Implementation of Pseudo Linear Feedback Shift Register Physical Unclonable Function on Silicon

Yasuhiro Ogasahara, Yohei Hori, and Hanpei Koike
AIST, Tsukuba 305-8568, Japan, e-mail:ys.ogasahara@aist.go.jp

***Abstract*—In this study, we demonstrate the first implementation of a pseudo linear feedback shift register physical unclonable function (PL-PUF) on silicon, and a proposal of the power supply design to obtain fine reproducibility. Unlike SRAM PUFs, a PL-PUF can generate responses without memory cells, and therefore is secure against attacks extracting internal memory values. We design a capturing signal-generation circuit that brings tolerance to the degradation of reproducibility due to supply voltage change, and implement PL-PUF on 65nm CMOS process. Implemented PL-PUF achieves fine reproducibility (μ=1.09-10.52% fractional HD) and uniqueness (μ=49.01-49.56%, σ=5.38-5.77% class-to-class HD, 0.983-0.941 entropy) on silicon.**

I. Introduction

Semiconductor devices are becoming more important for social infrastructures such as smart grid technology, intelligent transportation systems, and medical applications. For these infrastructures, counterfeit devices are a serious issue. Low-quality counterfeits cause performance degradation in devices, and malicious counterfeits may include backdoors. Such counterfeits can therefore result in unreliability of the infrastructure and serious damage to society. Physical unclonable functions (PUFs) [1] are a technology for generating unclonable device-specific response bits that can be used as a secret key from arbitrary challenge bits. PUFs are considered to be a promising countermeasure against counterfeiting.

PUFs can be categorized into two groups: memory-based PUFs and delay-based PUFs. Memory-based PUFs is based on a SRAM PUF [2], and there are several proposals for performance improvement [3], [4]. Delay-based PUFs include RO PUFs [5], an Arbiter PUF [6], and a pseudo-linear feedback shift register PUF (PL-PUF) [7], and so on. SRAM PUFs exploit the power-on initial state of SRAM which is determined by the process variability. However, the power-on initial values of memory-based PUFs are stored in the SRAM or latches, and therefore the PUFs are potentially vulnerable to attacks that extract memory values. In contrast, delay-based PUFs do not exploit memory cells, and the PUF circuit itself generates responses (i.e., output) directly from the challenge (i.e., input). Therefore, delay-based PUFs can be resistant to memory extraction attacks. PL-PUF is a highly efficient delay-based PUF that can generate a 128-bit response from a 128-bit challenge. Unlike other delay-based PUFs that generate a 1-bit response from a long-bit challenge, a PL-PUF can save the size of databases necessary to store challenge and response pairs (CRPs) for authentication.

This study presents the first implementation of a PL-PUF on silicon, and proposes the power supply and circuit designs to enhance tolerance to supply voltage change and to improve reproducibility of generated responses. The circuit block of the PL-PUF comprises a much smaller number of gates on silicon than the previous implementation on FPGA [7], and we expect that the randomness of the circuit block delay originating from the random process variability will also be improved on silicon, resulting in an enhancement of the uniqueness and randomness of the responses.

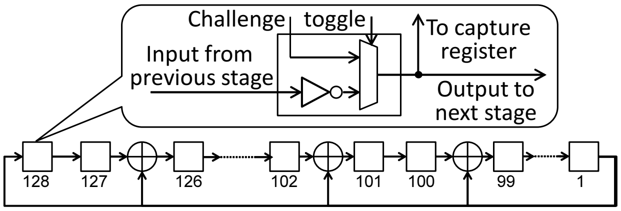

Fig. 1. The circuit structure of the PL-PUF.

II. PL-PUF structure and implementation issues

A. Structure of the PL-PUF

Figure 1 shows the circuit structure of 128 bit PL-PUF. The PL-PUF comprises 128 circuit blocks and 3 XOR gates. Each circuit block contains a multiplexer and an inverter. An output of each circuit block is connected to a capture register. The PL-PUF obtains response bits from challenge bits through the following procedure.

1. Set the “toggle” signal to 0.
2. Input challenge bits to the “challenge” signal in each block.
3. Set the “toggle” signal to 1 to start PL-PUF oscillation.
4. Capture the output of each circuit block (i.e., the response bits) with registers after a certain period.

The delay of each circuit block depends on process variability, and the initial challenge value fluctuates because of the accumulated delay of the circuit blocks. To enable the fine uniqueness, diffuseness and entropy [8] of the response, the PL-PUF exploits a primitive feedback polynomial in Eq. (1) [9], which is used in linear feedback shift registers.

$$x^{128} + x^{126} + x^{101} + x^{99} + 1 \tag{1}$$

The output of the 1st circuit block is fed back to the inputs of 126th, 101st, and 99th circuit blocks with the XOR gate. The input of the 128th circuit block is the output of 1st circuit block.

B. Reproducibility and uniqueness challenges of PL-PUF in previous FPGA implementation

In our previous study, we have demonstrated an implementation of PL-PUF on FPGA [7]. This FPGA implementation captured a PL-PUF response with an 24 MHz external clock

978-1-4799-5341-7/16/$31.00 ©2016 IEEE

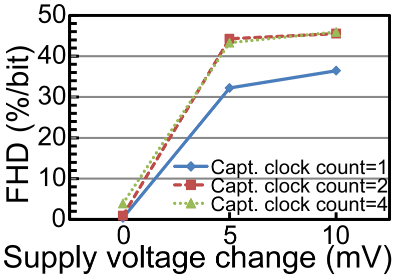

Fig. 2. Relationship between FHD and supply voltage change for the PL-PUF FPGA implementation in previous study [7].

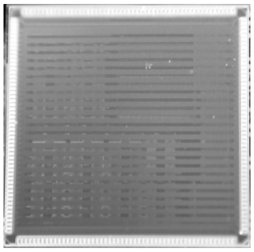

Fig. 3. The micrograph of the test chip.

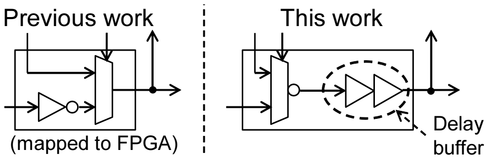

Fig. 4. Improvement of PL-PUF circuit block in this study. The PL-PUF implemented on silicon is estimated to operate too fast, and two delay buffers comprising four inverters are inserted to adjust the oscillation speed. An inverter and a multiplexer used previously for the FPGA implementation are replaced with a negative-logic multiplexer in the standard cell library.

signal. Though fine entropy and diffuseness were obtained in the previous study, there were still several challenges facing a fine PUF performance: tradeoff between class-to-class hamming distance (C2C HD) and fractional hamming distance (FHD), and sensitivity to the power supply fluctuation.

The performance of PUFs has frequently been discussed in terms of C2C HD, FHD, and entropy. C2C HD is the hamming distance (HD) between two PUF responses generated under different conditions (PUF circuit, challenge, and so on.). PUF is expected to generate unique response in different conditions, and C2C HD presents the uniqueness of the PUF responses. An ideal average of C2C HD is 50% of the block length and an ideal distribution of C2C HD would be binomial. The ideal entropy of responses is 100% of the sum of the response lengths. FHD is the average of HD among PUF responses repetitively obtained in the same condition. An ideal PUF would perfectly reproduce an identical response under the same conditions, and FHD, which indicates the reproducibility of the PUF responses, is expected to be small.

The distribution of C2C HD observed on the previous FPGA implementation was not sufficiently close to an ideal binominal distribution when the capturing clock count was small [7]. On the other hand, FHD suffered from serious degradation in a large capturing clock count, and there was a tradeoff between C2C HD and FHD of PL-PUF responses. Furthermore, we here show the average FHD of measured responses when supply voltage was changed in the FPGA implementation in Fig. 2, which was obtained in experiments following the previous study. The PL-PUF was implemented on Xilinx Spartan-6 FPGA, and the nominal supply voltage is set to 1.200V. Responses are captured at clock counts of 1, 2, and 4 with a 24MHz clock. The average FHD reaches 17.7-45.3%, even with a 5 mV supply voltage change, and the implementation in the previous study is too sensitive to the supply voltage change. FHD degradation due to supply voltage change was a serious issue in the previous implementation of a PL-PUF.

III. PL-PUF IMPLEMENTATION ON SILICON AND A PROPOSAL TO IMPROVE OF REPRODUCIBILITY

In this section, we explain our implementation of a PL-PUF on silicon, and propose designs to resolve the FHD and C2C HD issues discussed in Sec. II-B. The test chip is fabricated on a 65 nm CMOS process. Figure 3 shows the micrograph of the test chip. The PL-PUFs and shift registers are implemented on the test chip, and the input values to PL-PUFs (challenge, capturing timing, and so on) are set to the shift registers.

1) Implementation with the minimum number of gates:

The implementation of a PL-PUF on silicon, rather than FPGA, is itself expected to improve C2C HD and FHD. PL-PUF exploits the delay variability of the PL-PUF circuit block originating from the random process variability. When each circuit block comprises a large number of gates, the impacts of the variability are averaged and weakened, and C2C HD and FHD are degraded. The circuit block mapped onto FPGA included many gates, resulting in insufficient FHD and C2C HD in the previous implementation. In contrast, the PL-PUF implementation on silicon presented in this study requires a minimum number of standard cells, and an improvement of the PUF performance is expected.

A negative logic multiplexer can be implemented with fewer transistors than a positive logic multiplexer, and we integrated an inverter and a multiplexer in previous implementation to a negative logic multiplexer as shown in Fig. 4.

Here, the PL-PUF is similar to a ring oscillator comprising negative logic multiplexers as we utilize such multiplexers. The oscillation of the ring oscillator is estimated to be too fast, and capturing the signal will require strict timing control. We insert the delay buffers to reduce oscillation speed, as shown in Fig. 4.

2) Proposal for the capturing signal-generation circuit to alleviate the impact of voltage change:

In this paper, we designed an on-chip ring-oscillator-based capturing signal-generation circuit depicted in Fig. 5 instead of an external clock signal in the previous study or common PLL, and propose implementing both the capturing signal-generation circuit and the PL-PUF circuit in the same power supply domain for alleviation of the sensitivity of the PL-PUF to power supply change. Figure 6 explains the proposed implementation. The sensitivity of the PL-PUF to supply change is assumed to originate from the change in the PL-PUF oscillation speed resulting from voltage changes. The external capturing signal is not affected by power supply voltage change, and the variation of the oscillation speed due

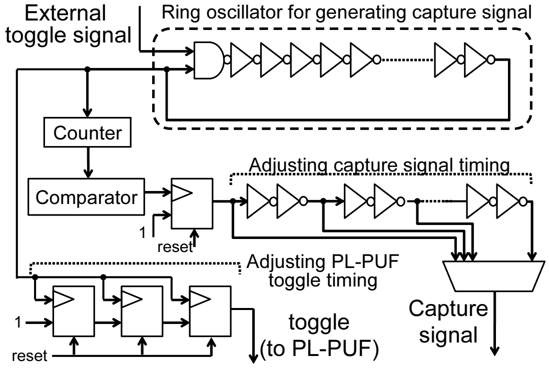
External toggle signal
Ring oscillator for generating capture signal
Counter
Comparator
Adjusting capture signal timing
1
reset
Adjusting PL-PUF toggle timing
1
reset
toggle (to PL-PUF)
Capture signal

Fig. 5. The structure of the ring-oscillator-based circuit for capture timing-generation.

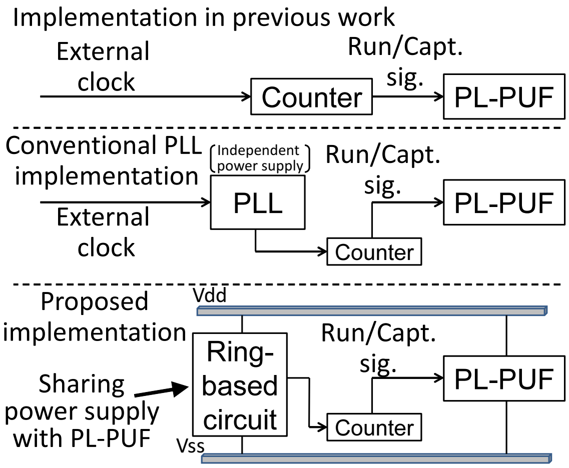

Fig. 6. Proposed method for reduction of FHD. Capture timing is generated by a ring-oscillator-based circuit, which shares V_{dd} and V_{ss} with the PL-PUF circuit. Capture timing change is accompanied by change in the PL-PUF oscillation speed.

to the supply voltage change results in fluctuation of the PL-PUF responses. In contrast, in proposed implementation, the ring-oscillation speed of capturing signal-generation circuit is also changed by the supply voltage change. According to Ref. [10], the circuit delay is proportional to the supply voltage. The change in the oscillation speed of the PL-PUF is expected to be followed by the speed of the ring oscillator in the capturing signal-generation circuit, and the sensitivity of the PL-PUF to the supply voltage change is thus expected to be alleviated.

The detailed implementation of ring-oscillator-based capturing signal-generation circuit is as follows. The ring-oscillator cycle estimated with static timing analysis is approximately 2ns. The oscillation of the ring begins with the assertion of the "toggle" signal input to the PL-PUF. The counter counts the pulse signal of the ring oscillator output, and the comparator generates the capturing signal at a specific count. The circuit for further adjustment of the capturing signal timing is also implemented; however, it was not used for measurement in this study. The shift registers which is set by external signal contain the capturing signal-generation count and the number of adjusting delay blocks. As the counter and output FF of the comparator are synchronized with the ring-oscillator pulse, and the capturing signal is delayed by a few ring oscillator cycles. The PL-PUF "toggle" signal is also delayed by a few ring-oscillator cycles with the FFs synchronizing with the ring-oscillator pulse before it is input to the PL-PUF, and the timing window during which the PL-PUF output cannot be captured is eliminated.

IV. Measurement results

We measure 10 test chips, and 10 PL-PUFs are measured on each chip. 128 challenges generated by a pseudo-random number generator are input to the PL-PUF. The PL-PUF output capturing ring-oscillator count is set to 4-10 because initial value is captured at 0-3 count due to PL-PUF toggle delay described in Sec. III. The nominal supply voltage is set to 1.20V, and responses are acquired at 1.10, 1.15, 1.20, 1.25, and 1.30V. 100 responses are obtained under each condition. External control signals are input to the test chip with the external pattern generator, and outputs from the test chip are read using the external logic analyzer.

Figure 7 shows the histograms of the FHD and C2C HD distribution in the responses measured at capturing counts of 4 and 10 at 1.20V. The FHD and C2C HD distributions obtained when the supply voltage is changed from 1.10 to 1.30V are presented in Fig. 8. The binominal distribution, which is the ideal distribution of C2C HD, is also depicted in both of Figs. 7 and 8. Averages (μ) of both C2C HD and FHD, and standard deviations (σ) of C2C HD at 1.20V are shown in Fig. 9. Figure 10 compares the FHDs of the previous FPGA implementation and the implementation on silicon when the supply voltage is changed. As shown in Figs. 7 and 8, in all cases, the distributions of C2C HD are sufficiently close to the ideal binomial distribution. The measured C2C HD μ (49.01-49.56%) and σ (5.38-5.77%) depicted in Fig. 9 are sufficiently close to ideal values (μ=50% and σ=4.42%). The responses generated by the implemented PL-PUFs are sufficiently unique. In Figs. 9 and 10, we can observe that FHD distribution is sufficiently small (μ=1.09-10.52) in comparison with the C2C HD distribution, even at capturing count = 10 or when the supply voltage is changed. The FHD results when the supply voltage is changed are notably improved over those in the previous FPGA implementation. We achieved fine reproducibility and uniqueness of PL-PUF on silicon, and the measurement results indicated the validity of the implementation proposed in Sec. III; a ring-oscillator based capturing signal-generation circuit in the same power supply domain as PL-PUF.

Figure 11 shows the entropy values of the measured responses. Though entropy values at capturing counts 9 and 10 were below 0.9, fine entropy results (0.983-0.941) were observed at cycle counts of 4, 5, and 6, and the fine randomness [8] of the measured responses was confirmed.

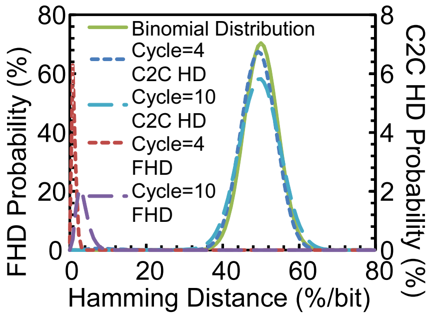

Fig. 7. Ideal binominal distribution and distributions of measured FHD and C2C HD at capturing signal cycles 4 and 10.

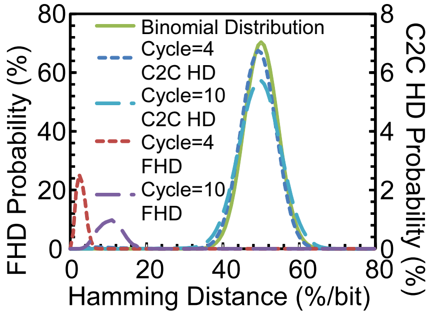

Fig. 8. Ideal binominal distribution and measured FHD μ and C2C HD (μ,σ) when V_{dd} is varied from 1.10 to 1.30V at capturing signal cycles 4 and 10.

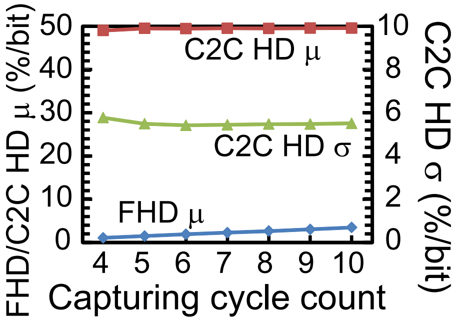

Fig. 9. Measured average (μ) of FHD and μ and standard deviation (σ) of C2C HD.

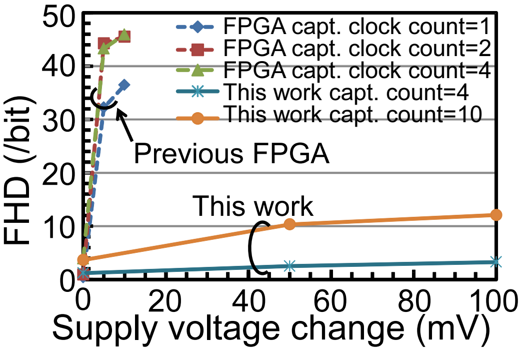

Fig. 10. Measured average (μ) of FHD and μ and standard deviation (σ) of C2C HD when the supply voltage is changed.

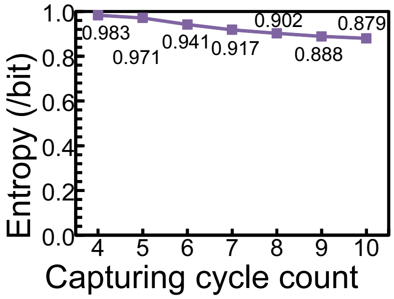

Fig. 11. Entropy values (/bit) of measured responses.

V. Conclusion

This study describes the first implementation of a PL-PUF on silicon. PL-PUF is a delay-based PUF, which is not vulnerable to attacks intended to extract memory values, unlike memory-based PUFs. Though previous FPGA implementation of PL-PUF did not achieve sufficient FHD and C2C HD results, the PL-PUF implemented on silicon has been shown to improve these quantities. Furthermore, we also proposed a ring-oscillator based capturing signal-generation circuit implemented in the same power supply domain as the PL-PUF circuit to alleviate the FHD degradation due to supply voltage change. Measurement results on test chips fabricated in a 65nm CMOS process demonstrated fine FHD, C2C HD, and entropy results even when supply voltage was changed. We achieved fine uniqueness and reproducibility for the PL-PUF on silicon.

References

[1] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, "Physical One-Way Functions," Science, Vol. 297, No. 5589, pp. 2026–2030, Sep. 2002.

[2] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," In Proc. *CHES*, pp. 63–80, 2007.

[3] K. Yang, Q. Dong, D. Blaauw, D. Sylvester "A Physically Unclonable Function with BER 10-8 for Robust Chip Authentication Using Oscillator Collapse in 40nm CMOS," *Dig. of Tech. papers in IEEE ISSCC* pp. 254–255, Feb. 2015.

[4] A. Alvarez, W. Zhao, and M. Alioto, "15fJ/b Static Physically Unclonable Functions for Secure Chip Identification with ¡2% Native Bit Instability and 140× Inter/Intra PUF Hamming Distance Separation in 65nm," *Dig. of Tech. papers in IEEE ISSCC* pp. 256–257, Feb. 2015.

[5] G. E. Suh, and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," In Proc. *IEEE/ACM DAC*, pp. 9–14, 2007.

[6] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting Secret Keys from Integrated Circuits," *IEEE Trans. VLSI Syst.*, Vol. 13, No. 10, pp. 1200–1205, Oct. 2005.

[7] Y. Hori, H. Kang, T. Katashita, and A. Satoh, "Pseudo-LFSR PUF: A Compact, Efficient and Reliable Physical Unclonable Function," In Proc.*ReConFig*, pp. 223–228, 2011.

[8] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," In Proc. *ReConFig*, pp. 298–303, 2010.

[9] M. George and P. Alfke, "Linear feedback shift registers in Virtex devices," Xilinx apprication note XAPP210, 2007.

[10] Y. Ogasahara, T. Enami, M. Hashimoto, T. Sato, and T. Onoye, "Validation of a Full-Chip Simulation Model for Supply Noise and Delay Dependence on Average Voltage Drop with On-chip Delay Measurement," *IEEE Trans. on CAS-II*, vol. 54, no. 10, pp. 868–872, Oct. 2007.