SCIS 2011 The 2011 Symposium on
Cryptography and Information Security
Kokura, Japan, Jan. 25-28, 2011
The Institute of Electronics,
Information and Communication Engineers

Performance Evaluation for PUF-based Authentication Systems with Shift Post-processing : Additional Experimental Results

Hyunho KANG * Yohei HORI * Toshihiro KATASHITA * Akashi SATOH *

Abstract— A physical unclonable function (PUF) is a physical system with a device manufacturing variations and could be useful for authentication of integrated circuits. However, it is claimed that the amount of randomness in the PUF output is limited. Therefore, the response of the PUF cannot be used directly as a key. In this paper we discuss a making method of the PUF output with much more randomness while maintaining the reliability. In order to do this, a simple shift post-processing will apply to the Arbiter and Ring Oscillator PUF output. The experimental results show that the authentication system using shifted response data have improved performance compared to non-shifted data.

Keywords: physical unclonable function (PUF), Arbiter PUF, Ring Oscillator PUF, authentication, shift post-processing

1 Introductions

A physical unclonable function (PUF) provide useful randomness property using a device manufacturing variations[1][2]. Arbiter PUF circuit[3] is one of the popular technique, which produce a particular output for each challenge input. However, it is claimed that the amount of randomness in the PUF output is limited[4]. Therefore, the response of the PUF cannot be used directly as a key.

In this paper we discuss a making method of the PUF output with much more randomness while maintaining the reliability. In order to do this, a simple shift post-processing will apply to the PUF output. We note that even though this approach is valid only having an intrinsic property (i.e., to know how many bits should be shifted against each PUF output) as assumption, this could be used as a good approach and we will consider applying shifting function to our Arbiter PUF from the point of view of circuit design in the near future. The experimental results show that the authentication system using shifted response data have improved performance compared to non-shifted data. This paper extends our recent work in Reconf [5] through doing an additional experiment using the Ring Oscillator PUF output [6][7][8].

This paper is organized as follows. Section 2 presents our evaluation approach. Section 2 briefly describes a concept with post-processing. Experimental results and conclusions are given in Section 4 and 5, respectively.

2 Evaluation Approach

The evaluation of PUFs can be tested into two categories: Intra– and Inter–PUF (also called one device and different devices). Furthermore, each category is divided into two variations: Intra– and Inter–class variation (also called the same challenge and the different challenge). To help describe our evaluation approach, we define four terms as follows: SC Intra–PUF, DC Intra–PUF, SC Inter–PUF and DC Inter–PUF (where SC is the same challenge and DC is the different challenge), illustrated in Fig. 1.

In this paper, we consider two main factors for performance evaluation: 1) Reliability and 2) Security. First, to evaluate the reliability of our PUF system, EER (Equal Error Rate) and d-prime experiments were conducted in each PUF system using SC Intra–PUF and DC Intra–PUF. Ideally, these two distributions should be satisfy small SC Intra–PUF and large DC Intra–PUF (see Fig. 1, below left). In other words, these two distributions should be sufficiently separated from each other.

Second, to test the security of the PUF systems (the same meaning as Uniqueness in this paper), we can usually consider using SC Inter–PUF and DC Inter–PUF of total PUF systems. Ideally, these two distributions should be satisfy large SC Inter–PUF and large DC Inter–PUF (see Fig. 1, above right). However, in this paper we concluded that the security evaluation using SC Intra–PUF and SC Inter–PUF (see Fig. 1, below right) should be consider, including the evaluation approach of the PUF systems with shift post-processing.

The overall accuracy in the biometric research community can be illustrated by Receiver Operation Characteristics (ROC) curve, which shows the dependence of False Reject Rate (FRR) on False Accept Rate (FAR)

[*] Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Sotokanda 1-18-13, Chiyoda-ku, Tokyo, 101-0021 Japan ({h-kang, hori-y, t-katashita, akashi.satoh}@aist.go.jp)

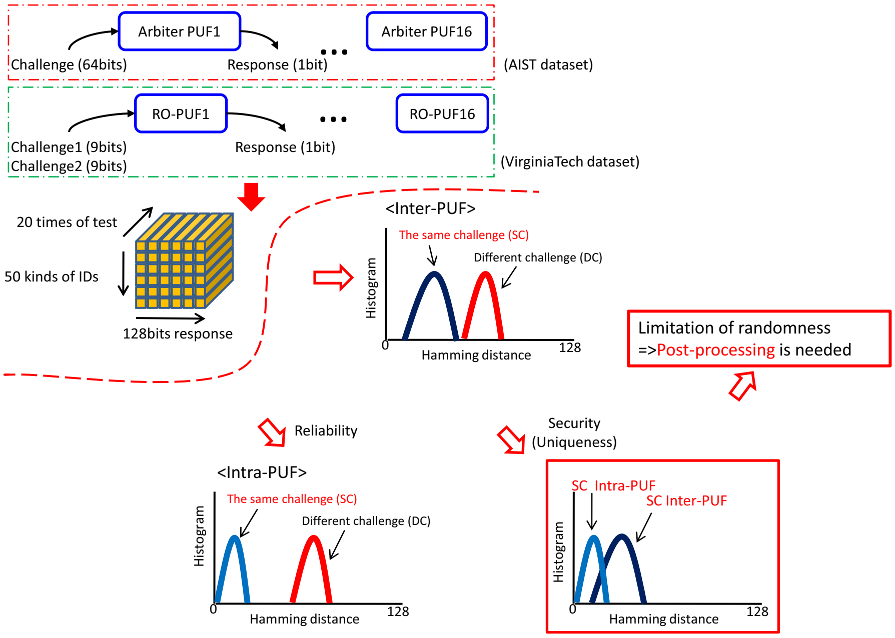

Figure 1: The diagram of evaluation approach.

at all thresholds. EER (equal error rate) is computed as the point where FAR is equal to FRR. To evaluate our PUF testing we also utilize these properties. In addition, to measure how well two distributions are separated, we use a measure called "d-prime" as suggested by Daugman[9].

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

where μ_m and σ_m are the mean and variance of one distribution (e.g., SC Intra–PUF of Fig. 1); μ_n and σ_n are the mean and variance of another (e.g., SC Inter–PUF of Fig. 1).

3 Evaluation with Post-processing

Considering post-processing of the PUF output can be refer to some research such as Majority voting or Fuzzy extractor[4][10]. Majority voting is a convenient method to transform poorly uniform and noisy measurements into more random distributions with less noise. Fuzzy extractor is to correct biterrors in the non-uniform PUF responses and extract uniform random bits. However, although using these methods, it is clear that the amount of randomness in the PUF output is not enough.

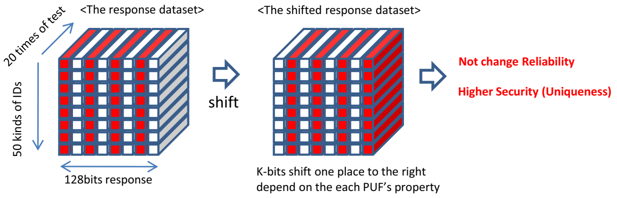
<The response dataset>
20 times of test
50 kinds of IDs
128bits response
shift
<The shifted response dataset>
K-bits shift one place to the right
depend on the each PUF's property
Not change Reliability
Higher Security (Uniqueness)

Figure 2: Making method of the shifted response dataset in case of one PUF output.

In this paper we test experimentally the effects of shift function in the PUF output. By doing so, we hope to get an ideal security (uniqueness) results while maintaining the reliability. Figure 2 shows a making of the shifted response database. Please note that shifting K–bit to the right depend on an intrinsic property of each PUF. In our experiment, the shifting we have used for testing is fixed K–bit, such as 8-bit for PUF1, 16-bit for PUF2 and 128-bit for PUF16.

4 Experimental Results

4.1 Testing of an Arbiter PUF output

The FPGA used in this experiment is Xilinx's Virtex–5LX (xc5vlx30–ffg324) and Spartan–3A (xc3s400a–ftg256) on SASEBO–GII evaluation boards[11]. In this paper we select only 16 PUF outputs with 20 times of test and 50 kinds of IDs (called "AIST dataset" in Fig. 1), out of a total of 45 Arbiter PUF (Fig. 3) outputs which are tested in Ref. [12].

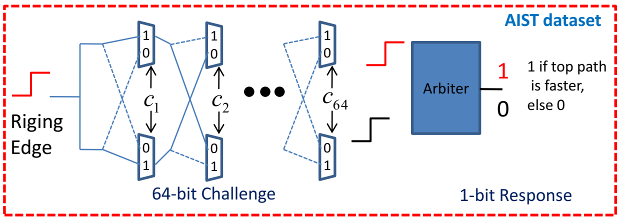

Figure 3: Arbiter PUF scheme.

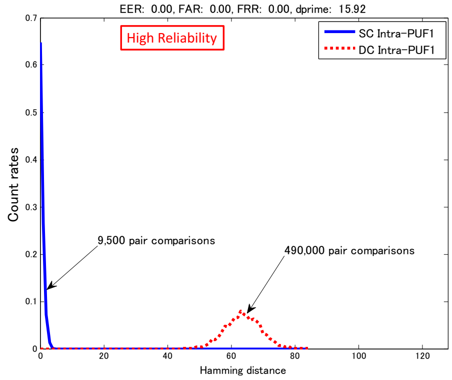

Figure 4: Distribution of SC Intra–PUF and DC Intra–PUF (Reliability in Arbiter PUF1).

We tested firstly the reliability of each PUF output. As shown in Figure 4, the SC Intra–PUF distribution and the DC Intra–PUF distribution are computed and graphically reported to show how the PUF algorithm separates the two classes. This shows the histogram of the count rates versus hamming distance against the PUF1 output. In this experiment, we can get an ideal results which does not have any errors. As shown in Table 1, all of the other results have also been achieved with zero error rate. Therefore, we can conclude that the reliability of each PUF output is high.

Table 1: Error rate and d-prime of each DC Intra–PUF against SC Intra–PUF (Reliability in 16 Arbiter PUFs).

PUF	EER(%)	FAR(%)	FRR(%)	d-prime
1	0	0	0	15.92
2	0	0	0	16.15
3	0	0	0	15.76
4	0	0	0	15.66
5	0	0	0	16.10
6	0	0	0	16.01
7	0	0	0	16.43
8	0	0	0	15.86
9	0	0	0	16.04
10	0	0	0	16.15
11	0	0	0	16.23
12	0	0	0	15.75
13	0	0	0	15.98
14	0	0	0	16.19
15	0	0	0	16.04
16	0	0	0	15.90

In addition, we have considered the error rate and d-prime to check security (uniqueness) among each others (SC Intra–PUF and SC Inter–PUF). Figure 5 shows the histogram of the count rates versus hamming distance against combined all of PUF output (16 Arbiter PUFs). In this experiment, the threshold number is set at 4 and EER is 2.72 %. Figure 6 shows ROC curve

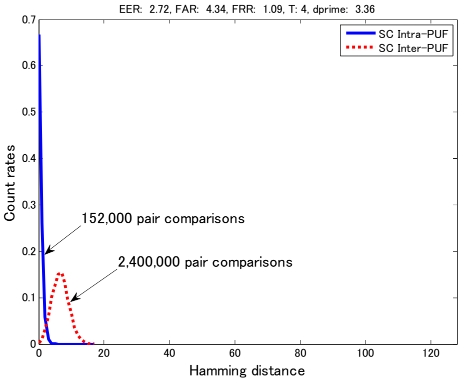

Figure 5: Distribution of SC Intra–PUF and SC Inter–PUF which are combined with all pair comparisons (SC Intra–PUF with 16 Arbiter PUFs is 9,500 pair comparisons × 16 PUFs = 152,000) (SC Inter–PUF with 16 Arbiter PUFs is 2,400,000 pair comparisons).

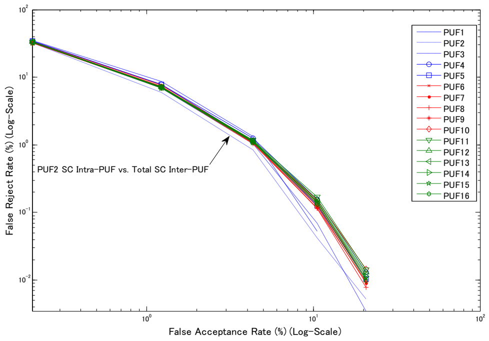

Figure 6: Receiver Operation Characteristics (ROC) curve of each SC Inter–PUF against SC Intra–PUF.

Table 2: Error rate and d-prime of each SC Inter–PUF against SC Intra–PUF (Security in Arbiter PUFs with non-shifted data).

PUF	EER(%)	FAR(%)	FRR(%)	d-prime
1	2.8334	4.3405	1.3263	3.3317
2	2.5887	4.3405	0.8368	3.3838
3	2.6931	4.3405	1.0456	3.3683
4	2.8005	4.3405	1.2605	3.3447
5	2.7345	4.3405	1.1284	3.3486
6	2.7325	4.3405	1.1246	3.3527
7	2.7056	4.3405	1.0707	3.3616
8	2.7071	4.3405	1.0737	3.3602
9	2.6849	4.3405	1.0292	3.3671
10	2.7224	4.3405	1.1042	3.3663
11	2.7626	4.3405	1.1847	3.3586
12	2.7488	4.3405	1.1570	3.3578
13	2.7306	4.3405	1.1206	3.3610
14	2.7281	4.3405	1.1158	3.3634
15	2.7376	4.3405	1.1347	3.3609
16	2.7173	4.3405	1.0941	3.3622

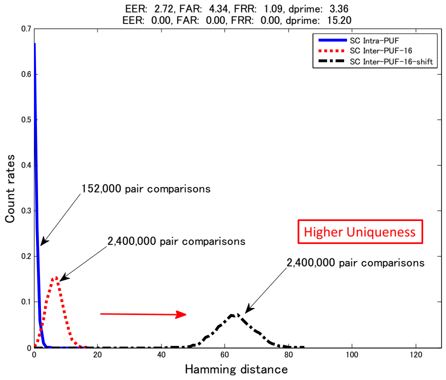

Figure 7: Histogram results using non-shifted data and shifted data (Security in Arbiter PUFs).

on a logarithmic scale. Table 2 shows the results of error rate and d-prime using Inter–PUF output. Even though this performance is applicable to non-strict authentication system, it is not suited for strict authentication system such as cryptographic applications. In order to solve this problem, we have applied a shift post-processing in the PUF output and got a perfect results applicable to strict authentication system.

Figure 7 shows the histogram of the count rates versus hamming distance against combined all of PUF output (16 Arbiter PUFs) including the result with shift post-processing. As shown in this figure, the distribution with shift post-processing (SC Inter–PUF–shift) had an ideal result, which does not have any errors and d-prime is 15.20, against SC Intra–PUF.

4.2 Testing of a Ring Oscillator PUF output

In this experiment we select only 16 PUF outputs with 20 times of test and 50 kinds of IDs out of a total of 125 Ring Oscillator PUF (Fig. 8) outputs (called "VirginiaTech Dataset" in Fig. 1) which has been collected in 125 Xilinx Spartan (XC3S500E) FPGAs[8] (In each output, there are 512 lines for 512 ROs and each of the line contains 100 RO frequencies).

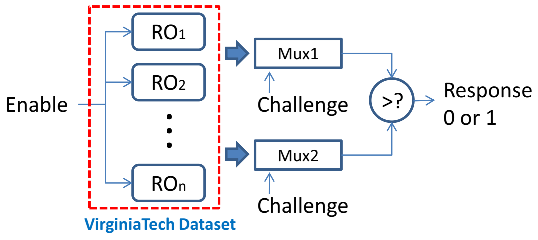

Figure 8: Ring Oscillator PUF scheme (512 ROs, so 9bits of two different challenges are used).

We tested firstly the reliability of each PUF output. As shown in Fig. 9 and Table 3, all of the results have been achieved with zero error rate. Therefore, we can conclude that the reliability of each RO–PUF output is high.

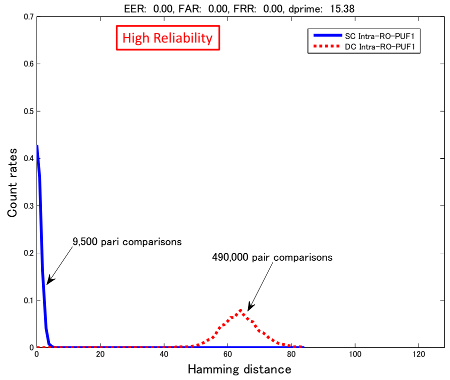

Figure 9: Distribution of SC Intra–PUF and DC Intra–PUF(Reliability in RO–PUF1).

Table 3: Error rate and d-prime of each DC Intra–PUF against SC Intra–PUF (Reliability in 16 RO–PUFs).

RO–PUF	EER(%)	FAR(%)	FRR(%)	d-prime
1	0	0	0	15.38
2	0	0	0	15.86
3	0	0	0	15.99
4	0	0	0	16.01
5	0	0	0	15.74
6	0	0	0	15.39
7	0	0	0	15.51
8	0	0	0	16.00
9	0	0	0	15.51
10	0	0	0	15.62
11	0	0	0	15.64
12	0	0	0	15.89
13	0	0	0	15.09
14	0	0	0	15.22
15	0	0	0	15.68
16	0	0	0	15.58

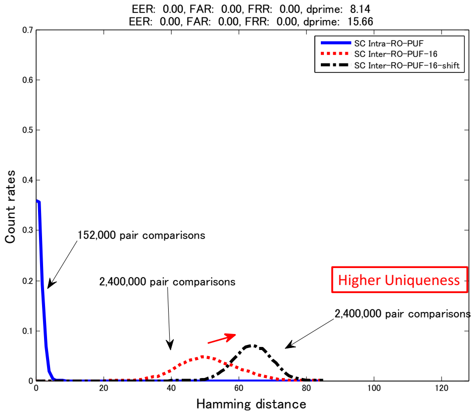

Figure 10: Histogram results using non-shifted data and shifted data (Security in RO–PUFs).

Table 4: Error rate and d-prime of each SC Inter–PUF against SC Intra–PUF (Security in RO–PUFs with non-shifted data).

RO–PUF	EER(%)	FAR(%)	FRR(%)	d-prime
1	0	0	0	8.1872
2	0	0	0	8.1182
3	0	0	0	8.1355
4	0	0	0	8.1367
5	0	0	0	8.1342
6	0	0	0	8.1335
7	0	0	0	8.1293
8	0	0	0	8.1330
9	0	0	0	8.1311
10	0	0	0	8.1333
11	0	0	0	8.1380
12	0	0	0	8.1406
13	0	0	0	8.1451
14	0	0	0	8.1424
15	0	0	0	8.1393
16	0	0	0	8.1363

In addition, we have considered the error rate and d-prime to check security (uniqueness) among each others (SC Intra–RO–PUF and SC Inter–RO–PUF). As shown in Fig. 10 (red dotted line) and Table 4, all of the results have been achieved with zero error rate. So, we can know that the security performance of the RO–PUFs using VirginiaTech dataset is reasonably good, even though d-prime is a little small (=8.14). In order to maintain the stable security, it is deemed desirable to sufficiently separate two distributions. Therefore we can apply the shift function to the PUF output in the same way as the previous section. As shown in Fig. 10 (black dash-dot line), the distribution with shift post-processing (SC Inter–RO–PUF–16–shift) had an ideal result, which does not have any errors and d-prime is 15.66 against SC Intra–RO–PUF.

5 Conclusion

This study showed experimentally the evaluation of the PUFs including the effects of shift post-processing. In particular, we note that even though this approach is valid only having an intrinsic property as assumption, we are convinced that this could be used as a good approach and will consider applying shifting function to our Arbiter PUF from the point of view of circuit design in the near future.

Acknowledgements

This work is conducted as a part of the project of Core Research for Evolutional Science and Technology (CREST) funded by Japan Science and Technology Agency (JST).

References

[1] Ingrid M.R. Verbauwhede, *Secure Integrated Circuits and Systems*, Springer, 2010.

[2] G. Edward Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," Design Automation Conference (DAC2007), 2007.

[3] J. Lee, D. Lim, B. Gassend, G.E. Suh, M. Dijk, and S. Devadas, "A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications," Symposium on VLSI Circuits, 2004.

[4] R. Maes, P. Tuyls and I. Verbauwhede, "Intrinsic PUFs from Flip-flops on Reconfigurable Devices," 3rd Benelux Workshop on Information and System Security (WISSec2008), 2008.

[5] H. Kang, Y. Hori, T. Katashita, and A. Satoh, "Performance Evaluation for PUF-based Authentication Systems," IEICE Technical Report, RECONF2010-49, Dec. 2010.

[6] A. Maiti, J. Casarona, L. Mchale and P. Schaumont, "A Large Scale Characterization of RO–PUF," IEEE Workshop on Hardware Oriented Security and Trust (HOST2010), 2010.

[7] A. Maiti and P. Schaumont, "Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive," Journal of Cryptology, 2010.

[8] On-chip Variability data. The secure embedded system group of the ECE Department at Virginia Tech,
http://rijndael.ece.vt.edu/variability/download.html.

[9] J. G. Daugman and G. O. Williams, "A proposed standard for biometric decidability," in Proceedings of CardTech/SecureTech Conference, pp. 223-234, 1996.

[10] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," Advances in cryptology-Eurocrypt 2004, LNCS3027, pp.523-540, Springer Verlag, 2004.

[11] National Institute of Advanced Industrial Science and Technology (AIST),
http://www.rcis.aist.go.jp/special/SASEBO/.

[12] Y. Hori, T. Katashita, A. Satoh and T. Yoshida, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs," 2010 International Conference on ReConFigurable Computing and FPGAs (ReConFig 2010), 2010.