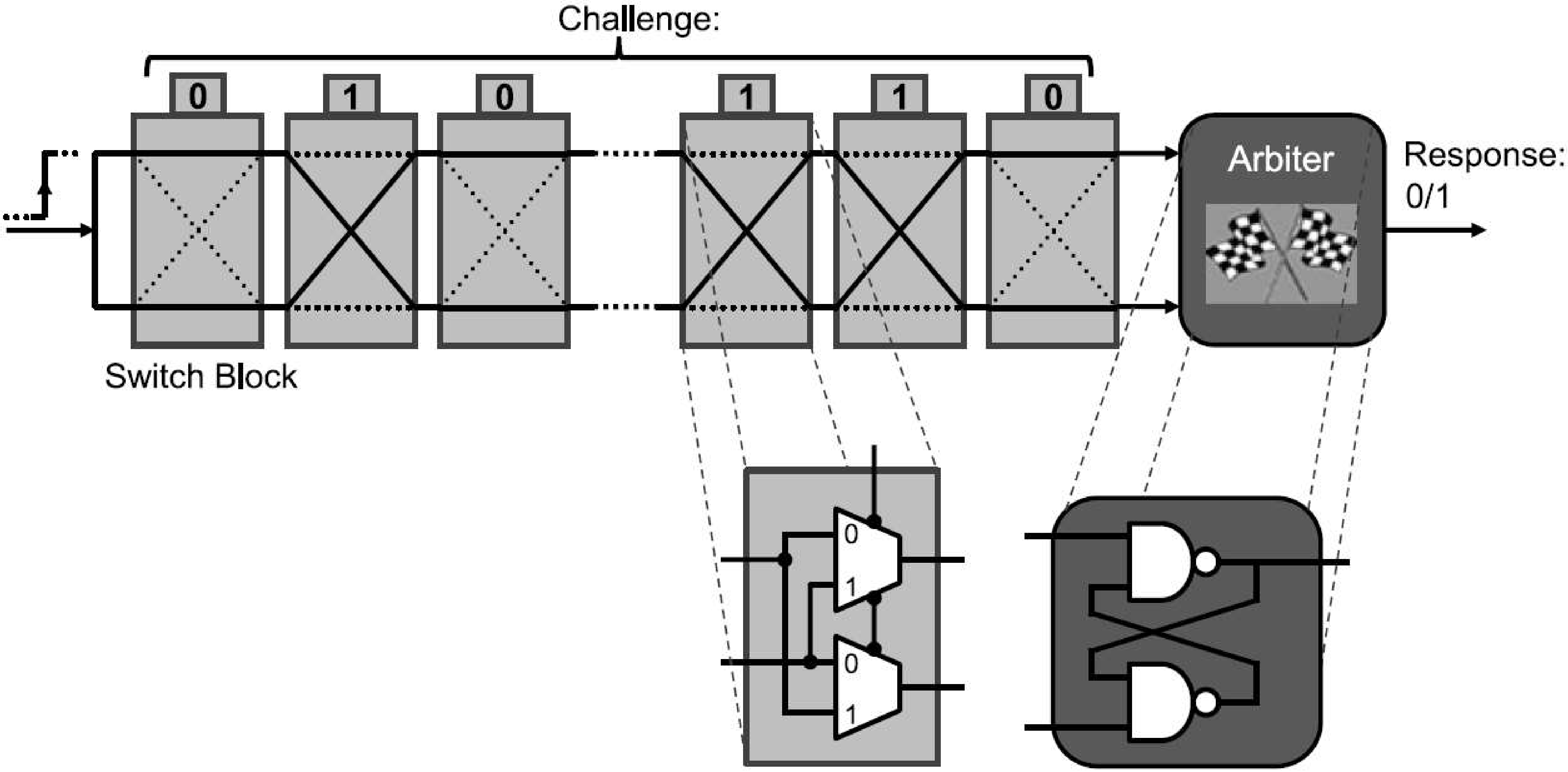
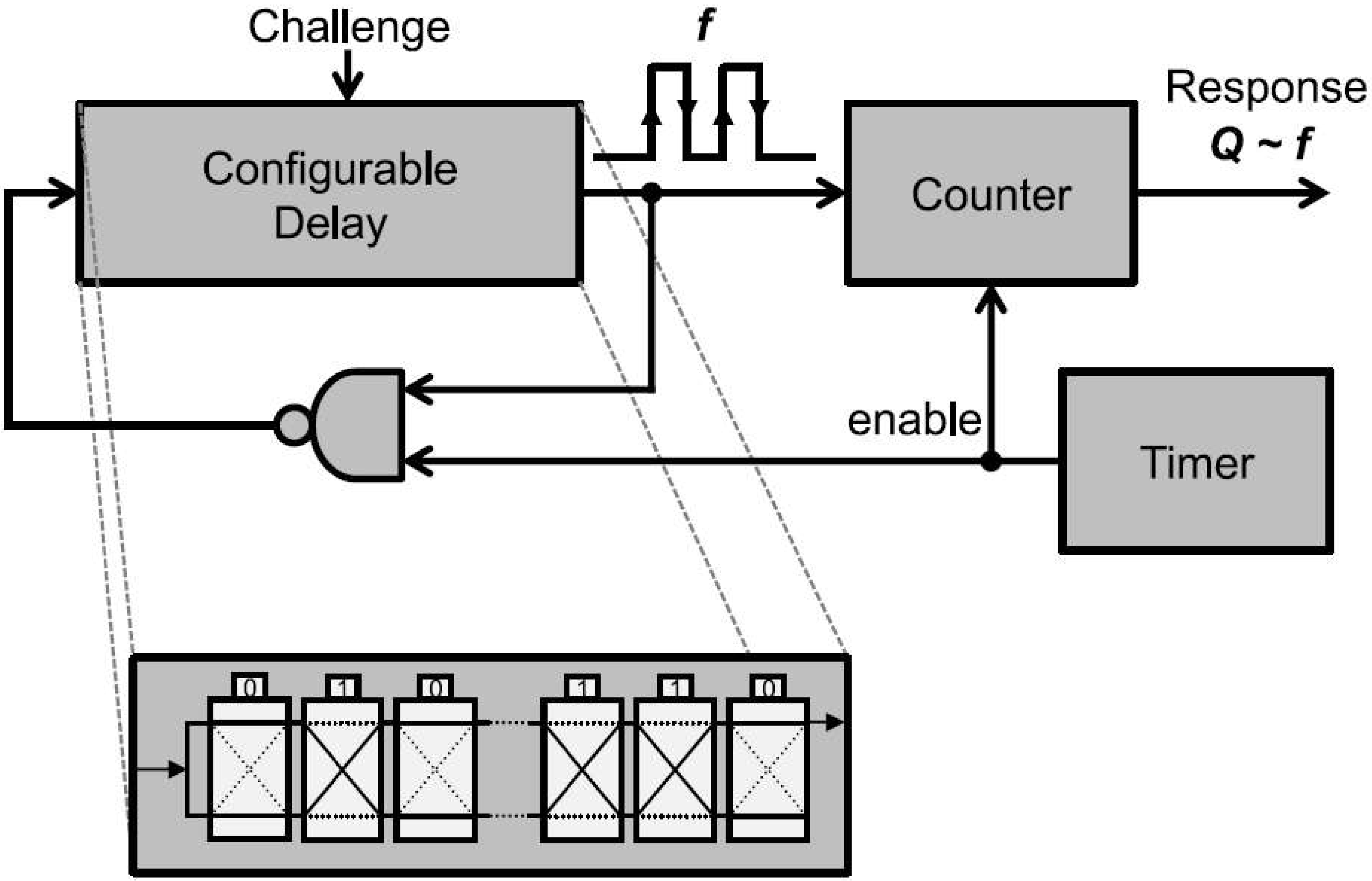


Fig. 2.1 Construction of a basic arbiter PUF as proposed by Lee et al. [43, 75, 78]

The Arbiter PUF is Machine Learnable

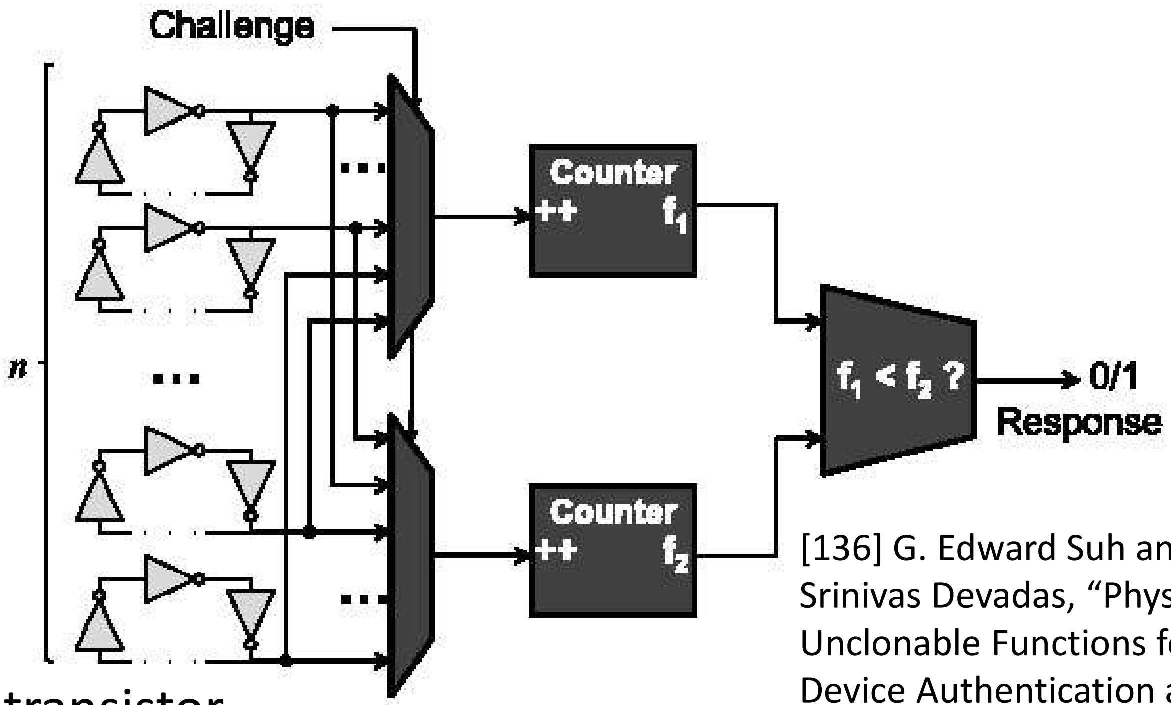
- How?

Fig. 2.2 Construction of a simple ring oscillator PUF as proposed by Gassend et al. [42]



Ring Oscillators: Example of a Physically hard for yoU to clone Function (PUF)

Fig. 2.3 Construction of a comparison-based ring oscillator PUF as proposed by Suh and Devadas [136]



- Page 32 of Maes
- Each microchip will have transistor variations resulting in distinct timing characteristics for the ring oscillators

[136] G. Edward Suh and Srinivas Devadas, “Physical Unclonable Functions for Device Authentication and Secret Key Generation,” Design Automation Conference (DAC), 2007, pp. 9-14.

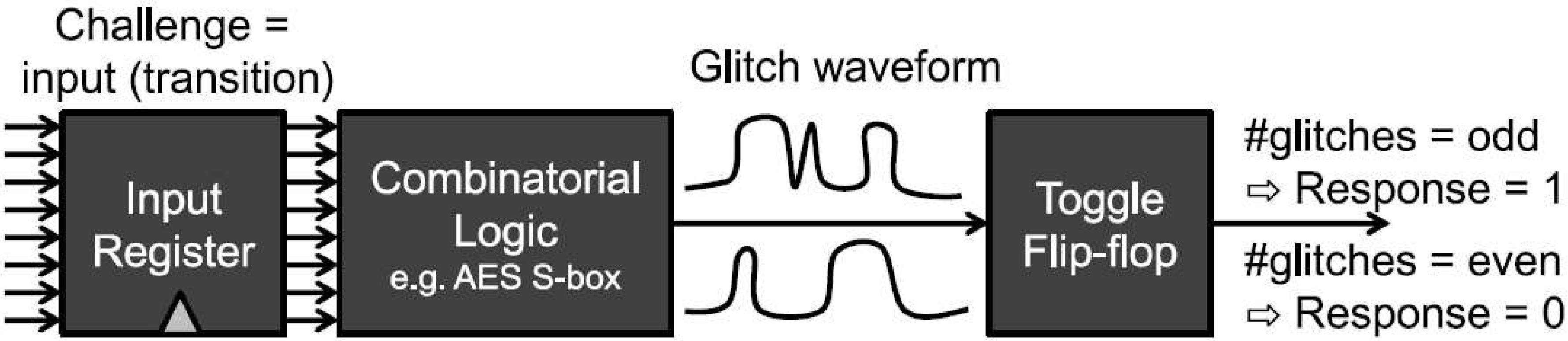
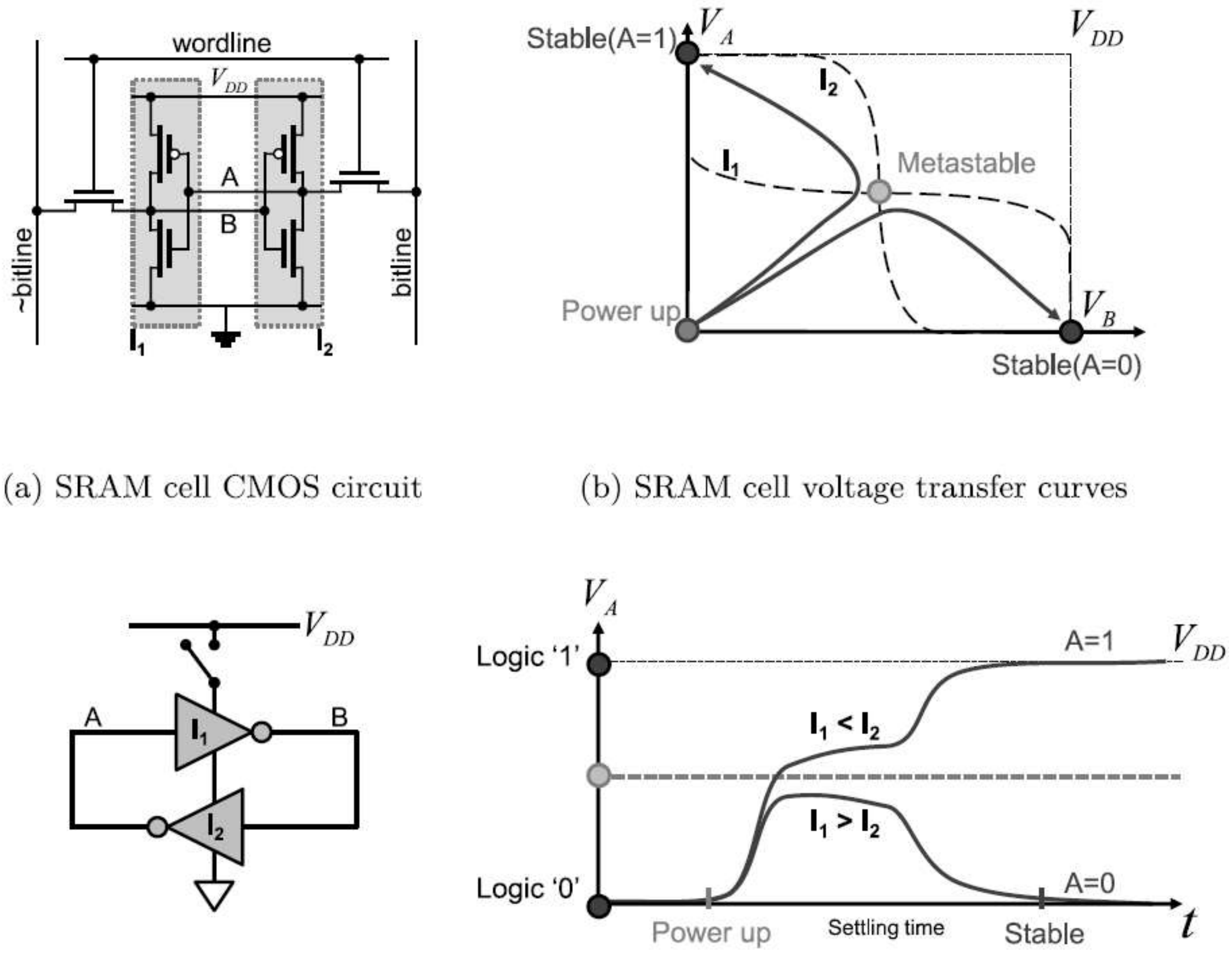


Fig. 2.4 Construction of a glitch PUF as proposed by Shimizu et al. [129]



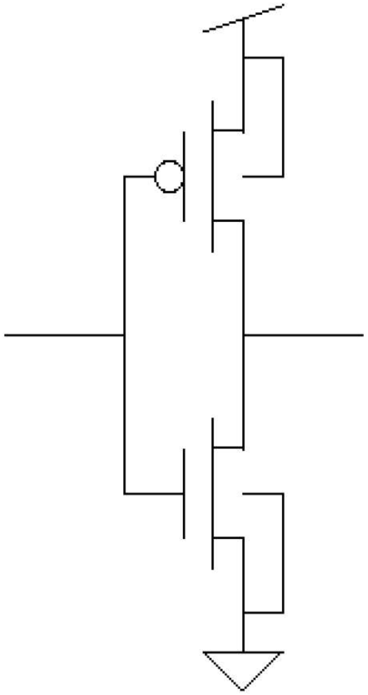
(a) SRAM cell CMOS circuit

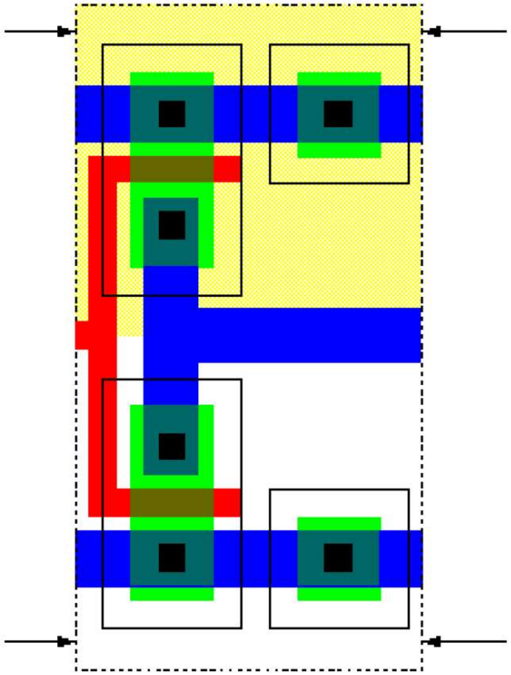
(b) SRAM cell voltage transfer curves

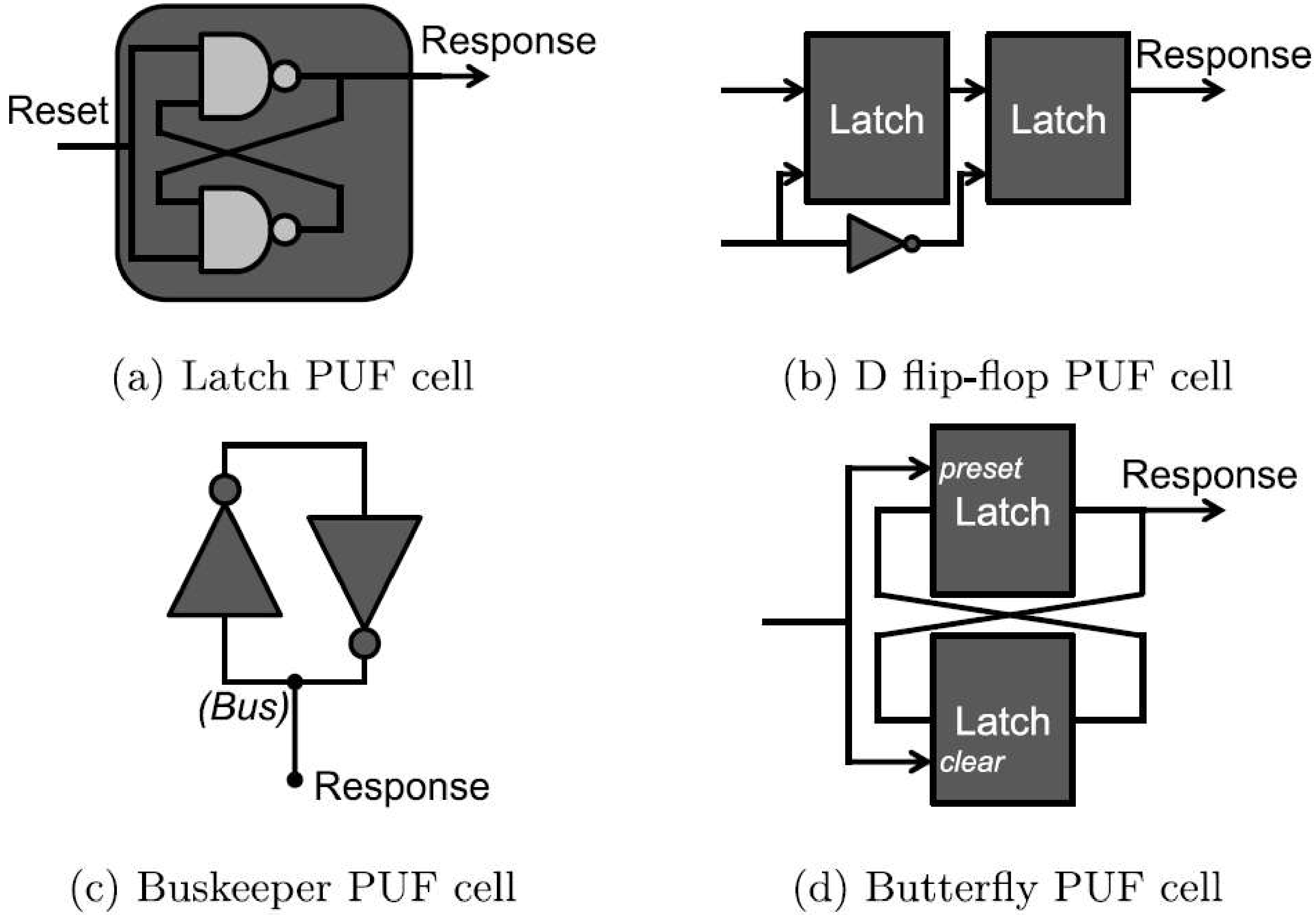
(c) SRAM cell logic circuit

(d) SRAM cell power-up transient analysis

Fig. 2.5 Construction and power-up behavior of an SRAM cell







(a) Latch PUF cell

(b) D flip-flop PUF cell

(c) Buskeeper PUF cell

(d) Butterfly PUF cell

Fig. 2.6 Different PUFs based on bistable memory elements

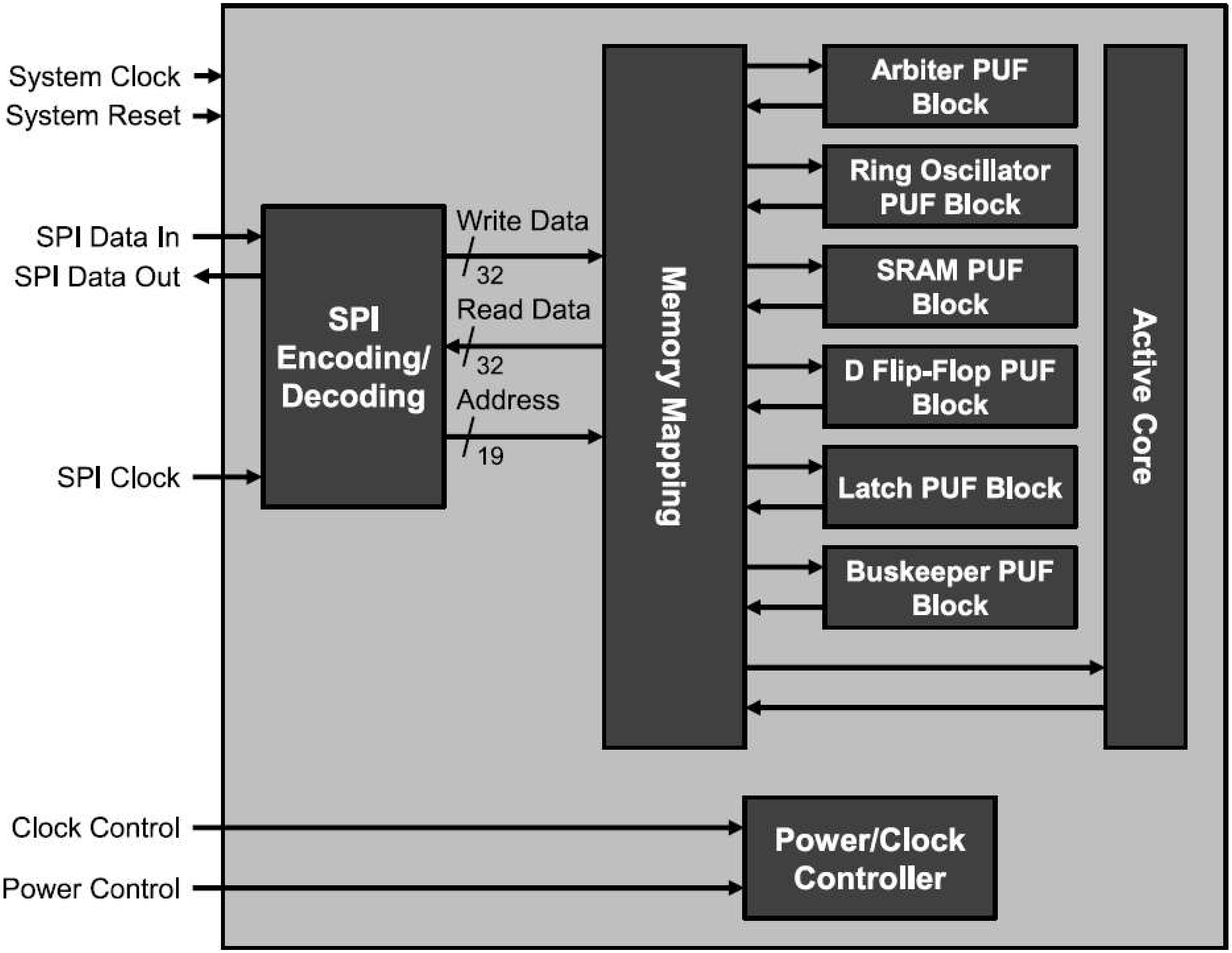
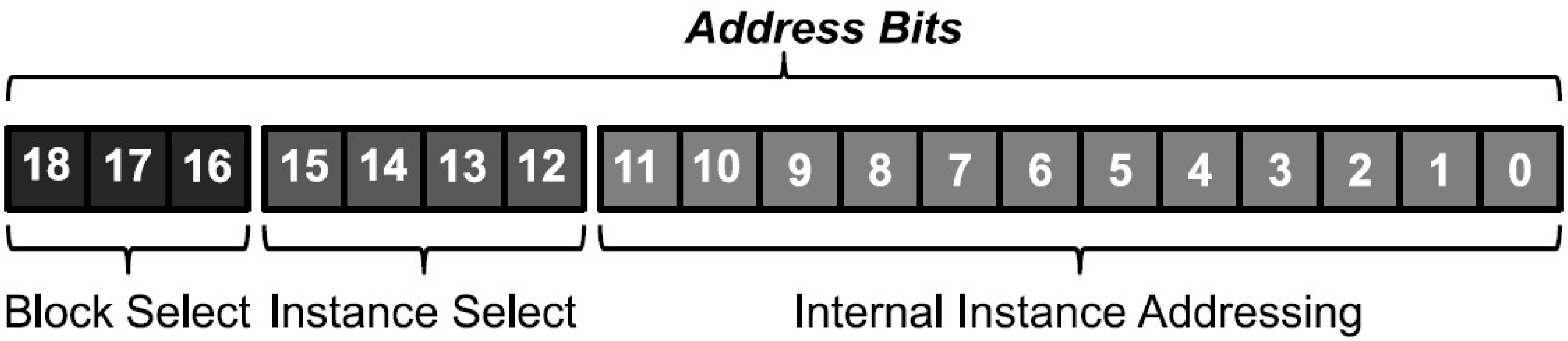


Fig. 4.1 Top-level block diagram of the test chip



Block Select	Block Name
0x0	Ring Oscillator PUF Block
0x1	Latch PUF Block
0x2	SRAM PUF Block
0x3	D Flip-flop PUF Block
0x4	Arbiter PUF Block
0x5	Buskeeper PUF Block
0x6	Active Core

Instance Select	Block Name
0x0 – 0x7	Select PUF Instance 0...7
0xF	Select PUF Controller

Fig. 4.2 Address structure of the internal memory map of the test chip

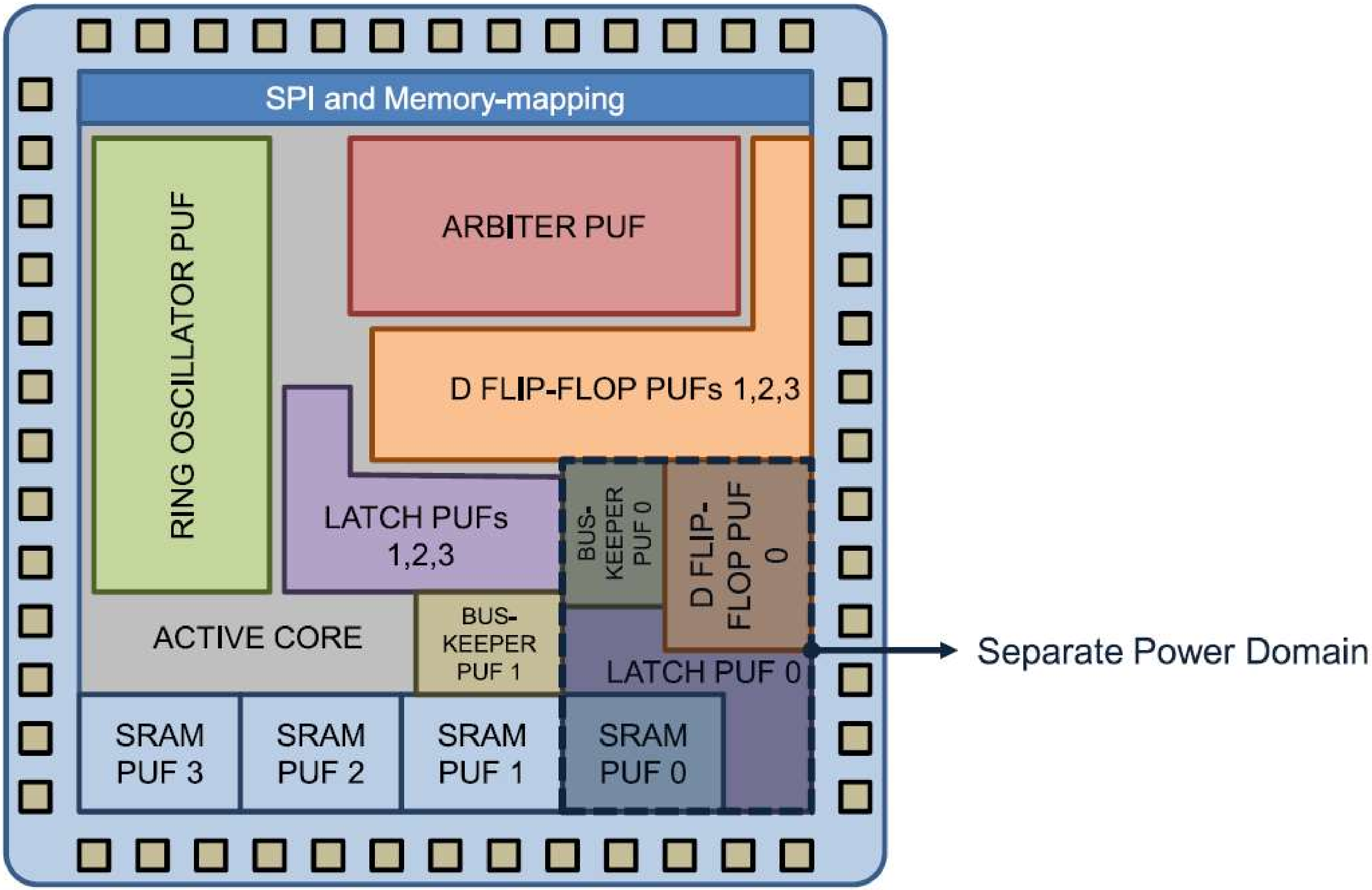


Fig. 4.3 Floor plan of the structures on the test chip

Table 4.1 Silicon area breakdown of the different test chip building blocks

Building block	Silicon area (mm^2)	Relative area (·/total logic)	Building block content
Ring Oscillator PUF	0.241	10.7 %	4096 ring oscillators + 16 × 32-bit counters + control
Latch PUF	0.272	9.5 %	4 × 8192 latches + 2 × multiplexer tree
SRAM PUF	0.213	12.1 %	4 × 64 kbit SRAM array
D Flip-Flop PUF	0.392	17.4 %	4 × 8192 D flip-flops + 2 × multiplexer tree
Arbiter PUF	0.279	12.4 %	256 × 64-bit arbiter PUF + control
Buskeeper PUF	0.076	3.4 %	2 × 8192 buskeeper cells + 2 × multiplexer tree
Active Core	0.353	15.7 %	32 × 128-bit substitution-permutation rounds
Additional Blocks	0.425	18.9 %	SPI interface, memory mapping, power control, ...
Total Logic Area	2.251	100.0 %	all of the above
Overhead	1.405	62.4 %	I/O pads, power/ground rings, empty space, ...
Complete Test Chip	3.656	162.4 %	1912 µm × 1912 µm silicon die

References

- Creative Commons, https://creativecommons.org/