哈爾濱工業大學（深圳）
Harbin Institute of Technology, Shenzhen

A Low-overhead PUF based on Parallel Scan Design

Presenter: Wenxuan Wang

Advisor: Aijiao Cui

Thursday, February 15, 2018

Outline

Outline

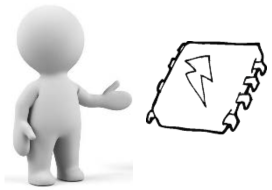
哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

Introduction

-*Security Issues*

Top five most counterfeited parts represent a $169 billion potential challenge for global semiconductor market.
(Cited from：https://technology.ihs.com/)

Economy loss



Affect enthusiasm

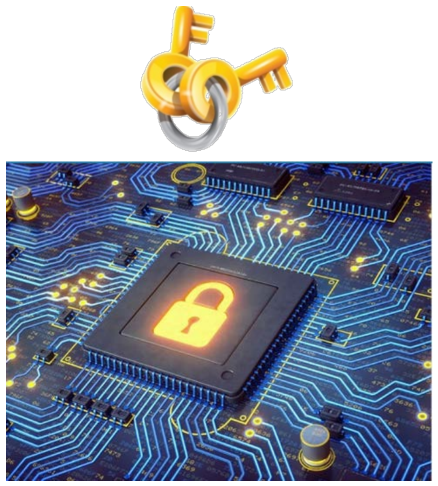
National security threat

How to protect the hardware IP?

Introduction

哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

-*Security Issues*



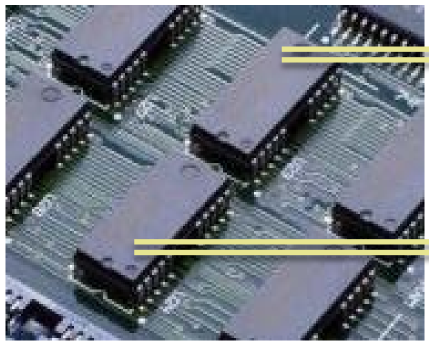
Micro-probing
Laser cutting
Side channel attacks
……

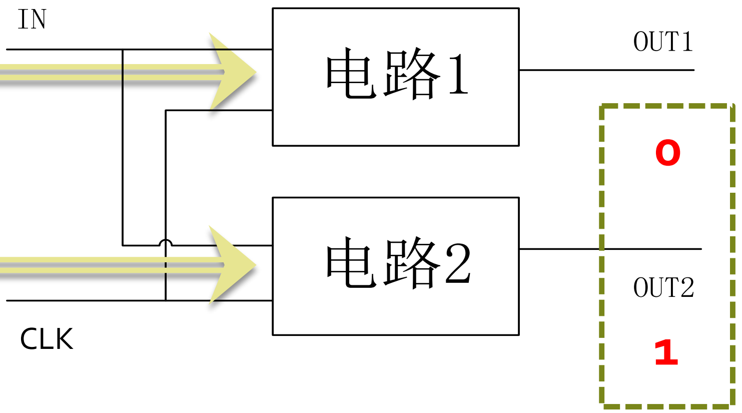
Get the key

How to generate and store the key in a more secure way?

Introduction

-Physical Unclonable Function





Physical Unclonable Function

PUFs transform the intrinsic random variations in device parameters (V_{th}, L_{eff}) to variations in circuit-level parameters.

Application:

- **IP Protection**
- **Key Generation**
- **System Certification**

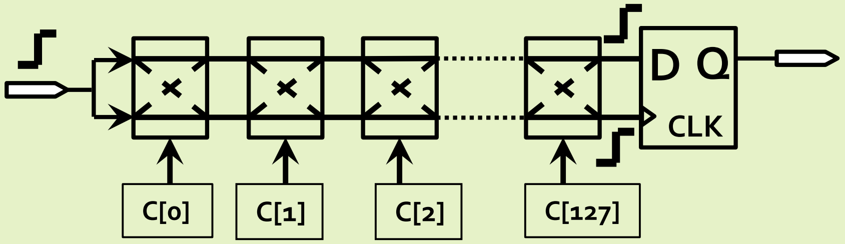
[1] Pappu R, Recht B, Taylor J, et al. Physical One-Way Functions[J]. Science, 2002, 297(5589): 2026-2030.

Introduction

-Physical Unclonable Function

Original Circuit

PUF Circuit



independent

ATTACK

Weakness:

- Easy to be found
- High area overhead

Outline

Literature Review of PUF

- The Classification of PUF

- **PUF:**

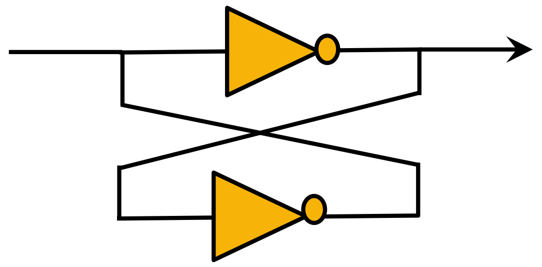
1. Memory-based PUF
   - SRAM PUF
   - Butterfly PUF
2. Delay-based PUF
   - Arbiter PUF
   - RO-PUF

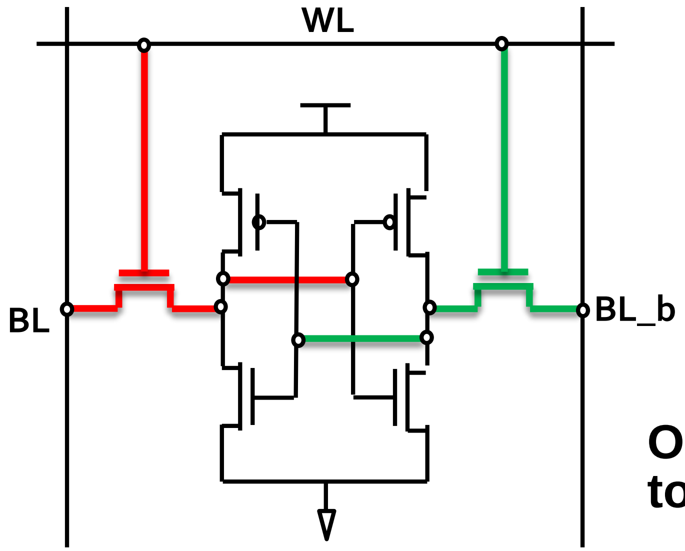
Literature Review of PUF

哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

-Memory-based PUF

SRAM PUF





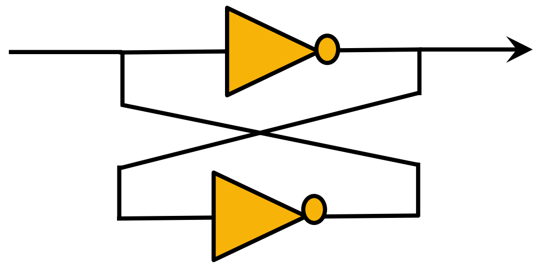
Output from '00' to '01' or '10'

[2] Hofer M, Boehm C. An Alternative to Error Correction for SRAM-Like PUFs[C]// ACM CHES - Workshop on Cryptographic Hardware and Embedded Systems, New York: ACM, 2010: 335-350.

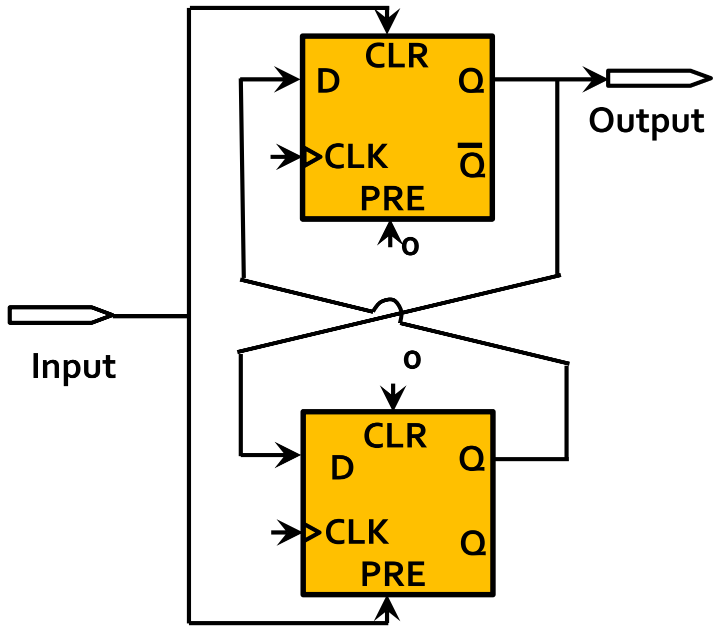
Literature Review of PUF

-Memory-based PUF

SRAM PUF



Butterfly PUF

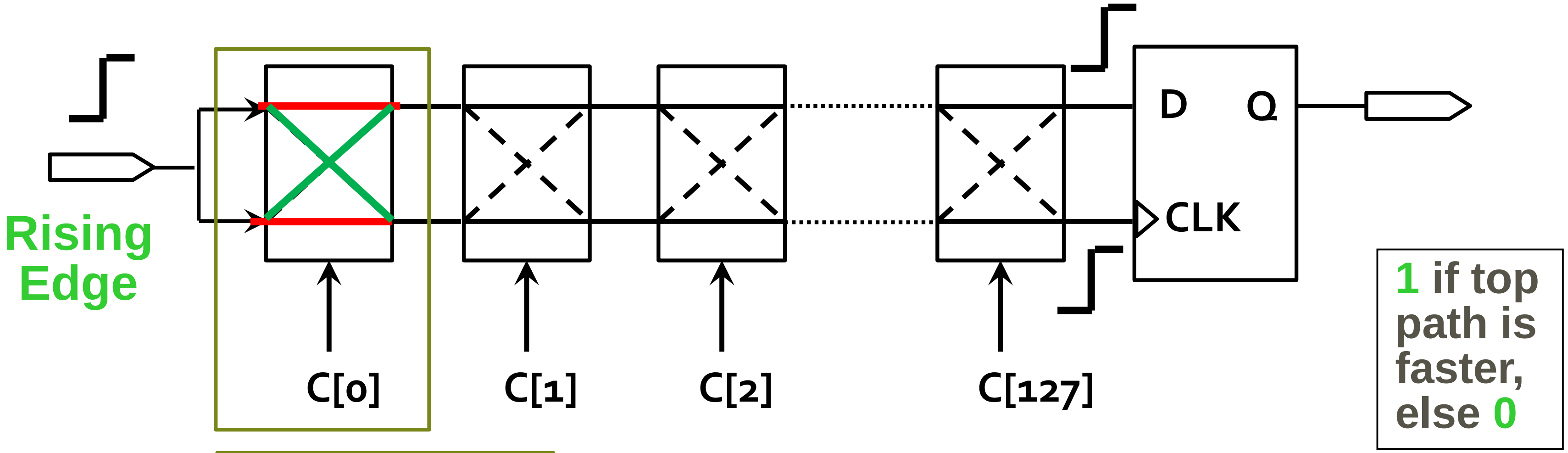


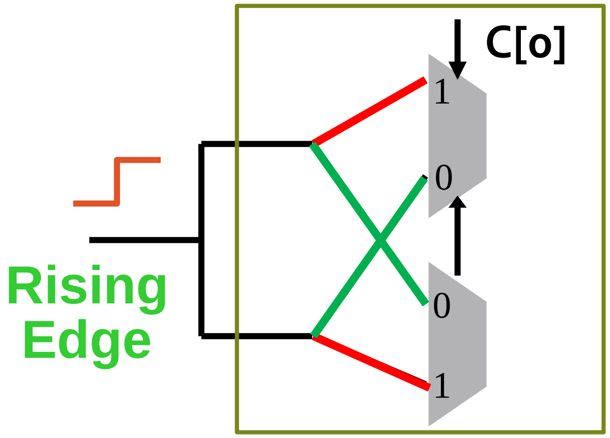
[3] Kumar, Sandeep S., et al. "Extended abstract: The butterfly PUF protecting IP on every FPGA." *IEEE International Workshop on Hardware-Oriented Security and Trust* IEEE Computer Society, 2008:67-70.

Literature Review of PUF

-Delay-based PUF

Arbiter PUF





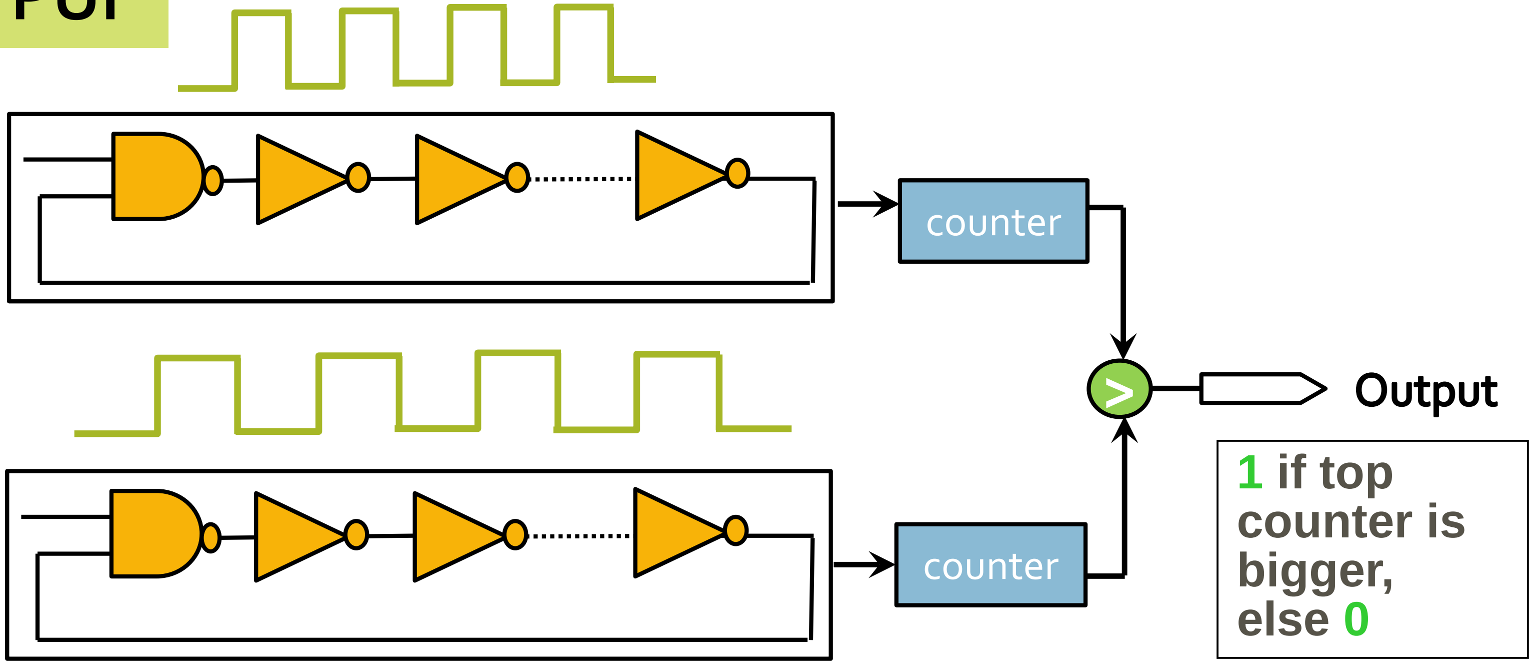
[4] Lee J W, Lim D, Gassend B, et al. A Technique to Build A Secret Key in Integrated Circuits for Identification and Authentication Applications[C]// VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on, Piscataway: IEEE, 2004: 176-179.

Literature Review of PUF

哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

-Delay-based PUF

RO PUF

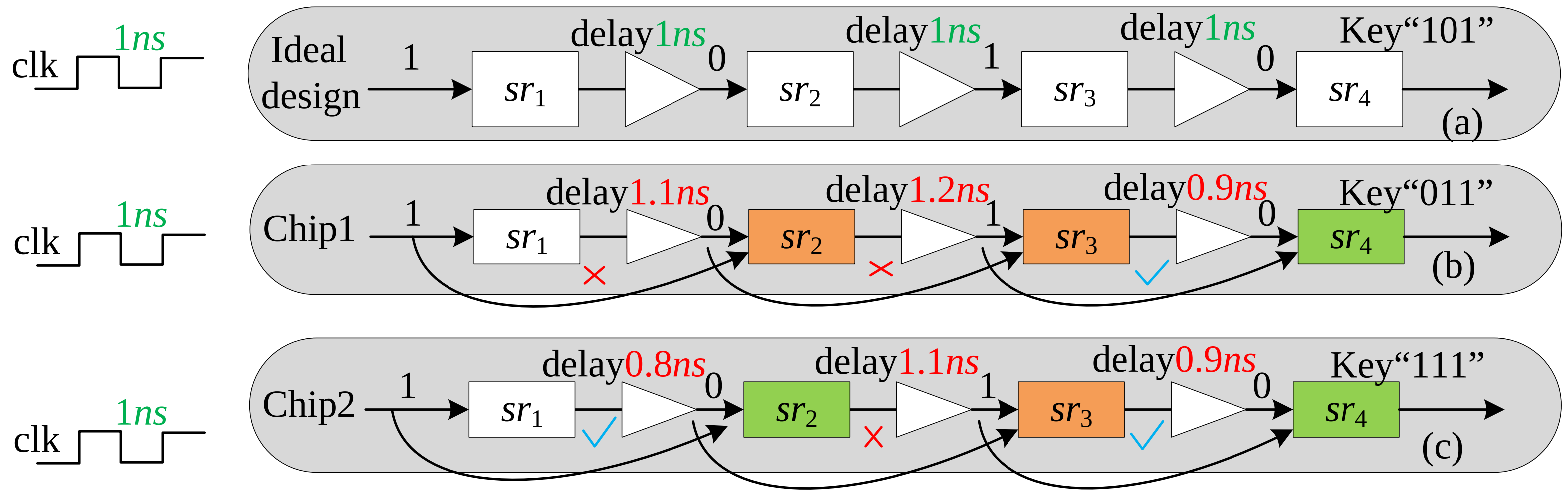


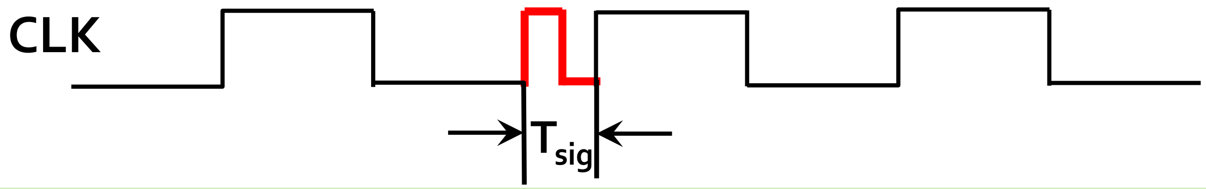
[5] Maiti A, Schaumont P. Improving The Quality of A Physical Unclonable Function Using Configurable Ring Oscillators[C]// International Conference on Field Programmable Logic and Applications, Piscataway: IEEE, 2009: 703-707.

Literature Review of PUF

哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

-Analysis of ScanPUF





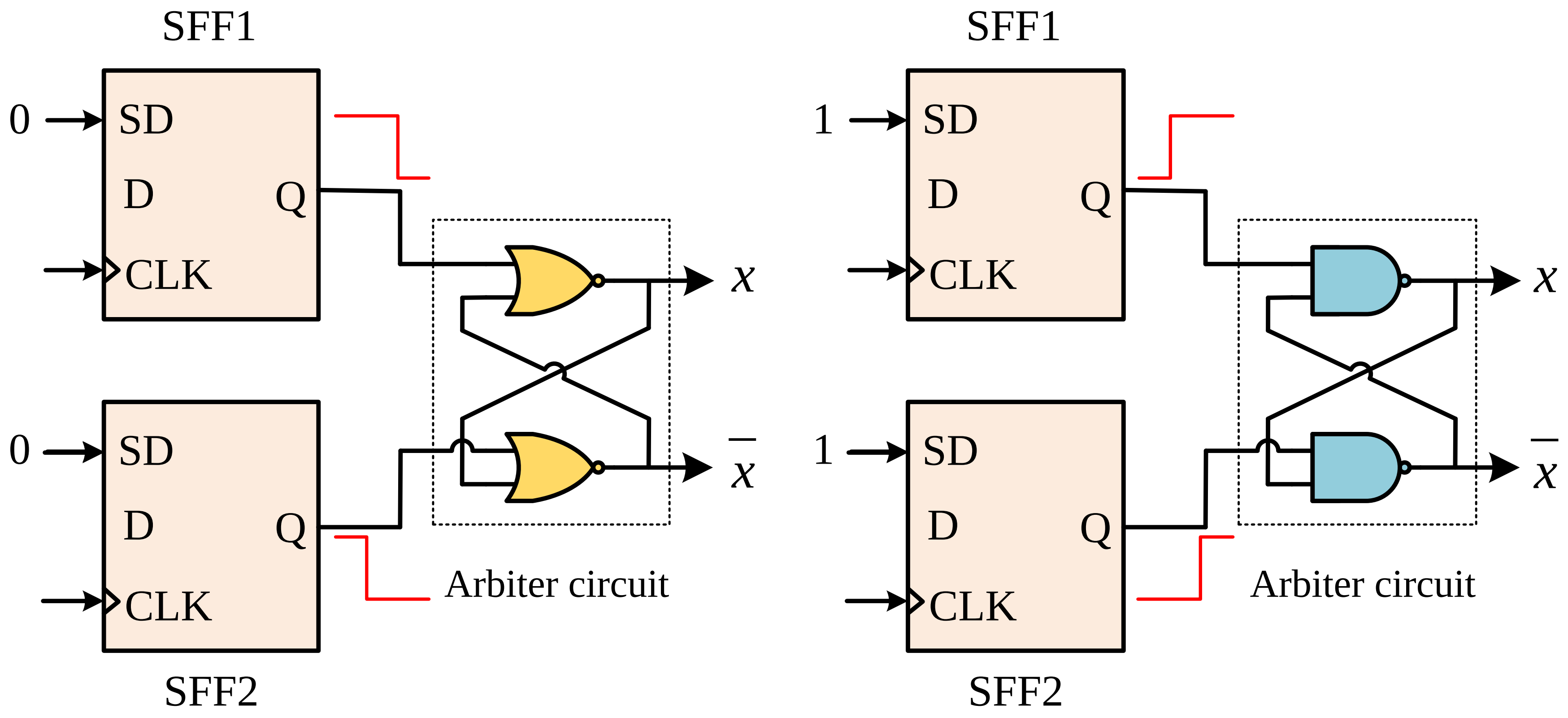
It is difficult to generate high frequency pulses.

[6] Zheng Y, Zhang F, Bhunia S. DScanPUF: A Delay-Based Physical Unclonable Function Built Into Scan Chain[J]. IEEE Transactions on Very Large Scale Integration Systems, 2016, 24(3): 1059-1070.

Outline

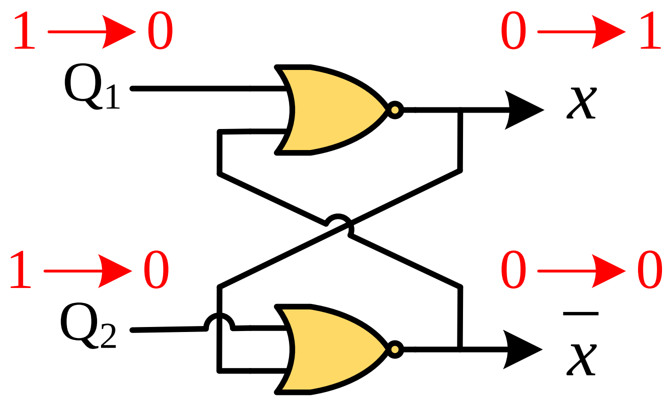
PUF Based on Parallel Scan

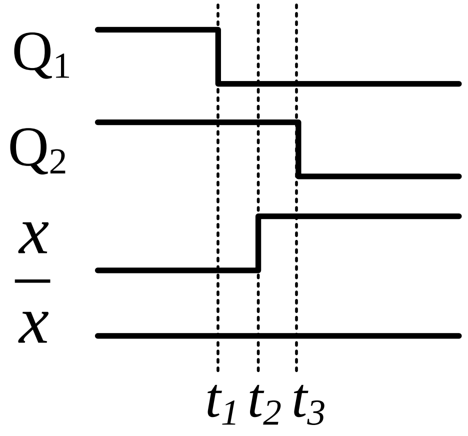
-The proposed PUF structure

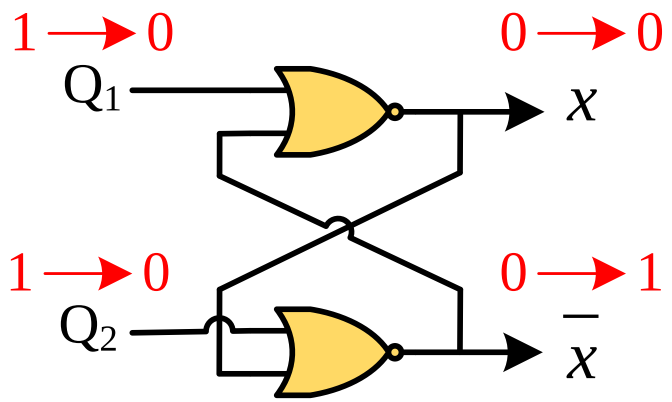


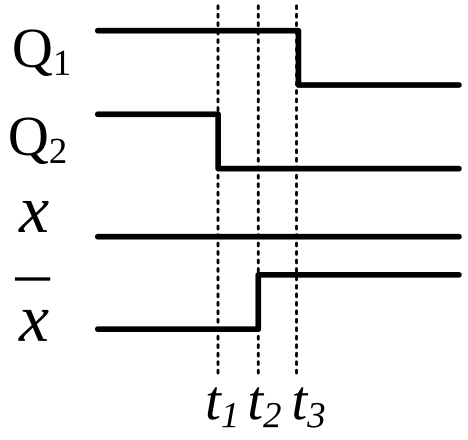
PUF Based on Parallel Scan

-NOR-type SR-latch Arbiter



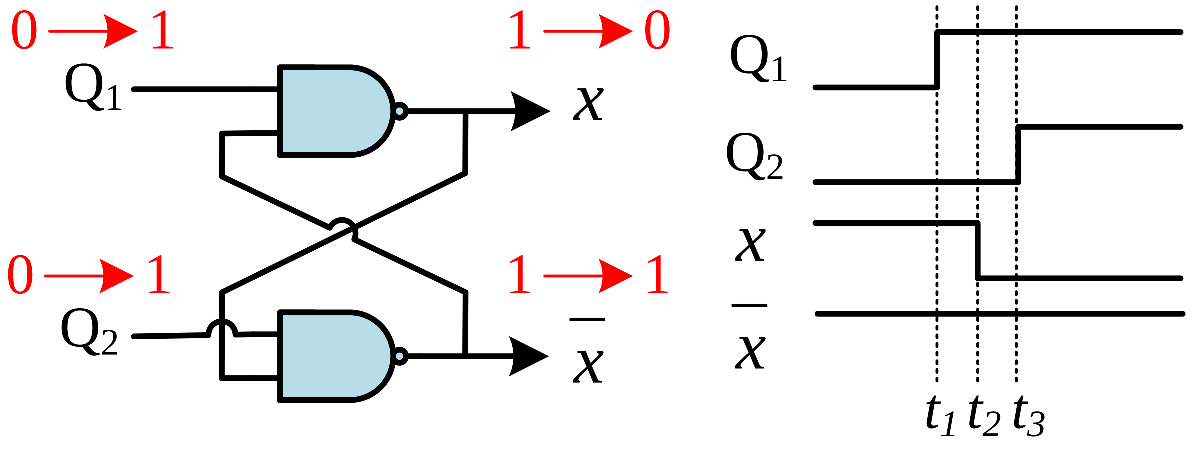


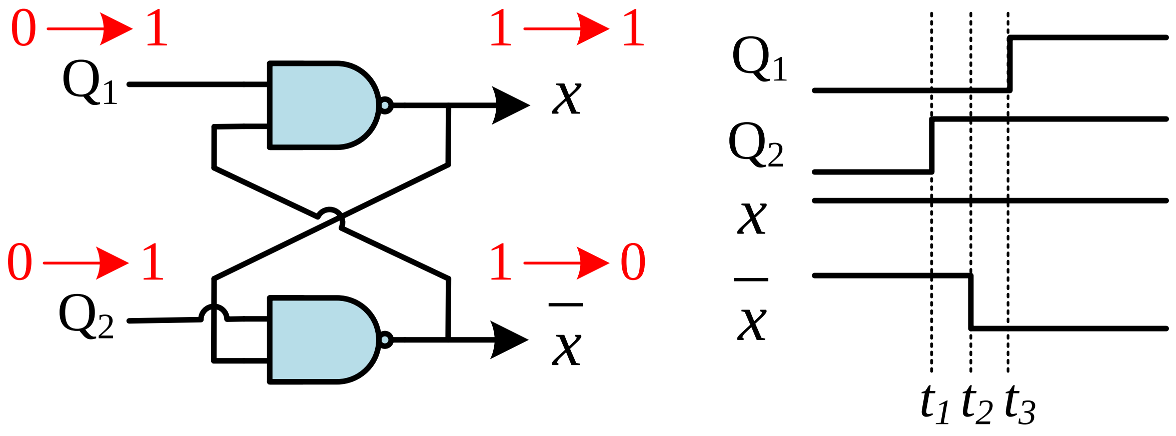




PUF Based on Parallel Scan

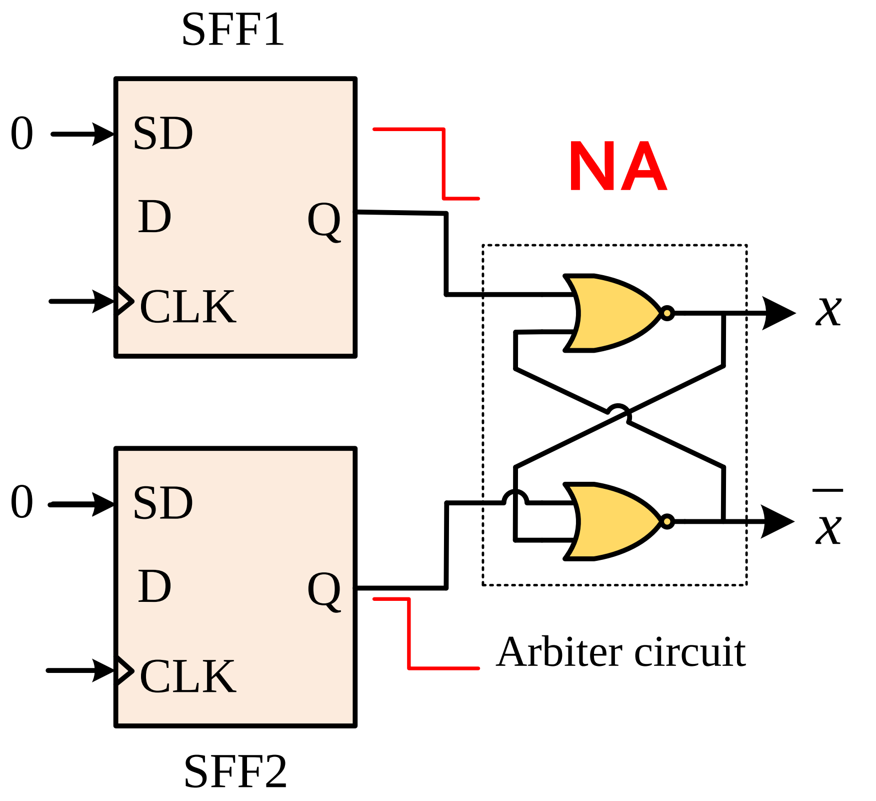
-NAND-type SR-latch Arbiter

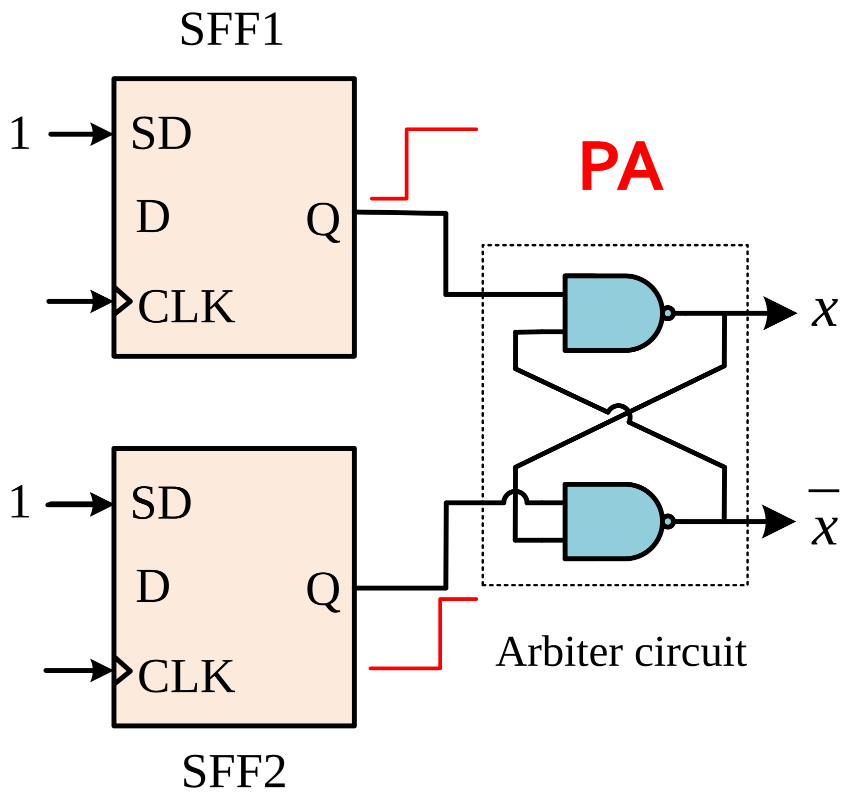




PUF Based on Parallel Scan

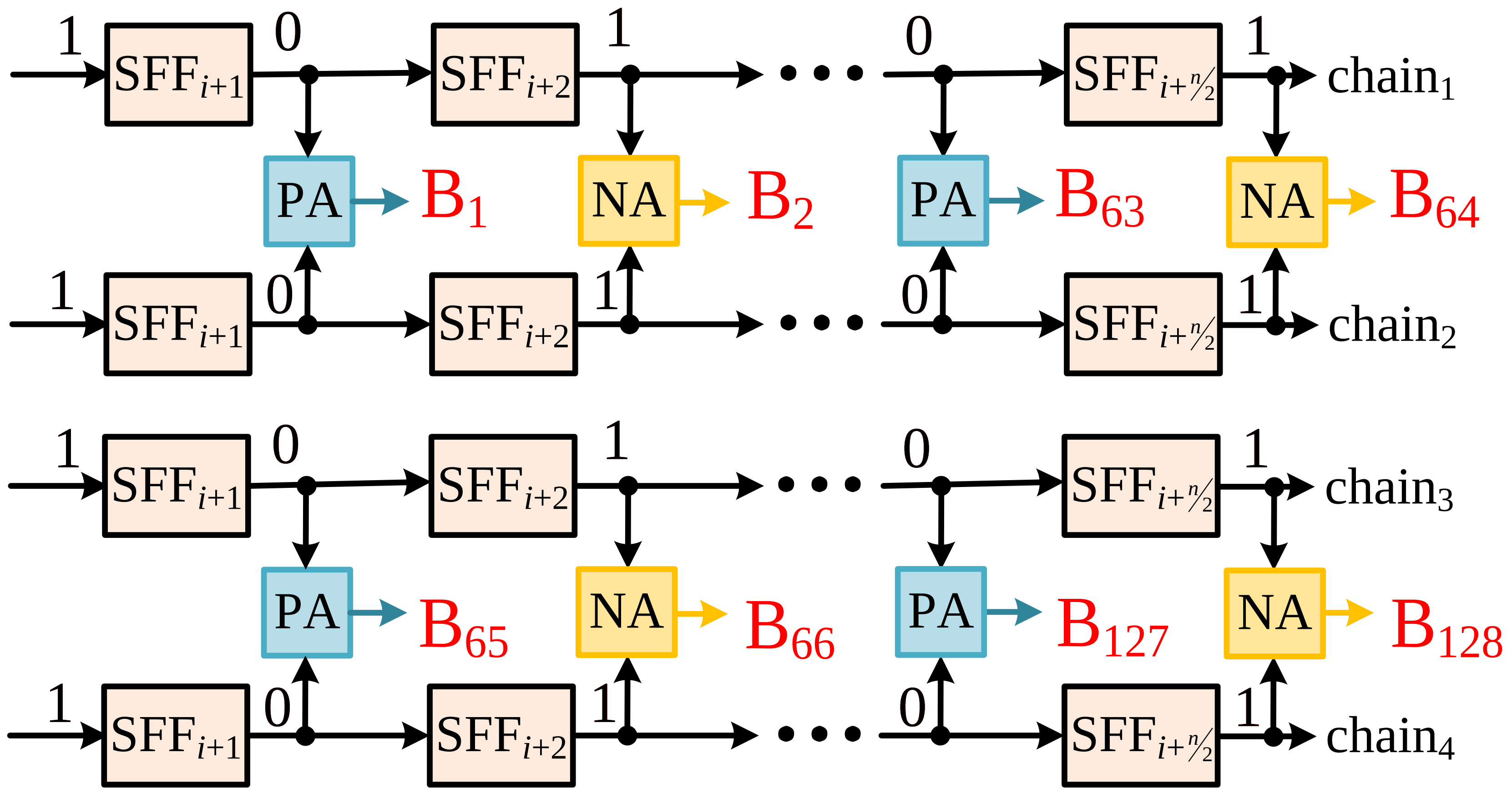
-The proposed PUF structure





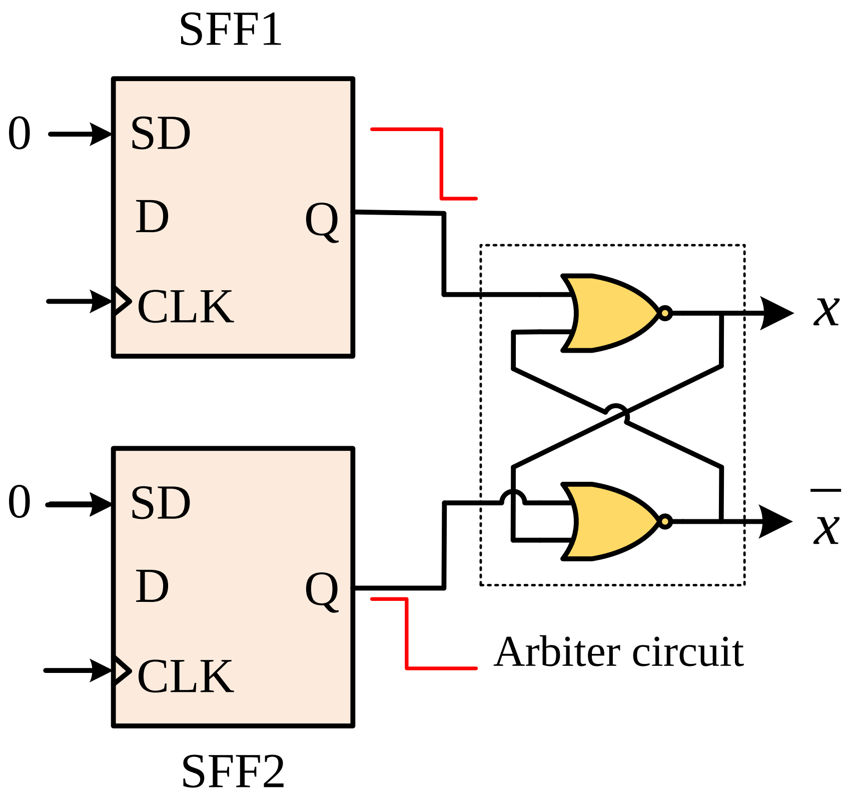
PUF Based on Parallel Scan

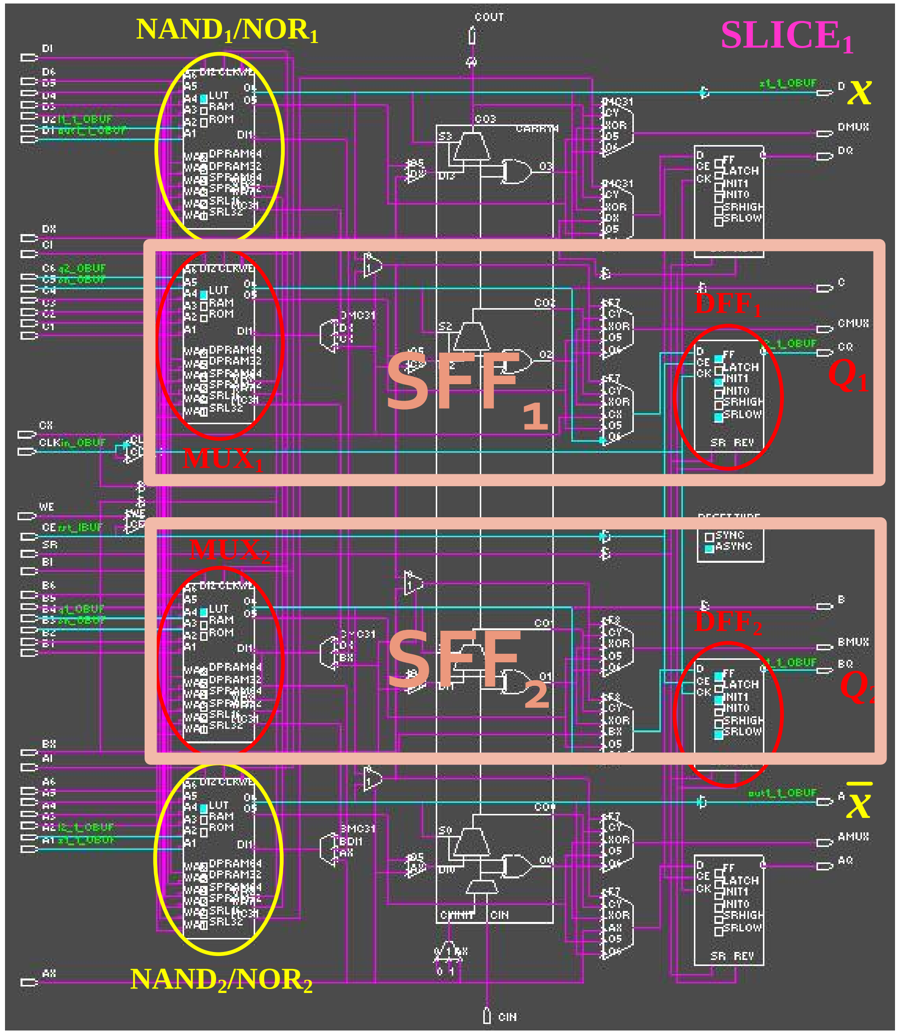
- The proposed PUF structure



PUF Based on Parallel Scan

-1 PUF bit design in FPGA

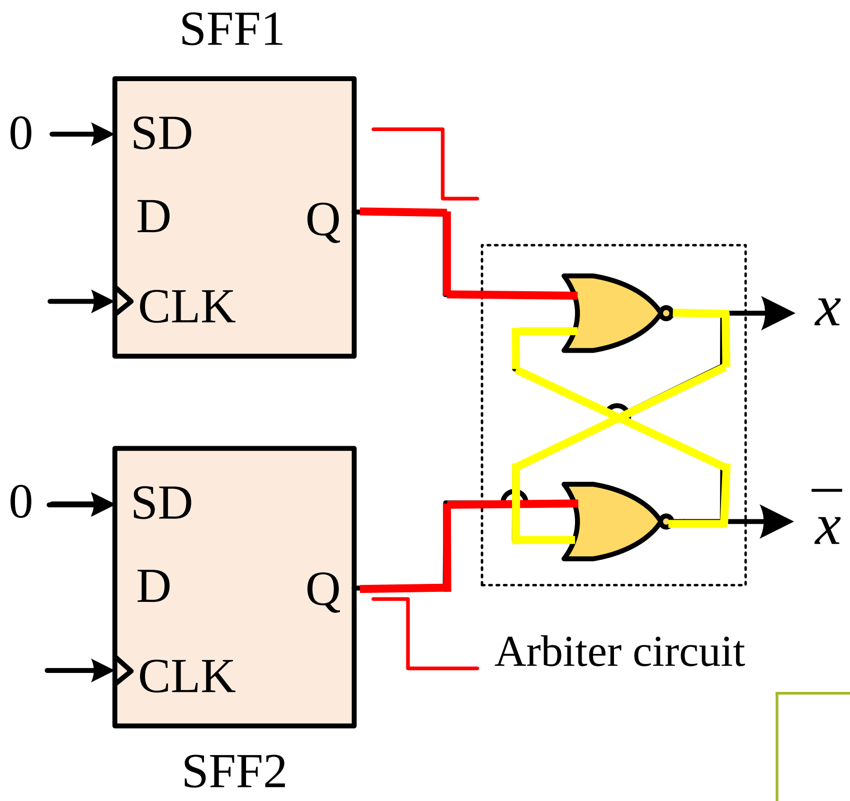


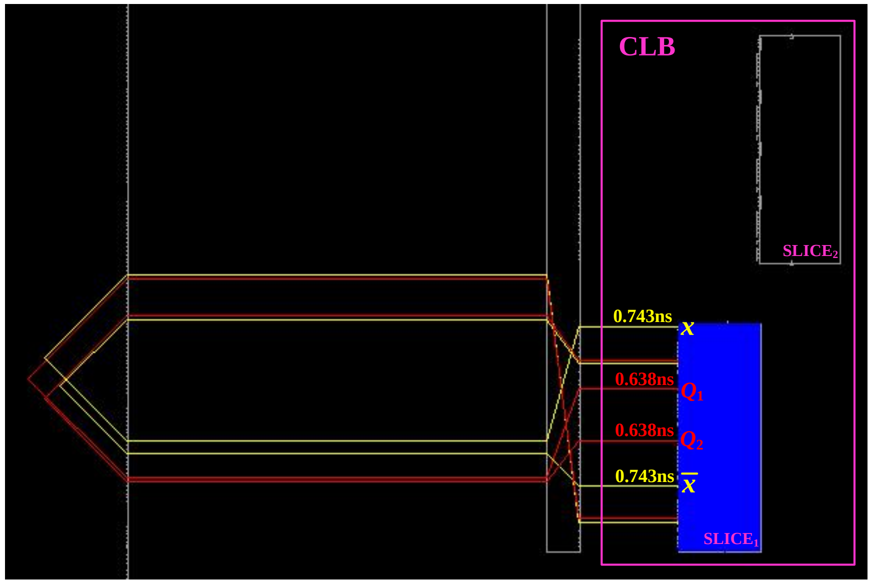


PUF Based on Parallel Scan

哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

-1 PUF bit design in FPGA





	Resource	Overhead
FPGA	256 LUTs	0.37

PUF Based on Parallel Scan

哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

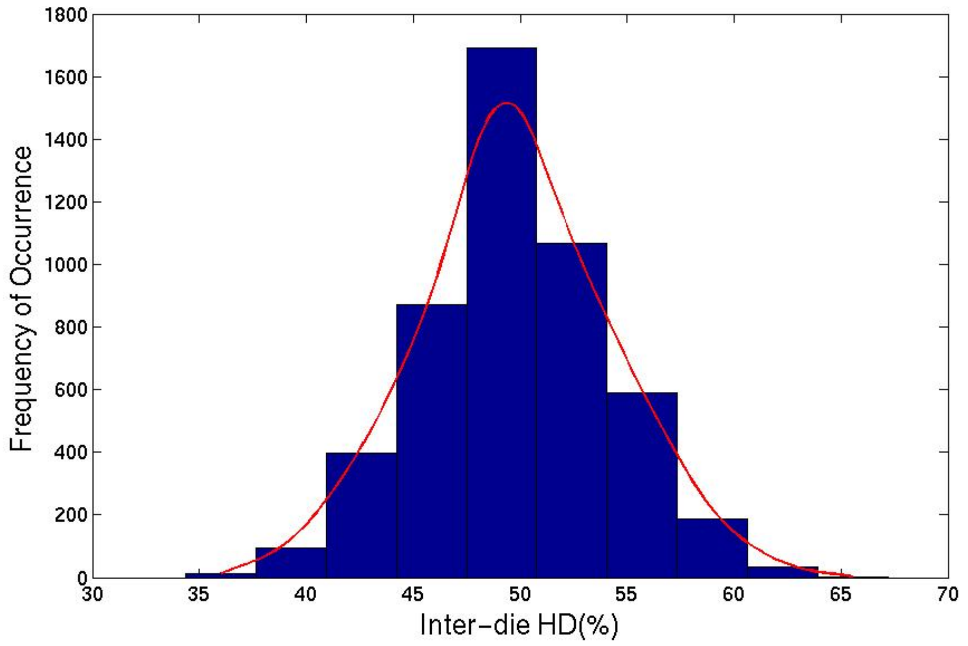
-Uniqueness Analysis

Uniqueness:

inter-die Hanming Distance(HD) of R_1 and R_2
Chip1:R_1=PUF(C_1)
Chip2:R_2=PUF(C_1)
Ideal value:50%

$$HD_{avg} = \frac{2}{m\cdot(m-1)}\sum_{i=1}^{m-1}\sum_{j=i+1}^{m} HD_{i,j} \times 100\%$$

HD_{avg} =49.86%
(forty responses from four FPGAs)



PUF Based on Parallel Scan

哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

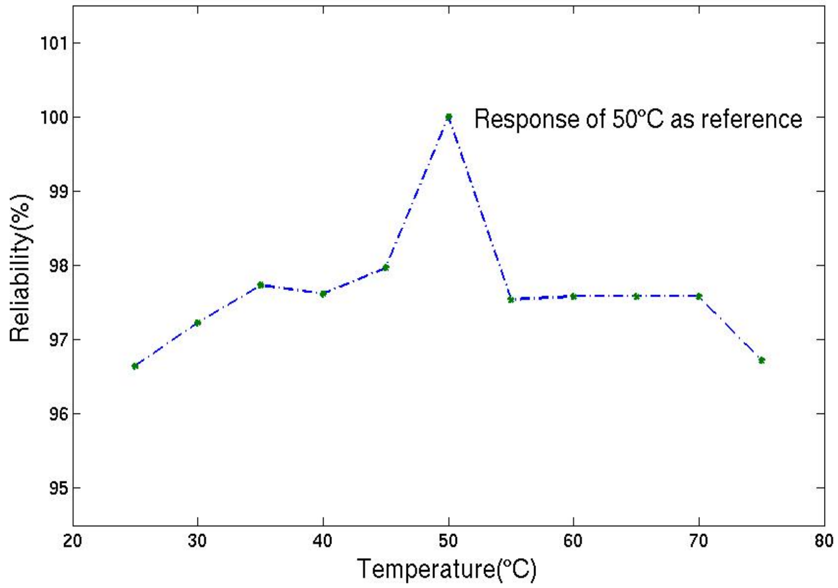
-Reliability for Temperature Variation

Reliability:
intra-die Hanming Distance(HD) of R_1 and R_2
Chip1:R_1=PUF(C_1)
Chip1:R_2=PUF(C_1)
Ideal value:100%

$$HD_{intra} = \frac{2}{m}\sum_{j=1}^{m}\frac{HD(R_i, R'_{i,j})}{n}\times 100\%$$

$$Reliability = 100\% - HD_{intra}$$

Reliability with temperature varying:
1. Worst: HD_{avg} >96%
(Temperature from 25℃to75℃)
2. HD_{avg}> 99%
(Temperature is 25℃, Voltage±0.002v)



PUF Based on Parallel Scan

哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

-*Reliability for Voltage Variation*

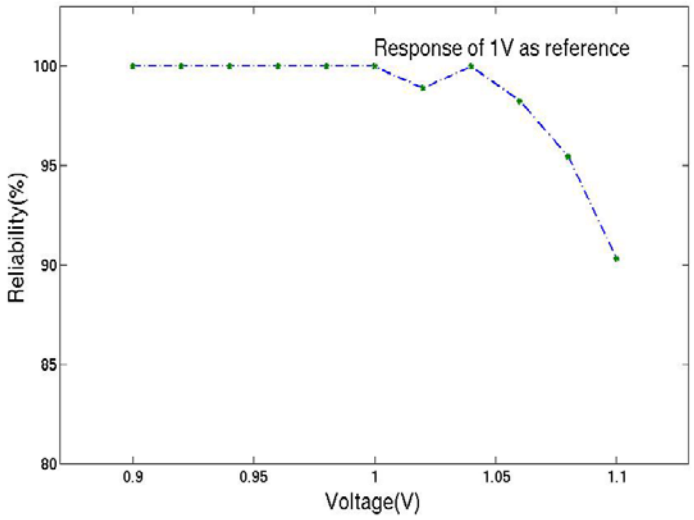
Reliability with voltage varying:

From 0.90v to 1.10v, step=0.05v

Monte-Calo analysis (PTM-65nm):

V_{thn}=agauss(0.423v,0.02,4)

V_{thp}=agauss(-0.365,0.02,4)



PUF Based on Parallel Scan

哈爾濱工業大學（深圳）
Harbin Institute of Technology (Shenzhen)

-Randomness Analysis (NIST)

	30°C	40°C	50°C	60°C	70°C
ApproximateEntropy	100%	100%	100%	100%	100%
BlockFrequency	97%	97%	98%	97%	97%
CumulativeSums	98%	98%	100%	98%	98%
FFT	100%	100%	99%	100%	98%
Frequency	97%	97%	98%	97%	97%
LongestRun	99%	99%	99%	98%	100%
Runs	100%	99%	100%	100%	98%
Serial	100%	100%	100%	99%	100%

Outline

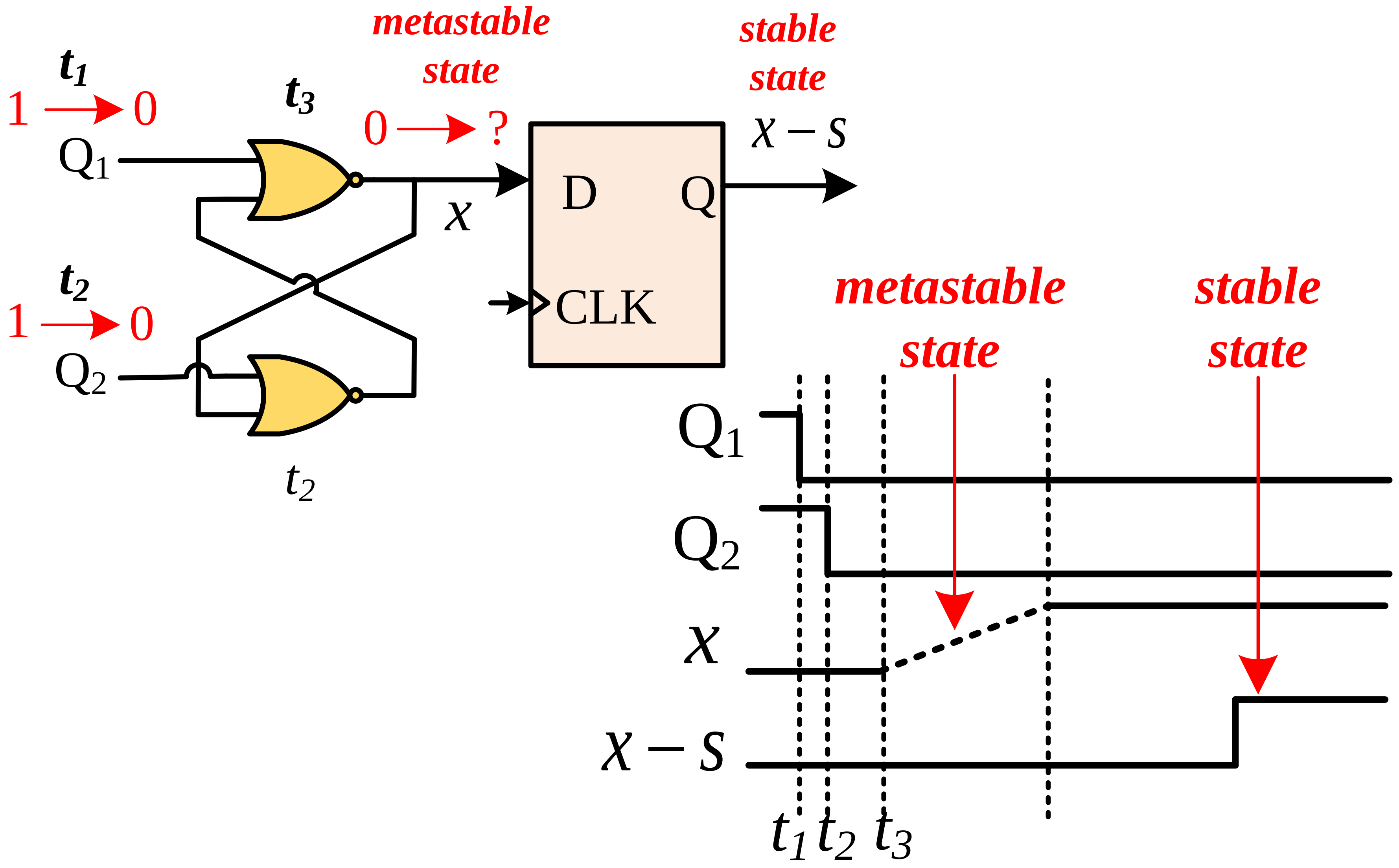
Conclusion and Future Work

- ➢ A Low-overhead PUF based on Parallel Scan Design
  - ✓ *-Ultra-low overhead*
  - ✓ *-PUF with good uniqueness and robustness*
  - ✓ *-Well integrated with original design*

- ➢ Future work
  - ✓ *-The application of PUF*
  - ✓ *-Improve PUF Reliability*

Thank you!

SR latch – metastable state


metastable state
stable state
t_1
$1 \rightarrow 0$
Q_1
t_3
$0 \rightarrow ?$
X
D
Q
CLK
$X-S$
t_2
$1 \rightarrow 0$
Q_2
t_2
metastable state
stable state
Q_1
Q_2
X
$X-S$
t_1 t_2 t_3