Evaluation of PLFSR PUF with Several Implementation Methods for FPGA

Yusuke Nozaki, Yoshiya Ikezaki, and Masaya Yoshikawa
Dept. of Information Engineering
Meijo University
Nagoya, Japan
143430019@ccalumni.meijo-u.ac.jp

Abstract—**Physical Unclonable Function (PUF) has been attracted attention as a countermeasure of an imitation of semiconductor. Pseudo linear feedback shift register PUF (PLFSR PUF) is one of the most popular PUFs. However, a performance evaluation of PLFSR PUF due to the difference of implementation has not been reported. Therefore, this study evaluates the performance of PLFSR PUF with several implementation methods.**

Keywords-security of semiconductor; physical unclonable function ; pseudo linear feedback shift register PUF

I. INTRODUCTION

Since an imitation of semiconductor becomes a serious problem, Physical Unclonable Function (PUF), which utilizes a physical dispersion of manufacturing, has been attracted attention as a countermeasure [1][2]. PUF cannot be cloned since a counterfeit of the physical dispersion of manufacturing is difficult. Several PUFs have been recently proposed, including an arbiter PUF [1], a ring oscillator PUF, a SRAM PUF, a pseudo linear feedback shift register PUF (PLFSR PUF) [2] and so on. PLFSR PUF is one of the most popular PUFs.

In previous studies for PLFSR PUF [2][3], a performance evaluation due to the difference of implementation has not been reported. Also, it is important that the verification of the performance with several implementations. Therefore, this study evaluates the performance of PLFSR PUF with several implementation methods by experiments using a field programmable gate array (FPGA).

II. PSEUDO LINEAR FEEDBACK SHIFT REGISTER PUF

Figure 1 shows the outline of PLFSR PUF. As shown in Fig.1, PLFSR PUF consists of core (combinational circuit) and exclusive-OR gate. This study targets a PLFSR PUF with 8 cores for simplicity. Generally, a linear feedback shift register (LFSR) uses a shift register. However, PLFSR PUF utilizes the core (combinational circuit) instead of the shift register.

In the operation of PLFSR PUF with 8 cores, 8-bit input signals (challenge) Dinit are set to each core. Next, by changing a SEL signal, PLFSR PUF circuit oscillates. Then, 8-bit output signals Dout of each core are latched as a PUF output (response) by an arbitrary clock (active duration). Here, the oscillating frequency of PLFSR PUF is decided by the semiconductor manufacturing. Therefore, the PUF response is characteristic [2].

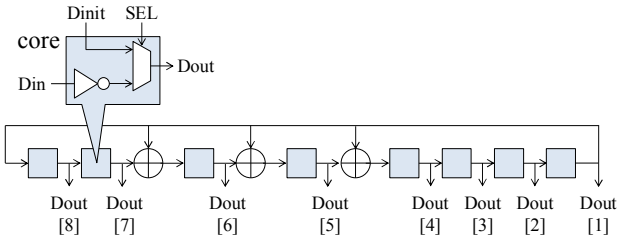


Figure 1. PLFSR PUF with 8 cores

III. PROPOSED IMPLEMENTATION METHOD

For the implementation of PLFSR PUF core, this study proposes two implementation methods, including a multiplexer (MUX) implementation and a lookup table (LUT) implementation. Figures 2 and 3 show the outline of the proposed implementation method.

As shown in Fig. 2, in the MUX implementation, a MUX primitive (MUXF7) is used for the core implementation. Then, in the LUT implementation, a LUT (LUT3) is used for the core implementation, as shown in Fig.3. In the LUT, 3 inputs and an output are assigned to SEL, Din, Dinit (challenge), and Dout (response), respectively.

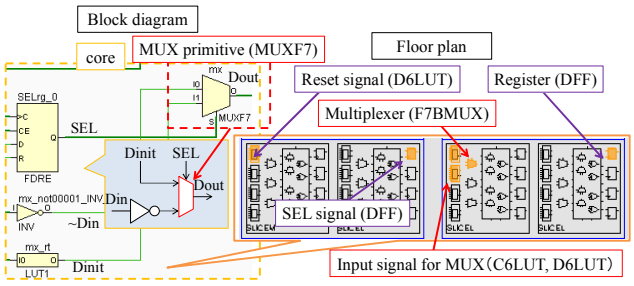


Figure 2. Outline of the MUX implementation

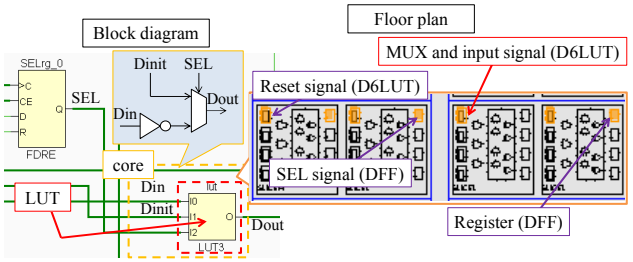


Figure 3. Outline of the LUT implementation

978-1-5090-3992-0/17/$31.00 ©2017 IEEE

IV. EXPERIMENTS

A. Experimental Environment

Experiments used 3 evaluation boards (board A, B, and C). Fig. 4 and Table I show the experiment environment. PLFSR PUF (MUX implementation or LUT implementation) with 8 cores was implemented into a FPGA on each board. Then, each core was placed from SLICE_X0Y0 to SLICE_X3Y7. Also, 200 IDs in total of 100 IDs for same challenge and 100 IDs for different challenge were obtained with 128-bit responses as an ID.

In the performance evaluation, same challenge intra-Hamming distance (SC Intra-HD) and different challenge intra-HD (DC Intra-HD) were used for Steadiness and Diffuseness which are typical PUF performance indicators [4]. Steadiness and Diffuseness are as follows.

- Steadiness is the performance that PUF outputs same responses for same challenges every time.
- Diffuseness is the performance that PUF outputs different response for different challenge.

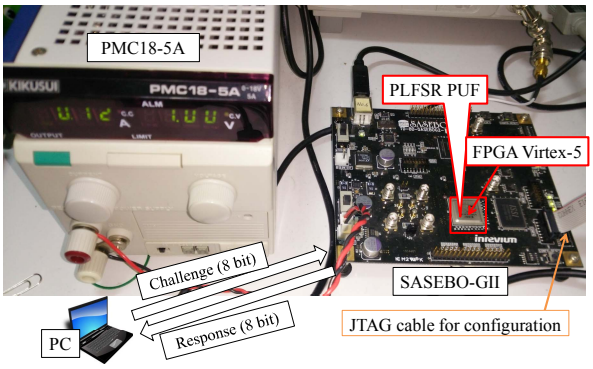


Figure 4. Evaluation system

TABLE I. EXPERIMENT CONDITION

PUF	PLFSR PUF
Active duration	1
Operation frequency	24 [MHz]
Voltage	1.00 [V]
# of boards	3
Evaluation board	SASEBO-GII
FPGA	Virtex-5 XC5VLX30
Power supply	PMC 18-5A
Development tool	Xilinx ISE Design Suite 14.1
Implementation tool	Xilinx PlanAhead v14.1
# of IDs	200

B. Experimental Results

Fig. 5 and Table II show the experimental results. Fig.5 (a), (b), and (c) show the results with board A, B, and C, respectively. Table II shows the average of each board. In Fig.5, the horizontal axis shows the HD between IDs and the vertical axis shows the frequency of HD. As shown in Fig.5 and Table II, in the MUX implementation, SC Intra-HD is smaller than it of the LUT implementation. Therefore, the MUX implementation can improve Steadiness than the LUT implementation since SC Intra-HD approaches 0 (PUF outputs same responses for same challenges).

Next, DC Intra-HD of each implementation approaches 64 which is half of the 128-bit ID. Therefore, Diffuseness is high regardless of implementation method (PUF outputs different response for different challenge).

V. CONCLUSION

This study implemented a PLFSR PUF by two implementation methods and evaluated the performance by using Steadiness and Diffuseness. Experiments using a FPGA clarified the MUX implementation could improve Steadiness than the LUT implementation.

Future works include the evaluation of PLFSR PUF with 128 cores in several implementation methods.

REFERENCES

[1] B. Gassend, D. E. Clarke, M. van Dijk, and S. Devadas, "Silicon Physical Random Functions," Proc. of the 18th Annual Computer Security Applications Conference, pp.148–160, Nov. 2002.

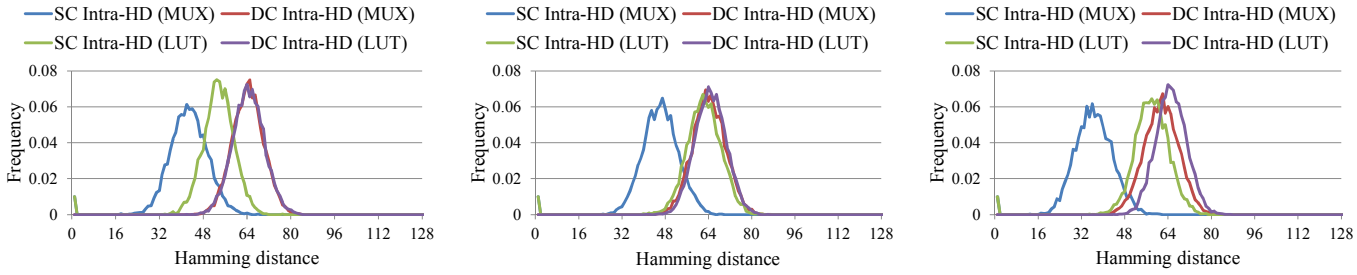
[2] Y. Hori, H. Kang, T. Katashita, and A. Satoh, "Pseudo-LFSR PUF: A compact, efficient and reliable physical unclonable function," Proc. of IEEE 7th Int. Conf. on ReConFigurable Computing and FPGAs (ReConFig'11), pp.223–228, Dec. 2011.

[3] Y. Hori, T. Katashita, H. Kang, A. Satoh, S. Kawamura, and K. Kobara, "Evaluation of Physical Unclonable Functions for 28-nm Process Field-Programmable Gate Arrays," Journal of Information Processing, vol.22, no.2, pp.344–356, 2014.

[4] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs," Proc. of IEEE 6th Int. Conf. on ReConFigurable Computing and FPGAs (ReConFig'10), pp.298–303, Dec. 2010.

TABLE II. AVERAGE OF RESULTS WITH EACH BOARD

		Board A	Board B	Board C
MUX impl.	**SC Intra-HD**	41.4	44.9	35.3
	DC Intra-HD	63.4	63.2	60.5
LUT impl.	**SC Intra-HD**	52.2	60.8	56.5
	DC Intra-HD	63.6	63.8	64.1



(a) Board A (b) Board B (c) Board C

Figure 5. Experimental results