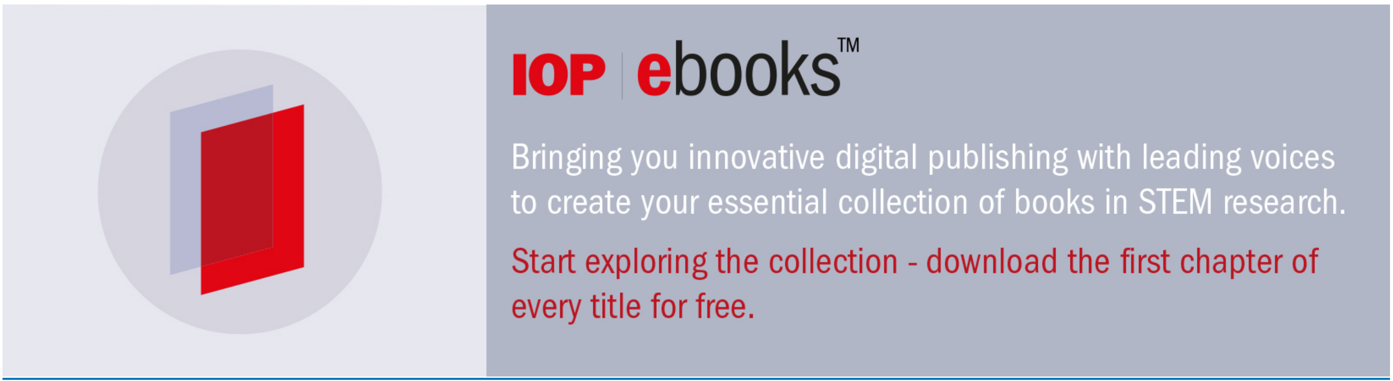
IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

Evaluation of Energy Harvesting Technique for Security Module

To cite this article: Y Nozaki and M Yoshikawa 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **575** 012008



Evaluation of Energy Harvesting Technique for Security Module

Y Nozaki[1*] **and M Yoshikawa**[1]

[1]Department of Information Engineering, Meijo University, 1-501 Shiogmaguchi, Tenpaku-ku, Nagoya, Aichi 468-8502, Japan

*143430019@ccalumni.meijo-u.ac.jp

Abstract. In internet of things (IoT), devices connect to external network in order to communicate data each other, and the improvement of human life is expected. However, IoT devices have problems to be solved, including design of low power and security such as authentication of devices. To overcome these problems, energy harvesting and physical unclonable function (PUF) have attracted attention. Actually, we have proposed a PUF using energy harvesting called energy harvesting PUF. However, since input of the energy harvesting PUF is fixed, available information for authentication is limited. Therefore, this study evaluates the energy harvesting PUF by increasing input value. Experiments using an actual energy harvester also showed the validity of the energy harvesting PUF.

1. Introduction

Energy harvesting technique, which harvests various energy and converts them to electric power, has attracted attention [1]–[4]. Energy harvesting is expected to apply for IoT devices because they have constraints including design of low power. By using energy harvesting technique, a system, which does not need battery replacement, can be developed [3]. Thus, energy harvesting can improve the energy efficiency of IoT devices.

IoT devices have problems to be solved [5]. Authentication of IoT devices is one of the problems. Generally, authentication utilizes an encryption technique using a secret key stored in a non-volatile memory on devices. However, it has been reported that the secret key is vulnerable against invasive attacks [6] and side-channel attacks [7], and countermeasures in high cost are required. Therefore, physical unclonable functions (PUFs) [8]–[10] have been proposed in order to ensure security of IoT devices in low cost. PUF is a circuit which extracts variations of semiconductor manufacturing as a device’s ID. The secret key generated by using PUF does not need to store in a non-volatile memory. As a result, it has the resistance against illegal attacks. Then, a low cost authentication method using PUF, which does not utilize encryption processing, has also been proposed [9].

We have proposed a PUF using energy harvesting called an energy harvesting PUF [11]. In energy harvesting PUF, a small variance of power generation time due to production dispersion is used for device’s authentication. The energy harvesting PUF can be also used in more low cost because it does not need to implement a dedicated PUF circuit additionally. On the other hand, in paper [11], input utilized in the energy harvesting PUF is fixed, and the generated unique value has only one type. Consequently, available information for authentication is limited, and a part of devices fails in authentication [11].

Therefore, this study evaluates the energy harvesting PUF by increasing input value. By experiments using an actual energy harvester, the validity of the energy harvesting PUF is evaluated.

2. Preliminaries

2.1. Energy Harvester

Figure 1 shows an energy harvester used in this study. As shown in figure 1, the energy harvester consists of a TWELITE-DIP, a power management module TWE-EH SOLAR, and a solar cell. In this energy harvester, when the power generation is finished, a TWELITE microcontroller is started. Then, wireless data communication is performed. Also, in this study, a MONOSTICK, including a TWELITE microcontroller, is used as a receiver.

In the TWEILTE microcontroller, the generated power by the photovoltaic generation is charged to a capacitor built in the TWE-EH SOLAR. At this time, when a voltage of the capacitor reaches 2.9 [V], the TWELITE microcontroller turns on. Then, wireless data communication is performed. When the voltage reaches below 2.0 [V], the TWELITE microcontroller turns off [12].

2.2. Related Works

First, E. Aponte has studied that the applying of energy harvesting for PUF [13]. In [13], the variance of the open-circuit voltage for each energy harvester, including solar cell and thermoelectric generator, was verified. Then, paper [13] showed the variance of the each energy harvester. However, in paper [13], methods for authentication of devices have not been studied.

Next, we have proposed energy harvesting PUF which uses the variance of the power generation time due to the production variation [11]. We have also shown that energy harvesting PUF can authenticate each device except for a part of devices. The detail of energy harvesting PUF is explained in section 3.

Also, S. D. Kumar et al. have proposed a solar cell based PUF for secure key generation [14]. The solar cell based PUF consists of 8 solar cells and a Tiva TM4C123GH6PM microcontroller, and it generates a 128-bit ID from the measured open-circuit voltage by using an analog to digital converter (ADC). In addition, in [14], evaluations of randomness and reliability were also performed. However, authentication between devices has not been studied. Then, the solar cell based PUF needs as much as 8 solar cells; therefore, cost increases.

3. Energy Harvesting PUF

Energy harvesting PUF utilizes the production variation of the power generation time with energy harvester [11]. The generated power by the photovoltaic generation can be calculated by

$$P_{\max} = V_{OC} I_{SC} ff , \qquad (1)$$

where V_{OC} is the open-circuit voltage, I_{SC} is the short-circuit current, and ff is the fill factor.

In addition, the open circuit voltage V_{OC} can be represented by

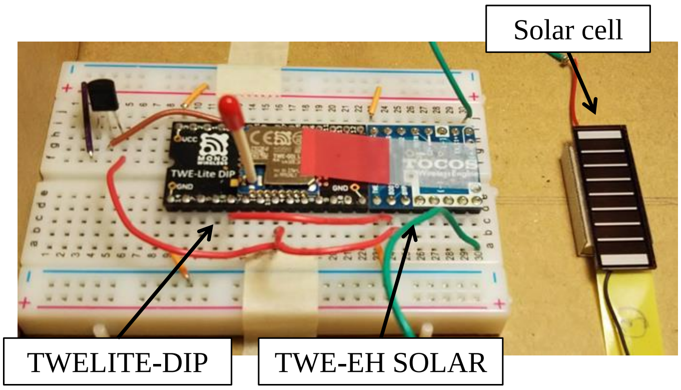


Figure 1. Energy harvester.

$$V_{OC} = \frac{kT}{q}\ln\left(\frac{(N_A + \Delta n)\Delta n}{n_i^2}\right), \tag{2}$$

where kT/q is the thermal voltage, N_A is the doping concentration, Δn is the excess carrier concentration, and n_i^2 is the intrinsic carrier concentration [15][16].

Since the doping concentration of each semiconductor is different due to the production variation, the open-circuit voltage V_{OC}, which is depend on N_A (see formula (2)), is different [13]; therefore, the generated power differs. As a result, the power generation time is changed in each energy harvester [11]. The energy harvesting PUF utilizes the power generation time for device's authentication. Figure 2 shows the outline of the energy harvesting PUF. Here, the energy harvester used in this study communicates data when the voltage of the capacitor is charged to reach 2.9 [V] (see subsection 2.1). Then, when the voltage reaches below 2.0 [V], the TWELITE microcontroller turns off, and the charging of the power generation is carried out again. The energy harvesting PUF calculates the power generation time between the data receiving times t_1 and t_2. At this time, t_1 is the receiving time when the TWEILTE turns on, and t_2 is the receiving time before the TWELITE turns off.

Specifically, the power generation time T can be calculated by

$$T = t_2 - t_1. \tag{3}$$

For the authentication, first, the power generation time $T_{register}$ is registered to the database. Then, the Euclid distance d between the power generation time during the authentication (T_{user}) and that during the registration ($T_{register}$). This can be calculated by

$$d = \left|T_{register} - T_{user}\right| = \sqrt{(T_{register} - T_{user})^2}\ . \tag{4}$$

Then, the Euclid distance, whose value is the minimum, is authenticated as a correct energy harvester. On the other hand, in [11], since light incident position as input is fixed, available information for authentication is limited. Therefore, it has been pointed out that a part of devices fails in authentication [11].

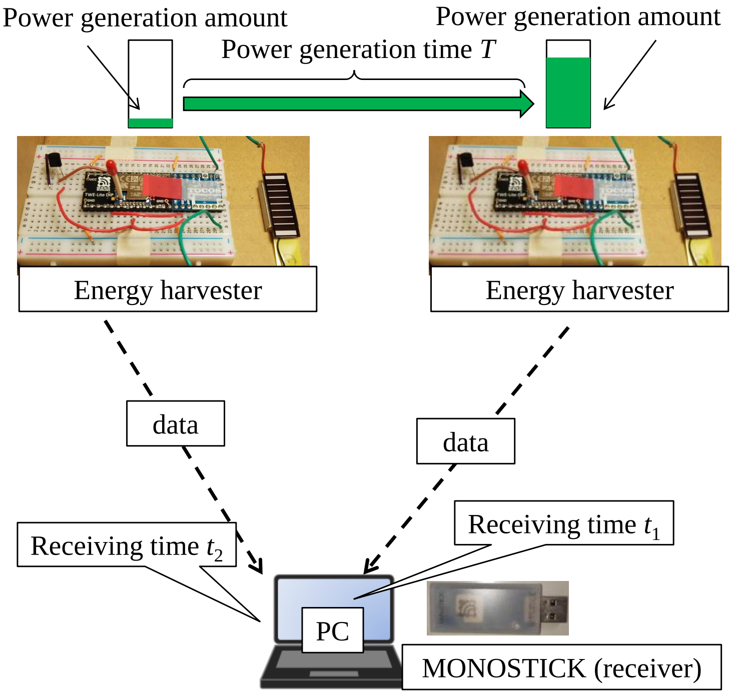


Figure 2. Outline of the energy harvesting PUF.

4. Experiments

This study evaluates the energy harvesting PUF by increasing input value to improve the authentication accuracy.

4.1. Experimental Environment

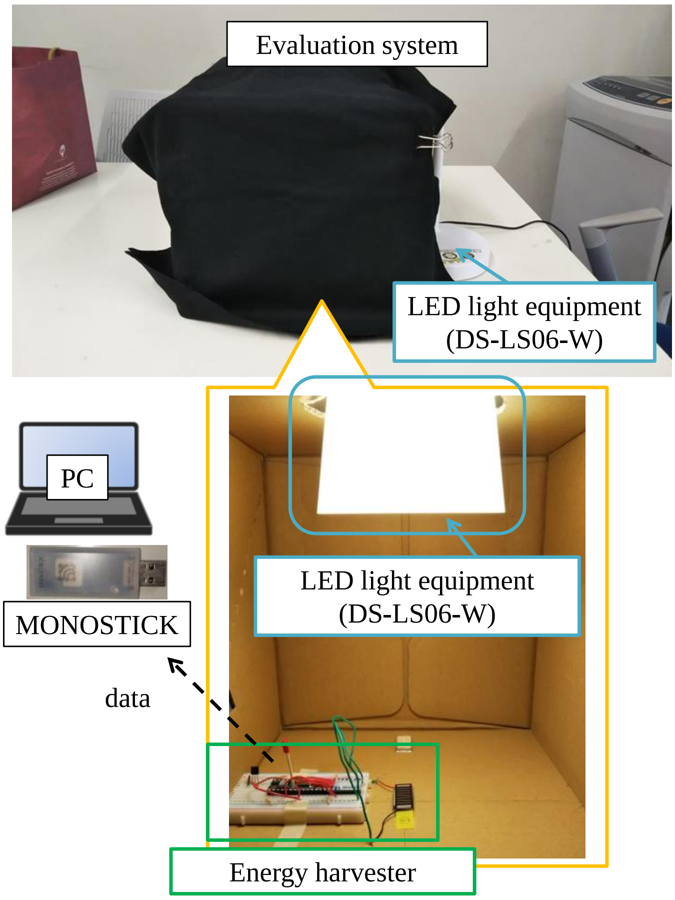

Evaluation system
LED light equipment (DS-LS06-W)
PC
MONOSTICK
data
LED light equipment (DS-LS06-W)
Energy harvester

Figure 3. Evaluation system.

Table 1. Experimental condition.

Energy harvester	TWELITE-DIP
	TWE-EH SOLAR
	Solar cell (Panasonic AM-5815)
LED light equipment	DL-LS06-W
Receiver	MONOSTICK

Figure 3 and table 1 show the experimental environment. Experiments used an evaluation system covered with black cloth to reduce the influence of light from the outside. An energy harvester, which consists of a TWELITE microcontroller (TWELITE-DIP), a power management module (TWE-EH SOLAR), and a solar cell, was placed in the evaluation system. In addition, LED light equipment (DS-LS06-W) was set on the energy harvester, and it irradiated constant light to the solar cell. At this time, the illuminance of the LED light equipment is 1,000 [lx] against directly under 25cm. Then, to

measure the power generation time, constant light was irradiated into 3 types of solar cells (A, B, and C). For the measurement of the power generation time, a MONOSTICK was used as a receiver.
To utilize additional information for authentication, experiments by changing of light incident position was conducted. Here, by changing the device’s position, the light incident position can be changed. Specifically, experiments utilized 3 types of device’s positions: middle, bottom, and top. Figure 4 shows the device’s positions.

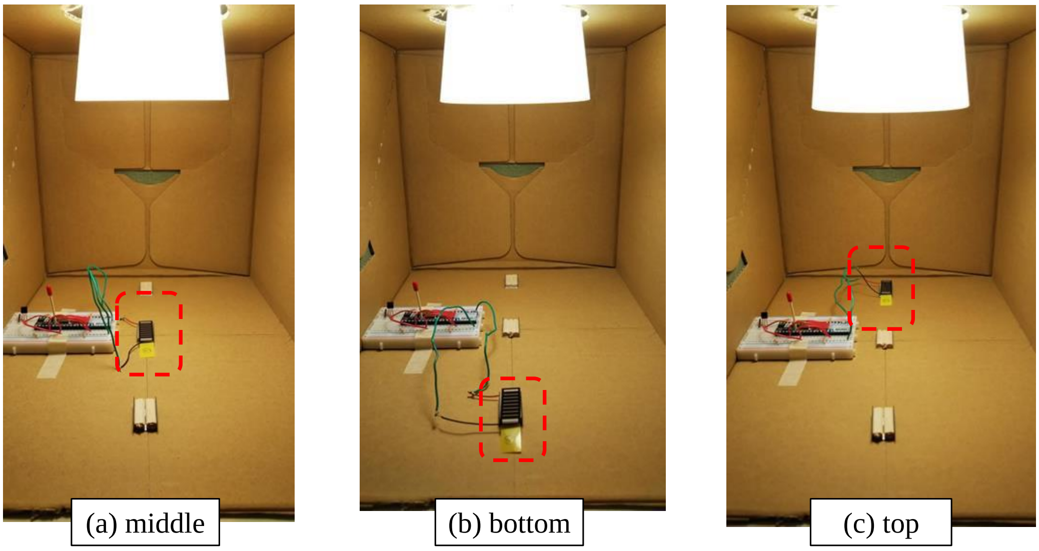


Figure 4. Device’s positions.

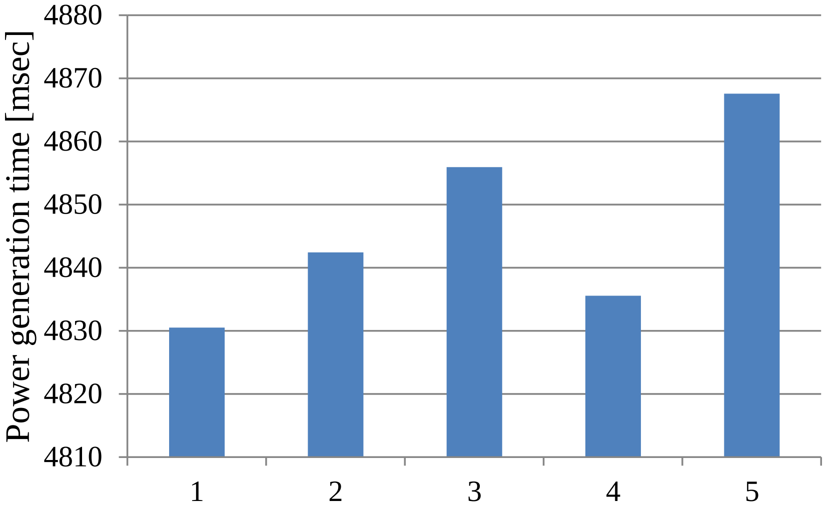


Figure 5. Results of preliminary experiments.

4.2. Experimental Results

First, the steadiness of energy harvesting PUF was verified as preliminary experiments. Experiments measured the average power generation time of a same solar cell for 5 times. Figure 5 shows the verification results. In this figure, the vertical line shows the average power generation time. Then, the difference between the minimum (the first of figure 5) and the maximum (the fifth of figure 5) of the power generation time was calculated by the Euclid distance. It was confirmed that the calculated value was 37.

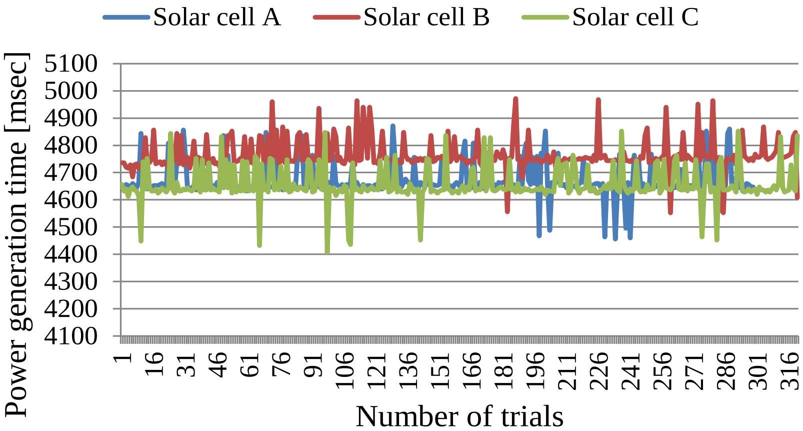


Figure 6. Results of the middle position.

Table 2. Comparison results (middle).

	A	B	C
A	—	93.92	15.49
B	93.92	—	109.4
C	15.49	109.4	—

Table 3. Comparison results (bottom).

	A	B	C
A	—	350.8	164.1
B	350.8	—	186.6
C	164.1	186.4	—

Table 4. Comparison results (top).

	A	B	C
A	—	176.4	44.77
B	176.4	—	131.7
C	44.77	131.7	—

Next, experiments verified the variance of the power generation time similar to paper [11], which placed solar cells in one type of position (middle position). Figure 6 shows the experimental results. In this figure, the vertical line shows the power generation time. In addition, table 2 shows differences of average power generation time between solar cells. The values of table 2 were calculated by the Euclid distance. As shown in figure 6 and Table 2, the power generation time of solar cell B differs from other solar cells (A and C) due to the production variation. By contrast, the power generation time of solar cell A and C is very similar, and its difference is 15.49 (see table 2). As discussed in the previous paragraph, the difference of the power generation time in the same solar cell is 37 in the maximum. Therefore, authentication between solar cells A and C is difficult because its difference is less than 37. Thus, authentication of a part of devices may fail when device’s position is fixed to only one.

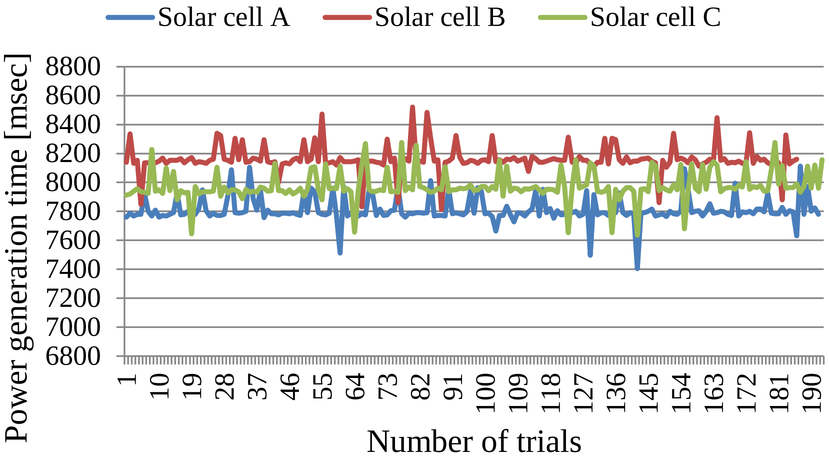


Figure 7. Results of the bottom position.

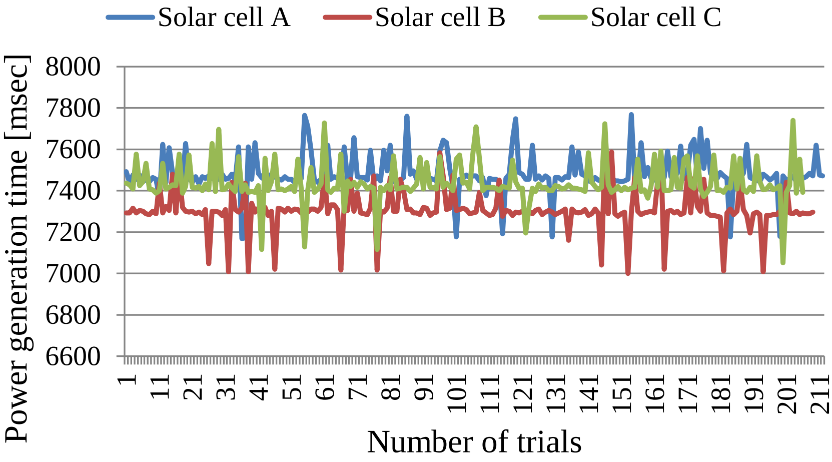


Figure 8. Results of the top position.

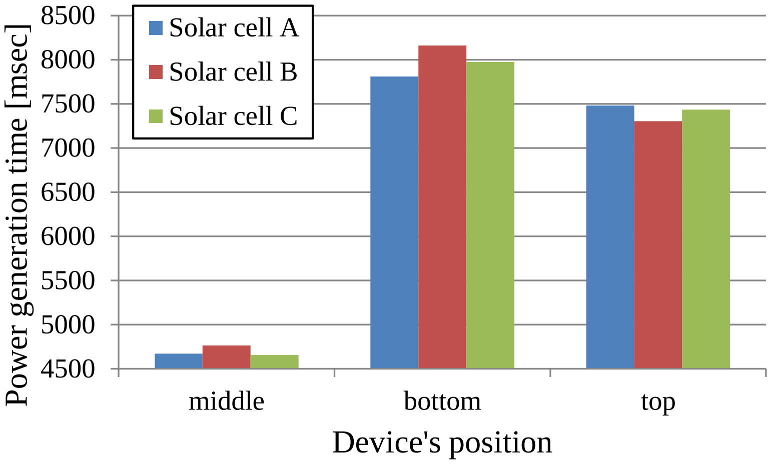


Figure 9. Comparison of average power generation time in each position.

Finally, experiments by changing the device's position were conducted. Figures 7 and 8 show the experimental results. Figure 7 is the results of the bottom position and figure 8 is that of the top position. Moreover, tables 3 and 4 show the results of average power generation time, and figure 9 shows the comparison results. As shown in these figures, in particular, the power generation time between solar cells A and C differs compared with that of the middle position. For example, on the bottom position, the power generation time of solar cell A is larger than that of solar cell C (difference is 164). This is presumably because the power generation efficiency is different in each device by different light incident position. Therefore, by using more information not only in the middle position but also in the bottom and the top position, the authentication accuracy can be improved.

5. Conclusion

This study evaluated the energy harvesting PUF by increasing input value. In this study, to utilize more input values for the energy harvesting PUF, the light incident position was changed. For changing of the light incident position, 3 types of device's positions (middle, bottom, and top) were used. Experiments using 3 types of solar cells (A, B, and C) showed that when the device was fixed in middle position, the difference of power generation time between solar cells A and C was less than 37 which is the variance of a same solar cell. Thus, this study clarified that authentication fails when input value is fixed. In addition, experiments also showed that when the device was fixed in bottom, the power generation time of solar cell A was larger than that of solar cell C (its difference was 164), that is, the authentication succeeded. Thus, the authentication accuracy could be improved by using additional information not only in the middle position but also in the bottom and top position.

Future works include that the direction of solar cells is changed in order to use more information for energy harvesting PUF, and the study of other energy harvesters.

6. References

[1] Chalasani S and Conrad J M 2008 A Survey of Energy Harvesting Sources for Embedded Systems *Proc. IEEE SoutheastCon* pp 442–447

[2] Nicosia A, Pau D, Giacalone D, Plebani E, Bosco A and Iacchetti A 2018 Efficient Light Harvesting for Accurate Neural Classification of Human Activities *Proc. IEEE Int. Conf. on Consumer Electronics* pp 1–4

[3] Tentzeris M M, Georgiadis A and Roselli L 2014 Energy Harvesting and Scavenging *Proc. IEEE* **102** 11 pp 1644–1648

[4] Dell'Anna F, Dong T, Li P, Yumei W, Yang Z, Casu M R, Azadmehr M and Berg Y 2018 State-of-the-Art Power Management Circuits for Piezoelectric Energy Harvesters *IEEE Circuits and Systems Magazine* **18** 3 pp 27–48

[5] Sicaria S, Rizzardia A, Griecob L A and Coen-Porisinia A 2015 Security, privacy and trust in Internet of Things: The road ahead *Computer Networks* **76** pp 146–164

[6] Skorobogatov S P 2015 Semi-Invasive Attacks – A New Approach to Hardware Security Analysis *PhD thesis University of Cambridge*

[7] Kocher P, Jaffe J and Jun B 1999 Differential Power Analysis *Proc. CRYPTO'99* LNCS 1666 pp 388–397

[8] Gassend B, Clarke D E, Dijk M V and Devadas S 2002 Silicon Physical Random Functions *Proc. 18th Annual Computer Security Applications Conf.* pp 148–160

[9] Aman M N, Chua K C and Sikdar B 2016 Physical Unclonable Functions for IoT Security *Proc. 2nd ACM Int. Workshop on IoT Privacy, Trust, and Security* pp 10–13

[10] Marchand C, Bossuet L, Mureddu U, Bochard N, Cherkaoui A and Fischer V 2018 Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems* **37** 1 pp 97–109

[11] Nozaki Y and Yoshikawa M 2018 Physical Unclonable Function using Energy Harvesting *Proc. 2018 IEEE Int. Meeting for Future of Electron Devices, Kansai* pp 38–39

[12] https://mono-wireless.com/jp/index.html

[13] Aponte E 2017 A Study on Energy Harvesters for Physical Unclonable Functions and Random Number Generation *M.S. thesis Virginia Polytechnic Institute and State University*.

[14] Kumar S D, Labrado C, Badhan R, Thapliyal H and Singh V 2018 Solar Cell Based Physically Unclonable Function for Cybersecurity in IoT Devices *Proc. 2018 IEEE Computer Society Annual Symp. VLSI* pp 697–702

[15] Sinton R A, Cuevas A and Stuckings M 1996 Quasi-Steady-State Photoconductance, A New Method for Solar Cell Material and Device Characterization *Proc. 25th IEEE Photovoltaic Specialists Conference* pp 457–460

[16] Sinton R A and Cuevas A 2000 A Quasi-Steady-State Open-Circuit Voltage Method for Solar Cell Characterization *Proc. 16th European Photovoltaic Solar Energy Conf.* pp 1152–1155

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 17J11408.