The ISC Int'l Journal of Information Security
ISeCure

November 2022, Volume 14, Number 3 (pp. 1–8)
http://www.isecure-journal.org

Presented at the ISCISC'2022 in Rasht, Iran.

Mutual Lightweight PUF-Based Authentication Scheme Using Random Key Management Mechanism for Resource-Constrained IoT Devices [☆]

Amir Ashtari [1], Ahmad Shabani [1], and Bijan Alizadeh [1,*]

[1] *School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran, Iran.*

ARTICLE INFO.

Keywords:
IoT, Network Security, Radio Frequency Identification, Physical Layer Security

Type:
Research Article

doi:
10.22042/isecure.2022.14.3.1

dor:
20.1001.1.20082045.2022.14.3.1.5

ABSTRACT

This paper presents a novel RF-PUF-based authentication scheme, called RKM-PUF which takes advantage of a dynamic random key generation that depends upon both communication parties in the network to detect intrusion attacks. Unlike the existing authentication schemes, our proposed approach takes the physical characteristics of both involved parties into account to generate the secret key, resulting in securely mutual authentication of both nodes in a wireless network. The experimental results of the proposed authentication scheme show that the RKM-PUF can reach up to 99% in identification accuracy.

1 Introduction

The Internet of Things (IoT) refers to connected devices embedded with sensors, software, and other technologies to connect, monitor, and control things over the internet. As IoT devices become widespread without direct human supervision, secure communication ensuring confidentiality and authorized access using encryption and authentication would be necessary. Therefore, taking the proper security measures becomes one of the most critical issues in the IoT ecosystem. This problem is becoming more crucial for the resource-constrained IoT devices as the hardware realization of complex encryption primitives and counteraction approaches against hardware Trojans in these devices is limited [1–4].

The Physically Unclonable Function (PUF) exploits the physical characteristics of the involved devices as a unique fingerprint by measuring inherent randomness introduced during manufacturing. Using such a promising concept enables us to measure the unique physical characteristics of IoT devices for authentication purposes without incurring high design complexity, which is not tolerated, especially in resource-constrained IoT devices. Five fundamental aspects should be considered for any authentication scheme developed for resource-constrained devices. First, developing an authentication scheme with minimum prepossessing requirements is of interest. Second, in the absence of asymmetric cryptography schemes due to high complexity, the confidentiality of transmitted data should be ensured by empowering the symmetric schemes. Third, employing the authentication framework which is secure enough and is compatible with various network topologies. Fourth, deploying an authentication module that can either be added to the main block diagram or embedded as a portable module to the already fabricated devices

[*] Corresponding author.

[☆] The ISCISC'2022 program committee effort is highly acknowledged for reviewing this paper.

Email addresses: amirashtari.74@ut.ac.ir, ah.shabani@ut.ac.ir, b.alizadeh@ut.ac.ir

ISSN: 2008-2045 © 2022 ISC. All rights reserved.

is desirable. Fifth, the limited resources and battery-powered IoT devices necessitate the authentication scheme's lightweight hardware realization and small footprint.

A vast majority of research is devoted to addressing IoT devices' security challenges, mainly focusing on developing a lightweight cryptography scheme [5]. Authors of [6] developed a hybrid cryptography scheme using a random key to shorten encryption time. This approach, however, mainly suffers from high resource utilization which eventually makes it less practical for IoT applications. Following that, authors of [7] introduced a novel lightweight public key encryption scheme and a mutual authentication protocol faster than RSA and ECC algorithms. Although these schemes are robust from the security point of view, they incur high area and power overheads. On the other hand, lightweight cryptography blocks such as PRESENT [8] and CLEFIA [9] have been proposed to alleviate the high complexity of the traditional ciphers. Unlike the existing asymmetric ciphers, these new cipher blocks improve the hardware efficiency and shorten the execution time. Nevertheless, they still impose large areas and power overhead on IoT devices. In this regard, several studies were conducted to address the lightweight authentication schemes based on the asymmetric blocks, focusing on the cloud application [10–13]. In [13], a new approach based on deep machine learning for securing IoT data transmissions is proposed. In practice, most of the cryptography schemes are vulnerable to impersonation attacks (e.g., replay attack and man in the middle (MITM) attack [14, 15]). The possible attack scenarios recently proposed against authentication protocols bring up a new view of early challenges that raise more concerns about a security vulnerability in real-world applications [16–18]. Hence, authentication takes significant attention in novel research in various applications, such as biomedical instruments [19].

Concerning the shortcomings of RF fingerprinting frameworks [20–22], a new fingerprinting scheme featured by Physically Unclonable Functions (PUF) called RF-PUF was presented in [23]. Although the RF-PUF framework does not require any additional hardware for feature extraction, it still consumes significant hardware resources, which is only suitable for implementation on the gateways in the star topology rather than resource-constrained sender's nodes [23–26]. In [27, 28], authors take advantage of the concept of mutual authentication mitigation with PUF. Unlike the proposed method, they used the PUF concept to generate a secure key to improve security against tampering and spoofing attacks in the underlying hardware. Nevertheless, we focus on using RF-PUF, which is lightweight and robust, to improve network security against Reply and MITM attacks. Moreover, authors in [29] provide a detailed overview of different types of authentication and key agreement mechanisms based on the PUF concept. They examined the already-existing methodologies and discussed the pros and cons of those methodologies as well. The paper presented in [25] focused on using a random forest classification algorithm to secure the wireless network in a star topology using one-way PUF-based authentication. However, the proposed method presents the mutual lightweight authentication method that can be employed in mesh networks.

In this paper, we develop a new authentication framework, called RKM-PUF (Random Key Management PUF), by leveraging the key management mechanism based on the physical characteristics of both involved IoT nodes to address the shortcoming of symmetric cryptography schemes and using the inherent characteristics of the physical layers to mutually authenticate the nodes. In contrast to the RF-PUF [23], the RKM-PUF also applies to the mesh and tree topologies. The proposed framework can securely identify both the transmitter and receiver nodes with high accuracy and is robust against various attacks, including replay, MITM, and password attacks. The lightweight hardware realization of the proposed RKM-PUF framework and its parallel authentication flow enable us to perform the authentication mechanism in real time on all the receiving packets, resulting in resiliency against MITM attacks (including session hijacking and IP spoofing). Moreover, the dependency of the proposed authentication procedure on the physical characteristics of both transmitter and receiver nodes would make it less vulnerable to replay attacks. In the proposed approach, the In-situ adjustment of the encryption key mainly relies on the communication parameters leading to more data confidentiality and resiliency against password attacks. Another distinct feature of the proposed method is its portability, making it a suitable candidate to be easily employed in already-fabricated IoT devices. The main contribution of this paper is to present a new concept of mutual authentication of both transmitter and receiver nodes in an ad-hoc network, called RKM-PUF, to integrate the physical characteristic-based authentication of both sides with secret key management. This approach remarkably lowers the computational cost and augments the performance of the key management phase. The rest of the paper is organized as follows. In Section 2, the proposed authentication flow is explained, and the performance metrics are evaluated in Section 3. Finally, Section 4 concludes the results.

2 Proposed Authentication Flow

Recently, the IoT network is becoming more vulnerable to various types of attacks as a considerable amount of resource-constraint and connected nodes are distributed without any supervision. A secure and lightweight authentication scheme for resource-limited devices is required to overcome these threats properly. Concerning this issue, our proposed authentication flow presents a new solution based on the inherent physical characteristics of both involved parties in a communication network by developing a lightweight architecture that can simply be added to already-fabricated devices in parallel with the main block diagram of the receiver side. Figure 1 shows the proposed authentication scheme, which exploits the physical characteristics of both the transmitter and receiver sides to create a PUF instance. The proposed flow includes four steps: 1) communication framework, 2) feature specification and measurement, 3) key management, and 4) RKM-PUF, which are further explained in the following subsections.

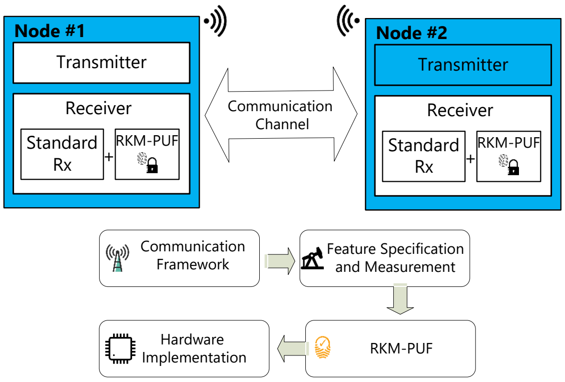

Figure 1. The proposed authentication flow for the IoT network

2.1 Communication Framework

A typical transmitter and receiver node's block diagram is illustrated in Figure 2. At the network's physical layer, we consider a communication framework based on the IEEE 802.15.4 standard, one of the preferred standards for IoT networks [30]. This standard outlines the different aspects of low power consideration for wireless sensor nodes, ensuring that the nodes can still operate without an external power supply for several years. Furthermore, Figure 3 shows the new receiver block diagram of IoT nodes in which the proposed RKM-PUF is embedded alongside the standard receiver. More specific details will be discussed in the following subsections. As Figure 3 shows, the proposed RKM-PUF can simply be added to the already-fabricated devices without requiring significant modification to the underlying hardware.

2.2 Feature Specification and Measurement

One of the key aspects of our proposed authentication scheme is to manage random yet secure keys. For doing so, a PUF instance is generated by exploiting the inherent features from both involved parties of a network. These features mainly depend on the process variations and are relatively immune to channel impairments. The intrinsic features required to generate a PUF instance can directly be derived from the already-existing modules embedded in the receiver side without requiring any additional circuitry.

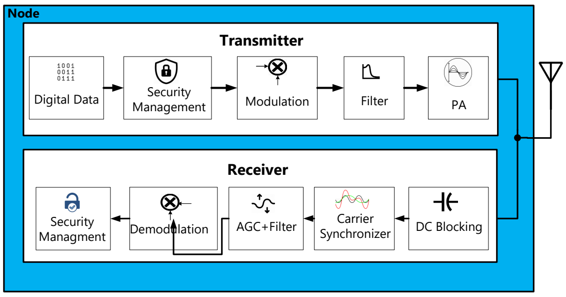

Figure 2. Block diagram of the communication framework

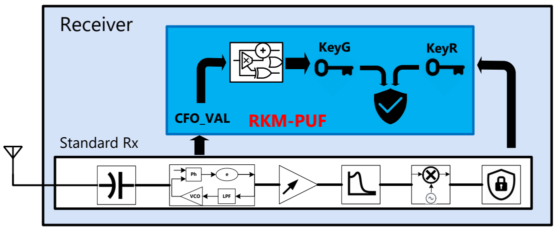

Figure 3. The proposed receiver block by embedding RK-M-PUF

In essence, even under ideal environmental conditions, there always is a frequency mismatch between the transmitter and receiver sides owing to the unique operating frequency of each transmitter relative to the ideal carrier frequency. This frequency offset mainly arises from the inherent variations in each node's Local Oscillators (LOs). To compensate for this offset, the synchronizer module is already employed on the receiver side so that the frequency offset is calculated concerning the high-quality reference clock. In fact, this frequency offset originates from two sources: 1) the difference between the receiver and transmitter oscillation frequencies and 2) the Doppler effect. This offset can directly be extracted from the carrier synchronizer module embedded at the receiver side, as shown in Figure 2. In this case, we assume that the connected devices are stationary. As the Doppler effect comes from mobile devices, stationary devices do not contribute to the frequency offset from the Doppler effect. Thus, the carrier frequency offset (CFO) of stationary devices will only depend on the difference between the receiver and transmitter oscillation frequencies which mainly relies on the process variations introduced during manufacturing and the aging effects. Based on the IEEE 802.15.04 standard, the CFO value (CFO_VAL) is restricted within ±40 ppm of the center frequency. This range corresponds to a 96 kHz distribution on each side of 2.4 GHz. Although other features, such as DC offset and IQ attendance, can be sued for feature measurement purposes in our PUF instance, we use CFO as the main feature. The main reason behind this decision is the ability to measure CFO values out of the receiver block diagram without changing the internal block diagram, which helps us to adapt RKM-PUF to already-fabricated IoT devices.

In the literature, different methods were proposed to measure the CFO as listed in Table 1. The first solution (GPS-Based) relies on the difference between the GPS signal and the transmitter's local oscillation frequency. This method, however, is limited to GPS-enabled devices. The second solution is Network Broadcasting, based on broadcasting a reference signal from a pre-identified source. The Constant Parameter's third solution uses a frequency offset relative to the reference oscillator measured in the manufacturing process. Although this way of offset measuring is more cost-effective than its counterparts, it is less reliable and suffers from channel effects. The final solution, the Two-node Differential, is to use the difference between the local oscillation frequency of the transmitter and receiver sides. Due to the higher reliability of the final solution and its robustness against replay attacks, this solution has been used as the base technique to measure the CFO values.

2.3 Key Management Mechanism

One of the essential modules in the proposed flow is the key management module. This module is responsible for generating the key (KeyG) using the CFO_VAL. Because the KeyG is generated using features extracted from both the involved nodes, it is called a real-time key management mechanism. As explained earlier, the CFO_VAL is in the range of [-96 kHz, 96 kHz]. To divide this range, two classifications are considered where their boundaries are shown in Figure 4 for $n_1 = 32$ and $n_2 = 8$, where n_i represents the number of classes corresponding to the classification i. In the first and second classifications, 32 and 8 classes with an equal interval of 6 kHz and different intervals for the second classification are considered, respectively. As shown in Figure 4, the boundaries of the two classifications have no overlap. Note that n_1 and n_2 are specified by the designer to achieve higher accuracy.

Table 1. Different methods of CFO measuring and their properties

Method	Reliable	comprehensive	aging effect	replay attack
GPS Based	4	×	4	×
Network Broadcasting	4	4	4	×
Constant Parameter	×	4	×	4
Two-node Differential	4	4	4	4

Figure 5 illustrates how the keyG is generated using the CFO_VAL. Two banks of keys KeyBank1 and KeyBank2 are considered to correspond to the first and the second classifications. These two banks can receive their secure keys (Keyi) from the network layer or a complex mathematical model in which the CFO_VAL feeds can be used. It should be noted that generating secure keys (i.e., Keyi in KeyBank1 and KeyBank2) is not the main focus of this work, and any secure key generation schemes available in the literature can be used [31, 32].

To clarify the key generation process, lets us take an example based on Figure 4. In the first classification, 32 classes ($n_1 = 32$) are taken into consideration. In order to classify the CFO_VAL with equal intervals, a division by constant value is needed. Each class maps the CFO_VAL to the corresponding KeyG from the KeyBank1. If the CFO_VAL is within the marginal of the boundary values, different KeyG values may be generated in both nodes, resulting in a false-negative case. It means that an authorized node is wrongly specified as a malicious node. In this case, the KeyG will be selected using the second classification, which contains the classes with different intervals rather

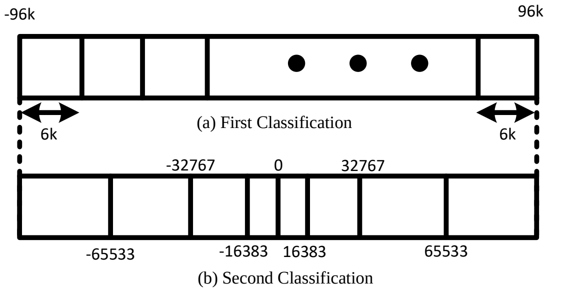

Figure 4. Example of class boundaries in the key management module, (a) the first classification, and (b) second classification

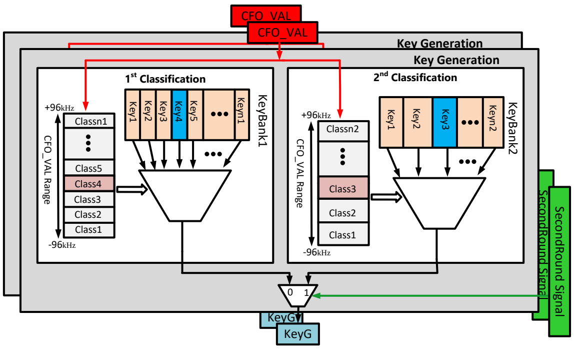

Figure 5. The proposed key management module

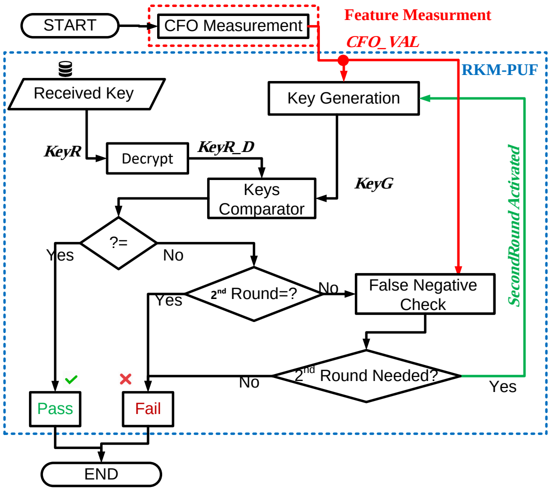

Figure 6. The proposed RKM-PUF authentication flow

than the fixed equal interval in the first classification. In the second classification, 8 classes ($n_2 = 32$) are generated, where each class maps the CFO_VAL to the related KeyG of the KeyBank2. It should be noted that due to the real-time key management based on the CFO_VAL, the RKM-PUF is entirely robust against drift effects and also the temperature and supply voltage variations.

2.4 RKM-PUF Based Authentication Flow

The main goal of the RKM-PUF is to provide a secure authentication framework for each receiving packet on both sides of the communication network. Figure 6 shows the proposed authentication flow. After measuring the feature from the synchronization module embedded in the receiver side, the KeyG is generated and compared with the KeyR_D (decryption of the KeyR received from the front device) to check whether the authentication passes or is denied. Note that the encryption and decryption of the KeyR are performed using a key received by the network layer to avoid transmitting the keys as plain texts. If the comparison matches, the authentication passes. Otherwise, due to the false-negative case discussed previously, we cannot deny the authentication for sure if the CFO_VAL is near the interval boundaries. As shown in Figure 6, the FalseNegativeCheck module decides whether the authentication fails or the second round of the authentication is needed to avoid the false-negative case. For doing so, the CFO_VAL and the interval boundary of the selected class are compared. If their difference is less than a pre-defined margin (i.e., 512), a second round is needed, and the procedure should be repeated for the second round of the classification. Otherwise, the authentication is denied. In the second round, if KeyGnew $\neq$ KeyRnew_D, the authentication fails without checking the threshold value.

3 Experimental Results and Security Analysis

To evaluate the efficiency of the proposed authentication scheme, the IEEE 802.15.04 standard is taken into account as the physical layer, and the communication toolbox of MATLAB software with the O-QPSK modulation and 2450 MHz band is used. In our experiments, 10,000 IoT nodes with normal distribution in their frequency offsets are evaluated regarding the communication cost when the RKM-PUF authentication is performed. The effect of channel variations on the authentication accuracy, false-positive, and false-negative rates are also measured.

3.1 Communication Cost

The proposed RKM-PUF method can be integrated into the cryptography schemes as a preceding step of key management. Authenticating using the proposed RKM-PUF can securely identify two parties in the communication network without side effects on the communication parameters, except for the latency just for the first frame. When the authentication procedure proceeds to the second round of the classification, the authentication performs twice for the first frame affecting the communication latency. Table 2 reports how many times the second round of the classification requires to authenticate different number of connected nodes (N) in the presence of different channel effects Eb/N0, and SPS values. Eb/N0 is the ratio of the signal energy to the noise spectral density, where Eb indicates the signal-to-noise ratio (SNR), and N0 is the noise spectral density. Also, the sample per symbol (SPS) defines the number of samples used to send each of the symbols where it is set to 12 in our case. The main finding is that only 4.24% of the cases, on average, need the second round of the classification. It indicates that only a tiny portion of the authentication time is related to the delay penalty introduced by the second round of the classification.

Table 2. Number of second round of classification for different number of connected nodes when performing RKM-PUF authentication

N	100	200	400	600	1000	10000
Number of 2nd-round	3	8	15	27	52	501
Average	4.24%					

3.2 False Positive Rate

Figure 7 shows the effect of the number of classes (NC) on the authentication accuracy (AA) in terms of the false-positive rate (FPR). If the NC increases, the FPR will significantly drop, leading to more AA. In this experiment, the AA abruptly increases when

NC varies from 5 to 50 classes, while this increase is nearly saturated for NC > 30. On the other hand, for many NC, the change in the NC has a negligible impact on the authentication accuracy. More analysis reveals that the FPR of 0.2% can be achieved for NC = 50. However, this high accuracy comes at the cost of higher design complexity on the receiver side. There is a trade-off between accuracy and design complexity. As the accuracy has less sensitivity for NC > 50, one of the best values for NC in terms of accuracy and design complexity can be set to 32, where the AA of 97.3% can be achieved. Moreover, the FPR has slightly reduced when NC > 30. By selecting 32 classes for the RKM-PUF, the FPR will be 2.7%, and in the worst-case scenario, the probability of error detection (PED) will be less than 10%. At the same time, the accuracy is almost 99% in normal situations.

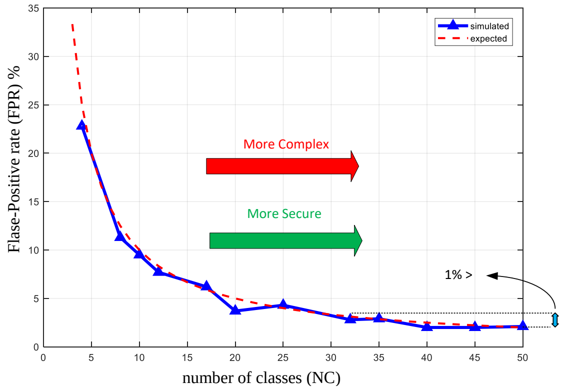

Figure 7. Impact of the number of classes on the false-positive rate

4 Conclusion

In this paper, a new portable and mutual authentication scheme, called RKM-PUF was presented by exploiting the physical characteristics of both involved parties in a communication network such that they can securely identify themselves without incurring high design complexity. The experimental results showed that the proposed architecture could effectively fill the absence of features introduced by the asymmetric cryptography schemes in resource-constrained IoT devices. In addition to the efficient and lightweight hardware implementation, the authentication accuracy was not affected by more than 5% in the presence of channel distortion so that the authentication accuracy is reached to 90% in the worst-case scenario.

References

[1] Ahmad Shabani and Bijan Alizadeh. Enhancing hardware trojan detection sensitivity using partition-based shuffling scheme. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 68(1):266–270, 2020.

[2] Mohammad Sabri, Ahmad Shabani, and Bijan Alizadeh. Sat-based integrated hardware trojan detection and localization approach through path-delay analysis. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 68(8):2850–2854, 2021.

[3] Ahmad Shabani and Bijan Alizadeh. Podem: A low-cost property-based design modification for detecting hardware trojans in resource-constraint iot devices. *Journal of Network and Computer Applications*, 167:102713, 2020.

[4] Fatemeh Khormizi, Ahmad Shabani, and Bijan Alizadeh. Hardware patching methodology for neutralizing timing hardware trojans using vulnerability analysis and time borrowing scheme. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2022.

[5] Mauro Conti, Ali Dehghantanha, Katrin Franke, and Steve Watson. Internet of things security and forensics: Challenges and opportunities, 2018.

[6] Michelle S Henriques and Nagaraj K Vernekar. Using symmetric and asymmetric cryptography to secure communication between devices in iot. In *2017 International Conference on IoT and Application (ICIOT)*, pages 1–4. IEEE, 2017.

[7] Dania Qara Bala, Soumyadev Maity, and Sanjay Kumar Jena. Mutual authentication for iot smart environment using certificate-less public key cryptography. In *2017 third international conference on sensing, signal processing and security (ICSSS)*, pages 29–34. IEEE, 2017.

[8] Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. Present: An ultra-lightweight block cipher. In *International workshop on cryptographic hardware and embedded systems*, pages 450–466. Springer, 2007.

[9] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher clefia. In *International workshop on fast software encryption*, pages 181–195. Springer, 2007.

[10] Peng Xu, Shuanghong He, Wei Wang, Willy Susilo, and Hai Jin. Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 14(8):3712–3723, 2017.

[11] Xiong Li, Jianwei Niu, Md Zakirul Alam Bhuiyan, Fan Wu, Marimuthu Karuppiah, and Saru Kumari. A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8):3599–3609,

2017.

[12] Rang Zhou, Xiaosong Zhang, Xiaojiang Du, Xiaofen Wang, Guowu Yang, and Mohsen Guizani. File-centric multi-key aggregate keyword searchable encryption for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8):3648–3658, 2018.

[13] Jafar A Alzubi, Ramachandran Manikandan, Omar A Alzubi, Issa Qiqieh, Robbi Rahim, Deepak Gupta, and Ashish Khanna. Hashed needham schroeder industrial iot based cost optimized deep secured data transmission in cloud. *Measurement*, 150:107077, 2020.

[14] SeungJae Na, DongYeop Hwang, WoonSeob Shin, and Ki-Hyung Kim. Scenario and countermeasure for replay attack using join request messages in lorawan. In *2017 international conference on information networking (ICOIN)*, pages 718–720. IEEE, 2017.

[15] Yuxiang Feng, Wenhao Wang, Yukai Weng, and Huanming Zhang. A replay-attack resistant authentication scheme for the internet of things. In *2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC)*, volume 1, pages 541–547. IEEE, 2017.

[16] Madiha Khalid, Umar Mujahid, Muhammad Najam-ul Islam, and Binh Tran. Probabilistic full disclosure attack on iot network authentication protocol. In *Future of Information and Communication Conference*, pages 728–738. Springer, 2019.

[17] Pavan Pongle and Gurunath Chavan. A survey: Attacks on rpl and 6lowpan in iot. In *2015 International conference on pervasive computing (ICPC)*, pages 1–6. IEEE, 2015.

[18] Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn. Iot goes nuclear: Creating a zigbee chain reaction. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 195–212. IEEE, 2017.

[19] Biswajit Kar, Anirban Mukherjee, and Pranab K Dutta. Stroke point warping-based reference selection and verification of online signature. *IEEE Transactions On Instrumentation and Measurement*, 67(1):2–11, 2017.

[20] Kevin Merchant, Shauna Revay, George Stantchev, and Bryan Nousain. Deep learning for rf device fingerprinting in cognitive communication networks. *IEEE Journal of Selected Topics in Signal Processing*, 12(1):160–167, 2018.

[21] P Padilla, JL Padilla, and JF Valenzuela-Valdés. Radiofrequency identification of wireless devices based on rf fingerprinting. *Electronics letters*, 49(22):1409–1410, 2013.

[22] Oktay Ureten and Nur Serinken. Wireless security through rf fingerprinting. *Canadian Journal of Electrical and Computer Engineering*, 32(1):27–33, 2007.

[23] Baibhab Chatterjee, Debayan Das, Shovan Maity, and Shreyas Sen. Rf-puf: Enhancing iot security through authentication of wireless nodes using in-situ machine learning. *IEEE Internet of Things Journal*, 6(1):388–398, 2018.

[24] Baibhab Chatterjee, Debayan Das, and Shreyas Sen. Rf-puf: Iot security enhancement through authentication of wireless nodes using in-situ machine learning. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 205–208. IEEE, 2018.

[25] Amir Ashtari, Ahmad Shabani, and Bijan Alizadeh. A new rf-puf based authentication of internet of things using random forest classification. In *2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, pages 21–26. IEEE, 2019.

[26] Amir Ashtari, Ahmad Shabani, and Bijan Alizadeh. A comparative study of machine learning classifiers for secure rf-puf-based authentication in internet of things. *Microprocessors and Microsystems*, 93:104600, 2022.

[27] Mario Barbareschi, Alessandra De Benedictis, Erasmo La Montagna, Antonino Mazzeo, and Nicola Mazzocca. A puf-based mutual authentication scheme for cloud-edges iot systems. *Future Generation Computer Systems*, 101:246–261, 2019.

[28] Priyanka Mall, Ruhul Amin, Ashok Kumar Das, Mark T Leung, and Kim-Kwang Raymond Choo. Puf-based authentication and key agreement protocols for iot, wsns and smart grids: a comprehensive survey. *IEEE Internet of Things Journal*, 2022.

[29] Karim Lounis and Mohammad Zulkernine. T2t-map: A puf-based thing-to-thing mutual authentication protocol for iot. *IEEE Access*, 9:137384–137405, 2021.

[30] Low-Energy Critical Infrastructure and Monitoring LECIM Physical Layer. Ieee standard for low-rate wireless networks. *IEEE Stand*, 2015:1–708, 2015.

[31] Chan Dai Truyen Thai, Jemin Lee, Jay Prakash, and Tony QS Quek. Secret group-key generation at physical layer for multi-antenna mesh topology. *IEEE Transactions on Information Forensics and Security*, 14(1):18–33, 2018.

[32] Abdelmoughni Toubal, Billel Bengherbia, Mohamed Ould Zmirli, and Abderrezak Guessoum. Fpga implementation of a wireless sensor node with built-in security coprocessors for secured

key exchange and data transfer. *Measurement*, 153:107429, 2020.

Amir Ashtari received his B.Sc. degree in electrical engineering from the University of Tabriz, Iran. He received his M.Sc. degree in electrical engineering from the University of Tehran. His current research interests include IoT, Network and Hardware Security, Hardware Acceleration, and Communication Engineering.

Ahmad Shabani received his B.Sc. degree in electrical engineering from Shiraz University, Shiraz, Iran, in 2014, the M.Sc. degree in digital electronic systems from Shahid Beheshti University, Tehran, Iran, in 2016, and the Ph.D. degree in digital electronic systems from Tehran University, in 2021. He is currently an Adjunct Lecturer at the University of Tehran, Tehran, Iran. Also, he has a joint collaboration with the Design, Verification, and Debugging of Embedded Systems (DVDES) laboratory of Tehran University. His research interests include image processing and video coding standards, medical image processing, hardware security, hardware trojan, and low-power & high-speed digital VLSI circuits.

Bijan Alizadeh received his Ph.D. degree in electrical and computer engineering from the University of Tehran, Iran, in 2004. He was with the School of Electrical Engineering, Sharif University of Technology, Iran, as an Assistant Professor from 2005 to 2007 and VDEC, the University of Tokyo, Japan, as a Research Associate from 2007 to 2010. He has been an Assistant Professor with the School of Electrical and Computer Engineering at the University of Tehran since 2011, where he is currently an Associate Professor. He has authored over 130 publications in international scientific journals and conferences. He has been engaged in the research and development of VLSI systems, FPGA-based reconfigurable computing, formal verification and debug, post-silicon debug, and high-level synthesis.