Physical Unclonable Function using Programmable Delay Lines

Jiho Park, Heehun Yang, Donghun Lee, and Hoyoung Yoo
Dept. of Electronics Engineering
Chungnam National University
Daejeon, Korea
{jhpark.cas, hhyang.cas, dhlee.cas, hyyoo.cas}@gmail.com

Abstract

In this paper, we propose a novel Ring-Oscillator Physical Unclonable Functions (RO-PUF) architecture using Programmable Delay Lines (PDL) in Field Programmable Gate Arrays (FPGA). Our proposed PUF uses PDL to change the propagation path inside the Look Up Table (LUT), thereby changing the output of RO. Depending on the output of the changed RO, different response outputs occur for the same RO-PUF architecture and challenge input. We have examined how the challenge-response pairs of the proposed PUF structure change according to the PDL. Additionally, we have analyzed the performance changes of the proposed PUF, finding that HD_{inter} showed a maximum difference of 7.1248%, and HD_{intra} showed a maximum difference of 3.9731%. We confirm that the performance of the proposed PUF structure can vary depending on the PDL, and our research results will provide an optimal PUF structure solution to enhance the performance of PUF.

Keywords: physical unclonable functions, ring oscillators, FPGA, programmable delay lines

1. Introduction

As the demand for IoT devices increases, the demand for technology to secure the security and reliability of IoT is increasing. Traditional hardware stored secret keys in non-volatile memory, which poses a risk of key extraction due to physical attacks. Storing secret keys in volatile memory is not suitable for IoT devices due to the increased cost and system complexity from additional power supply requirements [1]. PUF are a novel security technology that addresses these issues. By not storing keys in memory, they overcome vulnerabilities to physical attacks and operate with low area and low power, making them suitable for IoT devices [2]. PUF can generate unique and unclonable secret keys for each device, and these generated keys can be used for security tasks such as identification and authentication.

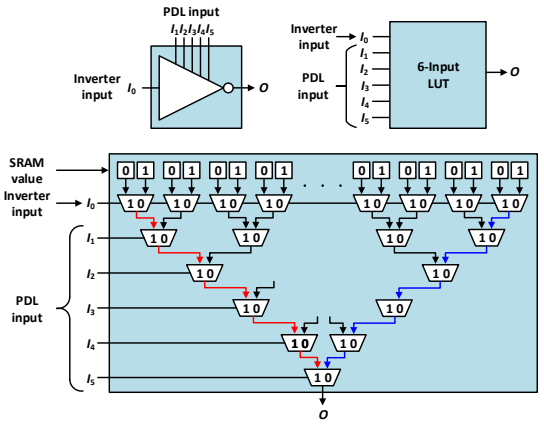

Figure 1. Programmable Delay Lines (PDL) using 6-input LUT

Using the physical variability generated during the circuit manufacturing process, each device has its own physical characteristics. PUF is a physical system that utilizes these characteristics to generate a unique challenge-response for each device. The response depends on the challenge, and the response should vary by device. Recently, RO-PUF [3], Arbiter PUF [4], and SRAM PUF [5] are continuously being studied as research on PUF.

In this paper, when configuring a PUF using a RO controlled by PDL, the performance index of the PUF according to the change of PDL is analyzed to find out the effect of PDL on PUF performance.

2. Background

A. Programmable Logic Delay

In the FPGA logic elements are composed of LUT. The output of a LUT is determined by its SRAM value and LUT input. It can operate as various logical elements by determining which SRAM value is connected through LUT input. By properly changing the LUT input, the operation of the logic element is maintained, but only the propagation path until the signal is output can be changed.

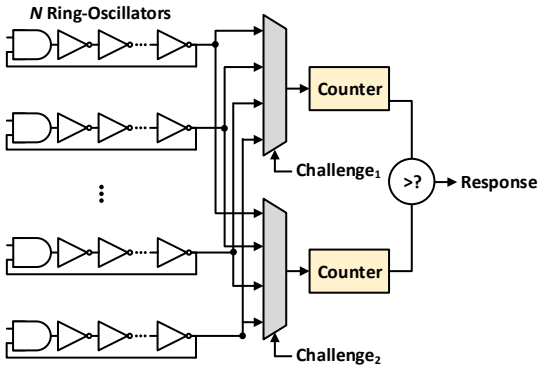

Figure 2. Conventional RO-PUF [3].

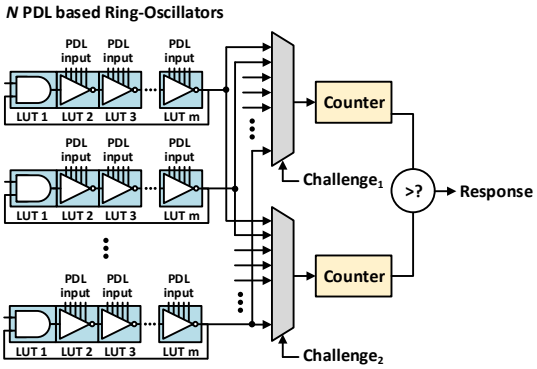

Figure 3. Proposed PDL-based RO-PUF.

For example, the LUT in Fig. 1 is configured to operate as an inverter. The output *O* of the LUT always comes out as an inverted bit of the inverter input I0. The PDL input ($I_1I_2I_3I_4I_5$) enters the input of the LUT, but acts as a don't care bit, affecting the path of the signal until the first input comes out. If $I_1I_2I_3I_4I_5$ = 00000, a signal is transmitted along the red line, and if $I_1I_2I_3I_4I_5$ = 11111, a signal is transmitted along the blue line.

B. Ring-Oscillator PUF

RO-PUF is used as a PUF using the properties of different frequencies generated for each independently operating RO. The RO consists of an odd number of consecutive inverters and is formed by a closed loop. The RO continuously vibrates in a closed loop, and the frequency of this vibration can vary from position to position in the circuit. In addition, if the FPGA used is different even in the same position, the value may vary due to changes in the manufacturing process.

The first RO-PUF was proposed in [3]. This RO-PUF consists of independent ROs and a Counter to measure the frequency of the ROs. By measuring and comparing the frequencies of a pair of ROs, a single bit is generated, where the selection of the RO pair is used as the challenge and the output bit is the Response. If there are *N* ROs, the maximum number of challenge-response pairs is *N(N-1)/2*, but for RO pairs that are not independent of each other, it is meaningless as output. Thus, the number of independent maximum challenge-response pairs is $log_2(N!)$.

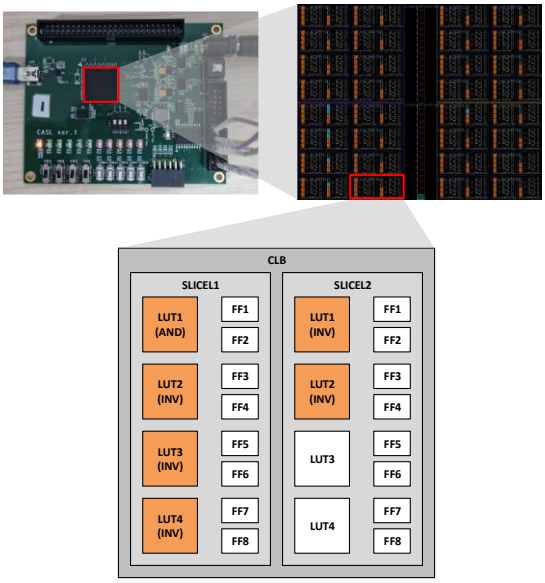

Figure 4. PUF configuration of Artix-7 device.

3. Proposed PDL-based RO-PUF

A. Design of PDL-based RO-PUF

The proposed RO-PUF based on PDL architecture is as shown in Fig. 3. The PUF is composed of *N* ROs each consisting of one AND gate and *(m-1)* inverters. As shown in Fig. 3, PDL input can be set for each LUT, which changes the propagation path inside the circuit. Due to these varied propagation paths, the output of the RO can possess different values based on the PDL value. Since the PDL value influences the RO output, the response value changes for the same challenge. This design was implemented on the Artix-7, and since the Artix-7 is made up of 6-input LUTs, the range for the PDL input is from 00000 to 11111. Therefore, the output of 32 PDL inputs per RO-PUF was exported, and characteristic changes were analyzed for each PUF.

For the implementation of the proposed architecture, Xilinx Artix-7 FPGA was used, as illustrated in Fig. 4. The FPGA is composed of an array of Configurable Logic Blocks (CLBs), and each CLB contains two SLICEs. The Artix-7 has both SLICEL and SLICEM, and within each SLICE, there are four 6-input LUTs and eight Flip-Flops [6]. To make the 6-input LUT operate as an inverter, the SRAM value of the LUT was fixed at 64'h5555555555555555.

The PDL-based RO-PUF design used for the experiment consisted of 32 ROs, with one AND gate and five inverters per RO. Fig. 4 shows that the six logical elements constituting one RO are implemented into six LUTs inside one CLB.

Table 1. HD_{inter} and HD_{intra} of PUF in different PDL input.

PDL input	HD_{inter} (%)	HD_{intra} (%)	PDL input	HD_{inter} (%)	HD_{intra} (%)	PDL input	HD_{inter} (%)	HD_{intra} (%)	PDL input	HD_{inter} (%)	HD_{intra} (%)
00000	48.5714	3.6735	01000	48.8235	2.9202	10000	48.2353	2.7941	11000	49.2754	2.2153
00001	49.0909	**1.4069**	01001	51.3433	4.3817	10001	48.4746	5.9201	11001	48.9655	5.6404
00010	50.4615	3.9341	01010	50.8772	3.3208	10010	50.6897	2.9187	11010	50.0000	5.5876
00011	50.0000	4.1133	01011	49.2593	**8.5317**	10011	49.6000	4.7000	11011	**48.1481**	1.8783
00100	49.8413	2.8798	01100	50.8108	2.7606	10100	50.7895	3.2895	11100	51.5000	5.1071
00101	50.4225	3.4507	01101	**52.1212**	2.7273	10101	51.8182	1.7100	11101	51.1429	2.2449
00110	51.5942	1.4493	01110	50.1449	2.3188	10110	50.4348	4.2754	11110	49.863	3.1311
00111	51.0345	3.3005	01111	49.5385	2.6593	10111	49.3103	3.3744	11111	48.3784	3.2722

B. Performance of PDL-based RO-PUF

Hamming distance (*HD*) is an index indicating the number of different bits between two bits strings. HD_{inter} and HD_{intra} are calculated as performance indicators of PUFs used to evaluate the performance of PUFs through *HD* [7]. The PUF designed for the experiment was implemented on five Artix-7 FPGA boards and tested.

HD_{inter} shows the uniqueness of each device by measuring the rate at which two PUFs implemented with the same circuit generate different responses for the same challenge. Ideally, the response from one device should not be predictable based on the response from the other device, and the *HD* between the two responses should be 50%. The HD_{inter} of the PUF can be calculated using

$$HD_{inter} = \frac{2}{N(N-1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \frac{HD(R_i, R_j)}{k} \cdot 100\% \cdot \quad (1)$$

In the above equation, N represents the number of devices, k represents the bit length of the response, and R_i and R_j represent the response of different devices. HD_{inter} showed a 3.9731% difference from a maximum of was 52.1212% to a minimum of 48.4181%. The average of the HD_{inter} was 50.0175%, close to the ideal value.

HD_{intra} shows the reliability of PUF circuits by measuring the rate at which PUFs continue to generate the same response for the same challenge. Ideally, one device should continue to output the same response for the same challenge, and the *HD* between the output responses should be 0%. The HD_{intra} of PUF can be calculated using

$$HD_{intra} = \frac{1}{N} \sum_{i=1}^{N} \frac{HD(R_i, R_i^t)}{k} \cdot 100\% \cdot \quad (2)$$

In the above equation, k is the total number of response samples, N is the bit length of the response, R_i is the response bit, and R_i^t is the response bit used as a reference. HD_{intra} showed a 7.1248% difference from a maximum of 8.5317% to a minimum of 1.4069%.

Table 1. presents HD_{intra} and HD_{inter} when varying from PDL input 00000 to 11111. The parts expressed in bold indicate the highest or lowest values in each performance indicator. Through this, it can be confirmed that a significant difference occurs in the characteristics of the PUF according to the change in the PDL. In addition, by selecting the PDL input with the best PUF performance, the most ideal PUF architecture for that FPGA can be implemented.

4. Conclusion

In this paper, we propose a PDL-based RO-PUF and examined the changes in PUF performance with variations in PDL when implemented on a FPGA. We implemented it on a Xilinx Artix-7 FPGA and investigated how much the HD_{inter} and HD_{intra} of the PUF vary by changing the PDL. HD_{inter} showed a maximum difference of 7.1248%, while HD_{intra} showed a maximum difference of 3.9731%. These findings confirm that significant changes in PUF performance occur with variations in PDL. Therefore, by fine-tuning the PDL input, we can select the optimal PUF structure showing the best performance within the same circuit. However, further research is needed to understand the correlation between PDL input and changes in RO-PUF performance. Future studies will focus on identifying the correlation between PDL input and RO-PUF performance, and through this, we plan to research low-area PDL-based RO-PUFs that can operate with fewer ROs.

Acknowledgement

This research was supported by National R&D Program through the National Research Foundation of Korea(NRF) funded by Ministry of Science and ICT(2020M3H2A1078119), supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1A5A8026986) and supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2021R1I1A3055806).

References

[1] M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust. Springer, 2011.

[2] Gassend, Blaise, et al. "Silicon physical random functions." Proceedings of the 9th ACM Conference on Computer and Communications Security. 2002.

[3] Suh, G. Edward, and Srinivas Devadas. "Physical unclonable functions for device authentication and secret key generation." Proceedings of the 44th annual design automation conference. 2007.

[4] Lim, Daihyun, et al. "Extracting secret keys from integrated circuits." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 13.10 (2005): 1200-1205.

[5] Guajardo, Jorge, et al. "FPGA intrinsic PUFs and their use for IP protection." Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. Springer Berlin Heidelberg, 2007.

[6] 7 Series FPGAs Configurable Logic Block User Guide (UG474) (v1.18), Xilinx: San Jose, CA, USA, 2016. [online] Available: https://docs.xilinx.com/v/u/en-US/ug474_7Series_CLB

[7] Ardakani, Amir, Shahriar B. Shokouhi, and Arash Reyhani-Masoleh. "Improving performance of FPGA-based SR-latch PUF using Transient Effect Ring Oscillator and programmable delay lines." Integration 62 (2018): 371-381.