PUFs Analysis for Unstable Signals Using Analog Circuit

Ryota Soga[1]* and Hyunho Kang[2]†

[1]Advanced Course of Electrical and Electronic Engineering
[2]Department of Electronic Engineering
National Institute of Technology, Tokyo College, Tokyo, Japan
s15109.kang@gmail.com, kang@tokyo-ct.ac.jp

Received: April 30, 2022; Accepted: June 24, 2022; Published: July 5, 2022

Abstract

To date, physical unclonable functions (PUFs) have been extensively examined, and are used to distinguish genuine and counterfeit products. Moreover, they are also attracting attention as one of the methods to solve the security problems of Internet of Things (IoT) devices. However, most PUFs are based on integrated circuit (IC) memory and use digital modulation for authentication. This study proposes a new PUF that uses analog circuits and analog values for authentication. The advantage of analog circuits is that they can handle analog values. Moreover, their characteristics do not change when the surrounding environment is adjusted. Research on analog PUFs that evaluate stable signals and DC voltages has been proposed to date. This study uses an astable multivibrator to analyze PUFs for unstable signals. For analysis, we examine the conventional method of calculating the hamming distance of digital values and the method using machine learning(ML). Consequently, we were able to identify individuals with unsteady signals from analog values when using ML.

Keywords: Physical Unclonable Function, Analog Elements, Astable Multivibrator, Machine Learning

1 Introduction

The physical unclonable function (PUF) is often referred to as the fingerprint of an object; it identifies objects using small differences that occur during manufacturing [1]. This technology is now being considered for use in identifying imitation products such as brand-name goods and vehicles [2], as well as for use in radio frequency identification (RFID) and other authentication circuits [3]. It can also be used for cryptographic key generation. It includes Internet of things (IoT) devices, which are rapidly expanding in the market. IoT devices will be used in a wide range of fields, including smart homes and smart cities, and will continue to develop as a technology, to enrich people's lives further. However, IoT [4, 5] entails a few problems like the security issue of vulnerability. It is impossible to manage unauthorized access by hackers owing to the hardware limitations of IoT devices. Therefore, PUFs, which can generate fingerprints in hardware, are attracting attention as a method to solve this problem [6, 7].

To date, most PUFs can be used in many products. Therefore, there has been extensive research on PUFs derived from arbiter PUFs [8–11], and memory-based PUFs [12] (such as SRAM PUFs [7,13]) that exploit the randomness of the initial memory state. In recent years, many studies have been conducted

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 8, Article No. 4 (July 5, 2022)
DOI:*10.22667/ReBiCTE.2022.07.05.004*

*He works at NTT communications from April 2022.

†Corresponding author: Department of Electronic Engineering, National Institute of Technology, Tokyo College, 1220-2, Kunugida-machi, Hachioji-shi, Tokyo, 193-0997, Japan

on PUFs that are resistant to attacks using machine learning(ML) [9, 14–19]. However, the original low cost of PUFs has been ignored.

This study proposes a PUF that uses analog devices. Because many IoT devices contain many analog elements, we assume it is possible to create a PUF for each device individually. Our research on analog PUFs proposes two methods, one using a resistor matrix circuit [20] and the other using a Hartley oscillator circuit [21]. However, research on analog PUFs is still in its early stages and cannot be applied to many devices. Therefore, this study proposes a PUF based on an astable multivibrator using analog devices. The advantages of using analog devices are as follows.

(1) It is possible to conduct an evaluation from the components installed in the device and authenticate with analog values instead of digital values.

(2) Analog devices contain non-linear elements such as diodes, which are considered highly unpredictable.

(3) Many analog devices entail errors.

(4) If the operating environment is the same, the characteristics do not change.

(5) Analog devices are inexpensive.

This study further attempts to identify individuals with PUFs using astable multivibrators. Although the output signal of an astable multivibrator is unstable, we show that it is possible to identify individuals using ML, which is usually used as an attack method. This study contributes to this field by developing a PUF that can manage unstable devices.

This paper proceeds as follows. In Section2, we briefly explain the PUFs and show the representative PUFs that have been studied so far. In Section3, we describe an astable multivibrator. The experimental methods and evaluation techniques are introduced in Section4. In Section5, we discuss the experimental results of PUFs based on astable multivibrators. In Section6, we present the future issues of analog PUFs and the conclusions of this study.

2 Physical unclonable function

PUFs are referred to as “fingerprints of things”; they are a system used for authentication based on minute internal differences that occur during manufacturing. Because these small differences are physically impossible to clone, they are expected to be a very powerful security system.

A PUF is a function that outputs response bits when a signal is input (Fig. 1) [22]. Although response bits are apparently the same products, they are randomized using uncontrollable parameters generated during manufacturing. Therefore, PUFs are easy to construct but highly robust against cloning attacks. The input signal is generally referred to as the challenge “C” and the output is referred to as the response “R”. The combination of these inputs and outputs is referred to as a challenge-response pair (CRP). Moreover, PUFs are inexpensive as they use the differences that are inherent in the product from its manufacturing.

2.1 Requirements for PUFs

There are several requirements for PUFs as follows:

(1) Uniqueness: There is a property that when the same challenge C is given to different PUFs, the response R will be different (Fig. 2a). This property must be considered in all individuals.

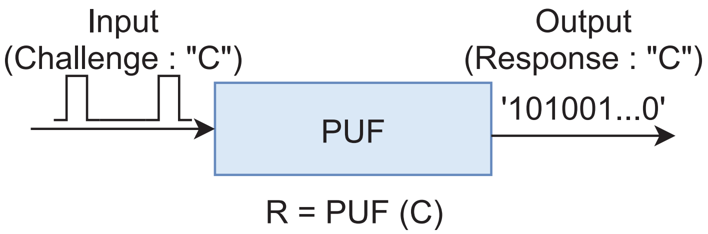
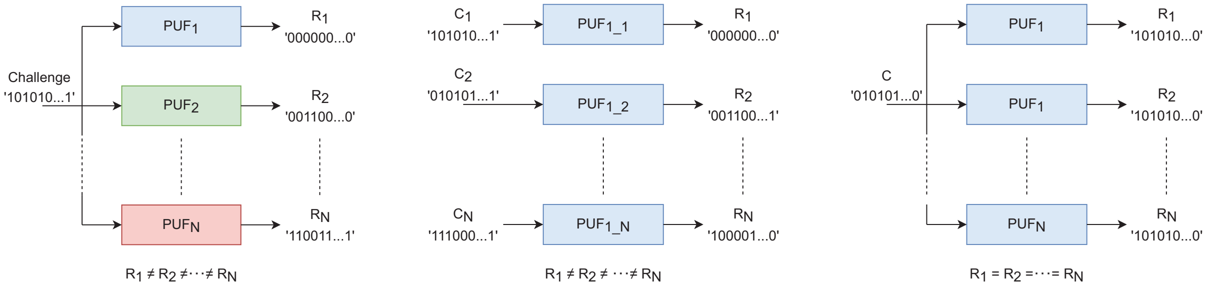


Figure 1: Physical Unclonable Function.



(a) Uniqueness.

(b) Different Responses.

(c) Reproducibility.

Figure 2: Uniqueness, Different Responses, Reproducibility.

(2) Different Responses: When the same PUF is given different challenges C, the responses R all have different properties (Fig. 2b).

(3) Reproducibility: When the same PUF is given the same challenge C N times, the response R remains the same for all N times (Fig. 2c). Reproducibility was evaluated by calculating the Hamming distance (HD), where the ideal HD is zero.

(4) Irreversibility: PUFs can get a response R if it is given a challenge C. However, it cannot obtain the challenge C from response R (Fig. 3). This indicates that this is an irreversible function. This property will not disappear despite a large number of responses R.

(5) Unclonability: The attacker analyzes the PUFs to misidentify the fake individual (cloned PUF) to the authentication system as if it were the real thing. PUFs cannot be physically replicated despite the attacker having physical access to the PUF system (Fig. 4).

(6) Unpredictability: Attackers are unable to predict the response R to challenge C even when an unlimited number of CRPs are obtained from the same PUF (Fig. 5). This property also holds when CRPs are obtained from different PUFs.

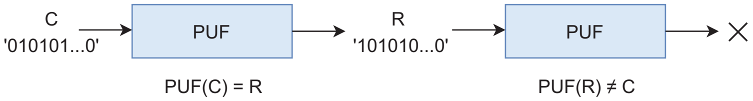


Figure 3: Irreversibility.

We consider the uniqueness (1) and the reproducibility (3) of the most important issues in this study. Therefore, this study focuses on two points.

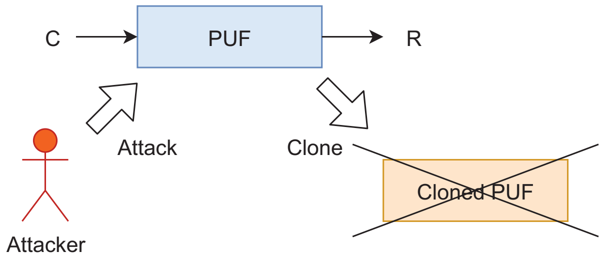


Figure 4: Unclonability.

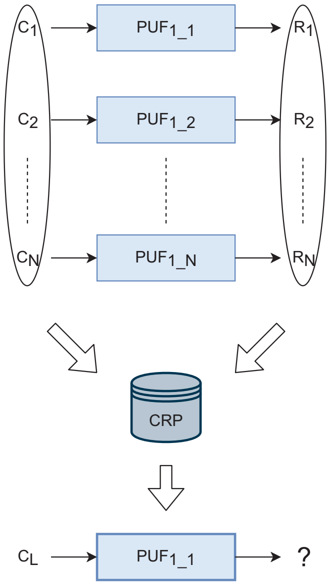


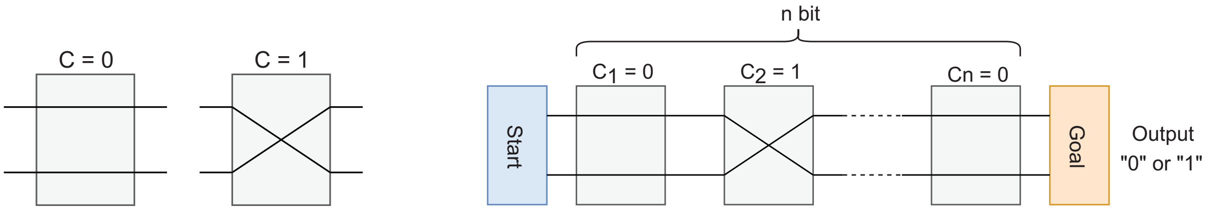
Figure 5: Unpredictability.

2.2 Representative PUFs

The number of PUF types is still increasing. In recent years, most of the research has been conducted using typical PUFs with good performance and low cost. There is a study that uses XOR on response "R" to generate a new response "R'", which is resistant to attacks. Additionally, other methods have been investigated, such as using representative PUFs multiple times to obtain response "R". This study gives only a few examples. In this section, we introduce the original PUFs that have been the core of recent research on PUFs.

(1) Arbiter PUF: APAF takes advantage of the inherent delay characteristics of ICs owing to manufacturing variations; it builds a delay path as shown in Fig. 6a and eventually contends transitions to generate a 1-bit response that outputs 0 or 1 depending on whether the rising edge reaches the output arbiter block first(Fig. 6b). Additionally, we can use an n-bit challenge as input. It also takes an n-bit challenge as input and constructs a delay path to generate 1-bit output. APUF has been the subject of extensive research so far, including XOR ArbiterPUF [10], and is considered vulnerable to ML attacks. Therefore, many related studies opt to apply APUF to overcome this problem.

(2) SRAM PUF: SRAM PUF is among the most useful practical PUFs. The SRAM memory element comprises a set of inverters and access transistors so that there are two stable situations at a given



(a) Arbiter block.

(b) Overview of Arbiter PUF

Figure 6: Arbiter PUF

input voltage. The threshold voltages of these devices vary according to variations during manufacturing. This randomness causes every SRAM cell to have a unique state every time the SRAM voltage is turned on. This means that the response of the SRAM PUF generates a unique and random pattern of 0 and 1.

Many of these PUFs rely on digital elements. We further introduce PUFs that perform authentication using analog elements.

(A) Resistor Matrix PUF: The RePUF generates response bits by evaluating the voltage of each resistor in a group of resistors connected in series and parallel [20]. Resistors are packaged with miscalculations from the time of manufacture and are considered to have high randomness. Additionally, resistors are used in many electronic circuits, including IoT devices, and are easy to construct.

(B) Hartley oscillator PUF: The Hartley oscillator PUF is composed of a Hartley oscillator circuit and an operational amplifier that amplifies its output [21]. The PUF is based on the error of the analog element. Moreover, sine waves can be used as a feature extraction method for analog PUFs following the advent of PUF. Moreover, continuous signals can be handled. PUF is also easy to construct and low in cost, as well as the resistor matrix PUF.

3 Astable multivibrator

A typical astable multivibrator consists of a circuit, as shown in Fig. 7. To date, circuit schemes other than those shown in Fig. 7 have been proposed for astable multivibrators [23–25]. This circuit generates a square wave, as shown in Fig. 7. However, because the pulse width is a function of the maximum output voltage of the operational amplifier, it is difficult to obtain a highly accurate period owing to the effects of voltage supply fluctuations, temperature changes, and errors in each element. This study takes advantage of this drawback and uses the unstable output as a PUF.

This circuit is a combination of an inverting input RC circuit and a Schmitt trigger circuit. Initially, when v$_a$ = 0 V in Fig. 7, the output voltage is v$_0$ = $+V_0$. Subsequently, the capacitor is charged and v$_a$ increases. Further, when v$_a$ exceeds the threshold value, the Schmitt trigger circuit sets the voltage to v$_o$=$-V_0$. Subsequently, the capacitor is discharged, v$_a$ becomes low again, and v$_0$=$+V_0$. This charging and discharging of the capacitor cause the output of a square wave. The oscillation frequency at this time is defined by Eq. (1).

$$f = \frac{1}{2R_f C ln(\frac{R_1+2R_2}{R_1})} \tag{1}$$

4 Verification method

4.1 Experimental Methods

To date, analog PUFs have been verified by taking the HD of each response. In this study, we compare and verify two methods: transforming the response and usinge the HD (conventional method), and discriminating the analog signal output from the circuit by ML.

The specific experimental procedure is described below.

Table 1: Analog device value.

Element	Value	Element	Value
R_1	1kΩ ± 5 %	R_{f1}	7.1kΩ ± 5 %
R_2	10kΩ ± 5 %	R_{f2}	1kΩ ± 5 %
R_3	10kΩ ± 5 %	C_1	0.01μF +80%∼-20%
R_x	3.4kΩ ± 5 %	C_2	0.1μF +80%∼-20%

(1) Construct a circuit as shown in Fig. 8. In this case, five identical circuits are prepared for comparison. The details of the elements used are given in Table 1. Unlike Fig. 7, R_f is divided into three resistors, to increase the number of elements that entail errors. Furthermore, R_x configured the circuit, as shown in Fig. 9, as a preliminary step to introduce future challenges. Additionally, capacitor C_1 was connected to reduce the input noise.

(2) Connect a DC power supply to the circuit. At this time, the voltage should be 5V.

(3) The output signal was evaluated using a Picoscope. The number of measurement plots was set to 10000, and the measurement resolution was set to 16 bits. The sampling cycle was set to 1μ s.

(4) Each circuit was evaluated 1000 times for a total of 5000 times.

(5) Process① according to the flowchart in Fig. 10 to calculate and evaluate HD.

(6) Evaluated the data by calculating HD for the same process as in (5) and the data processed in ②.

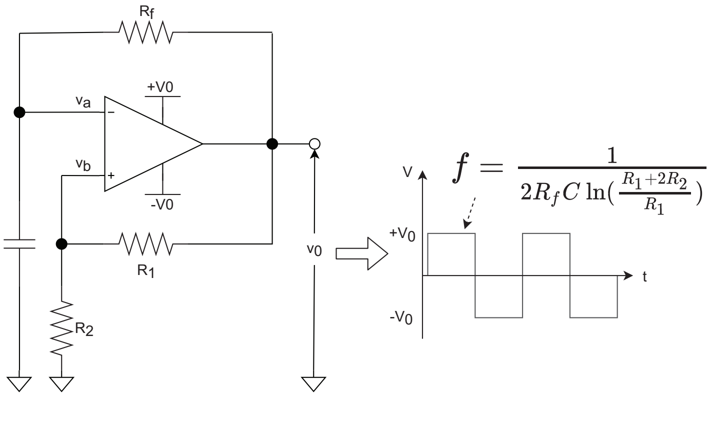


Figure 7: Astable multivibrator.

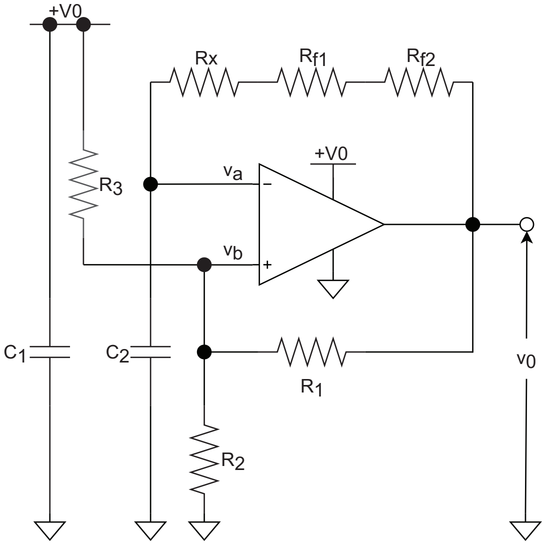


Figure 8: Astable multivibrator circuit for measurement.

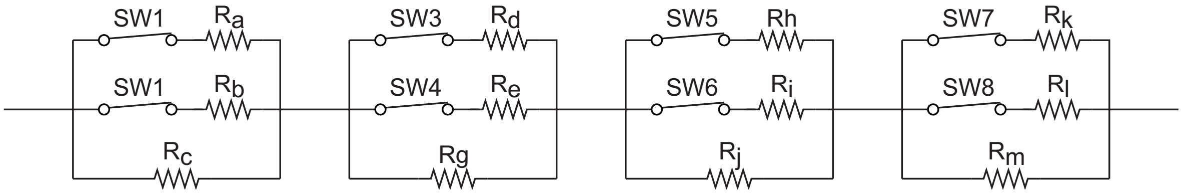


Figure 9: Combined resistance Rx.

(7) We used ML to identify the output signals. Fig. 11 shows the specific method for training the data. Here, we used XGBoost [26] to construct the model.

(8) The output signals were identified using the Deep Learning (DL). The details of the data used for training are an integration of feature data and measurement data in (7).

Note that (7) and (8) are analog values, unlike conventional PUFs. This analysis is a contribution of this study.

5 Performance evaluation

5.1 When calculating HD

First, Fig. 12 shows the result of calculating the HD of the output signal based on the process① in Fig. 10. The data length of the generated identification code was 5120 bits. The orange graph represents reproducibility. Ideally, the orange graph should be distributed at zero. The blue graph on the right side shows the uniqueness of the results, which is the result of the HD calculations for the same PUF. In the case of the blue graph, the farther away from the orange graph on the left, the higher the performance of the PUF. In other words, the distance between orange and blue graphs indicates that the PUFs can be identified, which means that the PUFs have minimum performance. The results of each evaluation based on Daugman's evaluation method are shown in Table 2.

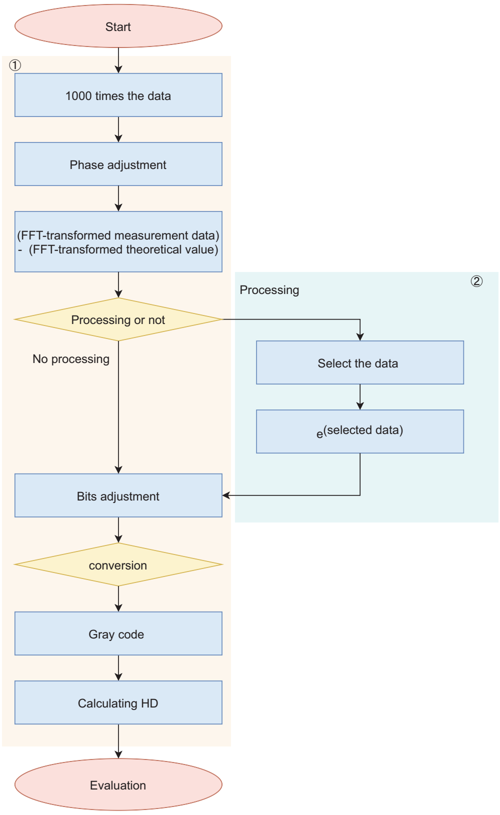


Figure 10: Data processing methods.

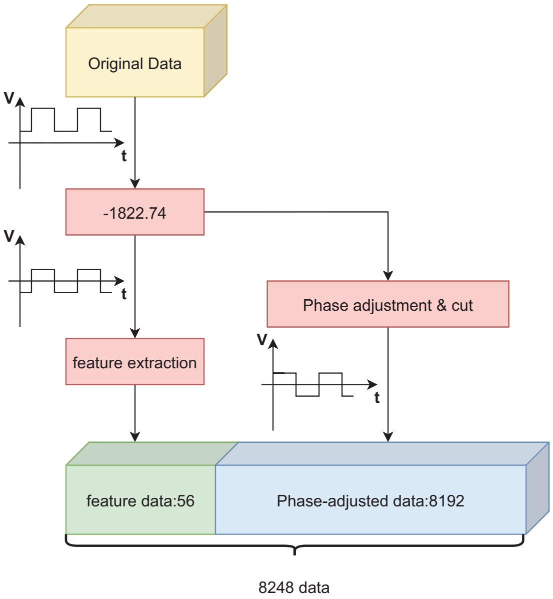


Figure 11: Training data processing methods.

From this result, it is clear that the graphs of reproducibility and uniqueness overlap over a wide range, as in PUF1 in Fig. 12. In other words, it does not demonstrate the performance of a PUF. The result of d', which indicates the degree of dispersion, is also not close to zero, which means that the

Table 2: d'in gray code.(process①)

Individual	Same individual HD maximum values	Other individual HD minimum values	d'
PUF1	376	6	0.7723
PUF2	349	6	1.363
PUF3	393	6	1.052
PUF4	395	6	1.152
PUF5	373	6	0.9384

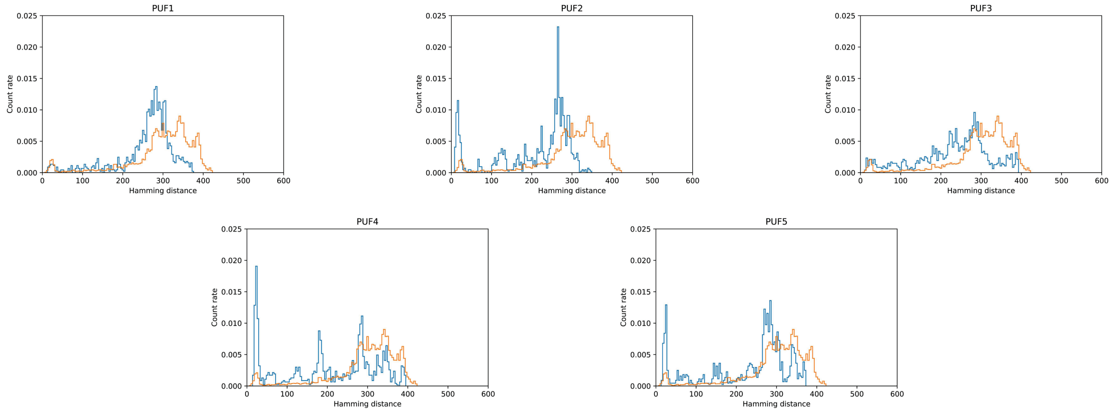


Figure 12: HD calculation result by Process① (gray code).

performance of the PUF is low. We believe that this is because of the characteristics of the astable multivibrator. The astable multivibrator outputs a square wave that is not stable, so the output values are similar, but not exactly the same. This is why the reproducibility graph was not distributed around zero. Furthermore, the reason why the uniqueness graph overlapped with the reproducibility graph is also attributed to the fact that no processing was conducted to increase the small difference with other

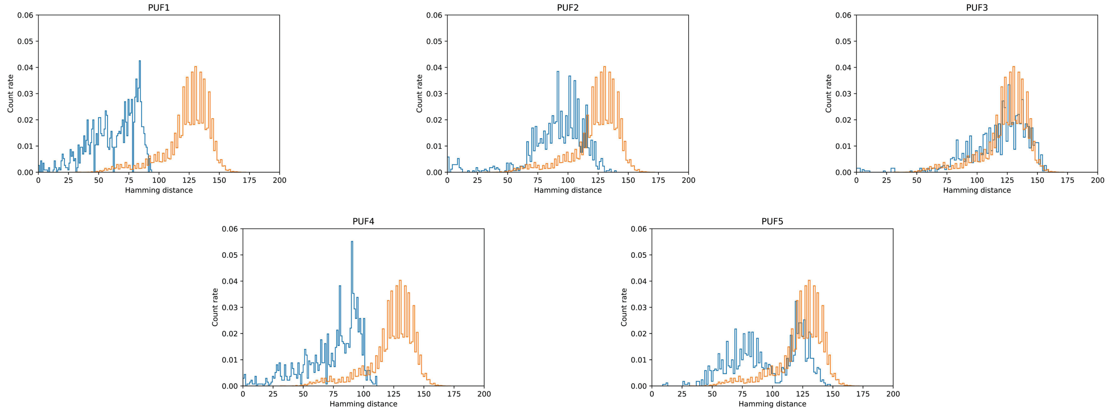


Figure 13: HD calculation result by Process①+② (gray code).

Table 3: d'in gray code.(process①+②)

Individual	Same individual HD maximum values	Other individual HD minimum values	d'
PUF1	94	31	3.749
PUF2	140	31	1.716
PUF3	159	31	0.2538
PUF4	111	31	2.680
PUF5	148	31	1.291

circuits. Further, Fig. 13 shows the results of the HD calculation when process① was added to process②. The results of d' are also shown in, Table 3. The result of the generated identification code has a greater value of d' compared to the result of processing① only, which means that the performance of a PUF is improved. Additionally, as shown in the figure, the range of overlap between reproducibility and uniqueness became narrower. This may be attributed to the fact that the small differences in the astable multivibrator were increased by processing②. Based on the above results, it is clear that the performance of reproducibility and uniqueness is improved, but the performance as a PUF is not satisfied by our method. However, although it requires improvement, we believe that it is possible to use it as fingerprint authentication. This is because by setting a certain threshold value, the graphs of reproducibility and uniqueness can overlap relatively, which is similar to the current authentication technology.

5.2 When using the ML

The process of generating the data used for training is presented in Fig. 11. This is a data set that integrates the original data of the waveform with the chromatogram, the root mean square (RMS) of each frame, the centroid, the spectral bandwidth of the second order, the roll-off frequency, the zero-crossing rate, the chord, and percussive components, and the mean and variance of the 20 Mel frequency cepstral coefficients (MFCCs) calculated from the waveform [27]. In this method, 4000 training data and 1000 test data were randomly selected for training and tuning. The results are shown in Fig. 14, which shows that the higher the accuracy, the better the discrimination. In this experiment, the accuracy of the test data was 99.7%, which satisfies the performance requirements for a PUF. We believe that this result was obtained because we trained the data with analogous values of the feature data and original data. Regarding the PUFs that were identified incorrectly, we believe that the probe contact and small changes in the voltage source were the factors. In other words, we show that it is possible to identify unstable signals, such as astable multivibrators with analog values.

5.3 When using the DL

The data used for training in this method were the same as those used in the ML method. We randomly selected 4000 training data and 1000 test data for training. A diagram of the trained model is presented in Fig. 15. Fig. 16 shows the results of training using this model, and the accuracy of the test data is 98.9%. This result indicates that the performance of the PUF is not satisfactory. However, it is possible to identify data with very high accuracy. We believe that this accuracy indicates the possibility of its use as an authenticator. Seemingly, the identification accuracy did not reach 100% owing to the effect of the probe and voltage source, as in ML. Additionally, the model used for learning was also significantly affected, which may have prevented the achievement. This means that we can achieve a 100% discrimination rate using DL by identifying the best model.

6 Conclusion

This study uses an astable multivibrator as an unstable signal source for the analysis. First, in the conventional method of calculating HD with digital values after processing the data, the graphs of reproducibility and uniqueness overlap, and the results do not show the performance of the PUF. However, the results of combining processes ① and ② during data processing showed that the graphs of the PUFs were relatively separated. Therefore, we believe that the PUFs can be used for authentication by setting a threshold.

The ML-based method resulted in a high identification rate of 99.7%. This result indicates that individual identification is possible, even from analog values. This means that even for IoT devices that use analog elements, PUFs can be used to provide security protection without the need for additional components, if periodic signals such as capacitor charge and discharge circuits can be evaluated. This means that security protection can be achieved easily and at a low cost. Additionally, we show the possibility of applying the PUF to other analog circuits that output waveform signals to protect the security of those circuits. We believe that this study makes a significant contribution to the development of this field.

The identification rate for the method using DL was 98.9%, which is lower than that of the method using ML, but still high. This result is significantly influenced by the model. However, we believe that security can be protected by preparing a suitable model for each circuit.

Comparing all the methods, the method using digital values did not show any performance as a PUF, while the method using analog values with ML/DL showed performance as a PUF. We believe that this indicates that the conversion from analog to digital values lacks information on small individual differences that occur during manufacturing.

We were unable to introduce a challenge. However, we propose a method to replace a single resistor R with 24 series-parallel connected resistors (Fig. 9), where the composite resistance is R_0. Here, the resistance value R and synthetic resistance R_0 should be equal. This ensures that the output value of the original circuit does not change. The connection can be treated as a digital value, depending on the resistor selected for substitution. Together with the ML/DL method used in this study, we can obtain both analog and digital value elements. This operation is expected to increase the complexity and improve the performance of the PUFs.

Additionally, it is necessary to consider whether the performance of the PUF can be maintained over time and in an ambient environment. As the next step in the development of PUFs, we believe that the

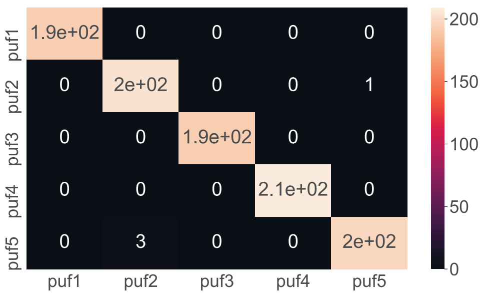


Figure 14: Results of PUF validation by ML.

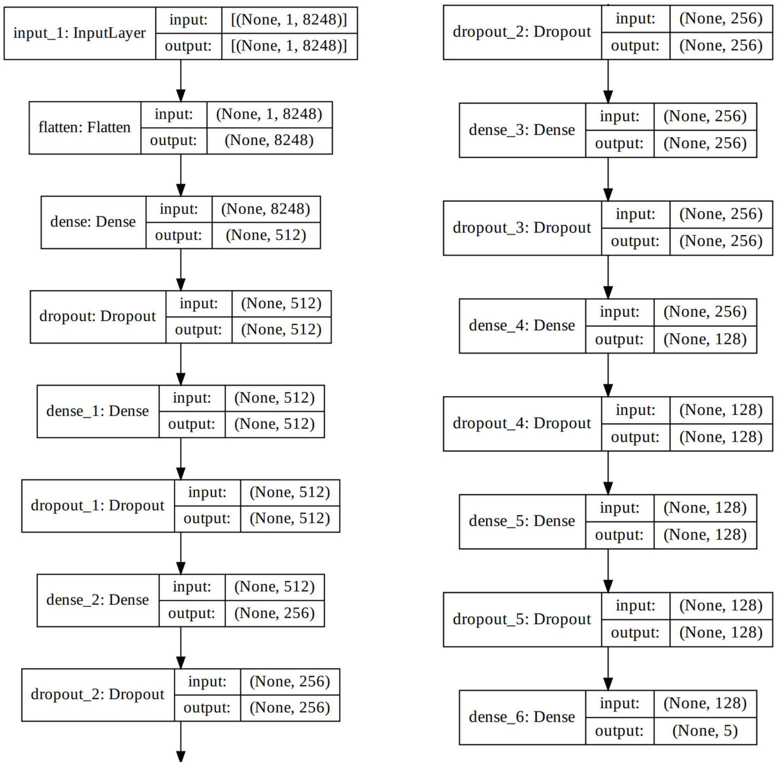


Figure 15: Learning model of DL.

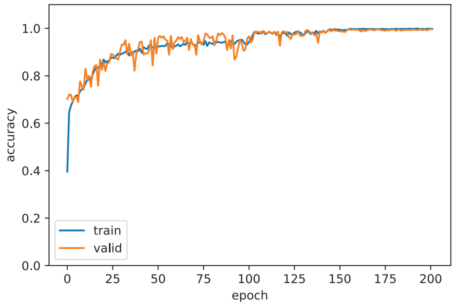


Figure 16: A look at accuracy by DL.

introduction of the ambient environment as a variable in the design of PUFs, such as treating the ambient environment as a challenge and using the change in the characteristics of the device itself as a PUF when the temperature is changed, will be further development in this field. The next step in the development of PUFs is to treat the ambient environment as a challenge and to use the change in the characteristics of the device itself as a PUF when the temperature is changed.

Acknowledgments

This work was supported by JSPS KAKENHI (Grant Number JP19K11977).

References

[1] B. Gassend, D. Clarke, M. Dijk, and S. Devadas. Silicon physical random functions. In *Proc. of the 9th ACM Conference on Computer and Communications Security (CCS'02), Washington, DC, USA*, page 148–160. ACM, November 2002.

[2] W. Adi and A. Mars. Physical and mechatronic security, technologies and future trends for vehicular environment. *arXiv preprint arXiv:1805.07570*, 2018.

[3] H. Xu, J. Ding, P. Li, P. Zhu, and R. Wang. A lightweight RFID mutual authentication protocol based on physical unclonable function. *Sensors*, 18, 2018.

[4] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni. A survey of internet of things (IoT) authentication schemes. *Sensors*, 19, 2019.

[5] S. Lee, M. Oh, Y. Kang, and D. Choi. Design of resistor-capacitor physically unclonable function for resource-constrained iot devices. *Sensors*, 20(2), 2020.

[6] A. K. Das, S. Kalam, N. Sahar, and D. Sinha. UCFL: User categorization using fuzzy logic towards PUF based two-phase authentication of fog assisted IoT devices. *Computers & Security*, 97:101938, 2020.

[7] V.K. Rai, S. Tripathy, and J. Mathew. 2SPUF: Machine learning attack resistant SRAM PUF. In *Proc. of the 3rd ISEA Conference on Security and Privacy (ISEA-ISAP'20), Guwahati, India*, pages 149–154. IEEE, February-March 2020.

[8] J.W. 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. In *Proc. of the 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), Honolulu, HI, USA*, pages 176–179. IEEE, June 2004.

[9] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni. A taxonomy of PUF schemes with a novel arbiter-based PUF resisting machine learning attacks. *Computer Networks*, 194:108133, 2021.

[10] G.E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proc. of the 44th ACM/IEEE Design Automation Conference (), San Diego, CA, USA*, pages 9–14. IEEE, June 2007.

[11] H. Kang, Y. Hori, and A. Satoh. Performance evaluation of the first commercial PUF-embedded RFID. In *Proc. of the 1st IEEE Global Conference on Consumer Electronics (GCCE'12), Tokyo, Japan*, pages 5–8. IEEE, October 2012.

[12] M.I. Khan, S. Ali, A.A. Ikram, and A. Bermak. Optimization of memristive crossbar array for physical unclonable function applications. *IEEE Access*, 9:84480–84489, 2021.

[13] J. Guajardo, S.S. Kumar, G. Schrijen, and P. Tuyls. FPGA intrinsic PUFs and their use for IP protection. In *Proc. of the 9th International Workshop on Cryptographic Hardware and Embedded Systems (CHES'07), Vienna, Austria*, volume 4727 of *Lecture Notes in Computer Science*, pages 63–80. Springer, Berlin, Heidelberg, September 2007.

[14] B. Gassend, D. Lim, D. Clarke, M. Dijk, and S. Devadas. Identification and authentication of integrated circuits. *Concurrency and Computation: Practice and Experience*, 16:1077–1098, 2004.

[15] V.S. Balijabudda, D. Thapar, P. Santikellur, R.S. Chakraborty, and I. Chakrabarti. Design of a chaotic oscillator based model building attack resistant arbiter PUF. In *Proc. of the 2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST'19), Xi'an, China*, pages 1–6. IEEE, December 2019.

[16] M.A. Alamro and K.T. Mursi. Machine learning attack on a multiplexer PUF variant using silicon data: a case study on rMPUFs. In *Proc. of the IEEE 6th International Conference on Computer and Communication Systems (ICCCS'21), Chengdu, China*, pages 1017–1022. IEEE, April 2021.

[17] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber. Modeling attacks on physical unclonable functions. In *Proc. of the 17th ACM Conference on Computer and Communications Security (CCS'10), Chicago, Illinois, USA*, page 237–249. ACM, October 2010.

[18] M.I. Khan, S. Ali, A. Al-Tamimi, A. Hassan, A.A. Ikram, and A. Bermak. A robust architecture of physical unclonable function based on memristor crossbar array. *Microelectronics Journal*, 116:105238, 2021.

[19] H. Kang, Y. Hori, T. Katashita, A. Satoh, and K. Iwamura. PUF evaluation with post-processing and modified modeling attack. *International Journal of Security and Its Applications*, 7:231–242, 2013.

[20] R. Soga and H. Kang. Physical unclonable function using carbon resistor. In *Proc. of the IEEE 9th Global Conference on Consumer Electronics (GCCE'20), Kobe, Japan*, pages 559–561. IEEE, October 2020.

[21] R. Soga and H. Kang. Physical unclonable function using hartley oscillator. In *Proc. of the 10th IEEE Global Conference on Consumer Electronics (GCCE'21), Kyoto, Japan*, pages 426–429. IEEE, October 2021.

[22] T. McGrath, I.E. Bagci, Z.M. Wang, U. Roedig, and R.J. Young. A PUF taxonomy. *Applied Physics Reviews*, 6:011303, 2019.

[23] S.D. Re, A.D. Marcellis, G. Ferri, and V. Stornelli. Low voltage integrated astable multivibrator based on a single ccii. In *Proc. of the 2007 Ph.D Research in Microelectronics and Electronics Conference (RME'07), Bordeaux, France*, volume July, pages 177–180. IEEE, 2007.

[24] A.V. Mancharkar. Performance comparison of astable multivibrator circuit using various circuit designing SPICE softwares. *Online International Interdisciplinary Research Journal*, 3:87–94, 2013.

[25] A. Gupta, R. Mathur, and M. Nizamuddin. Design, simulation and comparative analysis of a novel FinFET based astable multivibrator. *AEU - International Journal of Electronics and Communications*, 100:163–171, 2019.

[26] T. Chen and C. Guestrin. XGBoost: A scalable tree boosting system. In *Proc. of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'16), San Francisco, California, USA*, pages 785–794. ACM, August 2016.

[27] B. McFee, C. Raffel, D. Liang, D.P.W. Ellis, M. McVicar, E. Battenberg, and O. Nieto. librosa: Audio and music signal analysis in python. In *Proc. of the 14th python in science conference (SCIPY'15), Austin, Texas, USA*, pages 18–25, July 2015.

Author Biography

Ryota Soga received a Bachelor of Engineering degree from National Institute of Technology, Tokyo College, in 2022. He works at NTT communications from April 2022. He received the Excellent Poster Paper Award Gold Prize from the IEEE Global Conference on Consumer electronics in 2020. The title of the awarded paper is "Physical Unclonable Function Using Carbon Resistor". His main interests are physical unclonable functions and machine learning.

Hyunho Kang is currently an Associate Professor in the Department of Electronic Engineering at National Institute of Technology, Tokyo College, Japan; he has held this position since April 2017. He received his Ph.D. from the University of Electro-Communications, Tokyo, in 2008. From 2008 to August 2010, he was a Researcher/Assistant Professor at Chuo University, Tokyo, where he was part of a team that developed Biometric Security technologies. From September 2010 to March 2013, he was an AIST Postdoctoral Researcher at the National Institute of Advanced Industrial Science and Technology (AIST), Japan, where his research work focused mainly on the evaluation of physical unclonable functions. From April 2013 to March 2017, he was an Assistant Professor in the Department of Electrical Engineering at Tokyo University of Science, Japan. His main interests are machine learning, deep learning, information security applications, multimedia security (steganography, digital watermarking), biometric security and physical unclonable functions. He is a senior member of IEICE and a member of IPSJ.