Journal of Information Processing Vol.22 No.2 344–356 (Apr. 2014)

[DOI: 10.2197/ipsjjip.22.344]

Recommended Paper

Evaluation of Physical Unclonable Functions for 28-nm Process Field-Programmable Gate Arrays

Yohei Hori[1,a)] Hyunho Kang[2] Toshihiro Katashita[1] Akashi Satoh[3] Shinichi Kawamura[1,4] Kazukuni Kobara[1]

Received: May 2, 2013, Accepted: December 4, 2013

Abstract: In this study, the properties of physical unclonable functions (PUFs) for 28-nm process field-programmable gate arrays (FPGAs) are examined. A PUF is a circuit that generates device-specific IDs by extracting device variations. Owing to device variation, no two PUFs will generate the same ID even if they have identical structures and are manufactured on the same silicon wafer. However, because the influence of device variation increases as the size of the process node shrinks, it is uncertain whether PUFs can be built using recently developed small-scale process nodes, even though the technology of variation control is constantly advancing. While many PUFs using 40-nm or larger process nodes have been reported, smaller devices have not yet been studied to the authors' knowledge, and this is the first published journal article on PUFs for 28-nm process FPGAs. In this paper, within-die reproducibility, die-to-die uniqueness, and other properties are evaluated, and the feasibility of PUFs on 28-nm FPGAs is discussed.

Keywords: physical unclonable function (PUF), arbiter PUF, pseudo-LFSR PUF (PL-PUF), SASEBO-GIII, Kintex-7, Artix-7, performance evaluation

1. Introduction

Critical infrastructures of modern society, such as the electricity grid and transportation network, administrative services, national defense, and consumer electronics cannot be maintained without the use of semiconductor-driven devices. In the near future, the vast majority of devices including mobile phones, home appliances, automotive systems, and various sensors will be interconnected, forming a huge network called the machine-to-machine (M2M) network or the Internet of things (IoT). In the M2M/IoT, devices will automatically exchange and accumulate all types of information without human intervention. The market size of M2M is predicted to be 1,2 trillion U.S. dollars in 2020 [19]. A darker side to this economy, however, involves the counterfeiting of electronic parts, which was reported in 2011 to have cost defrauded consumers 169 billion U.S. dollars [13]. In one example of this, more than one million counterfeit electronic parts were found to have been purchased by the U.S. Department of Defense [2]. Considering that semiconductor devices are extensively used in critical infrastructures, such counterfeit electronic parts can cause destructive or even fatal damage along with monetary losses to society. It is therefore urgent to eliminate counterfeit parts from the market.

Two-dimensional codes and radio-frequency identification (RFID) tags are widely used to detect and prevent the dissemination of counterfeit products. However, as two-dimensional code tags can be easily cloned, their use is unsuitable for high security purposes. RFID tags typically have non-volatile memories that include an identification number, but the data inside such memories can be extracted relatively easily, allowing a tag to be cloned. On the other hand, tamper-resistant modules such as trusted platform modules (TPMs) [12] can function at high levels of security by performing cryptographic authentication based on a secret cipher located in a non-volatile memory. However, the same key in memory is usually used repeatedly for both encryption and decryption, making it vulnerable to extraction by side-channel attacks (SCAs) [15], [16], a form of attack that exploits side-channel information, e.g., power consumption, electromagnetic emanation, or processing time from the cryptographic device in order to extract the secret key within. As SCAs require large amounts of side-channel data from a given secret key, repeated use of the same key can render it vulnerable to such attacks.

Physical unclonable functions (PUFs) [21] are considered a promising approach to developing device-specific secret keys, without using a non-volatile memory. A PUF is a mathematical or physical structure that numerically converts physical features into device-specific information; for example, the fabric structure of a banknote can be translated into a numerical ID that can be used to detect counterfeit bills using a PUF [1]. In this paper,

1 National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Ibaraki 305–8568, Japan
2 Tokyo University of Science, Katsushika, Tokyo 125–8585, Japan
3 The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
4 Toshiba Corporation, Kawasaki, Kanagawa 212–8582, Japan
a) hori.y@aist.go.jp

The initial version of this paper was presented at DICOMO2012 held between July 4 and 6 in 2012. This paper was recommended to be submitted to Journal of Information Processing (JIP) by the chairman of SIGCSEC.

we will examine a silicon PUF constructed on a semiconductor device. This device (hereafter referred to simply as a PUF) is a circuit that extracts chip device variations in order to create sets of chip-specific information. As it is impractical to clone such device variations, this PUF can be considered unclonable.

As the miniaturization of complementary metal-oxide-semiconductor (CMOS) transistors progresses, device variation becomes a more serious problem in terms of potential disruption to chip operation, although the technology for controlling device variation has also made significant progress. It has therefore been entirely unclear whether PUFs can be fabricated using state-of-the-art semiconductor manufacturing processes. Many studies to date have concentrated on the manufacture of PUFs on 40-nm and larger process nodes [4], [8], [9]; however, no documented research has closely investigated PUFs using smaller transistor nodes. Although researchers have conducted preliminary experiments on arbiter PUFs (APUFs) and pseudo-LFSR PUFs (PL-PUFs) using 28-nm FPGAs [10], their results have been insufficient in providing insight into the properties of PUFs on small process nodes. In this paper, which is an extended version of Refs. [9] and [10], we closely examine the properties of PUFs for 28-nm process FPGAs. To do so, we have tested the APUF [24], one of the most popular PUFs worldwide, and a PL-PUF previously proposed by the authors [8]. In this paper, the properties of these two PUFs fabricated on 28-nm Kintex-7 [28] and Artix-7 [28] are studied and compared with the results obtained from previous PUFs fabricated using 65- and 45-nm process nodes.

2. Physical Unclonable Functions

Even though IC chips are manufactured using identical design data, the delay of the same signal or the initial state on a given memory bit differs among chips because of device variation. Therefore, the signal delay and initial memory state can be used to generate chip-specific information. Arbiter and PL-PUFs can be classified as delay-based PUFs, with other examples of such devices including ring oscillators [5] and glitch PUFs [25]. Examples of memory-based PUFs include SRAMs [7] and butterfly PUFs [18].

In this section, we describe the general properties of PUFs and then explain the features of APUFs and PL-PUFs.

2.1 PUF Properties

A PUF usually generates an output based on a challenge-response procedure, with the challenge (input) and response (output) data pair called the challenge-response pair (CRP). The physical implementation of a PUF Π is a function that maps the group of challenges $\mathcal{X}$ to the group of responses $\mathcal{Y}$ that can be expressed as:

$$\Pi := \mathcal{X} \to \mathcal{Y}, \tag{1}$$

and

$$\Pi(x) = y \ \ (x \in \mathcal{X}, y \in \mathcal{Y}). \tag{2}$$

Although a general definition of PUFs has not been developed, Maes and Verbauwhede described the properties of a PUF as follows [20]:

(1) **Evaluatable**: given Π and x, it is easy to evaluate $y = \Pi(x)$.
(2) **Unique**: $\Pi(x)$ contains some information about the identity of Π.
(3) **Reproducible**: $y = \Pi(x)$ is reproducible up to a small error.
(4) **Unclonable**: given Π, it is difficult to construct $\Gamma \neq \Pi$ such that $\forall x \in \mathcal{X} : \Gamma(x) \approx \Pi(x)$
(5) **Unpredictable**: given a set $Q = \{(x_i, y_i = \Pi(x_i))\}$ and x_c such that $(x_c, \cdot) \notin Q$, it is difficult to predict $y_c \approx \Pi(x_c)$ up to a small error.
(6) **One-way**: given only y and Π, it is difficult to find x such that $\Pi(x) = y$.
(7) **Tamper evident**: altering the physical entity Π transforms $\Pi \to \Pi'$, such that with a high probability $\exists x \in \mathcal{X} : \Pi(x) \neq \Pi'(x)$.

Komano et al. [17] produces eight PUF properties by dividing item 4 above into two types: physically unclonable and mathematically unclonable, defining the PUF family as the group of physical entities having all eight properties.

2.2 Arbiter PUF

As shown in **Fig. 1**, an APUF consists of two selector chains in which selected signals input into the selectors comprise the challenge, and the signal output from the arbiters is the response. If the upper signal reaches the arbiter earlier than the lower one, the response is 1; otherwise, it is 0. The path of the selector chains taken—and, consequently, the delay difference between two signals is determined by the challenge; thus, the response is also a function of the challenge [*1]. The procedure followed by the APUF Π^{APUF} is expressed mathematically as follows:

$$\Pi^{\mathrm{APUF}} := \{0,1\}^n \to \{0,1\}. \tag{3}$$

Because the speeds of the two signals in the selector chains are greatly affected by device variation, the response to a given challenge will not always be the same from different APUFs; therefore, a set of APUF CRPs constitutes chip-specific information that can be used for chip authentication.

2.3 PL-PUF

A PL-PUF is a delay-based PUF having a similar structure to that of a linear-feedback shift register (LFSR). Although a PL-PUF is not actually composed of shift registers, it instead comprises a large combinational logic consisting of multiplexers and inverters. **Figure 2** is a sketch of a 128-bit PL-PUF with the irreducible feedback polynomial [6]

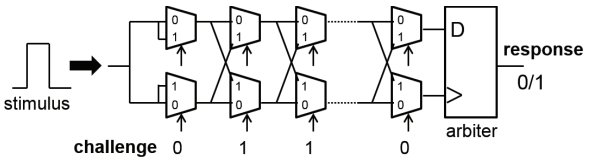

Fig. 1 The structure of an APUF.

[*1] The response fluctuates slightly owing to thermal noise, etc., as given by the mathematically non-rigorous relation *function*.

Table 1 Comparison of Nexys4, SASEBO-GIII, -W and -GII.

	Nexys4	SASEBO-GIII	SASEBO-W	SASEBO-GII
Board Size	109 × 121 mm^2	150 × 200 mm^2	150 × 200 mm^2	120 × 140 mm^2
FPGA for Cipher Module	28-nm Artix-7 100T (15,850 slices)	28-nm Kintex-7 325T (50,950 slices)	Smart card slot (23,038 slices)	65-nm Virtex-5 LX30/50 (4,800 / 7,200 slices)
FPGA for Control Logic	-	45-nm Spartan-6 LX45	45-nm Spartan-6 LX150	90-nm Spartan-3A 400
Serial Bus	USB-UART (RS232)	USB 2.0 (480 Mbps)	USB 2.0 (480 Mbps)	USB 1.0 (12 M bps)
Expansion Connectors	Four Pmod Connectors	Two FMCs (LPC)	64-bit header pins	Two 32-bit header pins
On-board Memory	128 M-bit CellularRAM	1 G-bit DDR3-SDRAM	-	2 M-bit SSRAM

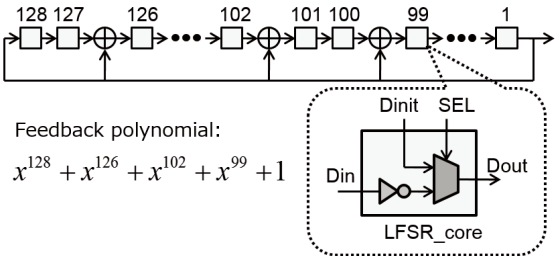

Fig. 2 Structure of a PL-PUF.

$$x^{128} + x^{126} + x^{102} + x^{99} + 1. \quad (4)$$

The operation of the PL-PUF can be summarized as follows. First, the initial vector (D_{init}) is set to the PL-PUF, and the select signals (SELs) of the multiplexers are set to the output D_{init}. Then, the SEL signals are flipped to activate the PL-PUF, and $D_{out} = D_{in}$; consequently, the PL-PUF starts to oscillate. After the PL-PUF has been activated for several clock cycles, D_{out} is latched and output as a response. The activated clock cycle is hereafter called the *active duration*.

While typical delay-based PUFs such as the APUF have an n-bit challenge (where typically $64 \leq n \leq 256$) and only a 1-bit response, a PL-PUF has both an n-bit challenge and an n-bit response. Mathematically, the procedure followed by a PL-PUF Π^{PL-PUF} is expressed as follows:

$$\Pi^{PL-PUF} := \{0,1\}^n \rightarrow \{0,1\}^n. \quad (5)$$

The throughput of a PL-PUF is correspondingly much higher than that of a typical delay-based PUF. In addition, the CRP property of a PL-PUF can be changed according to the active duration, and thus several families of PUFs can be realized with a single PL-PUF implementation. Furthermore, a short response to an unknown challenge can be predicted by means of machine learning [22], although the PUF will not be secure as the unpredictability property will be broken. Thus, machine learning is considered difficult to apply to PL-PUFs.

3. Test Environment

To study the properties of APUFs and PL-PUFs on 28-nm process FPGAs, we use SASEBO-GIII and Nexys4 [3] boards as the test environment. The main specifications of the boards are explained in the following subsections.

3.1 SASEBO-GIII

The latest version of the side-channel attack standard evaluation board (SASEBO), SASEBO-GIII, is equipped with a 28-nm process Kintex-7 FPGA to enable the testing of SCAs for state-of-the-art transistor nodes and a Spartan-6 FPGA for implementing control logic. Power can be supplied to the board externally and via USB.

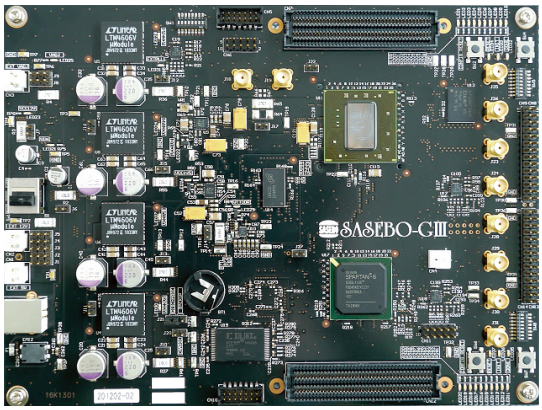

Fig. 3 Appearance of SASEBO-GIII.

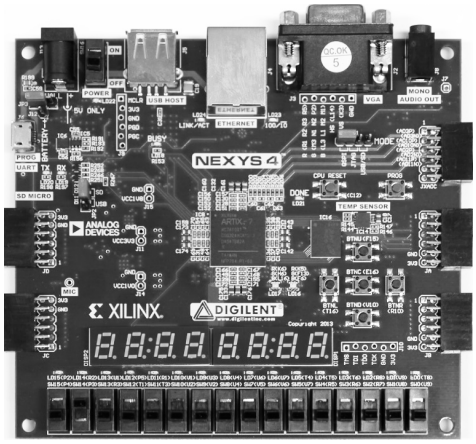

Fig. 4 Appearance of Nexys4.

SASEBO-GIII is chosen for the test environment because peripheral controllers, e.g., a controller communicating with a host PC, can be implemented on Spartan-6 so that PUFs on Kintex-7 can run in a low-noise environment. As far as authors know, SASEBO-GIII is the only off-the-shelf board equipped with a 28-nm FPGA along with a control FPGA that enables such a low-noise PUF implementation.

Figure 3 shows an image of a SASEBO-GIII, while **Table 1** shows a performance comparison with the previous SASEBO-W and -GII.

3.2 Nexys4

Nexys4 is an FPGA board provided by Digilent. Nexys4 is equipped with a 28-nm process Artix-7 FPGA, which is a low-price edition of Xilinx 7-series FPGAs. Nexys4 is chosen to compare the results of PUF implementations on two kinds of 28-nm FPGAs: Kintex-7 on SASEBO-GIII and Artix-7 on Nexys4.

Likewise SASEBO-GIII, power can be supplied to the board externally and via USB. **Figure 4** shows an image of a Nexys4, and Table 1 includes the specifications of the board.

4. Experimental Setup

4.1 Implementation of the PUFs

The APUF and PL-PUF are implemented on ten Kintex-7s on SASEBO-GIIIs and eight Artix-7s on Nexys4s. The selector stages of the APUF are set to 64 and 128. Therefore, the challenge length is 64 or 128 bits, and the response length is 1 bit. In the 64-stage APUF, one of the two selector chains is placed on SLICE_X1Y0 through SLICE_X1Y63 and the other on SLICE_X5Y0 through SLICE_X5Y63. The arbiter is placed on SLICE_X3Y65 CFF. In the 128-stage APUF, the selector chains are placed on SLICE_X1Y0 through SLICE_X1Y127 and SLICE_X5Y0 through SLICE_X5Y127. The arbiter is placed on SLICE_X3Y129 CFF.

The 64-stage APUF is labeled APUF64 or APUF64-K7-01 to explicitly specify the chip used (in this case, the first Kintex-7 out of ten). Likewise, the 128-stage APUF is labeled APUF128 or APUF128-K7-01 and so on. The 64- and 128- stage APUFs on the first Artix-7 are labeled APUF64-A7-01 and APUF128-A7-01, respectively, and so on.

In the PL-PUF, five types of active durations ($c = 1, 2, 4, 8, 16$) are tested with a single implementation. The PL-PUF with active duration 1 is called PL-PUF01, and a similar labeling scheme applies up to PL-PUF16. To explicitly specify the used chip, the PUFs are labeled PL-PUF01-K7-01, PL-PUF01-A7-01 and so on. The feedback polynomial used is the same as Eq. (4). Therefore, the challenge and response are 128 bits.

4.2 Test Parameters

In both the APUF and PL-PUF, the length of an ID is 128 bits. In the APUF, 128 different 64-/128-bit challenges are required to generate a single ID, whereas only one 128-bit challenge is required to generated a single ID in the PL-PUF. In our experiments, 1,024 different IDs are generated, and each ID is repeatedly generated 128 times. Therefore, a total of 131,072 IDs are generated for each chip in APUFs. In the PL-PUF, 131,072 IDs are generated for each active duration; thus, a total of 655,360 IDs are generated for each chip.

The operating frequency is 24 MHz for both PUFs. Thus, the active duration $c = 1$ indicates an oscillating time of 41.67 ns.

4.3 Evaluation Criteria

The performances of the APUF and PL-PUF are evaluated on the basis of the probability distribution of the Hamming distance (HD) among the generated IDs. There are four types of HD distributions: the same-challenge within-die Hamming distance (SC-wid HD), the different-challenge within-die Hamming distance (DC-wid HD), the same-challenge die-to-die Hamming distance (SC-d2d HD), and the different-challenge die-to-die Hamming distance (DC-d2d HD). These distributions are explained as follows:

- **SC-wid HD**: Hamming distance among IDs generated from the same challenge set on the same chip embedding the PUF. If the SC-wid HD of the PUF is small, the same ID is generated with a small error, and thus, the PUF is likely to be reproducible.
- **DC-wid HD**: Hamming distance among IDs generated from a different challenge set on the same chip embedding the PUF. If the DC-wid HD is close to 50% of the ID length, the generated IDs are likely to be distinct from each other.
- **SC-d2d HD**: Hamming distance among IDs generated from the same challenge set on different chips embedding PUFs. If the SC-d2d HD is close to 50% of the ID length, the chips embedding the PUFs are likely to be distinct from each other.
- **DC-d2d HD**: Hamming distance among IDs generated from different challenge sets on different chips embedding PUFs. If the DC-d2d HD is close to 50% of the ID length, the generated IDs are not likely to collide with each other.

Among these HDs, the SC-wid and SC-d2d HD are the most useful for obtaining the false acceptance rate (FAR) and false rejection rate (FRR), as shown in **Fig. 5**. The FAR is the probability of a counterfeit chip being accepted as genuine, whereas the FRR is the probability of genuine chip being rejected as counterfeit. In this study, the FAR is the area of the SC-d2d HD distribution in which SC-d2d HD $\leq$ SC-wid HD, and the FRR is the area of the SC-wid HD distribution in which SC-wid HD $<$ SC-d2d HD.

4.4 Performance Indicators

Besides FAR and FRR, the quantitative evaluation criteria are given in Ref. [8]. In Ref. [8], the following five indicators are proposed to quantify the properties of PUFs:

- **Randomness** (H): Balance between 0s and 1s in the responses of the PUF.
- **Steadiness** (S): Degree of how stably a PUF outputs the same responses to the same challenge sets.
- **Correctness** (C): Degree of accuracy of PUF outputs.
- **Diffuseness** (D): Degree of difference between IDs generated from different challenge sets in the same device.
- **Uniqueness** (U): Degree of difference between IDs generated from the same challenge sets in different devices.

The notation used in these indicators are given in **Table 2**. Let H_n be the randomness of the n-th device, and similar applies to S_n, C_n, D_n and U_n. Then, the performance indicators of the n-th

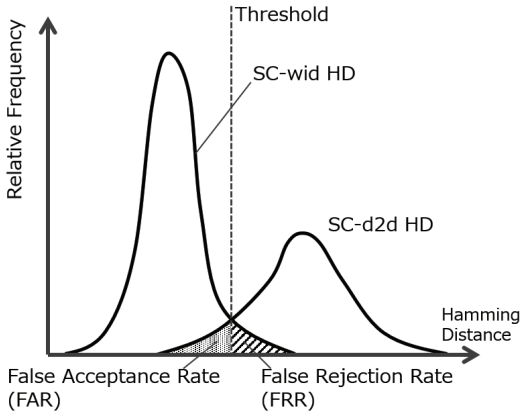

Fig. 5 False acceptance rate (FAR) and false rejection rate (FRR) derived from the distributions of SC-wid and SC-d2d HD.

Table 2 The notation used in the article.

Notation	Explanation
N	The number of devices.
K	The number of different IDs generated per device.
T	The number of tests performed per ID.
L	The length of an ID.
n	The index of a device. The n-th device is denoted by n for simplicity if not confusing. $1 \le n \le N$.
k	The index of an ID. The k-th ID is denoted by k for simplicity if not confusing. $1 \le k \le K$.
t	The index of a test. The t-th test is denoted by t for simplicity if not confusing. $1 \le t \le T$.
l	The bit position of an ID. The l-th bit is denoted by l for simplicity if not confusing. $1 \le l \le L$.
$\boldsymbol{ID}_{n,k}$	The correct ID k expected to be generated in device n.
$\boldsymbol{ID}_{n,k,t}$	The empirically generated ID k in test t in device n.
$b_{n,k,l}$	The correct response bit l of ID k expected to be generated in device n. $b_{n,k,l} \in \{0, 1\}$.
$b_{n,k,t,l}$	The empirically generated response bit l of ID k in test t in device n. $b_{n,k,t,l} \in \{0, 1\}$.

device are calculated by the following equations:

$$H_n = -\log_2 \max(p_n, 1 - p_n), \text{ where} \tag{6}$$

$$p_n = \frac{1}{K \cdot T \cdot L} \sum_{k=1}^{K} \sum_{t=1}^{T} \sum_{l=1}^{L} b_{n,k,t,l} \text{ with } \log_2(0) := 0. \tag{7}$$

$$S_n = 1 + \frac{1}{K \cdot L} \sum_{k=1}^{K} \sum_{l=1}^{L} \log_2 \max(p_{n,k,l}, 1 - p_{n,k,l}). \tag{8}$$

$$C_n = 1 - \frac{2}{K \cdot T \cdot L} \sum_{k=1}^{K} \sum_{t=1}^{T} \sum_{l=1}^{L} (b_{n,k,l} \oplus b_{n,k,t,l}). \tag{9}$$

$$D_n = \frac{4}{L \cdot K^2} \sum_{l=1}^{L} \sum_{i=1}^{K-1} \sum_{j=i+1}^{K} (b_{n,i,l} \oplus b_{n,j,l}). \tag{10}$$

$$\overline{U} = \frac{4}{K \cdot L \cdot N^2} \sum_{k=1}^{K} \sum_{l=1}^{L} \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} (b_{i,k,l} \oplus b_{j,k,l}). \tag{11}$$

Note that the uniqueness cannot be determined by a single device, and therefore, the uniqueness is expressed in $\overline{U}$ that is the average of U_n of all devices. For more details on the formulas of the indicators, refer to Ref. [11].

The advantage of these indicators is that all indicators are normalized and range from 0 to 1, where a larger number indicates a better performance. Therefore, these indicators are intuitive and useful for comparing the performance of different PUFs; however, simply using HDs may lead to confusing results. For example, the SC-wid HD is the best when HD = 0, and the SC-d2d HD is the best when HD = 50%.

In this study, the performances of the APUF and PL-PUF are compared using the above indicators.

5. Experimental Results

In this section, we discuss the results of the performance evaluation of APUFs and PL-PUFs. The performance of PUFs is evaluated on the basis of the criteria given in Sections 4.3 and 4.4. The tables and figures are all summarized in Appendices A.1 and A.2.

5.1 Results for the APUFs

5.1.1 Comparison of 64- and 128-bit APUFs in Kintex-7

For the APUF64 and APUF128 on the Kintex-7 in the **Table A·1**, the reproducibility of IDs in both PUFs is quite high, as the SC-wid HD is distributed in a narrow range around 0. The APUF128-K7 is more reproducible with a smaller mean and standard deviation than the APUF64-K7. These excellent properties are also known from the high steadiness and correctness values.

The distributions of the DC-wid HD for both APUFs are almost the same and are both good, as the distributions are in the narrow range around half of the ID length (= 64). The goodness of the DC-wid HD is also known from the high value for diffuseness.

The SC-d2d HDs of the two APUFs are not very high according to the value for uniqueness. The mean of the SC-d2d HD are both about 15; however, the standard deviation of APUF128-K7 is larger than that of APUF64-K7, resulting in a slightly larger uniqueness and slightly worse FAR and FRR. However, the error rates are only about 1%, and they would be acceptable for many applications.

A rough estimation for the possible ID patterns is given as follows:

$${}_{128}C_{15} = 1.32 \times 10^{19} = 2^{63.5}. \tag{12}$$

The ID space generated by the APUF64/128-K7 is considerably reduced compared to 2^{128}, but the space of $2^{63.5}$ would be acceptable. In APUF, the ID length can be easily changed without altering the architecture of the APUF, as the ID is created by collecting as many 1-bit responses as possible up to the ID length. Therefore, the possible ID patterns can be easily increased by generating a longer ID.

5.1.2 Comparison of 64- and 128-bit APUFs in Artix-7

For the APUF64 and APUF128 on the Artix-7 in the **Table A·2**, the reproducibility of IDs in both PUFs is better than those on Kintex-7. In contrast to Kintex-7, the APUF128 on Artix-7 is less reproducible than the APUF64-A7.

The distributions of the DC-wid HD for both APUFs are almost the same and are both good, and the goodness of the DC-wid HD is also known from the high value for diffuseness.

The SC-d2d HDs of the two APUFs are worse than those on Kintex-7, and the value for uniqueness is quite low. The mean of the SC-d2d HD are both about 7. In spite of the low SC-d2d-HD, the error rates are only about 3–4%, and they would be acceptable for many applications.

A rough estimation for the possible ID patterns is given as follows:

$${}_{128}C_{7} = 9.45 \times 10^{10} = 2^{36.5}. \tag{13}$$

The ID space generated by the APUF64/128 on Artix-7 is considerably reduced compared to 2^{128} and much less than that on Kintex-7. To use APUFs on Kintex-7 in practical applications, generating a longer ID would be required.

5.1.3 Comparison of 28-, 45-, and 65-nm APUFs

Here the performance of APUFs on 28-nm Kintex-7/Artix-7 are compared with those on 45-nm Spartan-6 [27] on SASEBO-W [14] and 65-nm Virtex-5 [26] on SASEBO-GII [23].

As shown in Tables A·1 and **A·3**, the SC-wid HD of the APUF64 on the Kintex-7 is slightly larger than that on the Spartan-6 and Virtex-5 FPGA; however, the values only slightly

differ from each other. APUF128-K7 is more reproducible with a smaller mean and standard deviation than APUF64-S6. With marginal differences, the reproducibility of all APUFs are quite good, as indicated by the high values for steadiness and correctness.

As shown in Table A·2, the SC-wid HD of the APUF64/128 on the Artix-7 is slightly smaller than that on the Spartan-6 and Virtex-5 FPGA. Therefore, the reproducibility of APUFs on Artix-7 are better than that of the previous studies, as indicated by the high values for steadiness and correctness.

The DC-wid HDs of those APUFs have similar distributions, as illustrated in **Figs. A·1–A·6**. The goodness of the DC-wid HD distribution is also known from the high value for diffuseness.

The SC-d2d HDs of the APUFs on the 28-nm Kintex-7 are smaller than those on the 45-nm Spartan-6 and larger than those on the 65-nm Virtex-5, as indicated by the values for the uniqueness. On the other hand, the SC-d2d HDs of the APUFs on the 28-nm Artix-7 are smaller than those of both Spartan-6 and Virtex-5. A rough estimation for the possible IDs in Spartan-6 and Virtex-5 is given below:

$$_{128}C_{20} = 1.20 \times 10^{23} = 2^{76.7} \quad (14)$$

$$_{128}C_{7} = 9.45 \times 10^{10} = 2^{36.5}. \quad (15)$$

Although the ID space of APUF64/128-K7 and APUF64/128-A7 are smaller than that of the 45-nm FPGAs, they can be easily extended as mentioned above. On the other hand, the APUFs on the Kintex-7s have quite superior values for uniqueness as compared to the 65-nm FPGAs; the APUFs on the Artix-7s have similar degree of uniqueness compared to the 65-nm FPGAs.

The reasons why Artix-7 shows the best reproducibility but worst uniqueness and why Spartan-6 shows the best uniqueness are not obvious. To clarify the reasons is left as future work of this study.

In summary, the APUFs on the 28-nm Kintex-7 would be quite feasible with superior performance compared to the 65-nm APUF, while the 45-nm APUF could further have better uniqueness. The APUFs on the 28-nm Artix-7 would be also feasible with an excellent reproducibility of IDs, though longer IDs would be preferable due to their low uniqueness.

5.2 Results for the PL-PUFs

5.2.1 Comparison of Different Active Durations in Kintex-7

For the SC-wid HD in **Table A·4**, the reproducibility of the PL-PUFs on the 28-nm Kintex-7 is high with a small active duration ($c = 1, 2$) and low with a long active duration ($c = 8, 16$). This is also explained by the fact that the steadiness and correctness decrease as the active duration increases. As also illustrated in **Figs. A·7–A·11**, the IDs of the PL-PUFs are reproducible only for small active durations. This would be due to the additivity of variance of the distance that a signal can reach. Let the distance be x that a signal progresses in active duration 1, and its probability distribution function be $N(x, \sigma^2)$. Then, the distance that a signal travels in active duration c follows the distribution $N(cx, c\sigma^2)$. Therefore, the variance of the distance that a signal can reach increases as the c becomes large, resulting in the low reproducibility of the IDs.

The FAR and FRR also increase according to the active duration, and for $c = 4$ and larger, they would be no more effective for chip authentication owing to the large error rate.

For all active durations, the DC-wid HDs of the PL-PUFs on Kintex-7 are distributed in the relatively narrow range around HD = 64, and their values for diffuseness are all quite high.

Although the SC-d2d HD of the PL-PUFs for $c = 1$ is large ($m = 44.8$) and the value for the uniqueness is high, it is distributed over a wide range, as illustrated in Fig. A·7. The shape of the SC-d2d HD curve is bizarre, but it seems acceptable considering the value for uniqueness, FAR, and FRR. Interestingly, the standard deviation of the SC-d2d HD for $c = 16$ is smaller than that for $c = 8$ and smaller. This means that the output of the PL-PUF could converge to some value after being activated for long clock cycles.

In Kintex-7, the PL-PUFs available for chip authentication would be the PL-PUFs with $c = 1$ or 2, and the number of possible IDs generated in those PUFs, PL-PUF01-K7 and PL-PUF02-K7, are estimated from the SC-d2d HDs as follows:

$$_{128}C_{45} = 8.17 \times 10^{34} = 2^{116} \quad (16)$$

$$_{128}C_{53} = 3.64 \times 10^{36} = 2^{121}. \quad (17)$$

The ID space of 2^{116} and 2^{121} will provide a sufficient security level for various applications.

5.2.2 Comparison of Different Active Durations in Artix-7

For the SC-wid HD in **Table A·5**, the reproducibility of the PL-PUFs on the 28-nm Artix-7 is as high as Kintex-7 with active duration $c = 1$ and 2, and higher than Kintex-7 with the active duration $c = 4$ and longer. As also illustrated in **Figs. A·12–A·16**, the IDs of the PL-PUFs are reproducible only for small active durations ($c \leq 4$), probably because of the same reason as the PL-PUFs in Kintex-7.

For all active durations, the DC-wid HDs of the PL-PUFs on Artix-7 are distributed in the relatively narrow range around HD = 64, and their values for diffuseness are excellent and as high as Kintex-7.

The SC-d2d HD of the PL-PUF01 on Artix-7 ($c = 1$) is larger than Kintex-7, and furthermore, its distribution is in the narrower range ($s = 12.4$) compared to the Kintex-7, as also illustrated in Fig. A·12. The shape of the SC-d2d HD curve looks normal, and the value for uniqueness is larger than that of Kintex-7. Different from Kintex-7, the standard deviation of the SC-d2d HD in Artix-7 decreases as the active duration increases. This would be because the output of the PL-PUF could converge to some value after being activated for long clock cycles.

The FAR and FRR increase basically according to the active duration. In contrast to Kintex-7, however, the FAR and FRR of PL-PUF-A7 with $c = 4$ and 8 are still sufficiently low and would be acceptable for chip authentication. In Artix-7, the PL-PUFs available for chip authentication would be the PL-PUFs with $c = 1$ through 8, and the number of possible IDs generated in those PUFs are estimated from the SC-d2d HDs as follows:

$$_{128}C_{59} = 1.62 \times 10^{37} = 2^{123.6} \quad (18)$$

$$_{128}C_{61} = 2.08 \times 10^{37} = 2^{124.0} \quad (19)$$

$$_{128}C_{60} = 1.87 \times 10^{37} = 2^{123.8} \quad (20)$$

$$_{128}C_{62} = 2.25 \times 10^{37} = 2^{124.1}. \quad (21)$$

The above ID space is large enough to provide sufficient security level for various applications.

5.2.3 Comparison of the 28-, 45-, and 65-nm PL-PUFs

As Tables A·4–**A·7** show, the distributions of the SC-wid HD for the PL-PUFs on 28-, 45-, and 65-nm FPGAs have basically similar tendencies: the SC-wid HD increases as the active duration increases. In Figs. A·7–**A·26**, particularly the figures where $c = 8$, the PL-PUFs on Spartan-6 seem to have the fastest oscillating frequency because the distribution of SC-wid HD moves to around HD = 64 earlier than Kintex-7, Artix-7 and Virtex-5. On the other hand, the DC-wid HD of the PL-PUFs on Spartan-6 is distributed aside from HD = 64, and its value for the diffuseness is much lower than that of Kintex-7 and Artix-7.

The SC-d2d HD of the PL-PUFs on the four types of FPGAs are basically good, and the uniqueness is high for small active durations. Considering the FAR and FRR, only $c = 1$ and 2 would be available for the PL-PUFs on Kintex-7 and Spartan-6; $c = 4$ would be also available for Artix-7 and Virtex-5; even $c = 8$ would be also acceptable for Artix-7.

In summary, the PL-PUFs on the 28-nm Kintex-7 are quite feasible for chip authentication for $c = 1$ and 2; 28-nm Artix-7 are feasible also for $c = 4$ and 8. The performance of the PL-PUFs on Kintex-7 and Artix-7 is excellent and higher than the performance on Spartan-6 and Virtex-5 for these active durations.

6. Conclusion

To explore the feasibility and practicality of PUFs on 28-nm process chips, we evaluated the performance of APUFs and PL-PUFs on Kintex-7 FPGAs on 10 SASEBO-GIII boards and Artix-7 on 8 Nexys4 boards. The performances of the PUFs on the Kintex-7 and Artix-7 were compared with those on the 45-nm Spartan-6 and 65-nm Virtex-5. According to the experimental results, both APUFs and PL-PUFs on the 28-nm FPGAs demonstrated good properties that were no worse than those on 45- and 65-nm FPGAs. Therefore, the PUFs can be implemented using the state-of-the-art process technology and used for various security-sensitive applications.

Our future work involves the investigation of the performance of the APUFs and PL-PUFs by using more boards and chips. It is also planned to conduct experiments by changing the environmental conditions, e.g., ambient temperature, humidity, and core voltage of the FPGA. Another plan involves the security evaluation of the APUFs and PL-PUFs against machine learning attacks. A further direction of this study will be to implement various types of PUFs on 28-nm FPGAs to evaluate their performance.

Acknowledgments This work is partly supported by the Core Research for Evolutional Science & Technology (CREST) funded by the Japan Science and Technology Agency (JST).

References

[1] Bauder, D.W.: An Anti-Counterfeiting Concept for Currency, Technical Report Systems Research Report PTK-11990, Sandia National Laboratories (1983).
[2] Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, Committee on Armed Services, United States Senate (2012).
[3] Digilent, Inc.: Nexys4™ FPGA Board Reference Manual (2013).
[4] Fujiwara, H., Yabuuchi, M., Tsukamoto, Y., Nakano, H., Owada, T., Kawai, H. and Nii, K.: A stable chip-ID generating physical uncloneable function using random address errors in SRAM, *SOCC 2012*, pp.143–147, IEEE (2012).
[5] Gassend, B., Clarke, D., van Dijk, M. and Devadas, S.: Silicon Physical Random Functions, *CCS 2002*, pp.148–160, ACM (2002).
[6] George, M. and Alfke, P.: Linear Feedback Shift Registers in Virtex Devices, Xilinx apprication note XAPP210 (2007).
[7] Guajardo, J., Kumar, S.S., Schrijen, G.-J. and Tuyls, P.: FPGA Intrinsic PUFs and Their Use for IP Protection, *CHES'07*, pp.63–80 (2007).
[8] (Anonymized for review): Pseudo-LFSR PUF: A Compact, Efficient and Reliable Physical Unclonable Function, *ReConFig2011*, pp.223–228 (2011).
[9] (Anonymized for review): Performance Evaluation of Physical Unclonable Functions on 45-nm Process FPGAs, *DICOMO 2012*, pp.1928–1933 (2012). (in Japanese).
[10] (Anonymized for review): Performance Evaluation of Physical Unclonable Functions on Kintex-7 FPGA, *IEICE Technical Report, RECONF2013-17*, pp.91–96 (2013). (in Japanese).
[11] (Anonymized for review): Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs, *Proc. ReConFig2010*, pp.298–303 (2010).
[12] Information Technology – Trusted Platform Module – Part 1: Overview, ISO/IEC 11889-1:2009 (2009).
[13] Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market, iSuppli (2012), available from ⟨http://www.isuppli.com/⟩.
[14] Katashita, T., Hori, Y., Sakane, H. and Satoh, A.: Side-Channel Attack Standard Evaluation Board SASEBO-W for Smartcard Testing, *NIAT 2012* (2012).
[15] Kocher, P., Jaffe, J. and Jun, B.: Differential power analysis, *CRYPTO'99*, pp.388–397 (1999).
[16] Kocher, P.C.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, *CRYPTO'96*, pp.104–113 (1996).
[17] Komano, Y., Ohta, K., Sakiyama, K. and Mitsugu, I.: Security of Pattern Matching Key Generation using Part of PUF Output, *SCIS 2013* (2013).
[18] Kumar, S.S., Guajardo, J., Maesyz, R., Schrijen, G.-J. and Tuyls, P.: The Butterfly PUF, *HOST'08*, pp.67–70 (2008).
[19] Lattibeaudiere, A.T.: Connecting Living Programme Overview, Technical Report, GSM Association (2011).
[20] Maes, R. and Verbauwhede, I.: Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions, *Towards Hardware-Intrinsic Security*, Sadeghi, A.-R. and Naccache, D. (Eds.), chapter 1, pp.3–37, Springer-Verlag (2010).
[21] Pappu, S.R.: Physical One-Way Functions, PhD Thesis, MIT (2001).
[22] Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S. and Schmidhuber, J.: Modeling Attacks on Physical Unclonable Functions, *CCS 2010*, pp.237–249, ACM (2010).
[23] Satoh, A., Katashita, T. and Sakane, H.: Secure implementation of cryptographic modules—Development of a standard evaluation environment for side channel attacks, *Synthesiology*, Vol.3, No.1, pp.56–65 (2010).
[24] Suh, G.E. and Devadas, S.: Physical Physical Unclonable Functions for Device Authentication and Secret Key Generation, *DAC'07*, pp.9–14 (2007).
[25] Suzuki, D. and Shimizu, K.: The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes, *Proc. CHES2010*, pp.366–382 (2010).
[26] Xilinx, Inc.: Virtex-5 Family Overview (2009).
[27] Xilinx, Inc.: Spartan-6 Family Overview (2011).
[28] Xilinx, Inc.: 7 Series FPGAs Overview, Advanced Product Specification (DS180 v1.13) (2012).

Appendix

A.1 Detailed Results for the Arbiter PUFs

The performance evaluation results for the 64- and 128-stage APUFs on 28-nm Kintex-7 and Artix-7 are provided in Tables A·1 and A·2, respectively. As space is limited, only the overall results are provided instead of showing the performance for all of the chips. That is, the mean (m) and standard deviation (s) for the SC-wid HD are calculated from all IDs generated for APUF64/128-01 through APUF64/128-10 without distinguishing

Table A·1 The results for the 64- and 128-stage APUFs on Kintex-7.

	SC wid-HD		DC wid-HD		SC d2d-HD		FAR	FRR	(Pr)	H	S	C	D	U
	m	*s*	*m*	*s*	*m*	*s*	(%)	(%)						
apuf64-k7	1.24	1.13	63.8	5.74	15.0	3.98	0.458	0.212	0.472	0.912	0.988	0.986	0.994	0.201
apuf128-k7	0.832	0.912	63.7	5.67	15.2	7.67	0.766	1.04	0.471	0.920	0.992	0.991	0.994	0.213

Table A·2 The results for the 64- and 128-stage APUFs on Artix-7.

	SC wid-HD		DC wid-HD		SC d2d-HD		FAR	FRR	(Pr)	H	S	C	D	U
	m	*s*	*m*	*s*	*m*	*s*	(%)	(%)						
apuf64-a7	0.578	0.759	63.6	5.65	6.91	2.64	3.24	2.08	0.460	0.889	0.995	0.994	0.992	0.0942
apuf128-a7	0.721	0.857	63.1	5.68	6.76	2.67	3.95	3.81	0.444	0.849	0.993	0.992	0.985	0.0918

Table A·3 The results for the 64-stage APUFs in the previous work [9], [11].

	SC wid-HD		DC wid-HD		SC d2d-HD		FAR	FRR	(Pr)	H	S	C	D	U
	m	*s*	*m*	*s*	*m*	*s*	(%)	(%)						
apuf64-s6	0.877	1.62	64.0	5.62	19.7	17.4	0.217	0.307	0.498	0.976	0.992	0.990	0.990	0.292
apuf64-v5	0.431	0.657	63.3	5.62	6.78	2.61	4.01	0.978	0.558	0.843	0.996	0.995	0.986	0.102

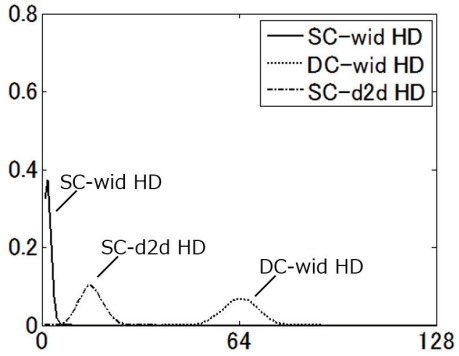

Fig. A·1 Distribution of the HD for the APUF64-01 on the Kintex-7.

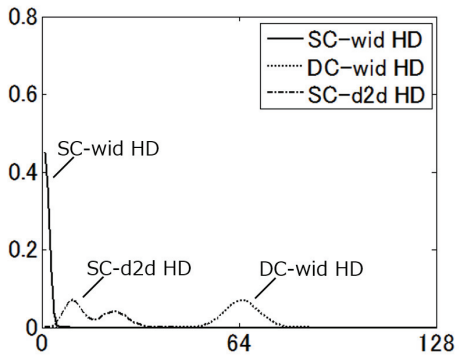

Fig. A·2 Distribution of the HD for the APUF128-01 on the Kintex-7.

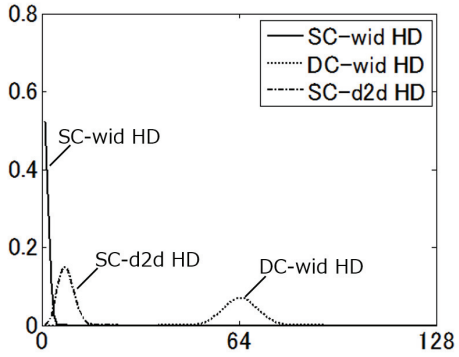

Fig. A·3 Distribution of the HD for the APUF64-01 on the Artix-7.

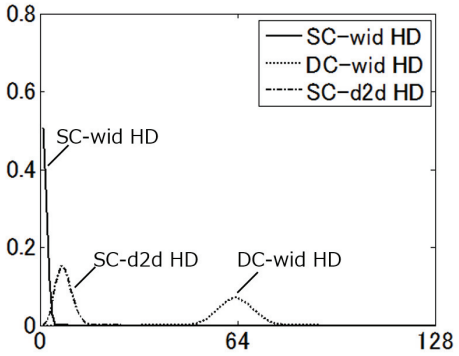

Fig. A·4 Distribution of the HD for the APUF128-01 on the Artix-7.

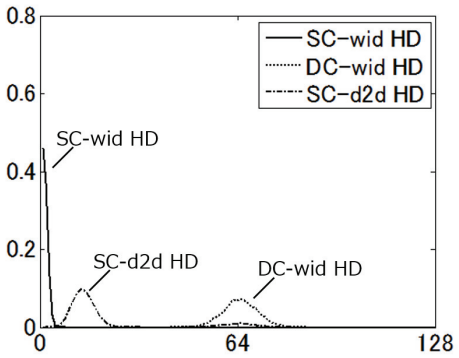

Fig. A·5 Distribution of the HD for the APUF64 on Spartan-6 [9].

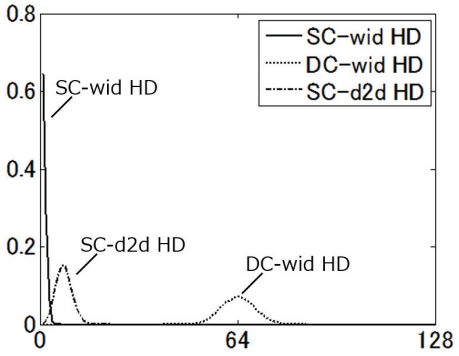

Fig. A·6 Distribution of the HD for the APUF64 on Virtex-5 [11].

Table A·4 The results for the PL-PUFs on Kintex-7 FPGAs.

	SC wid-HD		DC wid-HD		SC d2d-HD		FAR	FRR	(Pr)	H	S	C	D	U
	m	*s*	*m*	*s*	*m*	*s*	(%)	(%)						
pl-puf01-k7	1.48	1.42	62.8	5.89	44.8	19.0	0.572	0.403	0.485	0.958	0.986	0.984	0.992	0.623
pl-puf02-k7	2.97	2.32	62.7	5.86	53.4	16.8	0.823	0.722	0.493	0.978	0.971	0.967	0.979	0.750
pl-puf04-k7	8.46	4.38	62.9	5.89	58.8	10.4	11.7	2.77	0.493	0.979	0.918	0.905	0.981	0.822
pl-puf08-k7	32.8	9.41	63.3	5.82	63.3	32.0	21.9	5.44	0.490	0.971	0.668	0.625	0.996	0.884
pl-puf16-k7	62.8	5.92	63.2	6.83	63.5	5.82	40.9	54.5	0.492	0.978	0.139	0.105	0.500	0.658

Table A·5 The results for the PL-PUFs on Artix-7 FPGAs.

	SC wid-HD		DC wid-HD		SC d2d-HD		FAR	FRR	(Pr)	H	S	C	D	U
	m	*s*	*m*	*s*	*m*	*s*	(%)	(%)						
pl-puf01-a7	1.68	1.76	61.5	6.13	59.4	12.4	0.821	0.404	0.509	0.973	0.984	0.982	0.960	0.812
pl-puf02-a7	3.01	2.52	61.3	6.12	61.1	10.9	1.39	0.580	0.509	0.974	0.971	0.967	0.955	0.835
pl-puf04-a7	6.98	4.58	60.7	6.54	60.2	9.68	1.93	0.976	0.508	0.977	0.933	0.923	0.947	0.823
pl-puf08-a7	21.7	9.27	62.4	5.94	62.3	6.81	1.78	0.921	0.507	0.979	0.786	0.755	0.971	0.848
pl-puf16-a7	55.3	8.88	62.4	5.95	62.8	5.92	22.8	38.5	0.507	0.979	0.349	0.294	0.849	0.779

Table A·6 The results for the PL-PUFs on Spartan-6 FPGAs.

	SC wid-HD		DC wid-HD		SC d2d-HD		FAR	FRR	(Pr)	H	S	C	D	U
	m	*s*	*m*	*s*	*m*	*s*	(%)	(%)						
pl-puf01-s6	3.14	2.92	37.7	29.2	59.8	9.74	0.0838	0.0282	0.507	0.967	0.971	0.966	0.566	0.888
pl-puf02-s6	9.33	7.08	40.6	25.6	60.7	7.21	0.0620	0.0980	0.508	0.950	0.911	0.896	0.580	0.902
pl-puf04-s6	31.9	14.5	50.0	16.9	60.9	7.66	6.76	10.6	0.516	0.954	0.676	0.632	0.611	0.885
pl-puf08-s6	56.9	11.4	57.9	10.9	60.1	8.12	46.1	34.8	0.511	0.968	0.324	0.269	0.411	0.498
pl-puf16-s6	56.8	12.3	57.0	12.1	59.5	8.79	52.5	27.6	0.511	0.969	0.329	0.273	0.304	0.395

Table A·7 The results for the PL-PUFs on Virtex-5 FPGAs [8].

	SC wid-HD		DC wid-HD		SC d2d-HD		FAR	FRR	(Pr)	H	S	C	D	U
	m	*s*	*m*	*s*	*m*	*s*	(%)	(%)						
pl-puf01-v5	3.11	5.27	62.3	6.63	50.5	18.2	2.72	0.875	0.496	0.945	0.971	0.766	0.962	0.739
pl-puf02-v5	4.85	7.91	62.5	6.30	58.0	12.5	1.68	0.844	0.502	0.940	0.953	0.946	0.962	0.849
pl-puf04-v5	11.2	10.5	62.6	6.22	62.4	7.06	1.12	1.55	0.502	0.945	0.892	0.876	0.960	0.914
pl-puf08-v5	39.9	13.1	62.5	6.40	63.7	6.05	6.20	14.0	0.502	0.945	0.586	0.534	0.941	0.929
pl-puf16-v5	62.1	6.86	62.5	6.45	63.6	6.08	51.5	39.4	0.502	0.945	0.192	0.149	0.612	0.836

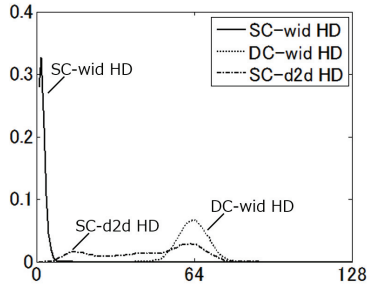

Fig. A·7 Distribution of the HD for the PL-PUF on the Kintex-7 for $c = 1$.

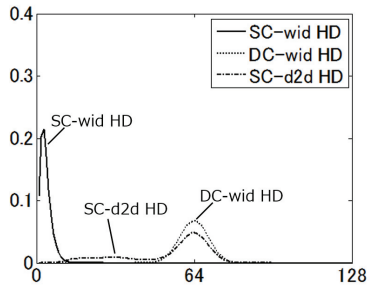

Fig. A·8 Distribution of the HD for the PL-PUF on the Kintex-7 for $c = 2$.

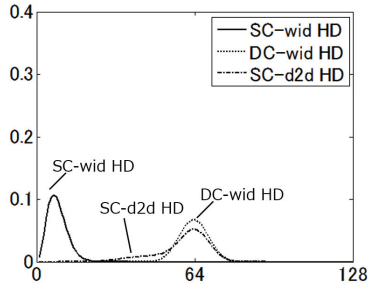

Fig. A·9 Distribution of the HD for the PL-PUF on the Kintex-7 for $c = 4$.

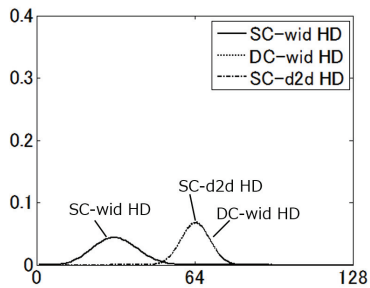

Fig. A·10 Distribution of the HD for the PL-PUF on the Kintex-7 for $c = 8$.

the chips. The same is also applied to the DC-wid HD. The SC-d2d HD is intrinsically calculated from the IDs generated in all chips. The distributions of these HDs are given in Figs. A·1 through A·4. The horizontal axis is Hamming distance and the vertical axis is the relative frequency of the ID having the corresponding Hamming distance. The FAR and FRR listed in the table are the mean of the FARs and FRRs obtained from each chip, respectively.

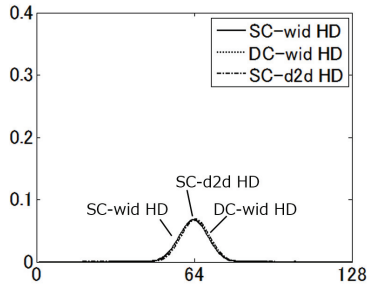

Fig. A·11 Distribution of the HD for the PL-PUF on the Kintex-7 for $c = 16$.

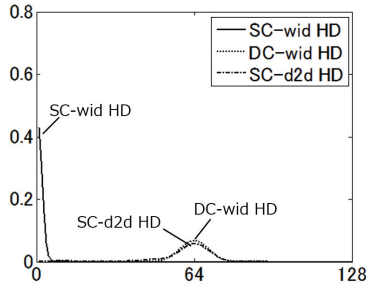

Fig. A·12 Distribution of the HD for the PL-PUF on the Artix-7 for $c = 1$.

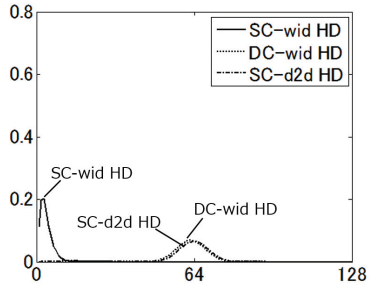

Fig. A·13 Distribution of the HD for the PL-PUF on the Artix-7 for $c = 2$.

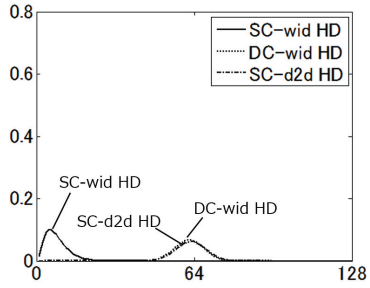

Fig. A·14 Distribution of the HD for the PL-PUF on the Artix-7 for $c = 4$.

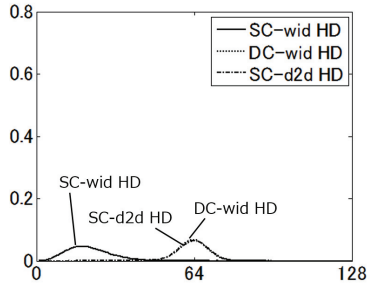

Fig. A·15 Distribution of the HD for the PL-PUF on the Artix-7 for $c = 8$.

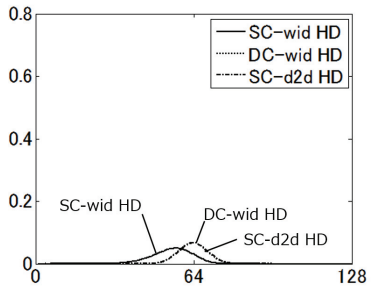

Fig. A·16 Distribution of the HD for the PL-PUF on the Artix-7 for $c = 16$.

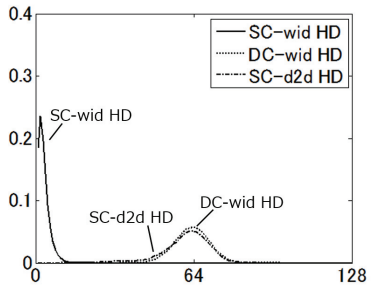

Fig. A·17 Distribution of the HD for the PL-PUF on Spartan-6 for $c = 1$.

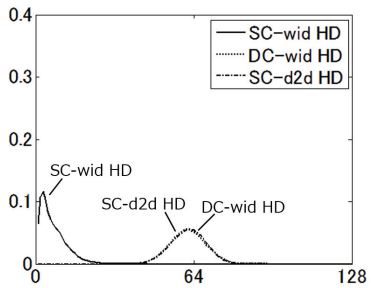

Fig. A·18 Distribution of the HD for the PL-PUF on Spartan-6 for $c = 2$.

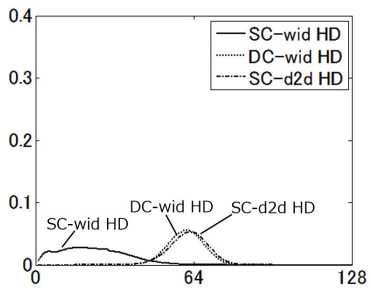

Fig. A·19 Distribution of the HD for the PL-PUF on Spartan-6 for $c = 4$.

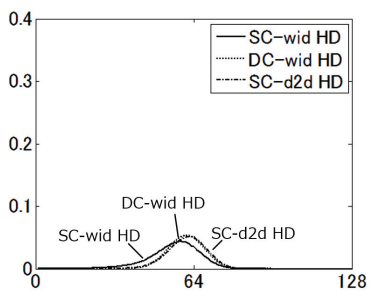

Fig. A·20 Distribution of the HD for the PL-PUF on Spartan-6 for $c = 8$.

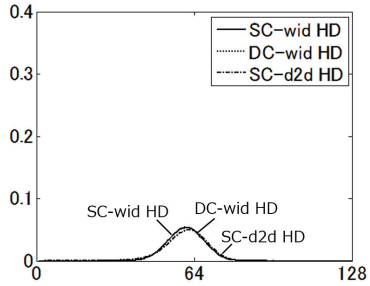

Fig. A·21 Distribution of the HD for the PL-PUF on Spartan-6 for $c = 16$.

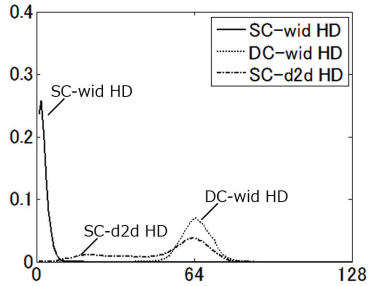

Fig. A·22 Distribution of the HD for the PL-PUF on Virtex-5 for $c = 1$.

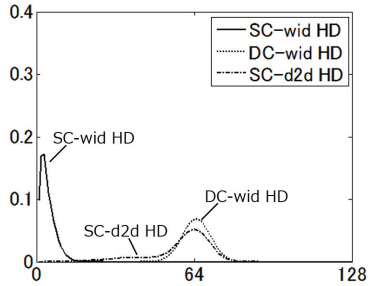

Fig. A·23 Distribution of the HD for the PL-PUF on Virtex-5 for $c = 2$.

Tables A·1 and A·2 also provide values for the performance indicators: randomness (H), steadiness (S), correctness (C), diffuseness (D), and uniqueness (U). Pr is the probability of the response bit being 1. The probability via the diffuseness is the mean of those obtained from all chips; the value for the uniqueness is intrinsically calculated from all chips.

For comparison, the performances of the APUFs on Spartan-6 [9] and Virtex-5 [8], [11] are provided in Table A·3, and the distributions of the HD are given in Figs. A·5 and A·6.

For the APUF on Spartan-6, twenty SASEBO-W boards are used for performance evaluation [9]. A hundred types of IDs were generated and each ID was repeatedly generated 100 times.

For the APUFs on Virtex-5, 44 SASEBO-GII boards are used for the performance evaluation. In Ref. [11], 45 boards were used, but the data from one board turned out to be buggy. Therefore, the data set, excluding the buggy data, are newly analyzed in this study.

A.2 Detailed Results for the PL-PUFs

The performance evaluation results for the PL-PUFs on 28-nm Kintex-7 and Artix-7 are provided in Tables A·4 and A·5, respectively, and the distributions of the HDs are illustrated in Figs. A·7–A·16. For comparison, the performance and HD distributions for Spartan-6 are given in Table A·6 and Figs. A·17–A·21 and those for Virtex-5 are given in Table A·7 and Figs. A·22–A·26.

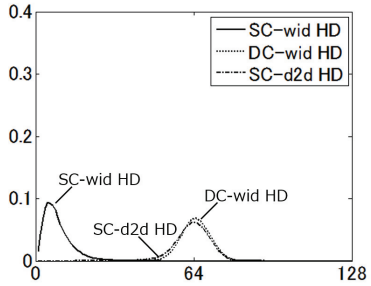

Fig. A·24 Distribution of the HD for the PL-PUF on Virtex-5 for $c = 4$.

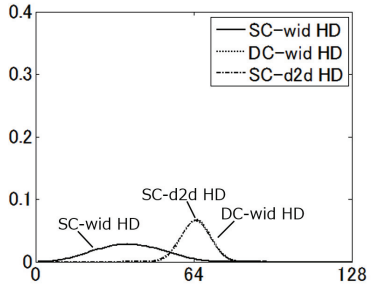

Fig. A·25 Distribution of the HD for the PL-PUF on Virtex-5 for $c = 8$.

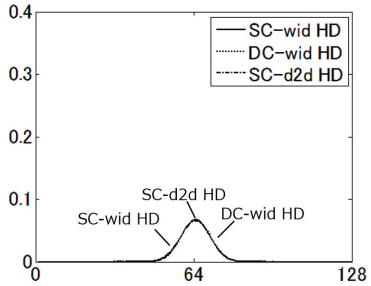

Fig. A·26 Distribution of the HD for the PL-PUF on Virtex-5 for $c = 16$.

For the PL-PUFs on Spartan-6, twenty SASEBO-W boards are used for the performance evaluation [9]. Likewise the APUFs, 100 types of IDs are generated and each ID is repeatedly generated 100 times.

Editor's Recommendation

Physically Unclonable Functions (PUFs) are an emerging technology and have been proposed as central building blocks in a variety of cryptographic protocols. In this paper, the authors implemented arbiter PUFs (APUFs) and pseudo-LFSR PUFs (PL-PUFs) and evaluated their performance in a reliable and reproducible manner; the main result is that PUFs on the smallest ever FPGA for this application is feasible and practical. This work is a significantly important step toward rigorous system security with device-specific secret keys without using a non-volatile memory.

(Chairman of SIGCSEC Kanta Matsuura)

Yohei Hori received his B.E., M.E., and Ph.D. degrees from the University of Tsukuba, Ibaraki, Japan, in 1999, 2001, and 2004, respectively. After receiving his Ph.D., he spent five years as a postdoctoral researcher at the National Institute of Advanced Industrial Science and Technology (AIST). He moved to Chuo University as a research scientist in 2008, before returning to AIST in 2010 as a researcher. His current research interests include partially reconfigurable systems, side-channel analysis, fault analysis, and physically unclonable functions. He is a member of IEICE, IEEE and IEEE-CS.

Hyunho Kang is currently an assistant professor in the Department of Electrical Engineering at Tokyo University of Science, Japan, from Apr. 2013. He received his Ph.D. from University of Electro-Communications, Tokyo, in 2008. From 2008 to Aug. 2010, he was a researcher/assistant professor of the Chuo University, Tokyo, where he was part of team that developed Biometric Security technologies. From Sep. 2010 to Mar. 2013, he was an AIST postdoctoral researcher of the National Institute of Advanced Industrial Science and Technology (AIST), Japan, where his research work has been mainly focused on the evaluation of Physical Unclonable Functions. His main interests are in digital watermarking, biometric security and Physical Unclonable Functions.

Toshihiro Katashita completed the doctoral program of the Graduate School of Systems and Information Engineering, University of Tsukuba, in 2006, whereupon he joined AIST as a fixed-term researcher. In 2008, he became a tenure-track researcher at AIST. He is involved in research projects on high-performance computation circuit design and hardware security. He is engaged in the development of cryptographic hardware and software as well as side-channel attack experiments.

Akashi Satoh received his B.S. and M.S. degrees in Electrical Engineering from Waseda University, Tokyo, Japan, in 1987 and 1989, respectively. In 1989, he joined IBM Research, Tokyo Research Laboratory, and was involved in the research and development of digital and analog VLSI circuits. He received a Ph.D. in Electrical Engineering from Waseda University in 1999. In 2007, he joined the National Institute for Advanced Industrial Science and Technology (AIST) and managed the SASEBO Project. Since 2013, he has been with the University of Electro-Communications where he is currently a professor of the Graduate School of Informatics and Engineering. His current research interests include algorithms and architectures for data security and high-performance VLSI implementations.

Shinichi Kawamura received his B.E., M.E., and Dr. E. degrees in Electronic Engineering from the University of Tokyo, in 1983, 1985, and 1996, respectively. He joined Toshiba Corporation in 1985 since then, has been working on the research and development of cryptography and information security. From 1992 to 1994, he was a visiting researcher at the Center for Telecommunications Research (CTR), at Columbia University, NY. From 2009 to 2011, he was Deputy Director of Research Center for Information Security, at the National Institute of Advanced Industrial Science and Technology (AIST). He returned to Toshiba Corporate Research and Development Center in 2012 and currently he is Senior Fellow at Toshiba and has been Invited Senior Researcher of Research Institute for Secure Systems, at AIST from 2012. He received the Young Researchers' Award of IEICE and "Kohrohsho" Award of IEICE Engineering Sciences Society in 1993 and 2006, respectively. Dr. Kawamura is a senior member of IEEE and IEICE, and a member of IPSJ, and IACR.

Kazukuni Kobara received his B.E. and M.E. degrees from University of Yamaguchi, Japan, in 1992 and 1994, respectively. He also received his Ph.D. degree in engineering from the University of Tokyo in 2003. He joined the Institute of Industrial Science of the University of Tokyo in 1994, and then moved to the National Institute of Advanced Industrial Science and Technology (AIST) in 2006 where he is the Leader of Control System Security Research Group at Research Institute for Secure Systems (RISEC). His research interests include cryptography, computer security and cybersecurity. He received the SCIS Paper Award and the Vigentennial Award from IEICE in 1996 and 2003, respectively. He also received the Best Paper Award of WISA, the ISITA Paper Award for Young Researchers, the IEICE Best Paper Award and Inose Award, the JSSM Best Paper Award and RISONA Industry-Academia-Government Coordination Award in 2001, 2002, 2003, 2006 and 2013, respectively. He served as a member of ETC (Electronic Toll Collection System) security committees from 1999 to present, CRYPTREC (Cryptography Research and Evaluation Committees) from 2000 to 2008, the vice chairperson of MIC WLAN security committee in 2003, the chief investigator of INSTAC identity management committee from 2007 to 2009, ISO/IEC JTC1 SC27 WG2 expert from 2012 to present.