Performance of Physical Unclonable Functions with Shift-Register-Based Post-processing

Hyunho Kang[1], Yohei Hori[1], Toshihiro Katashita[1], and Akashi Satoh[2]

[1] Research Institute for Secure Systems,
[2] Nanoelectronics Research Institute
National Institute of Advanced Industrial Science and Technology (AIST),
Central 2, 1-1-1 Umezono, Tsukuba, Ibaraki 305-8568, Japan
{h-kang,hori.y,t-katashita,akashi.satoh}@aist.go.jp

Abstract. Physical unclonable functions (PUFs) are encoded in the unique physical structure of a system, which stems from process variation, and represent a minimalistic yet secure alternative for authentication on integrated circuits. However, the amount of randomness in the PUF output could be a significant limitation. However, by passing the PUF response to a shift register, the randomness of the PUF output could be greatly increased while maintaining reliability. Here we discuss the performance of an arbiter- and ring-oscillator-type PUF with a simple shift register from the viewpoint of biometrics. Experimental results show that authentication with the shifted response data is superior to that with non-shifted data.

Keywords: Physical Unclonable Functions (PUFs), Arbiter PUF, Ring Oscillator PUF, Shift Register, Biometrics.

1 Introduction

A physical unclonable function (PUF) exploits the randomness of process variations in device manufacturing to encode a secret function[1][2]. The arbiter PUF [3] and ring oscillator (RO) PUF[2][4] are the most popular designs, which produce a unique output for each challenge input. However, it has been claimed that the amount of randomness in the PUF output is limited[5]. Therefore, the response of the PUF cannot be used directly as a key.

Thus, several post-processing schemes for the PUF output have been developed, such as majority voting and the fuzzy extractor[5][6]. Majority voting is a convenient method to transform poorly uniform and noisy measurements into more random distributions with less noise. Further, the fuzzy extractor corrects bit errors in the non-uniform PUF responses and extracts uniform random bits. However, despite these methods, it is clear that the amount of randomness in the PUF output is not sufficient. Alternatively, if the PUF output is passed to a simple shift register, randomness could be greatly increased while maintaining reliability.

T.-h. Kim et al. (Eds.): SecTech/CA/CES[3] 2012, CCIS 339, pp. 14–21, 2012.

In this paper, we discuss the performance of shift-register-based post-processing from the viewpoint of biometrics, that is, using the equal error rate (EER). In addition, we focus on determining the reliability and security (uniqueness) of the system on the basis of the differences in the outputs from the same and different PUFs for the same challenge (SC intra-PUF and SC inter-PUF, respectively).

This paper is organized as follows. Section 2 presents our evaluation approach. Section 3 briefly describes the concept of shift-register post-processing. The experimental results and conclusions are given in Sections 4 and 5, respectively.

2 Evaluation Approach

PUFs can be evaluated on the basis of differences in the responses of the same device (intra–PUF) and for differences between devices (inter–PUF). Furthermore, they can be evaluated for differences in the responses to the same challenge (SC) and to different challenges (DC). Thus, we define the following four parameters, as illustrated in Fig. 1: SC intra–PUF, DC intra–PUF, SC inter–PUF, and DC inter–PUF.

First, to evaluate the reliability of our PUF system, experiments were conducted to measure the EER and sensitivity index d' for each PUF system using SC intra–PUF and DC intra–PUF. Ideally, SC intra–PUF should be small and DC intra–PUF should be large; in other words, these two distributions should be sufficiently separated from each other. In the biometric research community, the overall accuracy is illustrated by the receiver operation characteristic (ROC) curve, which shows the dependence of the false rejection rate (FRR) on the false acceptance rate (FAR) at all thresholds. The EER is computed as the point where FAR is equal to FRR. To evaluate our PUF testing, we also utilize these properties. In addition, we define a metric d', as suggested by Daugman[7], to assess the degree of separation between the two distributions:

$$d' = \frac{\mu_m - \mu_n}{\sqrt{\frac{1}{2}(\sigma_m^2 + \sigma_n^2)}}, \tag{1}$$

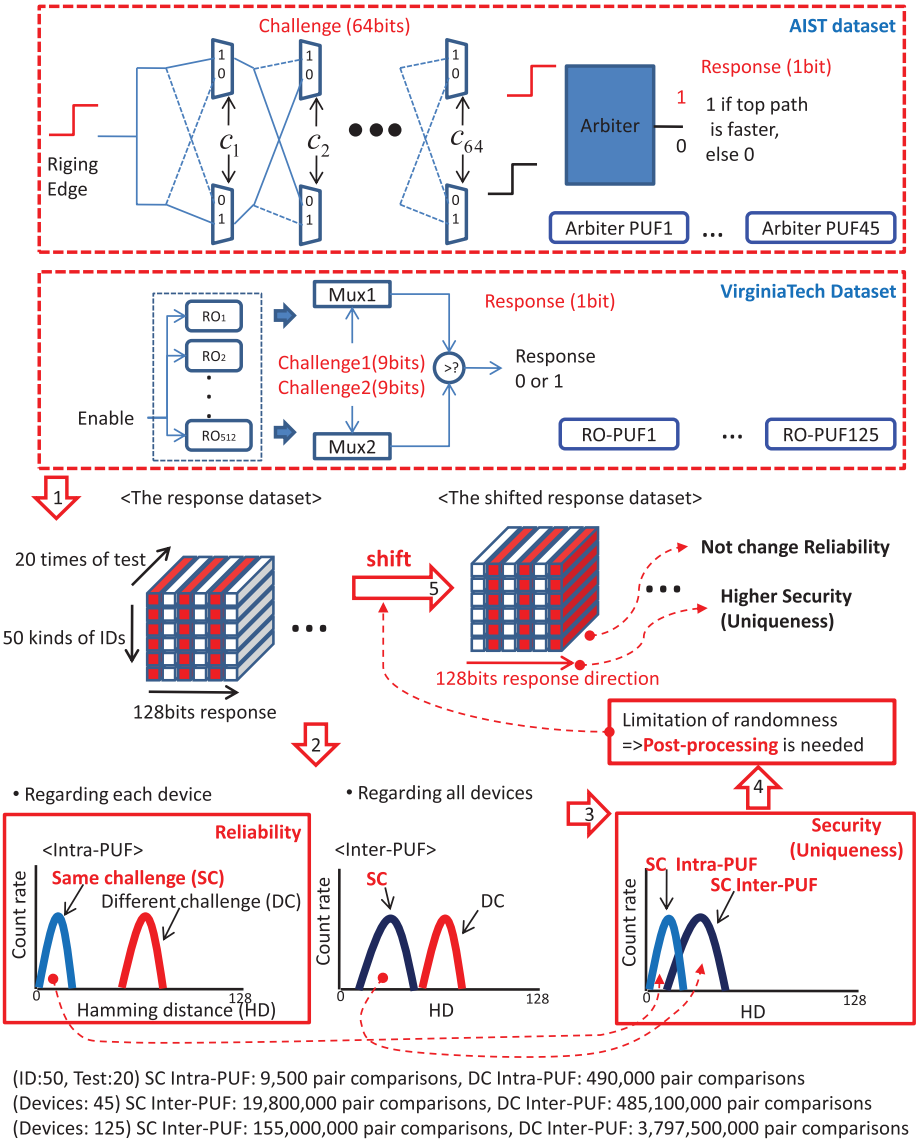
where μ_m and μ_n are the means, and σ_m and σ_n are the standard deviations, of the two distributions, respectively.

Second, to test the security of the PUF systems (i.e., uniqueness), we consider the SC inter–PUF and DC inter–PUF of complete PUF systems. Ideally, SC inter–PUF and DC inter–PUF should be large.

However, in this paper, we consider only SC intra–PUF and SC inter–PUF to evaluate the PUF systems with and without shift-register-based post-processing.

3 Shift Register

Figure 1 (arrow number 5) shows the creation of the shifted response database. Note here that shifting bits to the right depends on the intrinsic properties of



(ID:50, Test:20) SC Intra-PUF: 9,500 pair comparisons, DC Intra-PUF: 490,000 pair comparisons
(Devices: 45) SC Inter-PUF: 19,800,000 pair comparisons, DC Inter-PUF: 485,100,000 pair comparisons
(Devices: 125) SC Inter-PUF: 155,000,000 pair comparisons, DC Inter-PUF: 3,797,500,000 pair comparisons

Fig. 1. Schematic of evaluation approach

each PUF. In our experiment, fixed bits were shifted for testing, such as 1 bit for PUF1, 2 bits for PUF2, and 45 bits for PUF45. Notably, shifting with a 128-bit response direction is simple and easily applied to the PUF output while maintaining reliability.

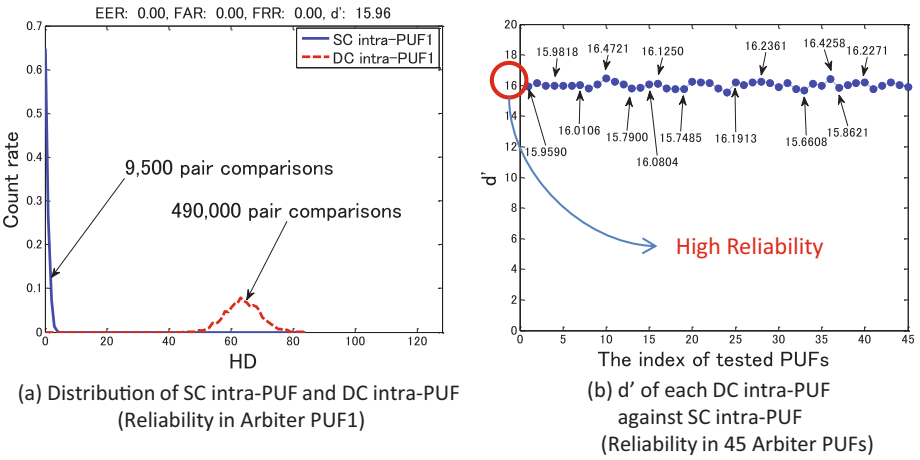


Fig. 2. Reliability for 45 arbiter PUFs

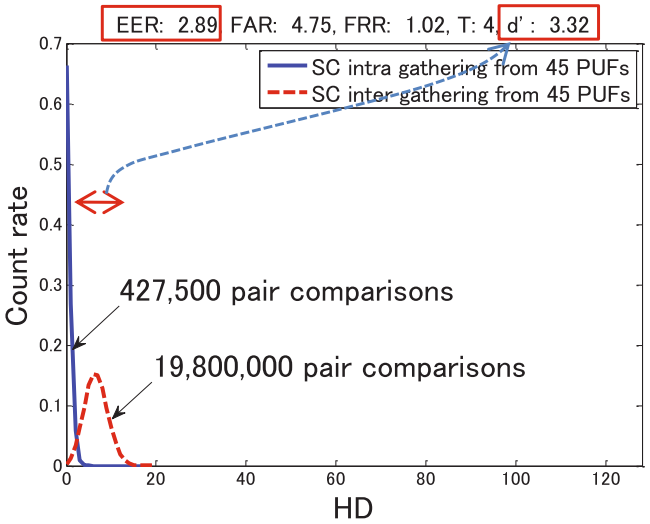
4 Experimental Results

4.1 Arbiter PUF

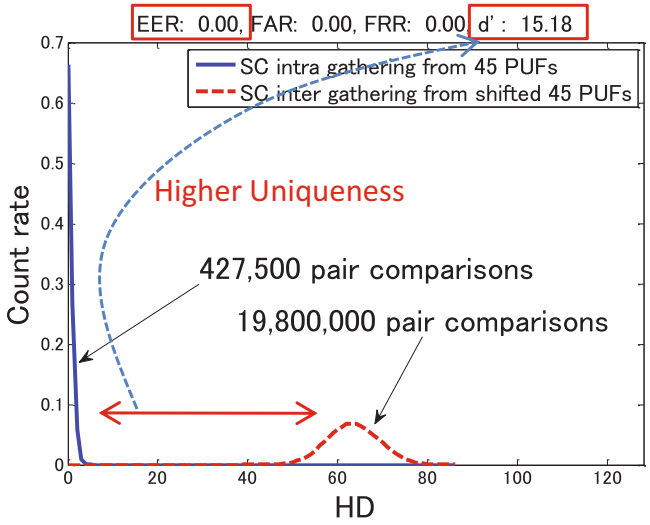
The FPGAs used in this experiment were a Xilinx's Virtex–5LX (xc5vlx30–ffg324) and a Spartan–3A (xc3s400a–ftg256) on SASEBO –GII evaluation boards [8][9]. We selected 45 arbiter PUF outputs from 20 tests and 50 kinds of IDs (called "AIST dataset" in Fig. 1) from a total of 45 outputs with 1024 tests and 1024 kinds of IDs [10].

First, we tested the reliability of each PUF output. As shown in Fig. 2 (a), the SC intra–PUF distribution and the DC intra–PUF distribution were computed and plotted to determine how the PUF algorithm separates the two classes. The figure shows a histogram of the count rates versus the hamming distance for the PUF1 output. In this experiment, we obtained ideal results with no errors. As shown in Fig. 2 (b), all of the other results also had zero error and a stable d'. Therefore, we can conclude that the reliability of each PUF output is high.

In addition, we considered the EER and d' values to evaluate the security (uniqueness) for 45 arbiter PUFs ('SC **intra** gathering from 45 PUFs' and 'SC **inter** gathering from 45 PUFs'). Figure 3 (a) shows a histogram of the count rate versus the hamming distance for all PUF outputs combined (45 arbiter PUFs). In this experiment, the threshold number was set at 4 and the EER was 2.89%. Even though this performance is sufficient for a non-strict authentication system, it is not suited for a strict authentication system such as in cryptographic applications.



(a) Distribution of SC intra-PUF and SC inter-PUF which are combined with all pair comparisons



(b) Histogram result using shifted data (Security in 45 Arbiter PUFs)

Fig. 3. Security (uniqueness) for 45 arbiter PUFs

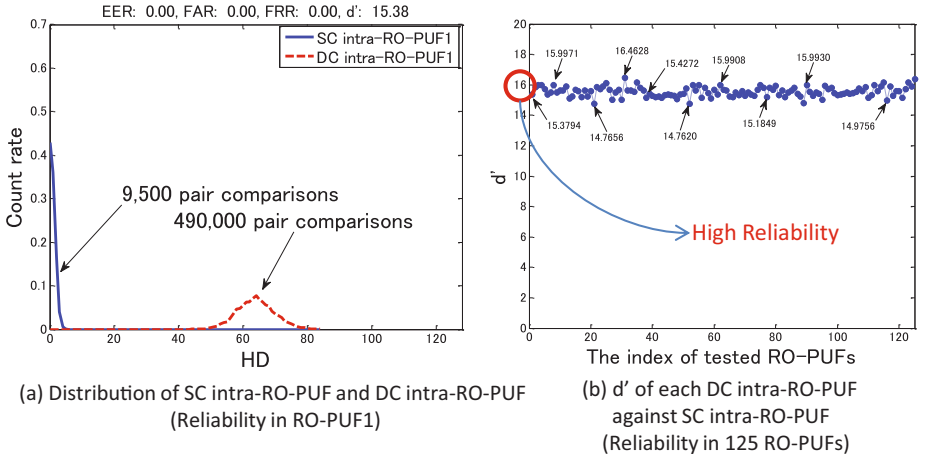


Fig. 4. Reliability for 125 RO-PUFs

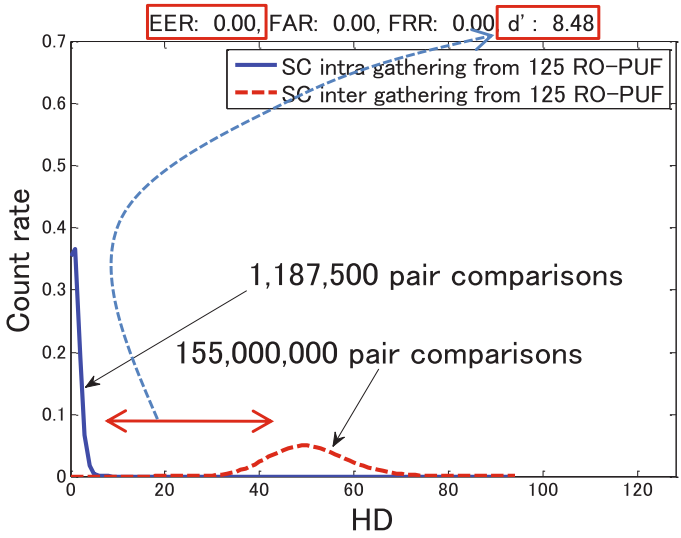
In order to solve this problem, we applied shift registers for post-processing the PUF output. As shown in Fig. 3 (b), the distribution with a shift register (SC inter gathering from shifted 45 PUFs) is ideal, that is, with no errors, and d' is 15.18 against 'SC intra gathering from 45 PUFs'.

4.2 Ring Oscillator PUF

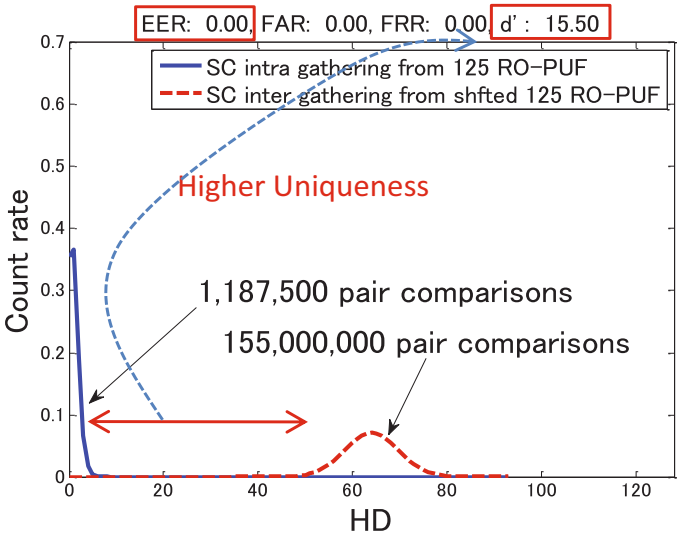
In this experiment, we selected 125 PUF outputs with 20 tests and 50 kinds of IDs from a total of 125 RO-PUF outputs (called "VirginiaTech Dataset" in Fig. 1) that were collected from 125 Xilinx Spartan (XC3S500E) FPGAs[11]. (In each output, there are 512 lines for 512 ROs, and each line contains 100 RO frequencies).

We first tested the reliability of each PUF output. As shown in Fig. 4 (a) and (b), all of the results had a zero error rate. Therefore, we can conclude that the reliability of each RO-PUF output is high.

In addition, we considered the EER and d' to evaluate the security (uniqueness) of the RO-PUFs ('SC **intra** gathering from 125 RO–PUF' and 'SC **inter** gathering from 125 RO–PUF'). As shown in Fig. 5 (a), the result showed a zero error rate. Thus, the security of the RO–PUFs using the VirginiaTech dataset is reasonably good, even though d' is a little small (8.48). In order to maintain stable security, it is desirable to sufficiently separate the two distributions. Therefore, we can apply the shift function to the PUF output in the same way as the previous sub-section. As shown in Fig. 5 (b), the distribution with the shift register (SC inter gathering from shifted 125 RO–PUF) is ideal with no errors, and d' is 15.50 against 'SC intra gathering from 125 RO–PUF'.



(a) Distribution of SC intra-RO-PUF and SC inter-RO-PUF which are combined with all pair comparisons



(b) Histogram result using shifted data (Security in 125 RO-PUFs)

Fig. 5. Security for 125 RO-PUFs

5 Conclusion

This study showed experimentally that the addition of a shift operation as post-processing is an effective approach. In particular, we note that even though this approach is valid only under the assumption that shifting is an intrinsic property, we are convinced that this could be an effective approach.

Acknowledgments

- This work was funded in part by the Core Research for Evolutional Science & Technology (CREST) program of the Japan Science and Technology Agency (JST).
- The MATLAB source code, including the AIST dataset, is available on our Web site[12].

References

1. Verbauwhede, I.M.R.: Secure Integrated Circuits and Systems. Springer (2010)
2. Edward Suh, G., Devadas, S.: Physical Unclonable Functions for Device Authentication and Secret Key Generation. In: Design Automation Conference, DAC 2007 (2007)
3. Lee, J., Lim, D., Gassend, B., Suh, G.E., van Dijk, M., Devadas, S.: A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications. In: Symposium on VLSI Circuits (2004)
4. Maiti, A., Casarona, J., Mchale, L., Schaumont, P.: A Large Scale Characterization of RO–PUF. In: IEEE Workshop on Hardware Oriented Security and Trust, HOST 2010 (2010)
5. Maes, R., Tuyls, P., Verbauwhede, I.M.R.: Intrinsic PUFs from Flip-flops on Reconfigurable Devices. In: 3rd Benelux Workshop on Information and System Security, WISSec 2008 (2008)
6. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 523–540. Springer, Heidelberg (2004)
7. Daugman, J.G., Williams, G.O.: A proposed standard for biometric decidability. In: Proceedings of CardTech/SecureTech Conference, pp. 223–234 (1996)
8. Satoh, A., Katashita, T., Sakane, H.: Secure implementation of cryptographic modules–Development of a standard evaluation environment for side channel attacks. Synthesiology-English Edition 3(1), 86–95 (2010)
9. The download site of Side-channel Attack Standard Evaluation BOard support file in AIST (National Institute of Advanced Industrial Science and Technology), `http://www.risec.aist.go.jp/project/sasebo/`
10. Hori, Y., Katashita, T., Satoh, A., Yoshida, T.: Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs. In: International Conference on ReConFigurable Computing and FPGAs, ReConFig 2010 (2010)
11. On-chip Variability data. The secure embedded system group of the ECE Department at Virginia Tech, `http://rijndael.ece.vt.edu/variability/download.html`
12. The introduction site of Physical Unclonable Function in AIST (Refer to the part of the Biometric approach to quantitative evaluation of PUF performance), `http://staff.aist.go.jp/hori.y/en/puf/index.html`