Performance Evaluation of the First Commercial PUF-embedded RFID

Hyunho Kang, Yohei Hori, Akashi Satoh
National Institute of Advanced Industrial Science and Technology (AIST),
Tsukuba, Ibaraki, Japan
Email: {h-kang, hori.y, akashi.satoh}@aist.go.jp

***Abstract*—Physical unclonable functions (PUFs) generate device-unique data streams by using manufacturing variations of each LSI. High-security authentication for counterfeiting prevention and secret key generation for data encryption are provided through PUFs. Such technology is a recent innovation, and Verayo Inc. created the world's first commercially available PUF only a few years ago. Toppan Printing Co., Ltd., has since integrated Verayo's PUF ICs into radio frequency identification (RFID) tags in order to develop a new security business in the near field communication market. In collaboration with Toppan, we have conducted acceleration tests on their PUF-embedded RFID tag to evaluate its performance and reliability.**

I. Introduction

The use of integrated circuit (IC) cards as a security device is becoming widespread. These cards are based on cryptographic algorithms. A secret key that cannot be accessed from the outside is stored in the nonvolatile memory of the IC, and is the essential information for guaranteeing security. However, the rapid evolution of research on side-channel attacks[1] has shown that a secret key can be obtained by analyzing the power consumption or electromagnetic radiation of a cryptographic device without having to access its internal memory. Along with a cryptographic circuit, an IC card thus requires considerable hardware resources as a countermeasure against such attacks.

The market for radio frequency identification (RFID) tagging is also expanding for product identification, traceability, and counterfeiting prevention. These tags are much cheaper to manufacture than IC cards but support only limited security functions such as a password. A cryptographic algorithm cannot be supported by RFID tags due to their small hardware resources. Therefore, ID data held in RFID tags can be copied, although it would be expensive to do so.

Some standardization activities pertaining to traceability have been conducted, such as the creation of ISO/PC 246 (anti-counterfeiting tools) and ISO/TC 247 (fraud countermeasures and controls) which require the issuing of a unique ID for each product. While such standards deter counterfeiting, copying of the ID itself is still possible. Moreover, this approach benefits only the manufacturers and suppliers, who want to prevent counterfeit goods from entering the market. Consumers, however, must also be able to check the authenticity of products at the time of purchase because an unscrupulous retailer may purposefully sell counterfeit goods.

The physical unclonable function (PUF)-embedded RFID tag developed by Verayo Inc.[2][3] and Toppan Printing Co., Ltd.,[1] is a unique device equipped with near field communication (NFC) functionality. This device is the first to enable consumers to check whether a product is an original or counterfeit by using a smartphone with built-in NFC.

In recent years, a number of studies have been conducted to evaluate the stability of PUFs, because their uniqueness is based on sensitive physical characteristics resulting from process variations[4][5][6]. Those studies used experimental PUF circuits on discrete application-specific IC or field-programmable gate array platforms, and were designed for research not commercial products.

In particular, the experimental PUFs receive power directly from voltage sources, whereas the operating power supplied to Verayo's PUF ICs is generated through electromagnetic induction from the RFID technology and is unstable. Therefore, a more careful stability evaluation of Verayo's PUF ICs is required.

In this paper, we evaluate Verayo's PUF ICs under low and high temperatures in order to ensure product quality, reliability, and safety. To the best of our knowledge, this study is the first examination of a commercial PUF.

II. Performance evaluation

Reliability and uniqueness are commonly used to evaluate the form of PUFs. Here, we consider these two evaluation points as shown in Figure 1. Two responses are identical if and only if they are for the same challenge in the same PUF. All other cases are treated as being unrelated.

For the data in this study, we selected the challenge response pairs for 10 test iterations using 100 IDs from each tested PUF-embedded RFID tag (10 different tags implemented by the same circuit structure). In particular, tests were conducted under four temperature environments ranging from -45 to 95 °C. More specifically, we present the change in reliability according to temperature variations by comparing the intra-PUF hamming distances (HDs) for the same challenge (*SC Intra*) and for different challenges (*DC Intra*). We also present uniqueness results from an HD comparison of SC Intra and *SC Inter* (inter-PUFs for the same challenge) when using the 10 RFID tags under each temperature environment.

[1]Toppan Printing Co., Ltd., is a major IC card supplier in Japan

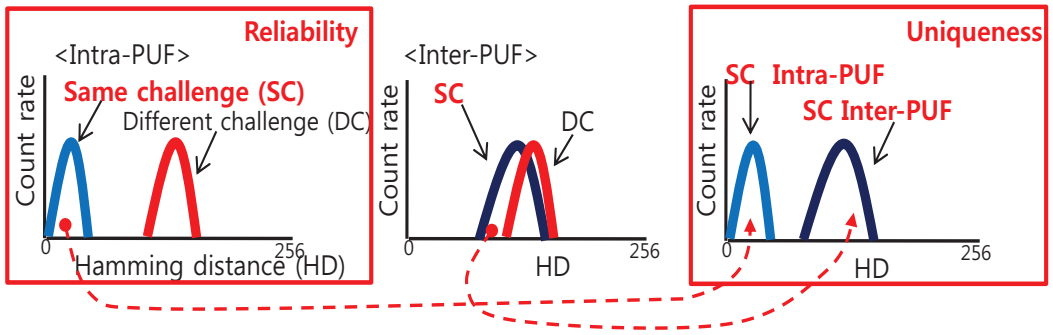

Fig. 1. PUF performance testing

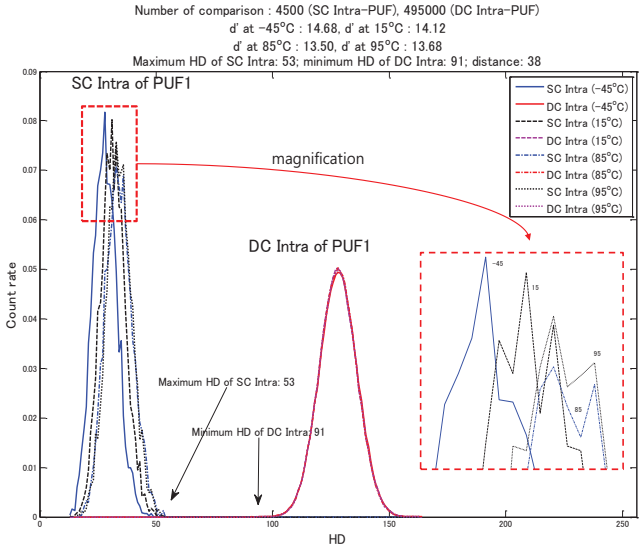

Fig. 2. Reliability of PUF 1: SC Intra and DC Intra HDs.

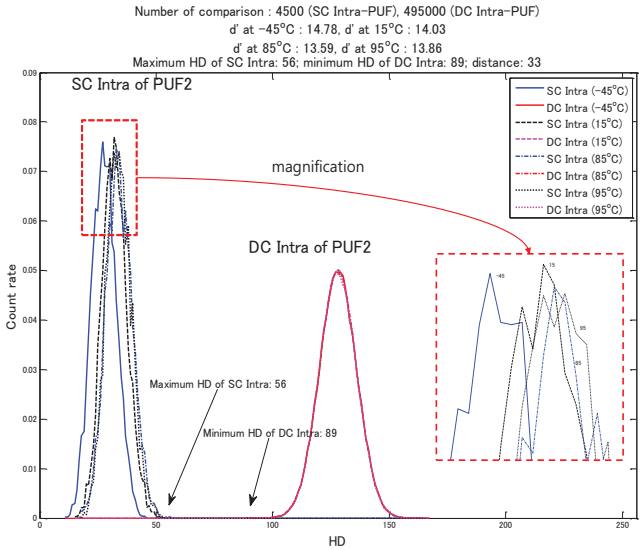

Fig. 3. Reliability of PUF 2: SC Intra and DC Intra HDs.

TABLE I
d' FOR EACH PUF-EMBEDDED RFID ACCORDING TO TEMPERATURE AND DISTANCE BETWEEN SC INTRA AND DC INTRA DISTRIBUTIONS. ("MAX" DENOTES THE MAXIMUM HD OF SC INTRA, "MIN" DENOTES THE MINIMUM HD OF DC INTRA, AND "DIS" DENOTES THE DIFFERENCE BETWEEN THE TWO VALUES.)

PUF Number	-45 °C	15 °C	85 °C	95 °C	MAX/MIN/DIS
1	14.68	14.12	13.50	13.68	53/91/38
2	14.78	14.03	13.59	13.86	56/89/33
3	15.36	15.01	14.56	14.58	53/88/35
4	14.11	13.34	13.17	13.21	58/91/33
5	15.56	14.69	13.95	14.17	55/87/32
6	15.02	14.31	14.09	14.15	57/89/32
7	15.05	14.04	14.01	13.71	53/91/38
8	15.38	14.45	14.22	13.94	57/89/32
9	14.55	13.74	13.24	13.56	58/88/30
10	15.36	14.97	14.14	14.04	54/92/38

A. *Reliability changes according to temperature variation*

Comparing *SC Intra* and *DC Intra* of PUF 1 and 2 in Figure 2&3, we see that the PUF's HD is divided into two distinct classes dependent on the properties of the challenge. The peaks of the two sets of histograms are clearly separated, indicating that errors do not occur in terms of false acceptance rate and false rejection rate. In addition, we define a metric d' 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. d' values are given in Figure 2&3 and are also listed in Table I.

B. *Uniqueness of 10 PUF-embedded RFID tags*

We tested the uniqueness of the 10 RFID tags by finding all *SC Intra* and *SC Inter* HDs under each temperature environment. As shown in Figure 4, identification errors do not exist, since there is no overlap of the intra and inter SC distributions. d' values are also shown in this figure. Figure 5 & 6 illustrate an error rate diagram, showing the dependency of FAR and FRR as a function of varying thresholds (from the result of figure 4).

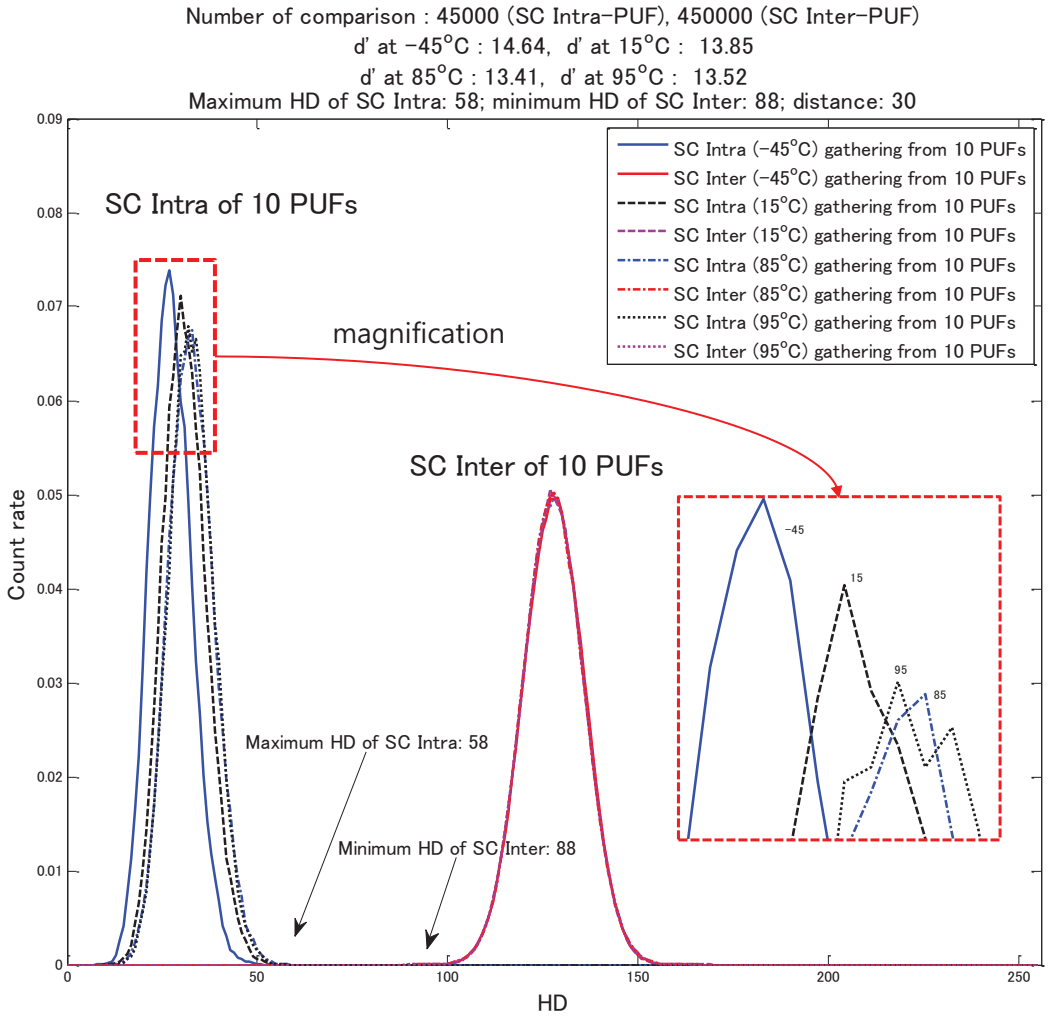

Fig. 4. Uniqueness of 10 PUFs: SC Intra and SC Inter HDs.

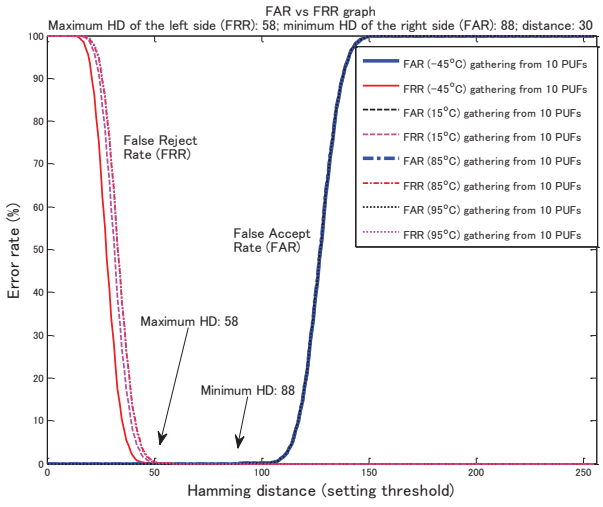

Fig. 5. Threshold-based error rate diagram.

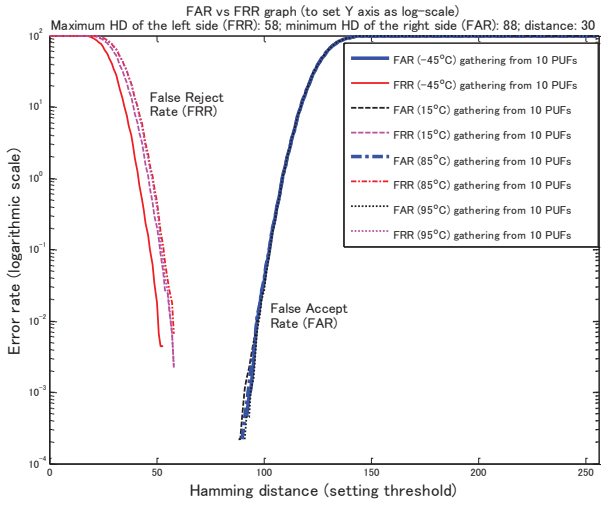

Fig. 6. Threshold-based error rate diagram.(a logarithmic scale for the y-axis)

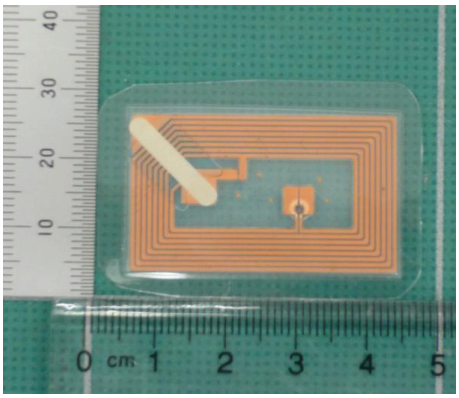

Fig. 7. PUF-embedded RFID used in the experiment.

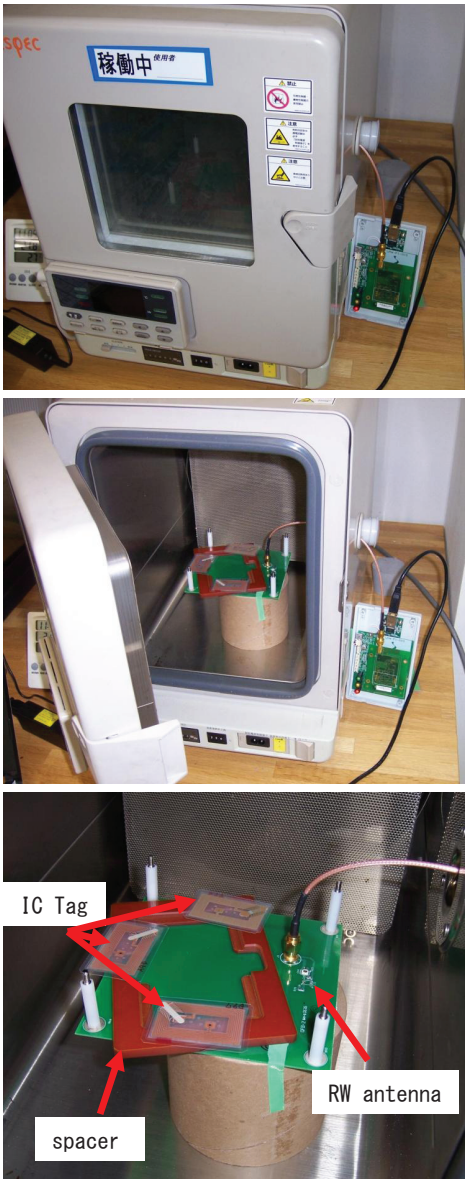

Fig. 8. Thermostatic oven used in the experiment.

C. Experimental setup

Figure 7 shows the PUF-embedded RFID used in our experiment. The tags were placed in the thermostatic oven (Figure 8). As I mentioned earlier, tests were conducted under four temperature environments ranging from -45 to 95°C.

III. Conclusion

The performance of a commercial PUF integrated into an RFID tag has been evaluated in terms of reliability and uniqueness. The results showed excellent performance under a wide range of temperatures without any operation errors or false identifications. Thus, this highly reliable PUF that supports the NFC interface provides real-time identification to prevent counterfeiting. Similar to conventional RFID tags, the PUF-embedded RFID tag can be manufactured at low cost, and a challenge-response authentication scheme using unclonable LSI process variation provides a considerable advantage over conventional tags whose IDs can be cloned. Hence, the investigated PUF-embedded RFID tag, which realizes these valuable features, is a promising technology to expand security applications that cannot be covered by conventional IC card and RFID tag technologies.

Acknowledgment

The authors would like to thank Toppan Printing Co., Ltd. for their valuable contribution in data collection, and Verayo Inc. for their useful comments.

References

[1] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," CRYPTO'99, LNCS 1666, Springer-Verlag, 1999.
[2] Verayo Inc. [Online]. Available: http://www.verayo.com.
[3] *Physical Unclonable Function Is Ushering a New Era for Security*, SmartCards Trends, OMNIPRESS, Dec-January 2012.
[4] B. Gassend, D. Clarke, M. Dijk and S. Devadas, "Silicon Physical Random Functions," Proceedings of the 9th ACM conference on Computer and Communications Security (CCS), 2002.
[5] M. Yu, A. Singh, R. Sowell, D. M'raihi and S. Devadas, "Performance Metrics and Empirical Results of a PUF Cryptographic Key Generation ASIC," IEEE International Symposium on Hardware-Oriented Security and Trust, June 2012.
[6] Y. Hori, T. Yoshida, T. Katashita and A. Satoh, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs," IEEE International Conference on ReConFigurable Computing and FPGAs (ReConFig), Dec. 2010.