Pseudo-LFSR PUF: A Compact, Efficient and Reliable Physical Unclonable Function

Yohei Hori*, Hyunho Kang*, Toshihiro Katashita* and Akashi Satoh*
Research Center for Information Security (RCIS)
National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Japan
Email: {hori.y, h-kang, t-katashita, akashi.satoh}@aist.go.jp

***Abstract*—A physical unclonable function (PUF) with a novel hardware architecture called *Pseudo-LFSR PUF* (*PL-PUF*) is developed. The structure of the PL-PUF is based on LFSR but it actually is large combinational logic. The long feedback signal of the PL-PUF effectively extracts the device variation, and consequently the output IDs generated in the different devices become completely dissimilar. The advantages of the PL-PUF are that (1) the size of the circuit is small since it simply consists of inverters and a few XOR gates, (2) it efficiently outputs a long-bit ID since all n bits of the ID are simultaneously output from a single n-bit challenge, and (3) the challenge-response mapping of PL-PUF can be easily changed without modifying its hardware structure. The reliability of the PL-PUF is also examined in terms of False Acceptance Rate (FAR) and False Rejection Rate (FRR) through the experimentation using FPGAs. The empirical results show that the intra-device Hamming distance among IDs generated in the same PL-PUF is quite small; the inter-device Hamming distance among IDs in different PL-PUFs is sufficiently large. As a consequent, it is demonstrated that the PL-PUF has quite low FAR/FRR and is quite effective for device identification and other security-sensitive applications. This paper describes the structure of the PL-PUF in detail and presents the experimental results of the performance evaluation using Virtex-5 FPGAs.**

***Keywords*-Physical Unclonable Function; Pseudo-LFSR PUF; SASEBO-GII; Virtex-5 FPGA; device authentication;**

I. Introduction

Nowadays Field-Programmable Gate Arrays (FPGAs) are widely used for consumer electronics, automotives, aerospace equipment and other various industrial products. Considering the fact that FPGAs are widespread among the vital and security-critical modules, protecting the confidentiality and integrity of FPGA bitstreams is of significant concern for both users and manufacturers. Since the bitstream is simply an electronic stream downloaded when the device is configured, it is always threatened by piracy such as illegal cloning and cracking.

For the security purpose, some of the recent FPGAs have an AES or Triple DES core to support encrypted bitstreams, and some of the latest FPGAs also have an HMAC core to enable bitstream authentication. However, the secret key of the encryption core embedded in the FPGA can be revealed by the state-of-the-art attack called *side-channel attack* [1], [2], which statistically analyzes the power consumption or electromagnetic emanation of the devices. Recently the bitstream security mechanisms of some FPGAs are reportedly broken by side-channel attacks [3], [4].

Considering the above situation, *Physical Unclonable Functions* (*PUFs*) [5] can be the solution to the security issues of FPGAs. A PUF is an object that outputs a device-specific response by extracting its intrinsic physical characteristics. A silicon PUF (hereafter simply "PUF") is a circuit constructed on semiconductor and outputs a unique ID by exploiting variation of gate length, threshold voltage, non-uniform density of impurity and so on. By using a PUF for key generation, the secret key need not be fixed in the FPGA, and therefore, the PUF can protect the device against side-channel attacks. Another novelty of using the PUF for FPGAs is that different IDs can be generated from the *same* bitstream. The bitstreams are common for all devices but the device-specific data are generated from the device variation. Note that the bitstream itself need not include any secret information. As a consequent, the bitstream of the PUF can be transferred over non-secure network channels.

Maes and Verbauwhede categorized PUFs into non-electronic PUFs, analog electronics PUFs, delay-based intrinsic PUFs and memory-based intrinsic PUFs [6]. Among these PUFs, the delay-based and memory-based ones can be applied to FPGAs. The examples of the delay-based PUFs are arbiter PUF [7], ring oscillator (RO) PUF [8], Glitch PUF [9], etc., and the examples of the memory-based PUFs include SRAM PUF [10], butterfly PUF [11], tri-state PUF [12], etc.

However, these PUFs have some shortcomings. The delay-based PUFs usually output only one- or several-bit response at once and consequently have low throughput. Memory-based PUFs output multiple bits in parallel but the output values are fixed; addressable memory-based PUFs are possible to output variable IDs but the circuit size becomes considerably large.

To eliminate these shortcomings, we developed a PUF with the new structure called *Pseudo-LFSR PUF* (*PL-PUF*). The structure of the PL-PUF is based on the Liner Feedback Shift Register (LFSR) but it actually does not consist of shift register; it composes large combinational logic. The PL-PUF efficiently outputs a long-bit and variable ID, and the size of the PL-PUF circuit is reasonably small. Furthermore, the challenge-response mapping of the PL-PUF is variable depending the active duration of the circuit, that is, a single PL-PUF behaves as if it has multiple different PUF cores.

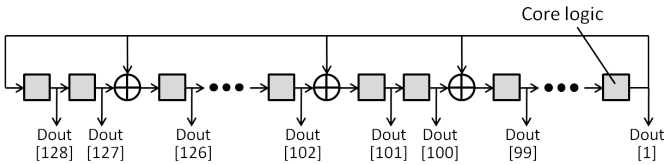

Figure 1. The structure of the Pseudo-LFSR PUF.

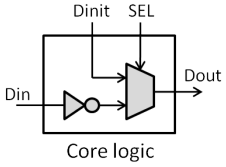

Figure 2. The structure of the core logic.

We implemented the PL-PUF to 16 FPGAs and evaluated its performances—reproducibility, individuality and multi-functionality. This paper explains the features of the PL-PUF in detail and demonstrates the effectiveness of PL-PUFs with the experimental results of the performance evaluation.

II. Pseudo-LFSR PUF

A PL-PUF is a delay-sensitive unclonable oscillator which realizes a compact, efficient and multi-functional PUF. A PL-PUF is not actually composed of a shift register but is large combinational logic based on the structure of LFSR. Figure 1 is the sketch of the 128-bit PL-PUF with the primitive feedback polynomial [13]

$$x^{128} + x^{126} + x^{102} + x^{99} + 1. \quad (1)$$

Note that in the PL-PUF, the core logic (Figure 2) is not a register but an inverter, and thus the PL-PUF composes a single combinational circuit. The output of the PL-PUF will oscillate since the output of the last core ($D_{out}(1)$) is fed back to the top-most core. The output value of the PL-PUF depends on the speed of the feedback signal, and the speed is significantly affected by the device variation. As a result, the output of the PL-PUF is expected to be device-dependent. The core logic is not necessarily an inverter. It can be any combinational logic that extracts the device variation as signal speed.

A PL-PUF realizes challenge-response pair (CRP) based authentication. In the case of Figure 1, the challenge is the 128-bit initial value given to the core logic, and the response (= ID) is the 128-bit output from the core logic. Note that only a single 128-bit challenge is necessary to generate a 128-bit ID.

After the initial value is set to each core logic, the PL-PUF is activated for c clock cycles. By changing the active duration c, the same PL-PUF will generate completely different outputs. This feature will be further examined in Section V.

The features of PL-PUF are summarized as follows:

- *Compact*
  The inverter-based PL-PUF achieves quite a small circuit. In the case of Figure 1, it requires only 128 inverters and 3 XOR gates. By comparison, an arbiter PUF has two selector chains and therefore a 128-stage arbiter PUF requires 256 multiplexers.
- *Efficient*
  A PL-PUF efficiently outputs long-bit IDs since all the 128 bits of the ID are generated from a single 128-bit challenge. This is a notable advantage of the PL-PUF when compared to other PUFs where only one- or several-bit output is generated from a long-bit challenge. By comparison, an arbiter PUF usually requires 128 CRPs to obtain a 128-bit ID.
- *Multi-functional*
  The output of the PL-PUF depends on the duration of the active clock cycles, and thus a single PL-PUF behaves like multiple PUFs by changing the active duration. That is, the challenge-response mapping of the PL-PUF can easily be changed without modifying its hardware structure. This property will lead the PL-PUF to being unclonable since cloning CRP mapping for all the possible durations is considered impractical.
- *Reliable*
  A PUF that is reliable is supposed to generate reproducible IDs which are unique among the devices. The PL-PUF has both high reproducibility and uniqueness, as will be demonstrated later. In addition, the reliability of the PL-PUF is configurable by changing the duration of the active clock cycles. A user can choose the duration which gives the preferable reliability.

III. Implementation

We implemented a 128-bit PL-PUF onto 16 FPGAs on SASEBO-GII evaluation boards [14]. SASEBO-GII is equipped with a Xilinx Virtex-5 XC5VLX30-1 and Spartan-3A, and the core voltage of the Virtex-5 can be changed by the variable resistor on the board. The PL-PUF is implemented on the Virtex-5 and the core voltage is set to 1.000 V.

The development tools used are Xilinx ISE 13.1 and PlanAhead v13.1. The PL-PUF is placed on the fixed area from SLICE_X0Y0 to SLICE_X7Y63.

IV. Experiments

A. Settings

Performance evaluation is done to the PL-PUFs implemented on the 16 FPGAs. The length of the ID is 128 bits and 100 kinds of IDs are generated from randomly generated 128-bit challenges. Each ID is generated 100 times under the same challenge for the test of reproducibility. Active duration c of the PUF is changed ranging from 1 to 16. The operation frequency of the PL-PUF is 24 MHz.

The SASEBO-GII board is connected to a personal computer (PC) via USB, and data input/output of the PL-PUF and other PUF operations are controlled by the PC.

B. Evaluation Strategy

To enable a comparison with the past study, we use the performance indicators presented in [15]: Randomness, Steadiness, Correctness, Diffuseness and Uniqueness. We also introduce a biometric strategy where PL-PUFs are evaluated by the following criteria:

- Reproducibility:
  Reproducibility is the *intra-device Hamming distance* (*intra-device HD*) among IDs generated under the same challenge and the same active duration. Obviously a PUF should have high reproducibility for the use of device identification, and in such a PL-PUF, the intra-device HD will ideally be 0.
- Individuality:
  Individuality of the PL-PUF is determined by False Acceptance Rate (FAR) and False Rejection Rate (FRR) as illustrated in Figure 3. FAR is the probability that a verifier wrongly accepts a different device as the target device, and FRR is the probability that a verifier wrongly rejects the target device. FAR and FRR are calculated from the intra-device HD given above and the *inter-device Hamming distance* (*inter-device HD*) among IDs generated under the same challenge and the same active duration. In the experiment, the threshold of the FAR and FRR is set to the HD giving the nearly-equal error rate (EER) where the FAR and FRR become approximately the same. Since the ID is 128-bit length, the inter-device HD will be 64 in the PL-PUF with the ideal individuality.
- Multi-functionality:
  Multi-functionality is the intra-device HD among IDs generated under the same challenge and the *different* active duration. We refer to this Hamming distance as *intra-device inter-duration HD*, or simply *inter-duration HD*. If the multi-functionality is high, the PL-PUFs activated for different duration will provide completely different IDs from the same challenge. Because the generated IDs are 128 bits in the experiment, the inter-duration HD will be 64 in the PL-PUF with the ideal multi-functionality.

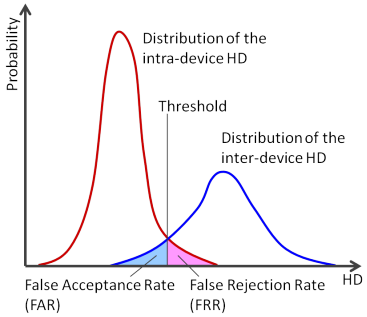

Figure 3. FAR and FRR of the PL-PUF.

Table I
THE PERFORMANCE OF THE PL-PUF EVALUATED BASED ON [15].

Active Duration	Randomness H	Steadiness S	Correctness C	Diffuseness D	Uniqueness U
1	0.984	0.982	0.979	0.988	0.656
2	0.975	0.966	0.960	0.987	0.728
3	0.964	0.954	0.947	0.985	0.746
4	0.967	0.925	0.913	0.989	0.755
5	0.966	0.878	0.859	0.990	0.766
6	0.944	0.804	0.775	0.988	0.772
7	0.969	0.726	0.686	0.989	0.776
8	0.960	0.622	0.572	0.988	0.772
9	0.967	0.516	0.460	0.985	0.773
10	0.964	0.415	0.357	0.978	0.771
11	0.966	0.324	0.269	0.974	0.760
12	0.964	0.253	0.203	0.958	0.756
13	0.964	0.200	0.155	0.950	0.744
14	0.962	0.165	0.126	0.929	0.739
15	0.965	0.145	0.109	0.914	0.738
16	0.963	0.131	0.097	0.900	0.734

The performance evaluation results are given and discussed in detail in the following section.

V. Results and Discussion

A. Performances Based on the Previous Criteria

Table I shows the evaluation results based on the criteria of the previous study [15]. As the space is limited, only the results of Device 1 are given in the table. The activated duration is varied ranging from 1 to 16. All the performance indicators range from 0 to 1, with 0 being the worst and 1 being the best performance.

Randomness and Diffuseness are stably high for all the active durations. Especially, Randomness is higher than that of the arbiter PUF in [15]. As a result, the PL-PUF is considered to have enough entropy for cryptographic purposes. Uniqueness of the PL-PUF is markedly higher than that of [15], and therefore the PL-PUF is considered suitable for the use of device identification. On the other hand, Steadiness and Correctness decreases as the active duration increases. This result indicates that the PL-PUF will fail to work as an ID generator when the active duration is too long, but can work as a random number generator.

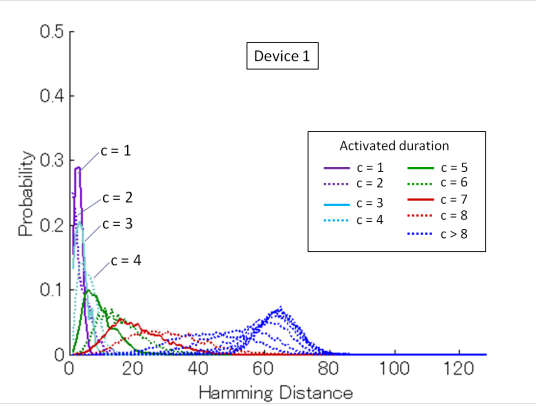

Figure 4. The distribution of the intra-device HD of Device 1.

B. Reproducibility

Here we evaluate the PL-PUF based on the biometric strategy. Figure 4 shows the probability distribution of the intra-device HD of Device 1. As the figure shows, when the active duration is short, the intra-device HD is quite small and consequently the reproducibility of the ID is quite high. On the other hand, the intra-device HD approaches 64 as the active duration increases, which indicates that the output of the PL-PUF is almost random.

Table II shows the means and deviations of the intra-device HDs of the PL-PUFs. In the table the eight devices out of 16 are listed due to the space limitation. As Figure 4 and Table II shows, the active duration of the PL-PUF can not be arbitrary clock cycles; it should be reasonably short for the reproducibility.

C. Individuality

Figure 5-8 show the intra-device HD of Device 1 and the inter-device HDs between Device 1 and the other devices. The duration of the active clock cycles are 1, 4, 8 and 16, respectively. When the active duration is short, the shapes of the distributions of the intra- and inter-device HD are sharp, and thus FAR and FRR are both zero (Figure 5 and 6). In Figure 7, the FAR and FRR become more than zero but sufficiently low, and thus Device 1 still looks distinguishable from other devices. When the active duration gets much longer, Device 1 can no more be identified since its intra- and inter-device HD distributions are indistinguishable (Figure 8).

Table III shows the FAR and FRR of the PL-PUFs under the active duration from 1 to 16. In the table, the FAR and FRR of the 8 devices out of 16 are described. As the table shows, the FAR and FRR get worse as the active duration of the PUF increases.

As Figure 5-8 and Table III show, the individuality of the PL-PUF are quite high under the sufficiently short active duration. However, a too much short active duration is not always preferable for individuality as the figures and table indicate. For example in Device 4 and 5, the FAR and/or FRR are more than zero for $c = 1$ but are zero for $c = 2$. The reason of the result is that the device variation is not fully extracted when the active duration is too much short.

D. Multi-functionality

Table IV shows the intra-duration HDs of the same device under the different active durations. We obtained the Hamming distance between the ID under $c = 1$ (ID_1) and IDs under the other durations (ID_c, $2 \leq c \leq 16$). As the table shows, the average inter-duration HDs between ID_1 and other ID_c are nearly 64 and the deviations are reasonably small. As a result, the outputs of the PL-PUF are considered quite dissimilar under the different active durations, and thus a single PL-PUF can equivalently operate as a chip with several PUF cores. This property could shrink the area of the circuit of the system adopting the 'defense-in-depth' strategy where multiple PUFs are needed. Additionally, this property could lead the PUF to being unclonable since cloning the challenge-response mapping for all the possible durations is considered impractical.

E. Overall Discussion

Considering the above results, the PL-PUF is thought to have notably high reproducibility and individuality, and therefore it is quite useful for device identification and other security-sensitive applications. That is, the PL-PUF realizes efficient ID generation without spoiling the reliability. The PL-PUF also has high multi-functionality, which is expected to lead the circuit to being compact and unclonable.

The suitable duration of the operation will differ from application to application. If the output of the PUF is used for secret key generation in the cryptographic modules, the reproducibility should be sufficiently high. We might want to restrict the bit error rate of the output to less than 10%, and in this case the active duration of less than 4 would be reasonable. If the output is used for device identification, it is required that the intra- and inter-HD distributions are distinguishable, and therefore the active duration less than 8 will suffice for the purpose.

VI. Conclusions

We developed a PUF with novel structure called a Pseudo-LFSR PUF (PL-PUF) and empirically demonstrated its feasibility and effectiveness. The PL-PUF realizes a compact, efficient, multi-functional and reliable device ID generator. The experimental results show that the PL-PUF has quite high reproducibility and low FAR/FRR, and consequently the PL-PUF is quite useful for device identification and other applications. The future work of this study is to implement the PL-PUF to more devices and evaluating the performance of them. Another future work is to evaluate the security against the existing attacks such as model-building attacks.

Table II
THE MEANS AND DEVIATIONS OF THE INTRA-DEVICE HDS.

Active duration	Device 1		Device 2		Device 3		Device 4		Device 5		Device 6		Device 7		Device 8	
	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ
1	1.76	1.18	2.84	1.85	3.33	2.25	2.33	1.98	2.11	1.76	5.39	4.33	3.52	2.27	0.51	0.90
2	2.60	2.64	3.36	2.27	2.12	1.76	2.83	1.97	1.29	1.15	7.71	5.90	2.45	1.87	3.08	1.89
3	2.61	1.89	7.20	4.42	4.70	3.11	2.28	1.87	3.75	2.86	16.55	10.92	5.35	2.47	7.41	3.56
4	4.70	2.79	11.89	7.50	5.21	4.14	6.07	3.21	4.35	3.51	21.28	11.50	14.12	6.15	9.74	5.85
5	8.18	4.59	18.62	10.13	8.82	4.68	10.63	5.52	8.18	3.44	22.84	12.13	18.52	8.10	14.83	7.50
6	14.59	6.68	30.20	14.90	15.86	8.92	15.82	6.86	18.71	7.21	33.91	15.30	23.20	9.16	19.68	7.66
7	19.76	8.35	36.01	15.86	20.44	8.90	25.12	8.48	31.27	10.89	34.25	15.05	31.15	10.15	32.90	10.74
8	29.13	10.91	37.37	12.27	32.10	11.09	32.02	10.96	34.07	9.64	41.33	16.04	43.70	10.32	41.44	10.16
9	42.28	11.21	40.37	12.21	40.11	13.25	41.21	12.02	42.71	10.15	44.70	14.74	47.56	9.90	49.26	10.89
10	50.40	10.25	46.05	10.29	46.91	13.16	46.12	9.85	50.46	11.11	49.97	12.08	54.21	8.24	55.20	9.16
11	57.87	8.49	52.35	9.47	56.67	9.93	54.72	8.73	56.07	8.04	53.79	8.78	60.08	7.39	57.81	7.24
12	61.06	7.18	57.67	7.63	57.89	8.58	58.93	7.68	59.31	6.86	55.41	7.86	61.52	6.42	59.52	6.49
13	62.57	6.32	57.75	6.38	61.32	6.91	61.08	6.98	60.08	6.41	60.28	7.33	62.77	5.97	60.52	6.24
14	63.31	6.01	59.50	6.34	62.26	6.19	63.29	6.09	60.93	5.96	62.27	6.55	62.73	5.99	61.78	5.98
15	63.61	5.99	59.44	6.38	63.31	6.07	63.62	5.93	61.80	6.31	62.93	6.54	63.61	6.01	61.26	6.10
16	63.56	5.91	61.65	6.11	63.65	5.92	64.03	5.93	61.38	6.20	62.52	6.38	63.59	6.00	61.62	5.89

Table III
THE FAR AND FRR OF THE DEVICES.

Active duration	Device 1		Device 2		Device 3		Device 4		Device 5		Device 6		Device 7		Device 8	
	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
1	0.00	0.00	0.00	0.00	0.00	0.00	0.91	0.71	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00
2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.89	0.81	0.00	0.00	0.00	0.00
4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.48	0.26	0.00	0.00	0.00	0.00
5	0.00	0.00	0.70	0.63	0.00	0.00	0.00	0.00	0.00	0.00	2.08	2.85	0.12	0.10	0.00	0.00
6	0.01	0.02	7.13	6.97	0.00	0.04	0.00	0.04	0.10	0.06	8.65	7.94	0.30	0.26	0.00	0.00
7	0.42	0.42	11.26	10.02	0.41	0.32	0.06	0.08	2.35	2.51	10.12	9.19	2.53	1.80	2.93	2.44
8	2.61	2.97	7.93	6.46	3.90	3.45	1.64	1.78	3.04	3.01	16.64	15.54	11.98	10.79	8.79	8.93
9	11.39	13.19	11.04	13.19	10.91	11.94	8.82	7.98	8.83	9.62	15.87	18.42	13.57	16.22	19.20	22.95
10	25.32	22.55	14.25	16.04	24.20	20.63	13.43	14.08	21.41	24.04	25.46	21.84	22.85	22.97	32.43	34.26
11	39.79	35.41	25.93	27.27	35.33	34.34	22.04	25.05	30.04	34.59	26.17	27.25	39.96	38.46	39.48	36.57
12	44.87	44.18	39.96	37.49	35.84	35.19	35.97	37.88	42.45	38.61	27.67	32.26	44.28	38.30	43.05	38.95
13	48.88	44.55	39.21	33.43	41.10	44.57	39.34	42.77	44.00	41.27	41.18	40.36	43.56	45.56	43.15	43.43
14	49.36	48.71	43.64	37.82	45.75	42.46	44.55	49.09	42.04	46.59	46.40	42.61	43.88	45.09	47.70	45.64
15	48.94	49.94	37.77	42.97	46.31	48.89	44.65	50.91	48.22	45.76	45.49	46.91	44.37	50.89	42.84	48.46
16	49.50	50.08	48.34	43.96	47.92	51.13	52.91	47.52	48.28	42.55	46.28	43.56	45.54	50.91	48.63	44.44

Table IV
THE MEANS AND DEVIATIONS OF THE INTER-DURATION HAMMING DISTANCE BETWEEN ID_1 AND OTHER ID_c.

Active duration	Device 1		Device 2		Device 3		Device 4		Device 5		Device 6		Device 7		Device 8	
	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ	μ	σ
ID_2	59.72	1.23	60.36	2.15	56.09	1.11	59.30	1.87	67.24	1.32	62.24	2.40	67.41	1.99	69.45	2.73
ID_3	58.64	1.66	59.73	1.83	71.11	1.73	45.77	1.52	59.13	1.78	76.45	2.25	68.01	1.98	65.77	2.07
ID_4	63.30	1.55	72.16	2.86	64.88	2.70	59.18	1.63	70.18	2.20	69.94	3.58	76.94	2.25	59.86	4.08
ID_5	77.56	2.25	58.47	2.69	65.81	2.64	63.40	1.48	56.26	2.62	63.44	3.42	61.88	3.03	59.19	3.84
ID_6	66.07	2.53	75.64	5.65	60.54	3.02	65.19	3.55	57.81	3.62	65.67	3.31	73.94	2.47	61.54	4.34
ID_7	67.39	3.76	70.48	4.49	66.31	4.09	54.15	1.69	66.35	4.31	67.49	5.75	61.72	2.66	60.79	5.28
ID_8	64.43	4.00	65.45	3.78	70.22	3.81	58.49	3.80	62.83	3.87	63.70	5.53	57.52	4.08	65.30	6.30
ID_9	68.14	3.87	66.95	5.04	59.29	4.07	65.84	3.57	63.09	4.88	59.87	6.63	61.64	5.10	64.96	6.11
ID_{10}	56.90	5.09	59.45	4.59	59.59	5.65	61.50	4.14	64.43	6.13	60.49	6.14	63.26	5.20	63.82	5.75
ID_{11}	63.22	5.55	66.70	5.27	59.78	5.01	58.74	4.65	61.39	5.43	72.35	5.87	61.07	4.73	64.94	6.56
ID_{12}	65.75	6.00	64.32	6.84	64.84	6.43	57.52	6.49	61.07	4.90	65.09	5.85	66.57	5.45	63.71	6.23
ID_{13}	61.83	5.47	60.74	5.65	65.27	6.27	61.05	6.02	61.30	5.47	62.96	6.11	64.27	5.29	64.09	6.47
ID_{14}	60.73	5.95	62.78	6.37	66.30	6.08	61.47	5.17	64.96	6.33	63.63	6.90	64.13	6.23	65.29	6.14
ID_{15}	63.94	5.98	63.63	5.76	63.67	6.00	59.08	6.44	64.58	5.85	63.73	6.38	64.15	6.16	65.05	6.17
ID_{16}	63.27	6.10	63.69	6.16	65.09	6.68	61.77	7.49	64.27	6.11	63.40	6.54	63.39	6.44	64.88	5.37

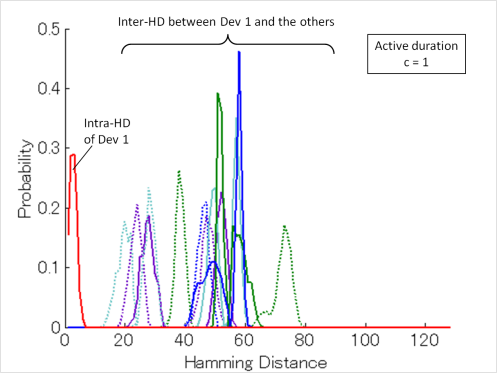

Figure 5. The distribution of the inter-device HD of Device 1 under the active clock duration is 1.

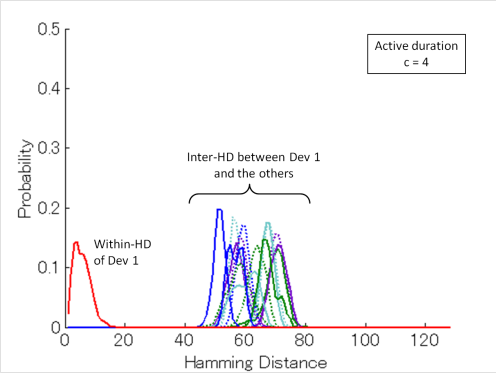

Figure 6. The distribution of the inter-device HD of Device 1 under the active clock duration is 4.

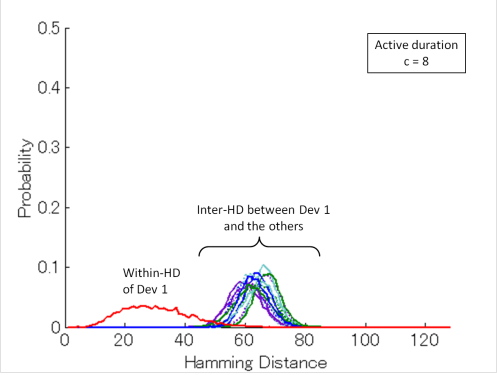

Figure 7. The distribution of the inter-device HD of Device 1 under the active clock duration is 8.

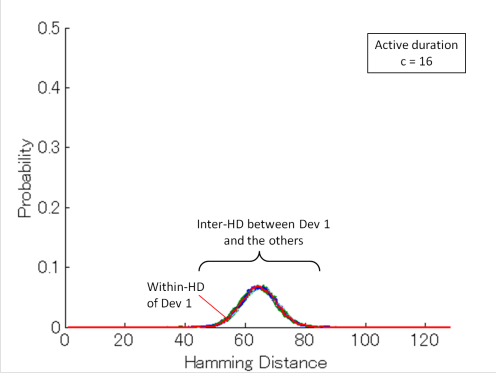

Figure 8. The distribution of the inter-device HD of Device 1 under the active clock duration is 16.

REFERENCES

[1] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems," in *CRYPTO'96*, 1996, pp. 104–113.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO'99*, 1999, pp. 388–397.

[3] A. Moradi, A. Barenghi, T. Kasper, and C. Parr, "On the vulnerability of FPGA bitstream encryption against power analysis attacks—extracting keys from Xilinx Virtex-II FPGAs," Cryptology ePrint Archive, 2011.

[4] A. Moradi, M. Kasper, and C. Paar, "On the portability of side-channel attacks –an analysis of the Xilinx Virtex 4 and Virtex 5 bitstream encryption mechanism," Cryptology ePrint Archive, 2011.

[5] S. R. Pappu, "Physical one-way functions," Ph.D. dissertation, MIT, 2001.

[6] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*, A.-R. Sadeghi and D. Naccache, Eds. Springer-Verlag, 2010, ch. 1, pp. 3–37.

[7] 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, 2005.

[8] G. E. Suh and S. Devadas, "Physical physical unclonable functions for device authentication and secret key generation," in *DAC'07*, 2007, pp. 9–14.

[9] D. Suzuki and K. Shimizu, "The glitch PUF: A new delay-PUF architecture exploiting glitch shapes," in *Proc. CHES2010*, 2010, pp. 366–382.

[10] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *CHES'07*, 2007, pp. 63–80.

[11] S. S. Kumar, J. Guajardo, R. Maesyz, G.-J. Schrijen, and P. Tuyls, "The butterfly PUF," in *HOST'08*, 2008, pp. 67–70.

[12] E. Ozturk, G. Hammouri, and B. Sunar, "Physical unclonable function with tristate buffers," in *ISCAS'08*, 2008, pp. 3194–3197.

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

[14] S. Akashi, K. Toshihiro, and S. Hirofumi, "Secure implementation of cryptographic modules—development of a standard evaluation environment for side channel attacks," *Synthesiology*, vol. 3, no. 1, pp. 56–65, 2010.

[15] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," in *Proc. ReConFig2010*, 2010, pp. 298–303.