A Highly Reliable XNOR-XOR-RO PUF Design for IoT Security Applications

Jian-Jie Chen
Dept. of Electrical Engineering, National Sun Yat-Sen University,
Kaohsiung, Taiwan 80424

Ralph Gerard B. Sangalang
Dept. of Electrical Engineering, National Sun Yat-Sen University,
Kaohsiung, Taiwan 80424
Dept. of Electronics Engineering, Batangas State University– The National Engineering University,
Philippines 4200

Hsin-Che Wu
Dept. of Electrical Engineering, National Sun Yat-Sen University,
Kaohsiung, Taiwan 80424

Chua-Chin Wang*
Dept. of Electrical Engineering, National Sun Yat-Sen University,
Kaohsiung, Taiwan 80424

2024 IEEE 14th Symposium on Computer Applications &amp; Industrial Electronics (ISCAIE) | 979-8-3503-4879-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISCAIE61308.2024.10576561

***Abstract*—PUFs or Physical Unclonable Function is now an emerging trend for hardware and IoT (internet-of-things) security solutions. IoT solutions always have a poor security features and are vulnerable to external attacks. Hence, a highly reliable security solution is important for their implementation. This work presents a highly reliable physical unclonable function implemented in an FPGA for use in IoT security. The proposed PUF is implemented in Xilinx ZYNQ 7000 FPGA board and operates at 100 MHz. A novel XNX (XNOR-XOR) Ring Oscillator (RO) PUF with configurable frequency is presented in this report. A statistical measure is used to report the experiments done in the design. The proposed design gives a highly reliable output of 99.86%, uniqueness of 49.90%, and a uniformity of 67.30%. The proposed design offered the most reliable design compared to previous works.**

***Index Terms*—IoT security, physical unclonable functions, reliability, uniqueness, XNOR gate, FPGA**

I. Introduction

Internet of Things (IoT), which connects billions of objects in a dynamic ecosystem, is changing our world in an important way. However, because of the inherent vulnerabilities brought about by this interconnectedness, strong security solutions that are customized for the resource-constrained nature of these devices are required. Security threats poses a great challenge to these kinds of applications. Non-volatile memories like ROMs (read-only memory) are traditionally used as storage for authentication keys [1]. This type of authentication method is quite an expensive solution in terms of power and design area. It is also prone to invasive and non-invasive attacks. Several threats to IoT systems are as follows:

- Insecure Environments
- Limited Security Planning in Development Methodologies
- Limited Management Support
- Lack of Defined Standards
- Difficulties Recruiting and Retaining Skills
- The Low Price Point Increases the Potential Adversary Pool

The shortcomings of traditional cryptography techniques frequently call for creative substitutes. Physical unclonable functions (PUFs) are novel that integrates security into the hardware itself. These are also other cheap solutions without the use of expensive hardware and can easily be integrated with IoT systems.

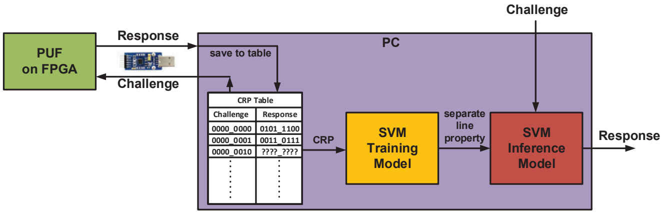


Fig. 1. PUF integrated with machine learning

PUFs take advantage of the small physical irregularities and intrinsic manufacturing variances present in integrated circuits (ICs) [2], [3]. These small variations result in unforeseen output reactions when an input stimulus is presented, giving each device a really unique identity known as an "unclonable fingerprint." This intrinsic distinctiveness outperforms software-based solutions vulnerable to reverse engineering and duplication, providing an unwavering basis for improved IoT security.

PUFs' incorporation into IoT security opens up an array of possible applications. Authentication protocols can use PUF-driven keys to build trust across various platforms and devices, preventing harmful impersonation and illegal access. Using PUFs' unclonable characteristics, secure key generation and storage can be accomplished without risky software-based key repositories. Moreover, PUFs can be used to fight counterfeiting by offering a nearly unforgeable hardware-based fingerprint, strengthening supply chain integrity and preventing the growing threat of hardware imitations.

PUFs can also be integrated with machine learning algorithm to further increase the strength of its security. Fig. 1 shows a PUF that is integrated with a support vector machine (SVM) to generate a stronger security code.

A. Contributions of this paper

This paper presents a novel ring oscillator PUF architecture. The new architecture is based on the combination of XOR and XNOR gates to which the frequency of oscillation can be controlled by an external input. The new architecture is simulated and implemented using an FPGA to prove its functionality and performance.

*Correspondence: Prof. Chua-Chin Wang. Prof. Wang is also with Institute of Undersea Technology (IUT), National Sun Yat-Sen University, Taiwan and an adjunct professor of Vel Tech, India. (ccwang@ee.nsysu.edu.tw)

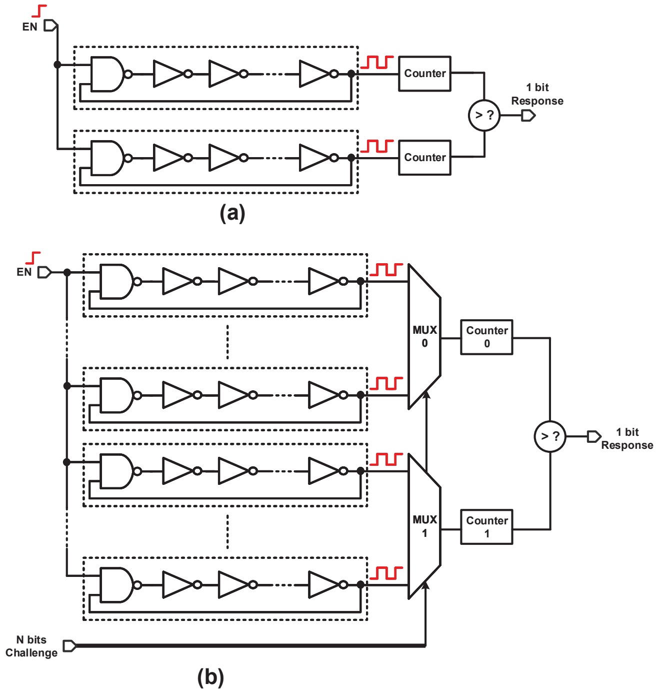


Fig. 2. Conventional RO PUF: (a) No challenge code; (b) With N-bit challenge [4]

B. Organization of this paper

The rest of this paper is organized as follows: Section II discusses the concept of a ring oscillator (RO) PUF while Section III details the proposed PUF design based on XNOR-XOR RO. Results of the experiments and implementation are discussed in Section IV and the report is concluded in Section V.

II. The Ring Oscillator PUF

A simplified 1-bit ring oscillator (RO) PUF as shown in Fig. 2(a) is used as an example, which is composed of two ROs that serves as the clock signal for two counters and an arbiter in the output of the counter usually in a form of an XOR gate. Though the ROs have the exact number of odd inverter stages, the frequency output still varies dues to the process variations of each devices. Suh *et al.* included a multiplexer in between the ROs and the counter to accommodate more ROs creating more unique frequencies, as shown in Fig. 2(b) [4]. The select signals of these multiplexers accepts the challenge code for the PUF. Once the challenge code is received, the counters are turned on at a fixed period, then the counting results are sent to the arbiter to compare of which the output has a higher value.

A PUF based on the feedforward RO is proposed in [5]. Fig. 3 shows an example of a 5-stage feedforward RO. The frequency is higher compared to the conventional RO PUFs and mainly depends on the feedforward strength [6]. The feedforward path also introduces more variations to the RO frequency adding randomness to the output. This type, however, poses several problems when implemented in a Field Programmable Gate Array (FPGA). First is the path sharing between the principal path and the feedforward path creating synthesis errors. Second is that the feedforward path inverters skip over two inverters in the principal path causing logic errors and oscillation failures. The consequences could be fatal to the security check.

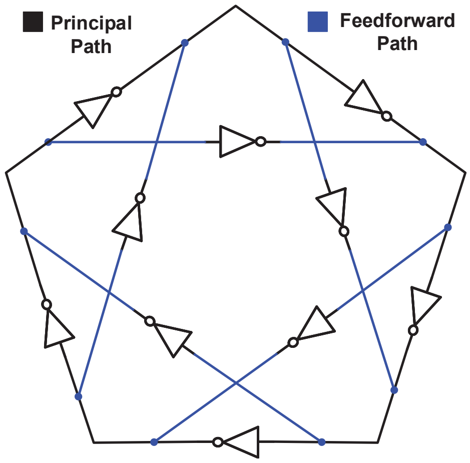


Fig. 3. 5-stage Feedforward Ring Oscillator PUF [5]

III. XNOR-XOR RO PUF Design

Fig. 4 shows the architecture of the proposed XNOR-XOR RO PUF. It is composed of the following sub-blocks:

- N XNOR-XOR Ring Oscillators
- 2 Multiplexers (MUX0, MUX1)
- 2 Counters (Counter0, Counter1)
- Race Arbiter
- Buffer
- Control

where N is the number of challenge bits. The challenge bit selects one of the ROs that is fed to the multiplexers. The schematic of a single RO is shown in Fig. 5. It is composed of a XNOR gates that can be configured as inverters or buffers through the inputs S0∼Sn (in Fig. 5). This will then determine the frequency output of the oscillator. An XOR gate is added at the end of the RO to create an odd number of stage satisfying the Barkhausen criteria to make sure there will be oscillations [7]. Once a challenge is entered, the output of the MUX are fed to the counters as clock signals. The output of the counter are then processed in the race arbiter and lastly the 1-bit output is fed through the Buffer.

IV. Implementation and Results

The XNOR-XOR RO PUF is implemented using the Xilinx ZCU 102 FPGA board, as shown in Fig. 6. To evaluate the PUF output quality, it is important to evaluate its statistical properties. Eqns. (1) – (3) are repetitively used to evaluate its uniqueness, reliability, and uniformity introduced in [8]. These results are post-processed using MATLAB using the given equations. Uniqueness in this report is reflected using different FPGA boards and same external environments to

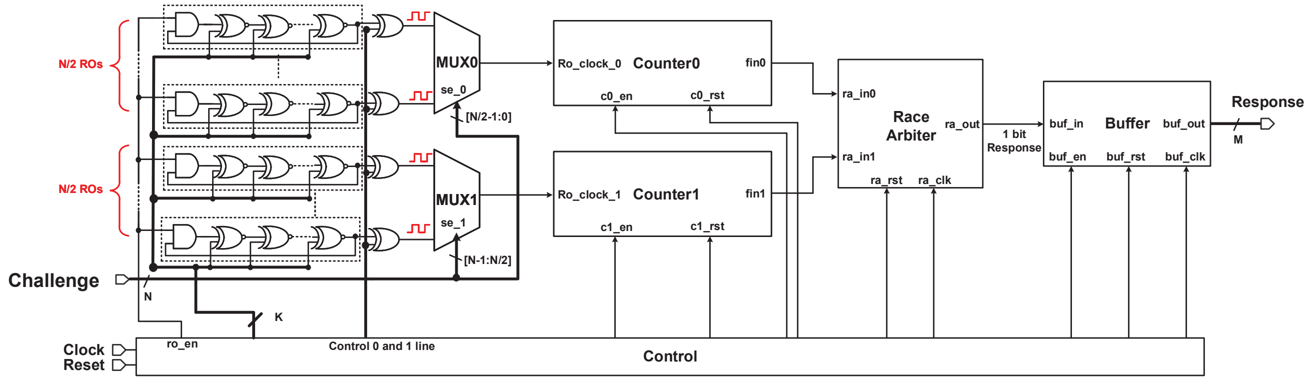


Fig. 4. XNOR-XOR RO PUF Architecture

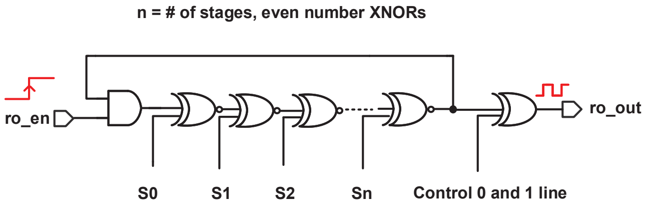
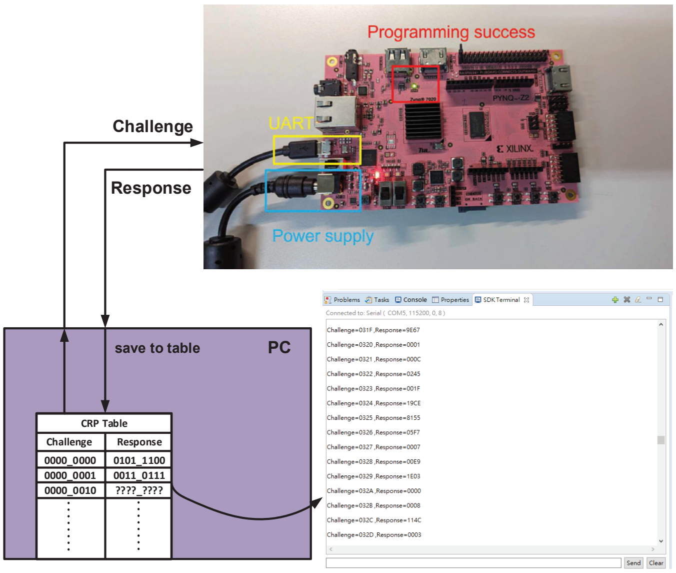


Fig. 5. XNOR-XOR Ring Oscillator



CRP Table	
Challenge	Response
0000_0000	0101_1100
0000_0001	0011_0111
0000_0010	????_????
⋮	⋮

```
Connected to: Serial ( COM5, 115200, 0, 8 )
Challenge=031F ,Response=9E67
Challenge=0320 ,Response=0001
Challenge=0321 ,Response=000C
Challenge=0322 ,Response=0245
Challenge=0323 ,Response=001F
Challenge=0324 ,Response=19CE
Challenge=0325 ,Response=8155
Challenge=0326 ,Response=05F7
Challenge=0327 ,Response=0007
Challenge=0328 ,Response=00E9
Challenge=0329 ,Response=1E03
Challenge=032A ,Response=0000
Challenge=032B ,Response=0008
Challenge=032C ,Response=114C
Challenge=032D ,Response=0003
```

Fig. 6. FPGA experiment with the output screenshot

TABLE I
EXPERIMENTAL RESULTS USING THE XILINX ZYNQ XC7Z020 FPGA BOARD

	Uniqueness	Reliability	Uniformity
RO PUF	49.94%	94.53%	48.73%
NOR PUF	50.51%	92.13%	47.17%
XOR PUF	53.33%	96.47%	48.80%
XNOR PUF	48.08%	98.07%	73.07%
XNX RO PUF	49.90%	99.86%	67.30%

produce a different probabilities of sequence. Eqn. (1) shows the average inter-Hamming distance (Inter-HD) formula used to evaluate the uniqueness of the proposed PUF.

$$HD_{inter} = \frac{2}{C(C-1)} \sum_{i=1}^{C-1} \sum_{j=i+1}^{C} \frac{HD(Ri, Rj)}{n} \times 100\% \quad (1)$$

where C is the number of synthesized arrangements used in the statistics, $\mathrm{R_i}$ is the response of arrangement i, $\mathrm{R_j}$ is the response of arrangement j, and HD is the Hamming distance [9] between the responses. In this report, C = 60, whereas we used 5 FPGA boards and 12 arrangements of the same design to make a fair comparison.

Any electronic device should be stable in any changing environment. Since the PUF is used to authenticate and identify the chip, authentication should not fail due to external influence. For the reliability test in the FPGA, the degree of the output change from the same challenge stimulus is considered. Eqn. (2) shows the intra-Hamming distance (Intra-HD) equation used for the reliability measure.

$$HD_{intra} = \frac{1}{m} \sum_{t=1}^{m} \frac{HD(R_i, R_{i,r})}{n} \times 100\% \quad (2)$$

where m is the number of tests done, $\mathrm{R_i}$ is the response from i chip, $\mathrm{R_{i,r}}$ is the response at different condition of the i chip, n is the size of the output sequence, and HD is the Hamming distance. In this report, n = 3000 and m = 10. The final reliability is computed by subtracting the inter-HD from 100%.

To be used as a security key, the PUF's response must satisfy the requirement that it contain an equal amount of 0's and 1's. The average uniformity is shown in Eqn. (3) [10]. Here, n is the response length and k is the bit position of the response. It is calculated that the average uniformity (U) during the experiment is 67.3%.

$$U = \frac{1}{n} \sum_{k=1}^{n} R[k] \times 100\% \quad (3)$$

TABLE II
PERFORMANCE COMPARISON WITH PREVIOUS FPGA-BASED PUF

	ISCAS [11]	ICET [8]	ISCAS [12]	ISOCC [5]	Ours
Year	2017	2021	2022	2022	2023
Process (nm)	45	28	28	28	28
VDD (V)	1.2	1	1	1	1
Design	XCRO	XOR RO	ERRO	Novel RO	XNOR-XOR RO
Power (mW)	∼	∼	∼	∼	8 @ 100 MHz
Timing (ns)	∼	∼	∼	∼	4.023
No. of RO	64	256	64	64	512
Frequency (MHz)	50	100	100	100	100
Uniqueness (%)	48.76	48.438	49.998	50.23	49.90
Reliability (%)	97.72	98.326	98.61	95.92	99.86
Uniformity (%)	∼	∼	∼	52.64	67.30
FPGA	Spartan-6	Virtex-6	Spartan-7	Artix-7	ZYNQ 7000

Table I summarizes the experiments done for different PUFs in the same FPGA board model. It can be seen that the proposed XNX (XNOR-XOR) RO PUF is the most reliable design with an average reliability of 99.86%. The uniqueness measure is just 0.04% lower than the RO PUF.

Referring to Fig. 7, it shows a histogram to showcase the uniqueness of the responses of the PUF during the experiments. The computed average inter-HD of the PUF is 49.90%. The computed central tendency is 0.14% which is equivalent to 99.86% reliability.

Referring to Table II, it shows the comparison of our proposed PUF with existing FPGA-based PUF in the previous years. Our proposed design is synthesized in the Xilinx Zynq 7000 FPGA board operating at a clock frequency of 100 MHz. It consumed 8 mW of power at the said clock and a slack time of 4.023 ns. It can be seen that our proposed design is the most reliable compared with existing designs.

V. CONCLUSION

This investigation presents a highly reliable physical unclonable function (PUF) implemented in an FPGA for use in IoT security. The proposed PUF is implemented in Xilinx ZYNQ 7000 FPGA board and operating 100 MHz. A novel XNX (XNOR-XOR) Ring Oscillator (RO) PUF with configurable frequency is presented in this report. It has a power consumption of 8 mW at 100 MHz clock rate. Experiments show that our design is highly reliable with 99.86% reliability, uniqueness of 49.90%, and a uniformity of 67.30%. The proposed design offered the most reliable design compared to previous works.

VI. FUTURE WORKS

The next step for this research is the fabrication of the new architecture into an integrated chip prototype using an advanced CMOS process. Multiple chips of the same design will be fabricated and measured to check the performance of the design. Once the proof of concept has been achieved, the design will then be ready to be included into other chip designs to have their own chip “fingerprint.”

ACKNOWLEDGMENT

The authors would like to show the appreciation to Taiwan Semiconductor Research Institute (TSRI) in National Applied Research Laboratories (NARL), Taiwan, for the assistance of EDA tool support. The study is funded by National Science and Technology Council (NSTC), Taiwan under grant MOST 110-2221-E-110-063-MY2, NSTC 111-2623-E-110-002-, and NSTC 112-2221-E-110-063-MY3.

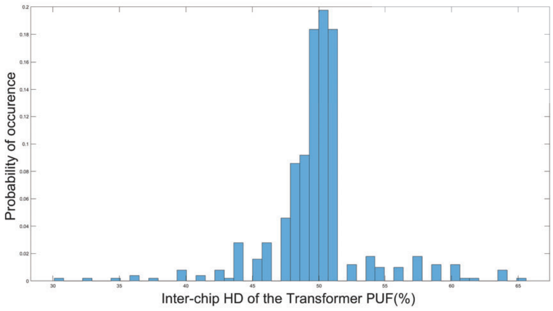


Fig. 7. Inter-HD histogram, Mean = 49.90%

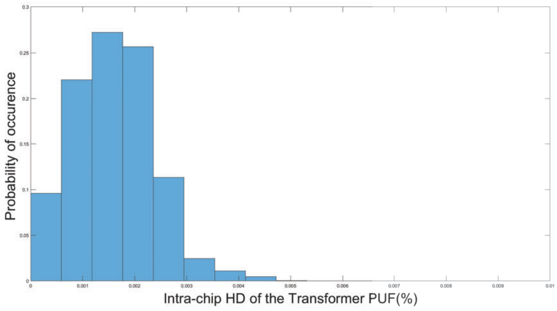


Fig. 8. Intra-HD histogram, Mean = 0.14%, Reliability = 99.86%

REFERENCES

[1] S. Elgendy and E. Y. Tawfik, “Impact of physical design on PUF behavior: A statistical study,” in *Proc. 2021 IEEE Int. Symp. Circuits Syst. (ISCAS)*, Daegu, Korea, May 2021, pp. 1–5.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, “Silicon physical random functions,” in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS ’02)*, Washington, DC USA, Nov. 2002, pp. 148–160.

[3] C.-H. Chang, Y. Zheng, and L. Zhang, “A retrospective and a look forward: Fifteen years of physical unclonable function advancement,” *IEEE Circuits and Systems Magazine*, vol. 17, no. 3, pp. 32–62, 2017.

[4] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *Proc. 2007 44th ACM/IEEE Design Automation Conference*, San Diego, CA, USA, Jun. 2007, pp. 9–14.

[5] T.-K. Dang, R. Serrano, T.-T. Hoang, and C.-K. Pham, “A novel ring oscillator PUF for FPGA based on feedforward ring oscillators,” in *Proc. 2022 19th Int. SoC Des. Conf. (ISOCC)*, Gangneung-si, Republic of Korea,, Oct. 2022, pp. 87–88.

[6] L. Sun, T. Kwasniewski, and K. Iniewski, “A quadrature output voltage controlled ring oscillator based on three-stage sub-feedback loops,” in *Proc. 1999 IEEE Int. Symp. Circuits Syst. (ISCAS)*, Orlando, FL, USA, Aug. 1999, pp. 176–179.

[7] B. Razavi, *Design of Analog CMOS Integrated Circuits*, 2nd ed. McGraw-Hill, 2017.

[8] L. Yao, H. Liang, Z. Huang, C. Jiang, M. Yi, and Y. Lu, “A lightweight configurable XOR RO-PUF design based on Xilinx FPGA,” in *Proc. 2021 IEEE 4th Int. Conf. Electron. Technol. (ICET)*, Chengdu, China, May 2021, pp. 83–88.

[9] B. Chuang and T. Li-jun, “A reliable physical unclonable function for chip fingerprint,” *Acta Electronica Sinica*, vol. 47, no. 10, pp. 2116–2125, Oct. 2019. [Online]. Available: https://www.ejournal.org.cn/EN/10.3969/j.issn.0372-2112.2019.10.013

[10] B. Srinivasu, P. Vikramkumar, A. Chattopadhyay, and K.-Y. Lam, “CoLPUF : A novel configurable LFSR-based PUF,” in *Proc. 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Chengdu, China, Oct. 2018, pp. 358–361.

[11] L. Zhang, C. Wang, W. Liu, M. O’Neill, and F. Lombardi, “XOR gate based low-cost configurable RO PUF,” in *Proc. 2017 IEEE Int. Symp. Circuits Syst. (ISCAS)*, Baltimore, MD, USA, May 2017, pp. 1–4.

[12] D. Rizk, R. Rizk, F. Rizk, and A. Kumar, “An economic uniqueness-improved reliable reconfigurable RO PUF for iot security,” in *Proc. 2022 IEEE Int. Symp. Circuits Syst. (ISCAS)*, Austin, TX, USA, May 2022, pp. 1680–1684.