IEEE 13th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC-2019)
Nanyang Executive Centre, Nanyang Technological University, Singapore
October 1-4, 2019

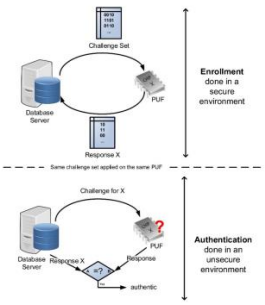
Enhanced ID Authentication Scheme Using FPGA-Based Ring Oscillator PUF

Van-Toan Tran, Quang-Kien Trinh, and Van-Phuc Hoang
Le Quy Don Technical University, Hanoi, Vietnam

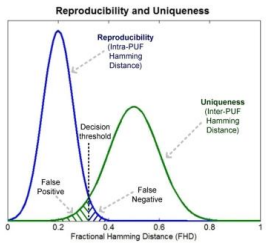
Contents

Introduction

- Physically Unclonable Functions (**PUFs**)



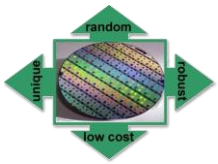
➡ *Diversity, Ambiguity*



Introduction

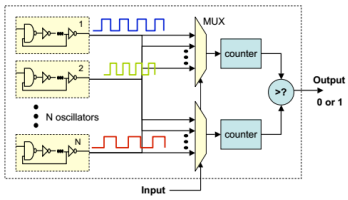
- FPGAs find sufficiently powerful for a majority of applications: flexibility, massive resources,…
- FPGA-based PUFs

"Silicon Biometric"



Introduction

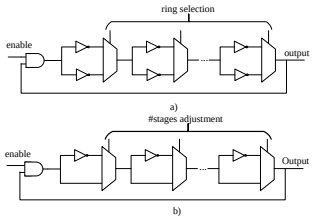
- FPGA-based RO PUFs



Suh, G. E., & Devadas, S. (2007, June). Physical unclonable functions for device authentication and secret key generation. In *Design Automation Conference, 2007. DAC'07. 44th ACM/IEEE*(pp. 9-14). IEEE.

Introduction

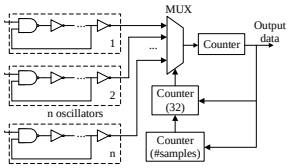
FPGA-based RO PUFs



Maiti, Abhranil, and Patrick Schaumont. "Improved ring oscillator PUF: An FPGA-friendly secure primitive." *Journal of cryptology*24.2 (2011): 375-397.

Gao, Mingze, Khai Lai, and Gang Qu. "A highly flexible ring oscillator PUF." *Proceedings of the 51st Annual Design Automation Conference*. ACM, 2014.

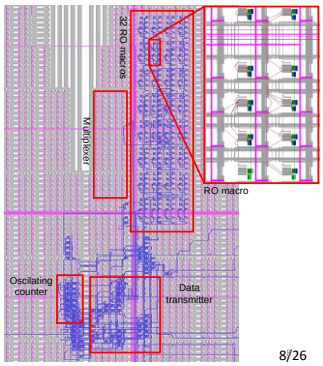
Implementation of FPGA-based RO PUFs



- Targeted for Xilinx Spartan 6 Series FPGA
- Delay element (inverter): One primitive LUT
- Basic RO: 2^N inverters + a NAND gate, manually routed by FPGA editor → FPGA hard macro
- RO macros are precisely placed

Implementation of FPGA-based RO PUFs

- 32 ROs × 16 inverter
- 5 ICs
- Evaluated by 1024 samples



Evaluation of the Designed ROs Frequency

Statistic model of RO frequencies

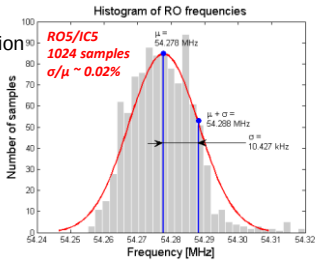
$$f_{RO} = f_{nominal} + \Delta f_{proc,local} + \Delta f_{proc,global} + \Delta f_{OP}$$

- Δf_{OP}: *Operating condition*
- $\Delta f_{proc,global}$: *Global process variation*
- $\Delta f_{proc,local}$: *Local process variation*
- $f_{nominal}$: *Measured for the nominal device under the nominal condition*

Evaluation of the Designed ROs Frequency

Impact of the Temporal Fluctuation

- Fluctuation ↔ Δf_{OP} variation under a fixed operating condition (25ºC, 1.0 V)
- **Reliability factor** $(1 - \sigma/\mu)$



R. Maes, *Physically Unclonable Functions*. Springer, 2013.

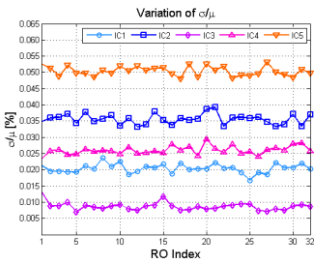
R. Maes. "Physically unclonable functions: Constructions, properties and applications." Katholieke Universiteit Leuven, Belgium (2012).

Evaluation of the Designed ROs Frequency

Impact of the Temporal Fluctuation

- 32 ROs × 5 ICs
- min σ/μ = 0.0069% (RO5/IC3)
- max σ/μ = 0.0532% (RO27/IC5)

→ *Reliability = 99.94% - 99.99%*

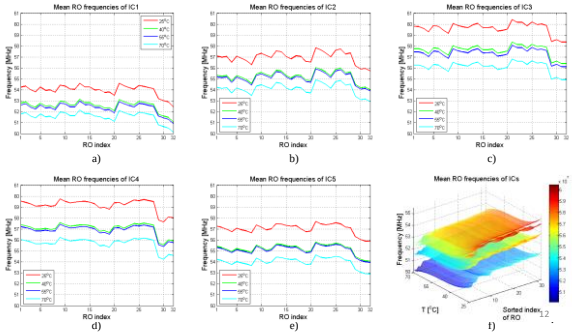


→ *The temporal fluctuation has little impacts on the ROs measured frequencies*

Evaluation of the Designed ROs Frequency

Impact of the Temperature

5 ICs × 32ROs × 256 samples (25ºC, 40ºC, 55ºC, 70ºC)

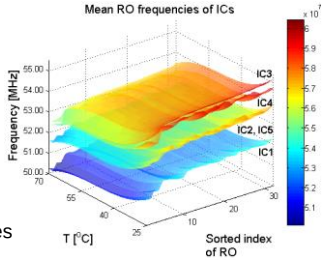


Evaluation of the Designed ROs Frequency

Impact of the Temperature

- RO indices are sorted by f_mean_IC3 → keep the 3D surface smooth
- The dependence on temperature is quite strong, follows a predicted pattern
- Increase temp. → Decrease RO frequencies

25ºC → 70ºC → shifting the mean frequencies of ROs by 2.34-3.59 MHz



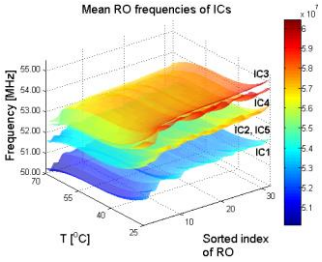
Evaluation of the Designed ROs Frequency

Impact of the Temperature

- ROs frequencies do not necessary to be linear

40 → 55ºC leads to decrease only 0.09-0.29 MHz

- *Absolute frequencies values are not suited for unique ID extraction*



N. Weste, and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective (4th ed.)*. Addison-Wesley Publishing Company, USA, 2010

Evaluation of the Designed ROs Frequency

Impacts of the Global And Local Process Variations

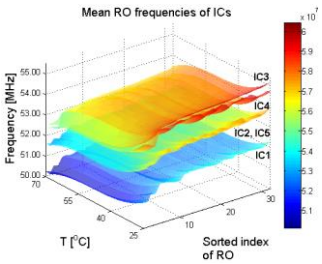
Global variation

- RO frequency vary significantly from die-to-die

RO5 at 25ºC: Up to 5.61 MHz from IC1 to IC3

- Zig-zag shapes shift up/down from temp.-to-temp.

→ *Weak uniqueness*



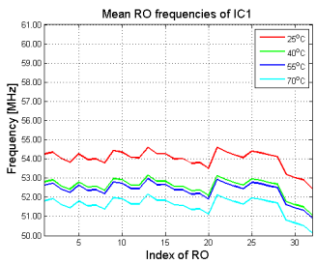
Evaluation of the Designed ROs Frequency

Impacts of the Global And Local Process Variations

Local variation

- Cases of RO frequencies being close are quite common
- IC1 in 25ºC:

RO indices	P
14-15	0.91
1-5	0.55
8-18	1
23-27	1
21-13	1

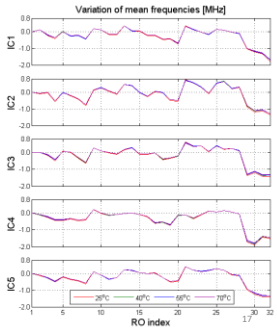


Evaluation of the Designed ROs Frequency

Impacts of the Global And Local Process Variations

Local variation

- Local differences are typically small (17 Hz to 65.27 kHz)
- *Pattern of local variation is very stable with respect to the temperature*



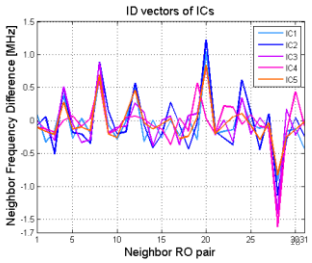
IC Identification Extraction and Authentication Scheme

Conventional ID Extraction Scheme

$$ID = F(\{\Delta f_{ij}\})$$

$\Delta f_{ij} = f_i - f_j$ - local variations

- Neighbor pairwise: $F \leftrightarrow$ sign function
- Strong correlation between the local variations/response bits



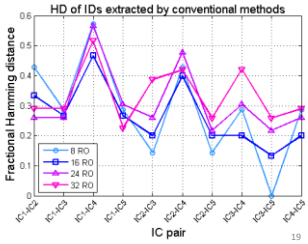
IC Identification Extraction and Authentication Scheme

Conventional ID Extraction Scheme

$$ID = F(\{\Delta f_{ij}\})$$

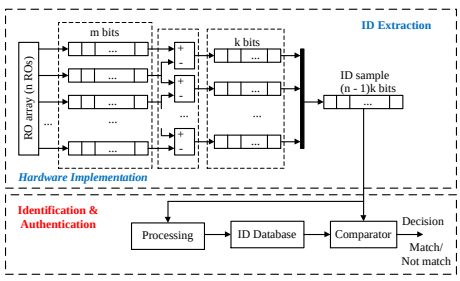
$\Delta f_{ij} = f_i - f_j$ - local variations

- Neighbor pairwise: $F \leftrightarrow$ sign function
- Strong correlation between the local variations/response bits



IC Identification Extraction and Authentication Scheme

Proposed ID Extraction Scheme



S. Eiroa and I. Baturone, "Circuit authentication based on Ring-Oscillator PUFs," 2011 *18th IEEE International Conference on Electronics, Circuits, and Systems*, Beirut, 2011, pp. 691-694.

IC Identification Extraction and Authentication Scheme

Proposed ID Extraction Scheme

- ID: $\boldsymbol{R}(\{\delta_i | i = \overline{1, n-1}\})$

$\delta_i = f_{i+1} - f_i$ k-bit value in 2's complement format

- Euclidean distance: $d(\boldsymbol{R_i}, \boldsymbol{R_j}) = \sqrt{\sum_{k=1}^{n-1} (\delta_{ik} - \delta_{jk})^2}$
- Normalized intra-distance: $d_{intra} = \frac{d(\boldsymbol{R_l}, \boldsymbol{R})}{2^k \sqrt{n-1}}$

$\boldsymbol{R_l}$ - ID of *l-th* measurement

$\boldsymbol{R}$ - The nominal magnitude of the ID vector, calculated from large samples ID

IC Identification Extraction and Authentication Scheme

Proposed ID Extraction Scheme

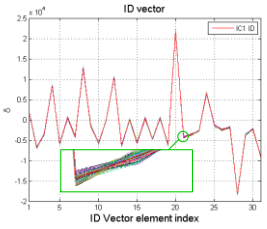
- Expect: $d_{intra} \approx 0$
- Inter-distance:

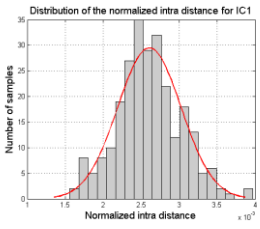
$$d_{inter} = 1 - \sum_{i,j} \frac{2d(\boldsymbol{R_i}, \boldsymbol{R_j})}{N(N-1)2^k \sqrt{n-1}}$$

IC Identification Extraction and Authentication Scheme

The ID Stability

ID for IC1, 256 measurements





- IDs of IC1 retain mostly the same from sample to sample

max norm. distance: 4×10^{-3} max std. dev. of the norm. intra-distance: $\sigma_{d_{intra}} = 4.2 \times 10^{-4}$

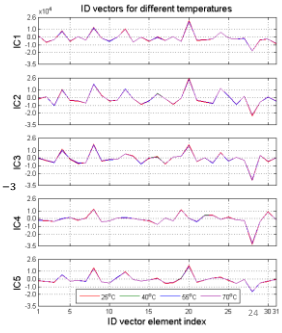
IC Identification Extraction and Authentication Scheme

The ID Stability

- ID for 5 ICs at 25°C, 40°C, 55°C, and 70°C
- Threshold of the ID authentication process

$d_{threshold} = 6\sigma_{d_{intra}}$

$d_{threshold} = 28.8 \times 10^{-3}$, $\sigma_{d_{intra}} = 4.8 \times 10^{-3}$



IC Identification Extraction and Authentication Scheme

The ID Uniqueness

- Normalized distance between the IDs:

IC2	IC3	IC4	IC5	
141×10^{-3}	146.4×10^{-3}	224.7×10^{-3}	$\mathbf{100.5\times10^{-3}}$	IC1
	154.4×10^{-3}	249.2×10^{-3}	140.2×10^{-3}	IC2
		194.5×10^{-3}	128.3×10^{-3}	IC3
			181.2×10^{-3}	IC4

- Minimum distance is 100.5×10^{-3} (IC1 - IC5)

→ ~4.5/ ~3.5 times greater than the thresholds when the authentication is conducted at the same temperature/when there is no restriction in operating temperature

Conclusions

- Systematically studied the impact of variations on RO PUFs
- Proposed an ID extraction and authentication scheme using FPGA-based RO PUF
- The experimental results show a very good level of reliability
- The circuit designs for both ROs array and ID extraction are kept simple and generic, thus, can be readily ported to other FPGAs with minimum modifications.

Conclusions

Thank you for your attention