2022 13th International Conference on Information and Communication Technology Convergence (ICTC) | 978-1-6654-9939-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICTC55196.2022.9952899

Enhancing IoT security with PUF-based authentication scheme

Seungyong Yoon, Byoungkoo Kim, Keonwoo Kim and Yousung Kang
Cryptographic Engineering Research Section
Electronics and Telecommunications Research Institute
Daejeon, Republic of Korea
{syyoon, bkkim05, wootopian, youskang}@etri.re.kr

***Abstract*— Physical unclonable function (PUF) technology has been proposed as a solution to solve the IoT security problem, and research on key generation or device authentication using it is being actively conducted. In this paper, we present a new PUF architecture, resistor-capacitor (RC) PUF, and a scheme for applying device authentication technology based on it to the open connectivity foundation (OCF) IoT platform. We greatly improve security level by using PUF technology in the process of acquiring ownership of IoT devices and device authentication of the OCF cloud server. Finally, we present the implemented prototype. In addition, we give experimental results and performance comparison from a security point of view.**

Keywords—IoT Security; PUF; authentication

I. Introduction

Many studies are being conducted to safely protect IoT devices from various security threats and vulnerabilities. Recently, as a security primitive to solve the security problems faced by IoT devices, PUF technology is attracting attention [1]. PUF is a technology that utilizes the inherent characteristics of each device. It is unique like biometric information such as a human fingerprint or iris. Therefore, even if the device is made by the same manufacturing process, it is fundamentally impossible to duplicate because it is a digital fingerprint having a different value.

PUF technologies of various architectures have been studied [2-6]. Since these PUF technologies have advantages and disadvantages depending on their unique characteristics, it is necessary to select an appropriate architecture for each application and environment. Basically, PUF as a security primitive is used for secret key generation or device authentication. It is more secure because there is no need to inject the key externally or store it in memory. In addition, since it can provide a lightweight and cost-efficient method, it is suitable for IoT device authentication.

Although studies on PUF and PUF-based authentication technology to solve IoT security problems are being actively conducted, attempts to solve security issues by applying PUF technology to the IoT standard open platform are insufficient. In this paper, we propose a new resistor-capacitor (RC) PUF architecture applicable to the IoTivity [7] open platform of OCF. In addition, we propose a method to further improve security by applying PUF technology to acquisition of ownership of IoT devices and certificate-based device authentication. Since the proposed scheme applies PUF technology while complying with the IoTivity standard specification of OCF, it is expected that it can be used in various application service fields by greatly improving the compatibility and security of IoT devices.

II. Proposed Scheme

A. Resistor-Capacitor PUF

We developed an RC PUF that can be used in most IoT devices using low-cost resistors, capacitors and the analog-to-digital converter (ADC) function of the microcontroller (MCU), which is essential in IoT devices [8]. After configuring one resistor and one capacitor as an RC filter circuit outside the MCU, the change in the RC filter output according to the MCU output is read using the ADC inside the MCU and the value is used as a response. That is, according to the challenge bit pattern, 0 or 1 was outputted using digital-to-analog converter (DAC) or general purpose I/O (GPIO) from MCU. The waveform is accumulated according to the RC time constant and the final value is input to the ADC and the response is outputted. Since the RC PUF can change the challenge length arbitrarily, the response bit increases exponentially as the challenge length increases. We can acquire numerous CRPs because RC PUF has the advantage of strong PUF.

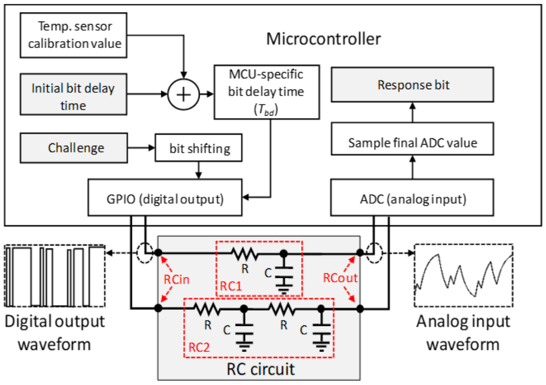

Fig. 1. Architecture of RC PUF

To handle noisy conditions of PUF, we propose a fuzzy extractor based on code-offset extraction as a stabilization technique in this paper. The proposed fuzzy extractor consists of two phases. The first is the generation phase, which obtains response and helper data from PUF and stores the helper data. FE.Gen outputs a key *(k)* and helper data *(hd)* - that is, *(k, hd)* = FE.Gen(R) - for a given input response (R). As the second reconstruction phase, a noisy response (R') is obtained from the PUF at run-time and the response (R) is restored together with the saved helper data *(hd)* - that is, *k* = FE.Rec(R', *hd*).

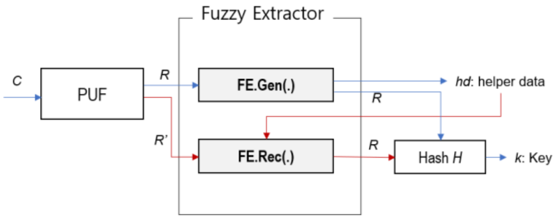

Fig. 2. Fuzzy extractor

In the generation phase, response R is obtained from PUF, and helper data *hd* = R - *cw* is obtained using *cw*, which is a random codeword of a specific code. This helper data, *hd*, is stored in the device. In the reconstruction phase, the PUF output is extracted again to obtain R'. This value is an output that is slightly different from the R obtained in the generation phase, and noise is included. Therefore, R' is expressed as R' = R + n, where n is modeled as random noise. Next, if you decode R' - *hd* = R + n - (R - *cw*) = *cw* + n using the saved helper data, you can get codeword *cw*, and add *hd* to it to get R = *cw* + *hd*. In the end, we get R, which is the response.

The code design related to the ability to correct errors in the reconstruction phase of the fuzzy extractor is similar to the coding theory of the existing communication area. The most commonly used error correction code (ECC) is the Bose-Chaudhuri-Hocquenghem (BCH) code [9]. However, the BCH code has a disadvantage in that it is not easy to implement in an IoT device due to its high implementation complexity. Therefore, in this paper, we propose to use a convolutional code. The convolutional code can use a viterbi decoder whose implementation efficiency has been verified, and has not only excellent error correction capability, but also advantages of operating speed and low cost.

B. Security Enhancement of IoTivity

OCF defines a standard specification that can connect and control IoT devices. It builds an architecture that guarantees interoperability between IoT devices and presents a model for managing resources. The standard specification consists of core, resource type device, bridging, and security. In addition, OCF has developed and provided IoTivity, an open source software framework for IoT.

This paper provides a scheme to strengthen security level by applying PUF-based authentication technology to the OCF IoTivity open platform. The IoT device executes the ownership transfer method (OTM) during the onboarding sequence. Utilizing PUF technology to run OTM makes it safer and more convenient to take ownership of a device. This is because, like random PIN based OTM, the process in which the user directly intervenes to input a PIN number can be omitted. In addition, after registering IoT devices in the OCF cloud, device authentication is essential to provide services. The security can be improved through the certificate generation and authentication process using PUF rather than the traditional certificate-based authentication method. This is because the private key is not stored in non-volatile memory (NVM) such as flash memory, and whenever necessary in real time, a key is generated and used through PUF and immediately deleted.

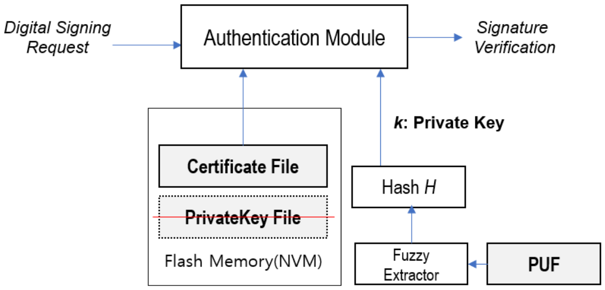

Fig. 3. Proposed certificate-based device authenticaiton

III. Implementation and Experiments

The proposed PUF-based IoT device authentication technique can minimize the threat of key exposure of existing IoT devices. To verify the proposed mechanism, a PUF-based IoT device authentication platform applicable to the OCF IoTivity standard was implemented. Fig. 4 shows our prototype implemented based on the IoTivity-lite 2.0.5 open source project, which is a lightweight implementation of the OCF standard. IoT devices basically operate on a commercial raspberry pi 3 model B, and a self-made board called a 'Kidden' board is used as a peripheral device. RC PUF is provided through this self-made PUF device.

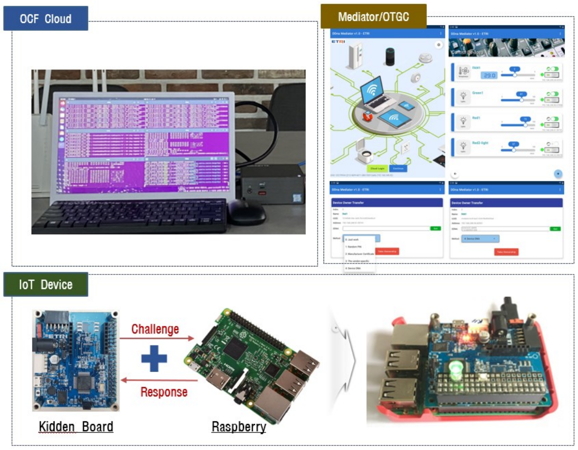

Fig. 4. Prototype of our system

The most important requirements for PUF output are largely known as reliability in a single PUF and uniqueness in multiple PUFs. However, ISO/IEC 20897-1 defines six security requirements in more detail: steadiness, randomness, uniqueness, unpredictability, tamper-resistance, and physical unclonability. In addition, the ISO/IEC 20897-2 standard provides two major metrics for evaluating the performance of PUF output. One is Intra-Hamming Distance (IntraHD) and the other is Inter-Hamming Distance (InterHD). In this paper, the entropy performance metric was additionally added to this evaluation and compared with other PUF architectures.

Table 1 shows the results of comparative analysis of performance metrics between the existing PUF architectures and the proposed RC PUF. RC PUF can output response in real time even during device operation. As a result of the experiment, the values of InterHD 49.2%, IntraHD 1.9%, and min-entropy 0.78-0.81 are shown.

TABLE I. PERFORMANCE COMPARISON

PUF Architecture	InterHD (%)	IntraHD (%)	Entropy (min)	Run-time extraction
Arbiter PUF [2]	36.75	1.52	not reported	possible
RO PUF [3]	47.3	0.9	not reported	possible
TERO PUF [4]	48.5	2.6	not reported	possible
DRAM PUF [5]	35.9	2.2	not reported	difficult
SRAM PUF [6]	49.7	3.8	0.57-0.7	difficult
Proposed RC PUF	49.2	1.9	0.78-0.81	possible

Since IoTivity basically uses the TLS security protocol for authentication and encrypted communication in the standard specification, it is safe from various security threats and attacks. Finally, we analyze the proposed scheme from the security point of view.

- Mutual authentication: Device authentication (access token based) and Cloud server authentication (certificate based) through mediator are performed. As a result, mutual authentication is performed between the device and the OCF Cloud server.
- Privacy of the IoT devices: Mediator requests a response using temporal device ID at first, and acquires access token using persistent device ID after ownership transfer process. The device registers and uses the device ID received from the mediator through TLS communication in the cloud server, thereby ensuring device privacy.
- Handling noisy conditions: A fuzzy extractor is applied to handle the unstable PUF output to generate a stable response.
- No secrets on the NVM: For the original purpose of PUF, no memory is used to store secrets. The secret key is used by requesting PUF whenever necessary, and deleted immediately after use.
- Protection against man-in-the-middle attack (MITM): All data transmission in IoTivity is performed over TLS-based encrypted communication channel. Therefore, representative MITM attacks such as spoofing attack, impersonation attack, message tampering attack, and replay attack are prevented.
- Protection against machine learning-based modeling attack: In order for this attack to be successful, CRP information is required during the learning process. However, any leakage of CRP information between the IoT device and the authentication server is blocked, so it can be defended.
- Protection against side channel attack: According to the test results, it is expected to be robust against passive attack by ensuring stable generation of PUF output dependent on temperature and voltage changes. More research and testing are needed for other side-channel attacks (invasive or active attacks).
- Protection against cloning attack: Due to the inherent nature of PUF, cloning is impossible.
- Protection against physical attack: The current implementation is in the form of a prototype, but it is possible to defend against the attack by applying the physical tamper-proofing technology.

IV. CONCLUSION

In this paper, we presented a scheme to enhance security level by applying PUF-based authentication technology to the OCF IoTivity open platform. A new RC PUF architecture was proposed and applied to OTM during the onboarding process and certificate-based IoT device authentication of IoTivity. RC PUF showed excellent results in performance metrics satisfying security requirements and applied to IoTivity to make the security protocol more robust. Our proposed scheme, which overcomes the limitations of existing PUF and PUF-based authentication technologies and complies with international standards, is expected to help safely and conveniently use more applications and services in the IoT environment.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2022-0-01019, Development of eSIM security platform technology for edge devices to expand the eSIM ecosystem).

REFERENCES

[1] C. Herder, M. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," In Proceedings of the IEEE, Vol. 102, No. 8, pp. 1126-1141, August 2014.

[2] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGA," In Proceedings of ReConFig, Quintana Roo, Mexico, pp. 298–303, 2010.

[3] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," In Proceedings of HOST, Anaheim, CA, USA, pp. 94–99, 2010.

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

[5] Q. Tang, C. Zhou, W. Choi, G. Kang, J. Park, K. Parhi, and C. Kim "A DRAM based physical unclonable function capable of generating $> 10^{32}$ challenge response pairs per 1Kbit array for secure chip authentication," In Proceedings of CICC, Austin, TX, USA, pp. 1–4, 2017.

[6] G. Schrijen and V. Leest, "Comparative analysis of SRAM memories used as PUF primitives," In Proceedings of DATE, Dresden, Germany, pp. 1–14, 2012.

[7] IoTivity, Open source for IoT, Available: https://iotivity.org/

[8] S. Lee, M. Oh, Y. Kang, and D. Choi, "RC PUF: A Low-Cost and an Easy-to-Design PUF for ResourceConstrained IoT Devices," In Proceedings of the 20th World Conference on Information Security Applications, Jeju, Korea, pp. 326–337, August 2019.

[9] G. Suh, and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," In Proceedig of ACM/IEEE Design Automation Conference, pp. 9-14, June 2007.