DOI: 10.1002/ecj.12276

TRANSLATED PAPER

WILEY

AI hardware oriented neural network physical unclonable function and its evaluation

Yusuke Nozaki[1] | **Kazuya Shibagaki**[2] | **Shu Takemoto**[2] | **Masaya Yoshikawa**[1]

[1] Faculty of Science and Technology, Meijo University, 1–501, Shiogamaguchi, Tenpaku-ku, Nagoya, Aichi 468–8502, Japan

[2] Graduate School of Science and Technology, Meijo University, 1–501, Shiogamaguchi, Tenpaku-ku, Nagoya, Aichi 468–8502, Japan

Correspondence
Yusuke Nozaki, Faculty of Science and Technology, Meijo University, 1–501, Shiogamaguchi, Tenpaku-ku, Nagoya, Aichi 468–8502, Japan.
Email: 143430019@ccalumni.meijo-u.ac.jp

Translated from Volume 140,Number 7, pages 689–696, DOI: 10.1541/ieejeiss.140.689 of *IEEJ Transactions on Electronics, Information and Systems* (Denki Gakkai Ronbunshi C)

Abstract

AI techniques are required for realizing society 5.0. For the issues of societal implementation for AI, an AI hardware, which is enhanced security performances including authentication, and so on, is needed in order to reduce security risks. This study proposes a new physical unclonable function (PUF) based on neural network (NN) called NN PUF. The proposed NN PUF uses a difference of calculation time in NN due to production variations of semiconductor. Evaluation experiments using a field programmable gate array (FPGA) prove the effectiveness of the proposed NN PUF.

KEYWORDS
AI hardware, authentication, hardware security, neural network, physical unclonable function

1 | INTRODUCTION

Presently, promotion of Society 5.0 is set up as one of the basic policies of the Government of Japan in science and technology.[1] Society 5.0 is intended to analyze data collected via Internet of Things (IoT) by means of artificial intelligence (AI), and to feed thus obtained results back to edge devices toward economic development and problem solving. With edge computing, big data analysis is conducted in the cloud where powerful computing resources are available, while the edge is involved mainly in reasoning when immediate solutions are required.[2] Thus AI technologies are essential to implementation of Society 5.0. On the other hand, regarding societal implementation of AI technologies, security risks associated with the use of AI are presented in AI White Paper by the Information-technology Promotion Agency.[3] The White Paper points out that unforeseen accidents occur when AI hardware has been hacked from outside, which may lead to life hazards. For this reason, reinforcement of AI hardware security is an extremely important issue.

Device authentication is a significant component of AI hardware security. One of the promising authentication techniques is physical unclonable functions (PUFs).[4–8] This technique utilizes manufacturing variations in devices (semiconductors) for their authentication. Manufacturing variations in semiconductors are hard to control, and therefore, PUF circuits are hard to replicate. In order to implement reasoning and authentication in AI hardware, one needs dedicated software for both neural network (NN) and PUF. However, available circuit size is limited in AI hardware and other embedded devices, and such dedicated hardware is hard to realize.

In this context, the present study proposes a new neural network physical unclonable function (NN PUF) that combines AI hardware with NN authentication function. In the proposed NN PUF, NN and authentication circuit are combined to reduce circuit size and overhead. Specifically, this study is focused on the fact that calculation time from input layer to output layer of NN is device-specific because of the manufacturing variations. This spread in calculation time is utilized for authentication. Besides, NN is oriented

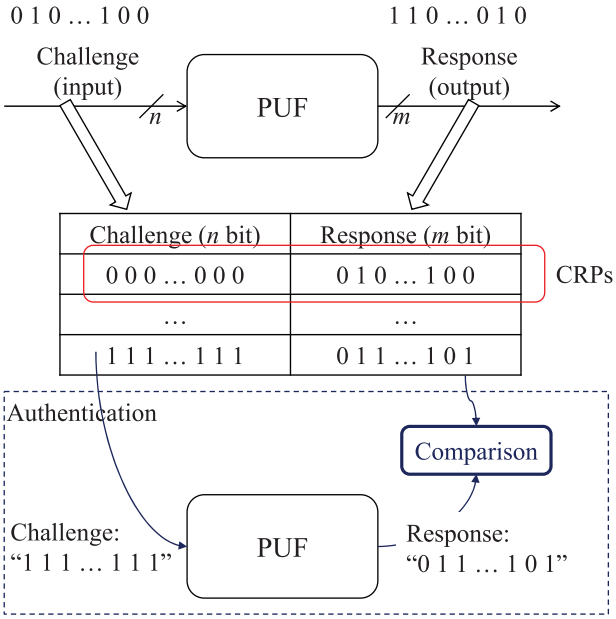


FIGURE 1 Outline of PUF [Color figure can be viewed at wileyonlinelibrary.com]

to implementation on widely used field programmable gate array (FPGA). Specifically, binary NN implementation is used as suitable for lookup tables (LUTs) of FPGA. Affectivity of the proposed NN PUF is verified via evaluation experiments with actual devices.

2 | PREPARATIONS

First, PUF overview is given in ⟨2.3⟩, and PUF performance evaluation is explained in ⟨2.2⟩. Then NN is presented in ⟨2.3⟩, and related researched is reviewed in ⟨2.4⟩.

2.1 | Physical unclonable function

PUF is a technique to extract manufacturing variations in semiconductors, and to generate a unique identifier for each device. An overview of PUF is shown in Figure 1. As shown in the diagram, PUF is a circuit that outputs an m-bit value called response against an n-bit input (challenge). This operation is performed repeatedly in PUF to collect multiple challenge and response pairs (CPRs), and to store them in a database. Authentication process means comparison between pre-collected CPRs and acquired CPRs. A number of PUF types were proposed so far, such as arbiter PUF,[4] ring-oscillator PUF (RO PUF),[5] SRAM PUF,[6] etc.

2.2 | PUF performance indices

Randomness, steadiness, diffuseness, uniqueness and other indices are used in evaluation of PUF performance. Particularly, randomness is an index that shows uniform occurrence of 0 and 1 in responses. Steadiness is an index that shows how steadily same responses are outputted to same challenges. Diffuseness is an index that shows how different are responses to different challenges. Uniqueness is an index that shows how different are responses to challenges for different devices.

Hamming weight (HW) of ID is calculated to evaluate randomness. The closer is HW to half ID length, the higher is randomness. Steadiness is evaluated by calculation of same challenge intra-Hamming distance (SC Intra-HD). The closer is SC Intra-HD to 0, the higher is steadiness. Diffuseness is evaluated by calculation of different challenge intra-Hamming distance (DC Intra-HD). The closer is DC Intra-ID to half ID length, the higher is diffuseness. Uniqueness is evaluated using Hamming distance between IDs of different devices obtained to same challenges (SC Inter-HD). The closer is DC Inter-ID to half ID length, the higher is uniqueness.

Specifically K types of L-bit IDs are acquired T times for each device. When this procedure is applied to N devices, a total of $L \times K \times T \times N$ responses are obtained. In evaluation, except for steadiness, the most frequent 0–1 value in T trials is adopted as Correct ID.

2.3 | Neural network

NN is a mathematical model of calculations performed in human brain.[10] NN is composed mainly of input, hidden, and output layers to perform learning and reasoning. In learning, weights of all neurons in NN are updated according to NN outputs corresponding to given inputs. Then in reasoning, an output for some input is estimated based on the updated weights. With edge computing, cloud-side machines with powerful computing resources are used to learn big data, while the edge side is involved mainly in reasoning. There are a number of studies dealing with hardware implementation of NN.[11,12]

2.4 | Related research

Wilkie, Stoneham and Aleksander's Recognition Device (WiSARD) PUF based on weightless NN (WNN) structure was proposed in literature.[13] WNN is a NN in which all neurons are expressed by random access memory (RAM), and a network is configured through learning process when values of RAM nodes are successively changed to 0 or 1. WiSARD PUF utilizes the fact that that initial RAM settings in WNN differ from device to device due to semiconductor manufacturing variations. However, WiSARD PUF is based on WNN structure, and does not have discriminative functions.

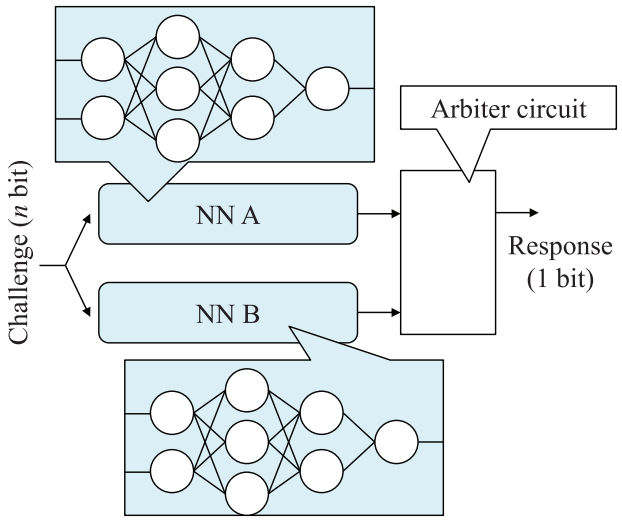


FIGURE 2 Outline of proposed NN PUF [Color figure can be viewed at wileyonlinelibrary.com]

There are reports on hardware implementation of NN[11,12] or on PUF inspired by NN structure,[13] but, to our best knowledge, there are no studies dealing with architectures that combine NN and PUF.

3 | PROPOSED NN PUF

3.1 | Overview of proposed NN PUF

This study proposes a new physical unclonable function using NN (NN PUF). AN overview of the proposed NN PUF is shown in Figure 2. High dependability is required for AI hardware; thus, a typical measure – multiplexing – is adopted in the proposed NN PUF. Specifically, two networks (NN A and NN B) with same number of neurons, layers, and weights are configured. Since both NNs have same layers and weights, same calculation results are obtained when same inputs (challenges) are given, and calculation time is also same in ideal case. However, because of semiconductor manufacturing variations, a difference occurs in calculation time of the two NNs. In the proposed NN PUF, this difference in calculation time is used when generating responses. Namely, outputs of the two NNs are connected to an arbiter circuit to derive the difference in calculation time. An example of arbiter circuit implemented as DFF is shown in Figure 3. Here output (response) is 0 when input signal to D is earlier, and 1 when input signal to CLK is earlier.

As explained above, in the proposed NN PUF, a difference in NN calculation time is utilized as response; thus functions of NN and PUF are combined, and there is no need to add a new PUF circuit. This makes possible reduction of the circuit size.

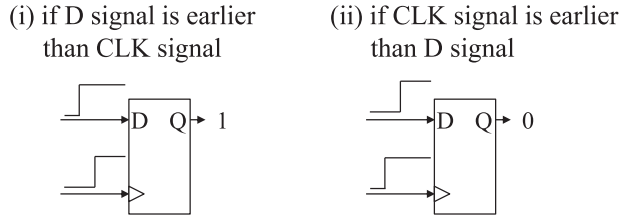
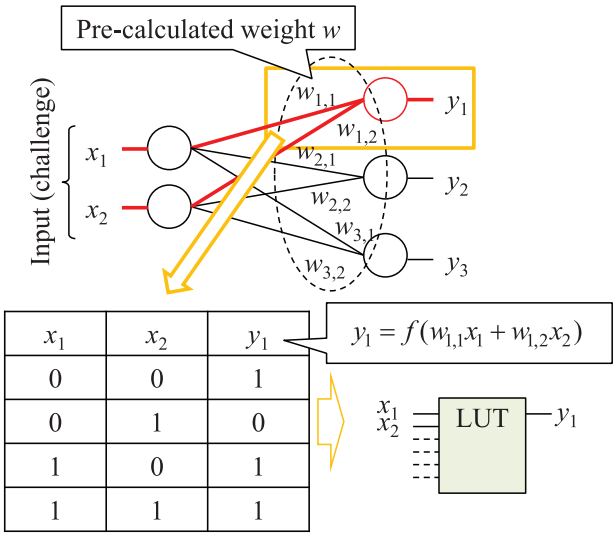


FIGURE 3 Response generation in arbiter circuit using DFF



x_1	x_2	y_1
0	0	1
0	1	0
1	0	1
1	1	1

FIGURE 4 LUT oriented binary NN implementation method [Color figure can be viewed at wileyonlinelibrary.com]

3.2 | LUT-oriented binarized NN implementation

Binary NN implementation with regard to FPGA LUT is introduced in this study. Specifically, every neuron in the proposed NN PUF is implemented using FPGA LUT. In so doing, neuron weights are pre-calculated with Chainer[14] or other software.

The implementation method is illustrated in Figure 4. First, only values are inputted to input layer according to Eq. (1). Here x in input to neuron, y is neuron's output, w_i is neuron's weight, and $f(x)$ is activation function.

$$y_i = f\left(\sum_{j=1}^{n} w_{i,j} x_j\right) \tag{1}$$

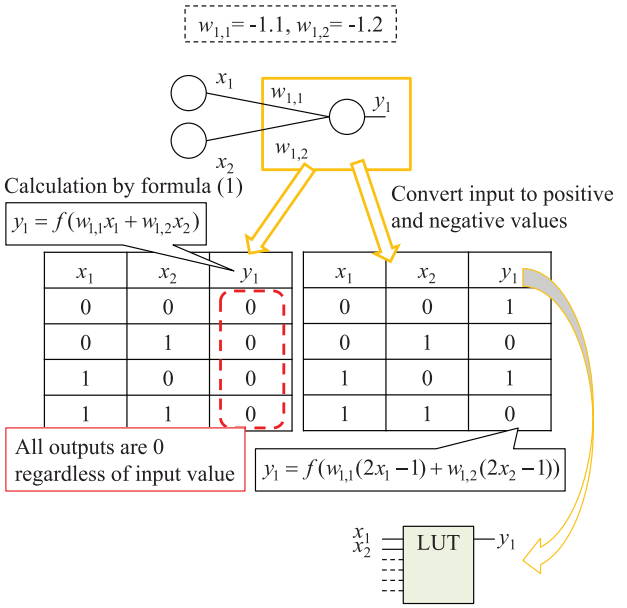


FIGURE 5 Implementation considering positive and negative values [Color figure can be viewed at wileyonlinelibrary.com]

Activation function $f(x)$ can be defined as follows.

$$f(x)\begin{cases} 1 \text{ for } x \geq 0 \\ 0 \text{ for } x < 0 \end{cases} \tag{2}$$

In the implementation, a truth table is created form binary results of the above calculation. After that, the truth table is implemented as LUT to realize neurons.

In so doing, all outputs in 3rd and subsequent layers (2nd hidden layer onward) may become 0 regardless of inputs. This case is illustrated by example in Figure 5. If the weights are $w_{1,1} = -1.1$, $w_{1,2} = -1.2$, all outputs become 0 regardless of inputs as shown in Figure 5. Thus, in calculations, binary inputs "0", "1" are converted to positive and negative values "–1", "1". Due to such conversion, calculation results are appropriately reflected even in binary LUT. This calculation is defined in Eq. (3).

$$y_i = f\left(\sum_{j=1}^{n} w_{i,j}\left(2x_j - 1\right)\right) \tag{3}$$

4 | EVALUATION EXPERIMENTS

Evaluation experiments were performed to verify the proposed NN PUF. First, the implemented NN is explained in ⟨4.1⟩. After that, the experimental environment is described in ⟨4.2⟩, and experimental results are presented in ⟨4.3⟩.

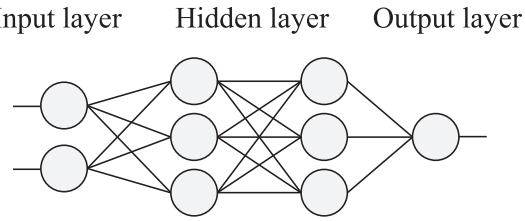


FIGURE 6 Basic unit of proposed NN PUF

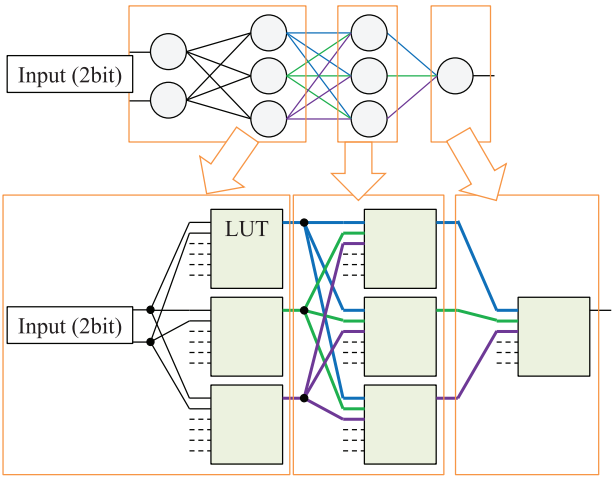


FIGURE 7 Implementation of basic unit using LUT [Color figure can be viewed at wileyonlinelibrary.com]

4.1 | Implemented neural network

In this study, NN is implemented for XOR calculation of 16-bit input values in the proposed NN PUF. In so doing, NN for XOR calculation is configured of basic units. First, the basic unit is shown in Figure 6. As shown in the diagram, this basic unit is a four-layer NN with an input layer, two hidden layers, and an output layer. In the implementation of basic unit, all neurons, except for the input layer, are realized using LUTs as shown in Figure 7. In so doing, 1st hidden layer is composed of two-input neurons so that two-input, one-output reasoning is implemented in LUTs. In addition, 2nd hidden layer is composed of three-input neurons so that three-input, one-output reasoning is implemented in LUTs.

In this study, NN is implemented by using multiple basic units. The implemented NN is shown in Figure 8. In the diagram, NN is composed of 36 basic units; 16-bit inputs correspond to challenges in NN PUF. In this implementation of the proposed NN PUF, two NNs shown in Figure 8 are configured, and difference in calculation time between the two networks is extracted as response.

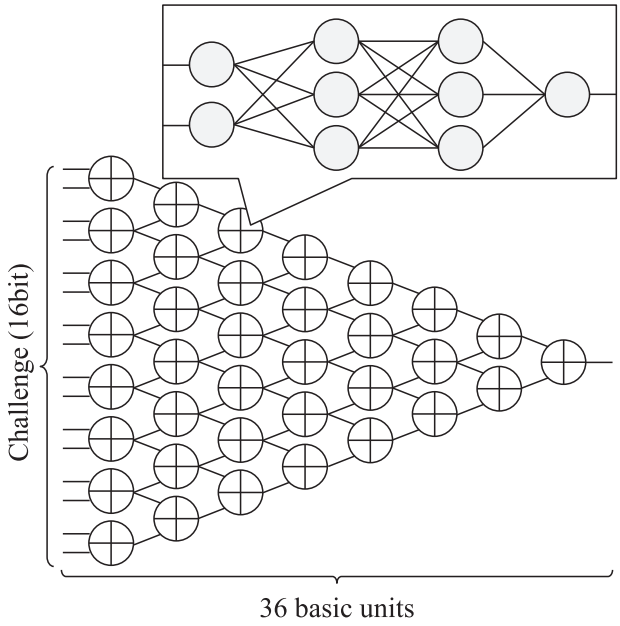


FIGURE 8 Implemented NN

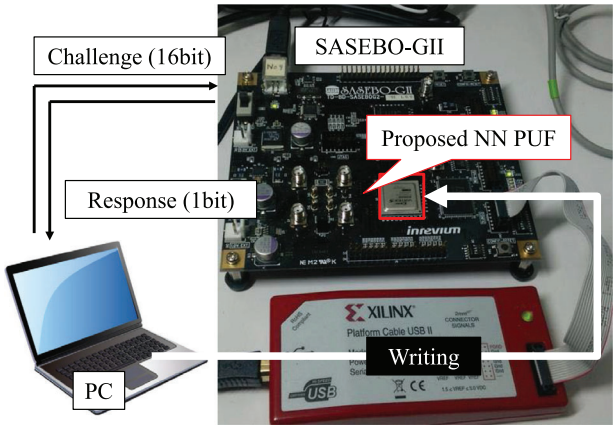


FIGURE 9 Evaluation system [Color figure can be viewed at wileyonlinelibrary.com]

4.2 | Experimental environment

In evaluation experiment, the proposed NN PUF was implemented on a FPGA board (SASEBO-GII[15]). Appearance of the evaluation system is shown in Figure 9; specifications of the experimental environment are listed in Table 1. NN weights were pre-calculated using Chainer.[14] Floorplan of the implemented NN PUF is shown in Figure 10. The left and right diagrams pertain to, respectively, overall view of the proposed NN PUF and close-up view of the basic units at the output stage.

In evaluation of PUF performance, ID length was $L = 128$, number of ID types was $K = 128$, and number of devices was $N = 3$; acquisition of one ID was repeated $T = 100$ times.

TABLE 1 Experimental conditions

PUF	Proposed NN PUF
Function of NN	XOR operation
Challenge size [bit]	16
Response size [bit]	1
FPGA board	SASEBO-GII
FPGA	Virtex-5 XC5VLX30
Development tool	Xilinx ISE Design Suite 14.7
Floorplan tool	Xilinx PlanAhead v14.7
Precalculation tool for weights	Chainer

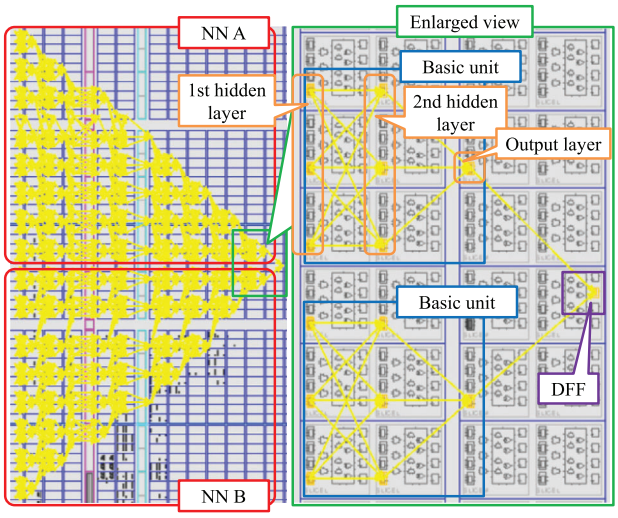


FIGURE 10 Floorplan of proposed NN PUF [Color figure can be viewed at wileyonlinelibrary.com]

4.3 | Experimental results

4.3.1 | PUF performance evaluation

First, the proposed NN PUF was evaluated in terms of randomness, steadiness, diffuseness, and uniqueness. Respective evaluation results are shown in Figure 11 to Figure 14. In the diagrams, the horizontal axes plot HW of same ID and between IDs (DC Intra-ID, SC Intra-HD, SC Inter-ID), and the vertical axes plot respective occurrence frequencies. In addition, every performance index is compared to that of a typical arbiter PUF. The arbiter PUF[9,16] is implemented on the same FPGA board as in this study (SASEBO-GII). Thus the corresponding results[9,16] were used for comparison (see Table 2).

First, regarding randomness, the mean ID HW is 69.71 as shown in Figure 11. As can be seen from Table 2, this index of the proposed NN PUF is closer to half-length of 128-bit ID than 71.4 of arbiter PUF, which confirms good randomness. Next, regarding steadiness, the mean

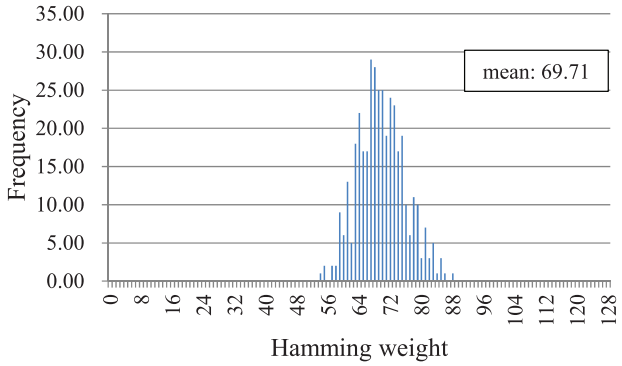


FIGURE 11 Evaluation result of randomness [Color figure can be viewed at wileyonlinelibrary.com]

TABLE 2 Comparison of PUF performance indicators

PUF	Proposed NN PUF	Arbiter PUF[9,16]
ID's HW	69.7	71.4
SC Intra-HD	8.06	0.431
DC Intra-HD	63.4	63.3
SC Inter-HD	43.9	6.78

value of SC Intra-HD is 8.063 as shown in Figure 12. That is, steadiness is slightly poorer than 0.431 of arbiter PUF (Table 2). As regards diffuseness, the mean value of DC Intra-HD is 63.38 shown in Figure 13, which is very close to Arbiter PUF in Table 2. Finally, as regard uniqueness, the mean value of SC Inter-HD is 43.89 in Figure 14. That is, the proposed NN PUF features higher uniqueness than arbiter PUF (6.78 in Table 2).

PUF steadiness and uniqueness are extremely important in device authentication. Particularly, false rejection rate (FRR) and false acceptance rate (FAR) can be used to evaluate whether stable device authentication is possible. Here FRR is a probability that an actual device is recognized as counterfeit, and FAR is a probability that a counterfeit device is recognized as actual. FRR and FAR can be evaluated using SC Intra-HD and SC Inter-HD employed in this study.[16] Specifically, FRR can be calculated as a proportion of SC-Inter ID overlap in distribution of SC Intra-HD, and FAR can be calculated as a proportion of SC-Intra ID overlap in distribution of SC Inter-HD. Thus the results for SC Intra-HD of Figure 12 and SC Inter-HD in Figure 14 are shown in Figure 15 by blue and red lines, respectively. The diagram confirms that there is no overlap between SC Intra-HD and SC Inter-ID in the proposed NN PUF, which is indicative of low FRR and FAR. Besides, one can assume

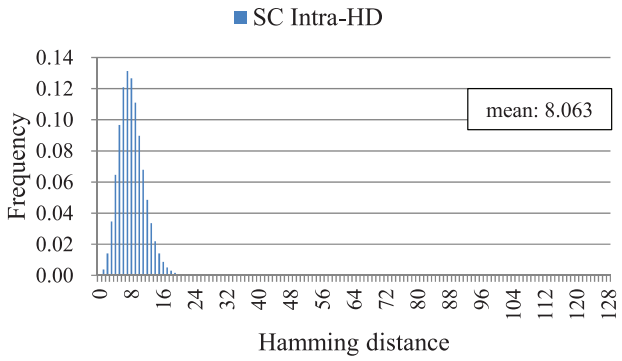


FIGURE 12 Evaluation result of steadiness [Color figure can be viewed at wileyonlinelibrary.com]

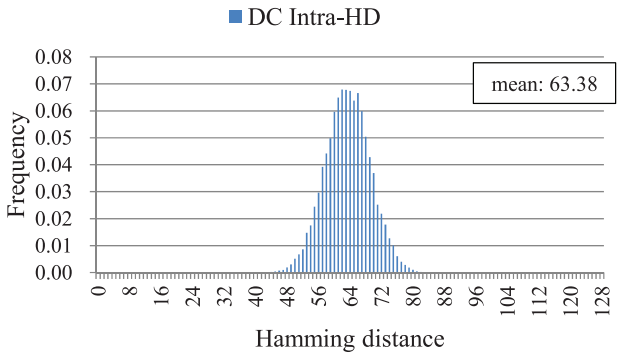


FIGURE 13 Evaluation result of diffuseness [Color figure can be viewed at wileyonlinelibrary.com]

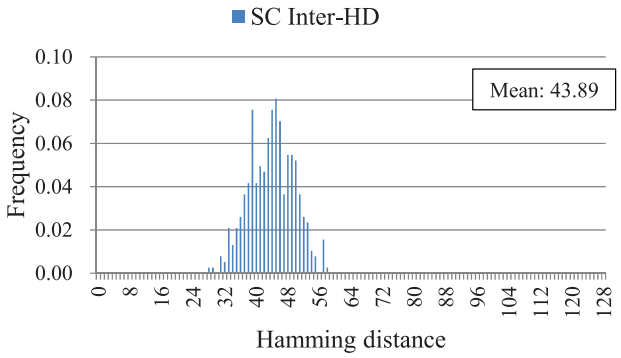


FIGURE 14 Evaluation result of uniqueness [Color figure can be viewed at wileyonlinelibrary.com]

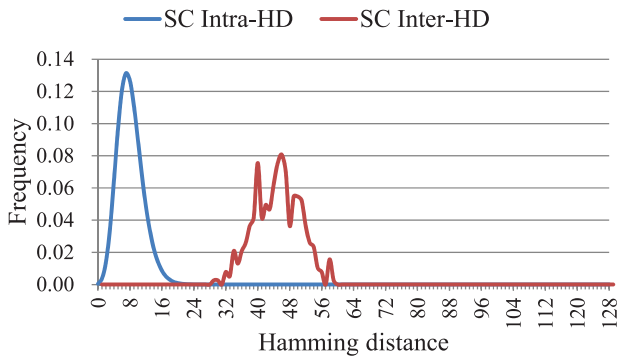


FIGURE 15 Comparison of SC Intra-HD and SC Inter-HD [Color figure can be viewed at wileyonlinelibrary.com]

TABLE 3 Evaluation with different supply voltage

Supply voltage [V]	HD
0.95	14
1.05	13

that stable authentication can be performed with a HD threshold set to 24 at the boundary between two distributions.

In addition, it is important the influence of environment changes on PUF performance. An experiment was conducted to examine how environment changes affect performance of the proposed NN PUF. In this experiment, response of the proposed NN PUF was evaluated while applied voltage was varied. Specifically, reference voltage of 1.00 V was varied at ±5% using a stabilized source (Kikusui PMC18-5A), and response was acquired under 0.95, 1.00, and 1.05 V. In so doing, same 128-bit ID was acquired 100 times, and the most frequent 0–1 value was adopted as Correct ID. Then HD between IDs was calculated with reference to ID acquired under 1.00 V. The experimental results are presented in Table 3. As can be seen from the table, inter-ID HD is 14 at maximum, and about 11% responses are unstable. Besides, regarding temperature dependence of PUF response, evaluation of arbiter PUF in literature[17] showed that the effect of source voltage is stronger than that of temperature. Considering that an arbiter circuit is used for response generation in the proposed NN PUF, one can assume that up to 11% responses are unstable at changing temperature.

4.3.2 | Circuit size comparison

Circuit size of the proposed NN PUF was compared to other designs. Specifically, the proposed NN PUF, NN and arbiter PUF,[4] and NN and RO PUF[5] were implemented on FPGA. In the implementation of NN PUF proposed in this study, challenges are 16-bit, and the challenge space size is $2^{16} = 65{,}536$. Thus the other PUFs were implemented so that their challenge spaces were close to this size. Namely, arbiter PUF was implemented with 16-0stage selector units (challenge: 16-bit, challenge space: $2^{16} = 65{,}536$), and RO PUF was implemented with 256 ROs (challenge: 15-bit, challenge space: ${}_{256}C_2 = 32{,}640$). The results of comparison are given in Table 4. As indicated by the table, the proposed NN PUF can be implemented with lower overhead than the other PUFs. Therefore, there are no implementation-related problems even if input bit-width is increased to a scale of practical applications.[18,19]

TABLE 4 Comparison results of circuit area

		# of LUTs	# of registers
Proposed NN PUF		532	17
NN and arbiter PUF	Total	598	21
	NN and peripheral	533	18
	Arbiter PUF	65	3
NN and RO PUF	Total	2,893	90
	NN and peripheral	853	39
	RO PUF	2040	51

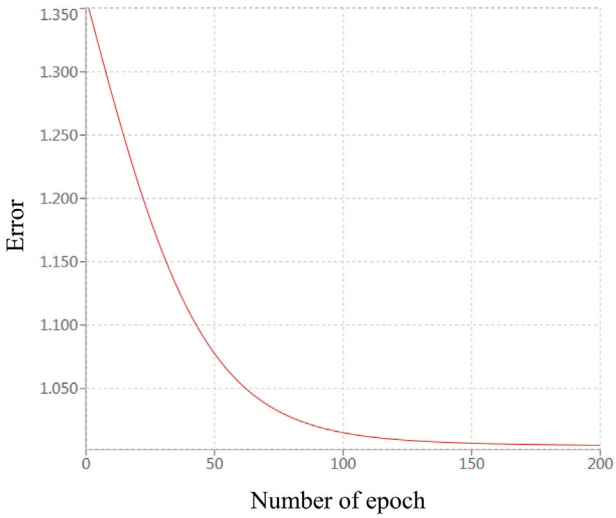


FIGURE 16 Error of proposed NN PUF [Color figure can be viewed at wileyonlinelibrary.com]

4.3.3 | NN authentication performance

In closing, NN performance of the proposed NN PUF was confirmed. All weights in the proposed NN PUF are precalculated using the Chainer software. In so doing, relationship between the number of epochs and error is as shown in Figure 16. As can be seen from the graph, errors decrease with greater number of epochs.

In addition, discrimination performance was confirmed in case of FPGA implementation of the proposed NN PUF. As a result, correct XOR calculation as obtained for all inputs. Thus, the discrimination performance was proven sufficient even in binarized implementation.

Evaluation experiments conducted in this study dealt with XOR operations in the NN; thus let us consider effectiveness in case of applying to another NN. In the proposed NN PUF, two redundant NNs are prepared, and response is generated based on the delay difference. Besides, the NNs are realized via LUT combinatorial circuits. Therefore, one can assume that the proposed method can be

applied universally as long as two redundant NNs are realized via combinatorial circuits. There are a number of methods for combinatorial circuit implementation of NN; particularly, one can think of methods based on the NN implementation in this study or LUT-network reported in literature.[20]

5 | CONCLUSION

This study proposed NN PUF that combines AI hardware-oriented NN and PUF. The proposed NN PUF is focused on a difference in NN calculation time due to manufacturing variations, and uses it for authentication. In experiments using FPGA, typical performance indices of PUF – randomness, steadiness, diffuseness, and uniqueness – were evaluated to prove that the proposed NN PUF offers good performance. In addition, circuit size comparison showed that circuit overhead is suppressed and circuit area is reduced in the proposed NN PUF due to combining NN with PUF.

In future, we are going to evaluate performance of the proposed NN PUF in case of varied NN layers and different learning patterns, and to elaborate temperature dependence of performance. We are also going to evaluate security of the proposed NN PUF in terms of tolerance to machine learning attacks using deep learning.[21]

ACKNOWLEDGMENT

This paper is based on results obtained from a project, JPNP16007, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

REFERENCES

1. https://www8.cao.go.jp/cstp/society5_0/index.html.
2. Yu W, Liang F, He X, Hatcher WG, Lu C, Lin J, Yang X. "A Survey on the Edge Computing for the Internet of Things", *IEEE Access*, 2018;6:6900-6919.
3. Information-technology Promotion Agency, Japan: "*Artificial Intelligence White Paper 2019*", KADOKAWA (in Japanese)
4. Lee JW, Lim D, Gassend B, Suh GE, Dijk MV, Debadas S. "A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications", *Proc. of IEEE VLSI Circuits Symposium*, pp. 176-179 (2004).
5. Suh GE, Devadas S. "Physical Unclonable Functions for Device Authentication and Secret Key Generation", *Proc. of 44th ACM/IEEE Design Automation Conference (DAC'07)*, pp. 9–14 (2007).
6. Guajardo J, Kumar SS, Schrijen GJ, Tuyls P. "FPGA Intrinsic PUFs and Their Use for IP Protection", *Proc. of 9th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007)*, LNCS 4272, pp. 63–80, Springer-Verlag (2007).
7. Hori Y, Kang H, Katashita T, Satoh A. "Pseudo-LFSR PUF: A compact, efficient and reliable physical unclonable function", *Proc. of 7th Int. Conf. ReConFigurable Computing and FPGAs (ReConFig'11)*, pp. 223–228 (2011).
8. Shimizu K, Suzuki D. "Glitch PUF: Extracting Information from Usually Unwanted Glitches", *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, 2012;E95-A.1:223–233.
9. Hori Y, Yoshida T, Katashita T, Satoh A. "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs", *Proc. of 6th Int. Conf. ReConFigurable Computing and FPGAs (ReConFig'10)*, pp. 298–303 (2010).
10. Zhang GP. "Neural Networks for Classification: A Survey", *IEEE Trans. Systems, Man, and Cybernetics*, 2000;30.4:451–462.
11. Zhao W, Fu H, Luk W, Yu T, Wang S, Feng B, Ma Y, Yang G. "F-CNN: An FPGA-based Framework for Training Convolutional Neural Networks", *Proc. of IEEE 27th Int. Conf. Application-specific Systems, Architectures and Processors (ASAP 2016)*, pp. 107–114 (2016).
12. Nakahara H, Yonekawa H, Sasao T, Iwamoto H, Motomura M. "A memory-based realization of a binarized deep convolutional neural network", *Proc. of Int. Conf. Field-Programmable Technology (FPT 2016)*, pp. 277–280 (2016).
13. Santiago L, Patil VC, Prado CB, Alves TAO, Marzulo LAJ, França FMG, Kundu S. "Realizing strong PUF from weak PUF via neural computing", *Proc. of IEEE Int. Symp. Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pp. 1–6 (2017).
14. https://chainer.org/.
15. http://satoh.cs.uec.ac.jp/SASEBO/ja/board/sasebo-g2.html.
16. Hori Y, Katashita T, Kang H, Satoh A, Kawamura S, Kobara K. "Evaluation of Physical Unclonable Functions for 28-nm Process Field-Programmable Gate Arrays", *Journal of Information Processing*, 2014;22.2:344–356.
17. Fukushima A, Shiozaki M, Furuhashi K, Murayama T, Fujino T. "Evaluation of Environmental Stability on Unique-ID Generated by Arbiter-PUF Chips", *Proc. of 2011 Symp. on Cryptography and Information Security (SCIS 2011)*, 2011;2D2-2:1-7. (in Japanese)
18. Lu L, Liang Y, Xiao Q, Yan S. "Evaluating Fast Algorithms for Convolutional Neural Networks on FPGAs", *Proc. of IEEE 25th Annual Int. Symp. on Field-Programmable Custom Computing Machines (FCCM)*, pp. 101–108 (2017).
19. Zhuge C, Liu X, Zhang X, Gummadi S, Xiong J, Chen D. "Face Recognition with Hybrid Efficient Convolution Algorithms on FPGAs", *Proc. of 2018 ACM Great Lakes Symp. on VLSI (GLSVLSI'18)*, pp. 123–128 (2018).
20. Fuchikami R, Issiki F. "Fast and Light-weight Binarized Neural Network Implemented in an FPGA using LUT-based Signal Processing and its Time-domain Extension for Multi-bit Processing", *Proc. of 9th IEEE Int. Conf. on Consumer Electronics (ICCE-Berlin 2019)*, pp. 120–121 (2019).
21. Iizuka T, Ogasahara Y, Katashita T, Hori Y, Awano H, Ikeda M. "On Machine Learning Attack Tolerance for PUF-based Device Authentication System", *IEICE Technical Report, IEICE-HWS*, 2019;118.458:237–242. (in Japanese)

AUTHOR BIOGRAPHIES

Yusuke Nozaki, non-member In 2019 completed doctorate at Meijo University (Grad. School of Sci. and Tech., Electronics, Information and Materials Eng.), and was employed by the University as assistant. 2017–2019 JSPS research fellow (DC2). D.Eng. Research in cryptographic LSI security. IEICE CAS Student Award, IEEE GCCE2015 Excellent Poster Award, IEEE CEDA AJJC Academic Research Award 2018, and other awards. Membership: IPSJ, IEICE, JSFTII, IEEE.

Kazuya Shibagaki, non-member In 2018 graduated from Meijo University (Fac. of Sci. and Tech., Information Eng.), and started master's course (Grad. School of Sci. and Tech., Information Eng.). Research in cryptographic LSI security. 15th Informatics Workshop Best Presentation Award and other awards.

Shu Takemoto, non-member In 2019 graduated from Meijo University (Fac. of Sci. and Tech., Information Eng.), and started master's course (Grad. School of Sci. and Tech., Information Eng.). Research in cryptographic LSI security. 17th Informatics Workshop Best Presentation Award and other awards. IEEE member.

Masaya Yoshikawa, member In 2001 completed doctorate at Ritsumeikan University (Grad. School of Sci. and Tech.). D.Eng. Was employed by Ritsumeikan University (Fac. of Sci. and Tech.) as assistant and then lecturer, 2007 adjunct professor at Meijo University (Fac. of Sci. and Tech.), since 2012 professor. 2009–2015 CREST researcher. Research in LSI design and design automation technologies. 3rd LSI IP Design Award (Research Encouragement), 10th LSI IP Design Award (Research Achievement), FIT2003 Best Paper Award, 2007 SICE Industrial Technology Award, CAINE 2010 Best Paper Award, WCECS2011 Best Paper Award, and other awards. Membership: IPSJ, IEICE, ISCIE, JSFTII, IEEE.

How to cite this article: Nozaki Y, Shibagaki K, Takemoto S, Yoshikawa M. AI hardware oriented neural network physical unclonable function and its evaluation. *Electron Comm Jpn*. 2020;103:54–62. https://doi.org/10.1002/ecj.12276