TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 04/10 pp36–47
DOI: 10.26599/TST.2019.9010048
Volume 26, Number 1, February 2021

A PUF-Based and Cloud-Assisted Lightweight Authentication for Multi-Hop Body Area Network

Xiao Tan, Jiliang Zhang*, Yuanjing Zhang, Zheng Qin, Yong Ding, and Xingwei Wang

Abstract: Wireless sensor technology plays an important role in the military, medical, and commercial fields nowadays. Wireless Body Area Network (WBAN) is a special application of the wireless sensor network in human health monitoring, through which patients can know their physical condition in real time and respond to emergencies on time. Data reliability, guaranteed by the trust of nodes in WBAN, is a prerequisite for the effective treatment of patients. Therefore, authenticating the sensor nodes and the sink nodes in WBAN is necessary. This paper proposes a lightweight Physical Unclonable Function (PUF)-based and cloud-assisted authentication mechanism for multi-hop body area networks, which compared with the star single-hop network, can enhance the adaptability to human motion and the integrity of data transmission. Such authentication mechanism can significantly reduce the storage overhead and resource loss in the data transmission process.

Key words: Physical Unclonable Function (PUF); hardware security; Wireless Body Area Network (WBAN)

1 Introduction

With the rapid development of networks, wireless communication, and sensor manufacturing technology[1–4], a large number of portable wireless devices have emerged and the body-centric Wireless Body Area Network (WBAN) has attracted much attention. Telemedicine monitoring is a typical application of WBAN in the medical field. Physiological data are collected by arranging wireless sensors and implantable equipment on the patient's body, and then are sent to the Internet via sink nodes. A physician in a remote area can analyze the data and provide a treatment plan on time. Telemedicine monitoring avoids the inconvenience that traditional patients and doctors must meet face to face for treatment and can expand the patient's activity space. For healthy groups, WBAN can provide health monitoring. For example, during an athlete's exercise, the training rhythm and training plan can be effectively adjusted by monitoring the athlete's heartbeat, body temperature, and other physiological parameters in real time. Therefore, WBAN plays a significant part in our daily life, medical treatment, entertainment, and the military.

WBAN brings great convenience to people, while its open features also bring serious security risks. Sensors collect physiological data that are closely related to the human body. Any case of data leakage will result in many problems, including the following: (1) The disclosure of patient's privacy: Patients do not want others to know their illnesses; moreover, after adversaries intercept the data, they are likely to sell the illness information to some private medical institutions

• Xiao Tan, Jiliang Zhang, Yuanjing Zhang, and Zheng Qin are with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China, and also with Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen 518000, China. E-mail: bigdata413@hnu.edu.cn; zhangjiliang@hnu.edu.cn; zhangyuanjing@buaa.edu.cn; zqin@hnu.edu.cn.
• Yong Ding is with Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China. E-mail: stone-dingy@126.com.
• Xingwei Wang is with the College of Computer Science and Engineering, Northeastern University, Shenyang 110004, China. E-mail: wangxw@mail.neu.edu.cn.
* To whom correspondence should be addressed.
Manuscript received: 2019-04-01; revised: 2019-08-22; accepted: 2019-08-29

or insurance companies, which violates patients' privacy. (2) Security risks: Adversaries may sneak into the network by forging the identity of a node by node attacks or physical cloning attacks and send the fake data to the sink node; this would seriously affect the physician's diagnosis and the formulation of the corresponding treatment plan, and is even life-threatening. For example, by attacking the cardiac pacemaker on a wireless virtual patient, the heart rate can be increased or reduced. If the device contains a defibrillator, the attacker can make the defibrillator repeatedly vibrate, which endangers the lives of patients.

In recent years, several approaches have been proposed to address the privacy and security issues caused by the open features of WBAN[5]. However, most of the methods are oriented to data transmission process. It is necessary to establish a secure topology before data transmission. The authentication of sensor nodes and sink nodes in WBAN is the prerequisite for establishing security topology and guaranteeing secure data transmission. Therefore, it requires that the circulating data come from legitimate nodes. However, most of the current authentication schemes[6] are based on star single-hop networks, which have several disadvantages, including the following: (1) The data transmission between sensor nodes and sink nodes consumes a large amount of power and resources for authentication; (2) A compromised sensor node will have a significant impact on the data collection of WBAN; (3) Human motion affects the data transmission. Star single-hop networks are not suitable for WBAN because of the effect of human motion, whereas the tree multi-hop network can reduce the influence of human motion and support dynamic reconstruction.

This paper proposes a lightweight authentication mechanism for multi-hop WBAN based on crossover Ring Oscillator (RO) Physical Unclonable Functions (PUFs)[7], which can implement the hierarchical authentication on the body-centric WBAN. The cloud-assisted method is deployed between the sink nodes, and the adjacent sensor nodes can largely reduce the storage overhead of the WBAN. Sensor nodes and inlayer nodes that are far from the sink nodes are authenticated through a shared-key generated by the crossover RO PUF[8]. All sensor nodes are authenticated by the sink node via trusted transmission. In the authentication process, the outer node does not need to directly transmit the information required for authentication, and this largely reduces the resource overhead.

The rest of this paper is organized as follows. Related work is elaborated in Section 2. The proposed lightweight authentication mechanism for WBAN is elaborated in Section 3. Potential security threats and countermeasures are analyzed in Section 4. The detailed experimental results and analyses are reported in Section 5. Finally, we conclude in Section 6.

2 Related Work

2.1 Node authentication of WBAN

Along with the widespread usage of WBAN, its security issues have attracted much attention in the industry and academia. The important issues related to the security of WBAN were summarized in Refs. [5, 6, 9]: data reliability, data security, data freshness, scalability, and privacy protection. Among these problems, it is crucial to ensure data reliability, which is an important basis for the implementation of other security measures. In addition, it is necessary to consider the characteristics of severely limited resources for WBAN.

Data reliability is guaranteed mainly through node authentication in WBAN. In general, the node authentication is implemented by traditional symmetric encryption algorithms, such as the TinySec[10], Timed-Efficient Stream Loss-tolerant Authentication (TESLA)[11], and MiniSec[12]. The encryption algorithms involved in these schemes include data encryption standard, Triple Data Encryption Standard (Triple DES), XOR, or other low-cost modes. TinySec provides authentication, data integrity, and data confidentiality protection with lower computational and storage overheads. However, Almheiri and Alqamzi[13] found that for a key distribution mechanism, once a single node is compromised, the entire network will become insecure. Chuchaisri and Newman[14] proposed that TESLA provides origin authentication and message integrity protection by using a one-way hash chain and delayed key disclosure techniques. However, it requires time synchronization between all nodes in the network, which may cause a long delay in authentication. The MiniSec solution is publicly available and has a high level of security. However, high computational overhead is incurred when large packets are transmitted over the radio.

Zhao et al.[15] pointed out that the traditional authentication method implemented in the upper layer of the Open System Interconnection (OSI) reference

model usually consumes a lot of energy, and requires massive changes at the hardware or software level. Ma et al.[16] proposed TinyZKP, which is a WBAN authentication scheme based on zero-knowledge proof. Their experiments showed that it can defend against replay attacks and guessing attacks. Liu et al.[17] proposed the BGMM model, which is specially oriented to WBAN and enables it to better adapt to human movement. Salam et al.[18] proposed PMAS for two-way authentication between the sink node and the sensor node, and implemented key sharing by improving the Diffie-Hellman key exchange scheme. Yuan et al.[19] proposed ASK-BAN for fast authentication and key extraction in WBAN; the model can simultaneously perform authentication and key extraction without additional hardware to obtain physical layer features. Nevertheless, such authentication lacks stability.

2.2 PUF

PUF is a novel hardware security primitive for key generation and device authentication[20]. Most PUFs provide a unique device-dependent mapping from a set of challenges to a set of responses (Challenge Response Pairs, or CRPs) based on the unclonable properties of the underlying physical device[21, 22]. Even with the same design, different manufactured PUFs have different CRPs[23]. It is suitable for various security-related applications, such as two-factor authentication[24], anti-overbuilding[25], IP protection[23, 26], and resisting of FPGA replay attacks[27] and code-reuse attacks[28].

Moreover, they can be classified into strong PUFs and weak PUFs. Strong PUFs provide a huge number of unique CRPs for authentication protocols[21]. A typical PUF-based authentication includes two stages, registration and authentication[29]. In the registration stage, the PUF CRPs are collected from the devices and stored in the server. In the authentication stage, the challenge is sent to the device terminal, and then the terminal device sends the corresponding response to the server. Finally, the response is compared with the previous stored response. If the two responses are the same or within an acceptable error threshold, the authentication passes, otherwise, the authentication fails.

Compared with the star single-hop network, the tree multi-hop network is more adaptable to human motion and can enhance the data integrity of data transmission. This paper proposes a PUF-based and cloud-assisted lightweight authentication mechanism for multi-hop WBAN. The cloud-assisted authentication can reduce the WBAN storage overhead. The deployed CRO PUF[7] in the authentication mechanism has high reliability and flexibility. Especially, it is well-known that how to distribute keys securely and effectively is the most difficult problem in the key management, while the PUF-based shared-key generation method[8] provides a new solution to address the issue.

3 Proposed Lightweight Authentication for WBANs

The framework of the proposed hierarchical authentication is illustrated in Fig. 1.

In the proposed authentication scheme, the cloud acts as a Trusted Third Party (TTP) to store the CRPs of the PUF. The authentication between the inlayer node and the sink node aims to compare the PUF response of the sensor node with the stored response in the cloud. In addition, the authentication between the outer sensor nodes is primarily achieved by comparing the shared-key generated by the crossover RO PUF.

The traditional authentication protocols based on star single-hop network perform the authentication between sensor nodes and sink nodes, since the sensor nodes in this network topology communicate directly with the sink nodes. However, the nodes far away from sink nodes communicate with the sensor nodes closer to them rather than the sink nodes. If they are directly authenticated with sink nodes, communication will require large power consumption. Therefore, the hierarchical authentication is proposed to authenticate the sink nodes and sensor nodes in the body area network.

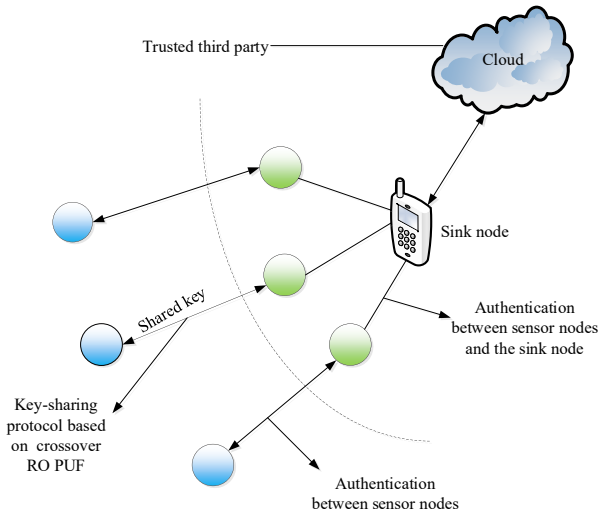


Fig. 1 Framework of the proposed hierarchical authentication.

Hierarchical authentication means that all sensor nodes are split into two parts according to the distance from the sink nodes. Nodes closer to the sink nodes are called inlayer nodes, and others are collectively termed as outer nodes. As shown in Fig. 1, the green nodes are considered as inlayer nodes and the rest nodes are outer nodes. Different methods are adopted to authenticate these two types of nodes. According to the transitivity of trust, the inlayer node passing the authentication of the sink node demonstrates that the sink node trusts the inlayer sensor node. In this case, if the inlayer node can be trusted by the outer node, the sink node will be also considered to trust the outer node, and the nodes in the entire network topology will trust each other.

3.1 Authentication between the inlayer node and sink node

In a tree multi-hop network, the inlayer node and the sink node are very close. Thus, the inlayer nodes centered on the sink nodes remain unchanged during human motion.

Several CRPs are generated based on a PUF. These responses are stable, unique, and unpredictable. The PUF can be embedded as a logical unit in the sensor node, and the set of PUF CRPs embedded in each sensor node can be stored in the cloud. The cloud separates the storage units based on different sink nodes, and the internals of each storage unit separately store the information corresponding to each sensor node.

Before the storage, each sensor node submits the features of the embedded crossover RO PUF to the cloud. Moreover, the cloud can derive the configuration information of the shared key between these sensor nodes.

When the sink node authenticates the sensor node, the sensor node serves as the initiator, and the sink node acts as the authenticator. Before authentication, the sink node broadcasts its own ID, and then the sensor node can obtain the ID and raise an authentication request to the sink node. During the authentication, the cloud is considered as a TTP, reducing the storage overhead in resource-constrained environments. Furthermore, when the sink node requests to access the CRPs of the PUF, the request can be verified according to the sink node ID. Thus, only the legitimate sink node can access the CRPs and the configuration information.

Figure 2 shows the authentication process between the sensor node and the sink node. Before sending data, Sensor A submits its ID (ID_A) to the sink node. After

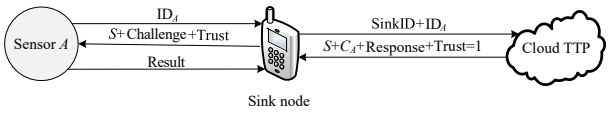


Fig. 2 Authentication between the inlayer node and sink node.

receiving ID_A, the sink node will send ID_A to the cloud along with its own ID (SinkID). If SinkID can be verified by the cloud, the cloud randomly selects the selection signal (S) and the challenge signal (Challenge) and acquires the corresponding response signal (Response) according to ID_A and SinkID. Challenge and Response are XORed to generate C_A. Subsequently, the cloud sends S, C_A, and Response to the sink node to ensure that the attacker cannot directly obtain the challenge response information. The CRPs are then removed from the database, and the Trust field value is set to 1. Trust$=1$ represents the cloud trusting the sink node. After receiving Trust, the sink node saves it and XORs the received C_A and Response to acquire the real challenge. The sink node sends Challenge and S, as well as the Trust field to the authentication requestor, Sensor A. On receiving this message, Sensor A extracts S and then inputs it to the PUF to acquire the response signal. In the meantime, Sensor A checks the value of the Trust field. In the case of Trust $= 1$, the Response and the received Challenge are XORed to generate Result. Sensor A compares the Result with the received Response information. If both are consistent or do not reach the threshold, Result is submitted to the sink node. Next, the sink node compares the received Result with the previously received Response from the cloud, thereby achieving the authentication of the sensor node by the sink node.

In brief, the authentication process of the inlayer node is as follows. Sensor A first verifies the received Trust field, and then compares the response signal generated by itself with the response signal from the sink node. The specific process is illustrated in Fig. 3.

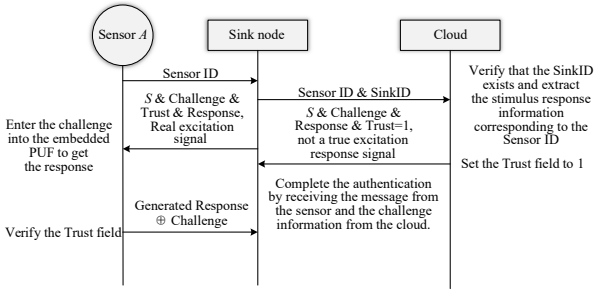


Fig. 3 Authentication process of inlayer node.

As shown in Fig. 3, although the cloud can ensure that the sink node is trusted by verifying the CRPs, this information may be maliciously tampered or hijacked when the challenge-response information is sent to the sink node. We assume that a malicious attacker cannot forge the ID of a sink node; if the attacker has such ability, the security of the remote end cannot be ensured. Under this assumption, in receiving the message from the sink node, the sensor node will compare the sink node ID with the previous ID, which is saved in the broadcast phase of the sink node. If the two IDs are consistent and the Trust field is displayed to be trusted, the sensor node will consider that the sink node is trusted, thereby authenticating the sink node. The sensor node gives the response to the sink node. After comparing the response at the sink node, the mutual authentication between the sink node and the inlayer sensor node is achieved.

3.2 Authentication between sensor nodes

The authentication between the outer sensor node and the inlayer sensor node is performed by a shared-key between the nodes, which is a one-to-many authentication process. The success of the shared-key comparison marks the passing of authentication.

The shared-key can be distributed through key pre-allocation. However, as described in the previous section, this will lead to additional overhead. Furthermore, once the key pool that lacks the dynamic update process is built, attackers can easily acquire all the keys by modeling attacks. After all the keys are obtained, the authentication link of the node is ineffective.

Thus, the authentication between the sensor nodes is implemented by the crossover RO PUF. By embedding the crossover RO PUF at different sensor nodes and configuring the selection of the challenge, a shared-key between the sensor nodes can be yielded. To be specific, first, the feature of the crossover RO PUF is sent to the TTP. Subsequently, the mapping between the challenges is completed under the same selection signal to gain the same response signal which serves as a shared-key between the nodes. The storage form of the configuration information in the TTP is shown in Fig. 4. What is stored in the TTP is the inverter delay information in each layer RO link in the crossover RO PUF. Accordingly, the output of the specific response can be derived by setting the selection signal and the challenge.

The outer sensor node will transmit its own ID when requesting authentication. The node that has achieved the authentication transmits the ID of the sensor node

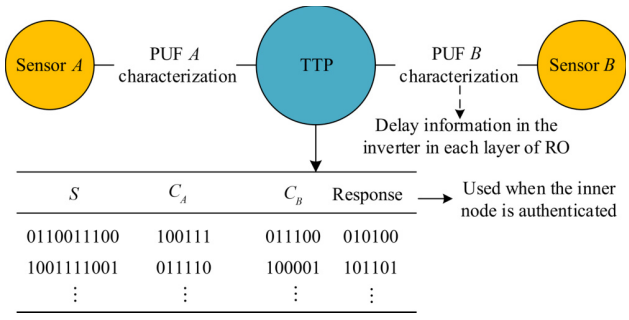


Fig. 4 Generation of shared key configuration information.

to the sink node, and the sink node takes the node with the highest trust as the authenticator to respond to the authentication request of the sensor node.

Sensor A serves as the initiator of the authentication request, and Sensor B completes the authentication, which is considered as a trusted node. The specific authentication process is presented as follows.

(1) Sensor A generates a random number Rand_A and then submits Rand_A and ID_A (Sensor A's ID) to the authenticator, Sensor B.

(2) After receiving the message from Sensor A, Sensor B generates a random number Rand_B and sends $\{\text{Rand}_A, \text{ID}_A, \text{Rand}_B, \text{ID}_B\}$ to the sink.

(3) Subsequently, the sink applies to the TTP for the previously stored selection signal S and challenge C_A and C_B.

(4) The sink node encrypts $\{S, \text{Rand}_A, \text{ID}_B, C_A\}$ using K_{AS}, which is the shared-key of Sensor A and the sink node, to yield $\{S, \text{Rand}_A, \text{ID}_B, C_A\}K_{AS}$. Next, $\{\{S, \text{Rand}_A, \text{ID}_B, C_A\}\ K_{AS}, \text{ID}_A, \text{Rand}_B, C_B, S\}\ K_{BS}$ is generated using K_{BS}, which is the shared-key between the sink node and Sensor B. Then, the message is returned to Sensor B.

(5) Sensor B decrypts the message with K_{BS} and then verifies whether Rand_B is consistent with the previous one. If not, the authentication process will be terminated. Otherwise, Sensor B will send $\{S, \text{Rand}_A, \text{ID}_B, C_A\}K_{AS}$ and the selected intermediate value MidNum to Sensor A according to ID_A. Moreover, S and C_B generate a response by the crossover RO PUF.

(6) After receiving $\{S, \text{Rand}_A, \text{ID}_B, C_A\}K_{AS}$ and MidNum, Sensor A decrypts the message with K_{AS} to yield S, Rand_A, and C_A. Afterward, it judges whether Sensor B is trusted by comparing Rand_A. If Rand_A is consistent with the previous one, S and C_A are used for the crossover RO PUF to obtain a response. The response and the received MidNum are XORed to derive MidNum1, and then Sensor A sends MidNum1 to Sensor

B according to ID_B.

(7) After receiving the MidNum1, Sensor B performs an XOR operation with the response generated by the previous Sensor B. If the result is consistent with MidNum, Sensor A is considered to be trusted. Sensor B will return the authentication result to the sink node and send an ACK/Reject message to Sensor A.

The entire authentication process is illustrated in Fig. 5.

4 Security Analysis

4.1 Security analysis of CRO PUF

In recent years, the unpredictable, unclonable, and tamper-proof features of PUF have been questioned. As a result, the security of PUF has also aroused huge attention. Some attacks against PUF have been proposed, e.g., model attacks and physically clonable attacks. The defense methods of the crossover RO PUF against these two common attacks are discussed below.

4.1.1 Modeling attacks

Machine learning is the most well-known attack on strong PUFs which have a public access interface for CRPs. Therefore, attackers are easy to collect sufficient CRPs for modeling. Machine learning can model strong PUFs with high prediction accuracies. However, the modeling attack requires considerable CRPs and hence is not applicable to weak PUFs.

4.1.2 Physically clonable attacks

Merli et al.[30] successfully implemented a physically clonable attack on SRAM PUF for the first time. The major reason is that the SRAM will emit near-infrared light when it is read, and the power value of the unit can be obtained by the emitted light. Since the inter-stage crossovers and the inverters in the crossover RO PUF are independent of each other, malicious attackers

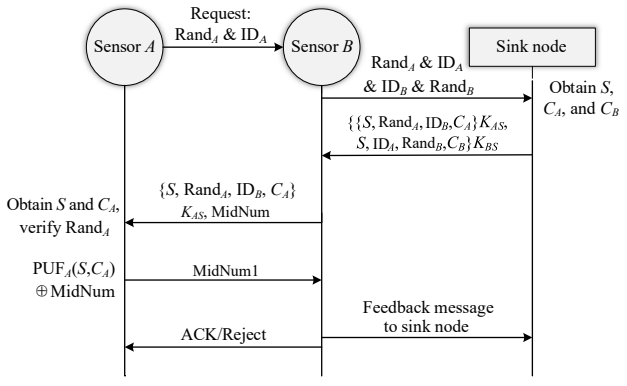


Fig. 5 Authentication process between sensor nodes.

cannot derive any delay information of the inverter by acquiring the configuration information. In addition, the CRO PUF can dynamically change the number of inverters in the RO, which can be implemented using different configuration data to generate an unclonable bits string. In this case, the physical location of each RO is not fixed, and it is also a novel method to resist side-channel attacks. In addition, the security level of the crossover RO PUF can be improved by increasing the number of ROs and inverters in each RO. Furthermore, the generated response can be XORed with the challenge and the result is used as the configuration of the next challenge.

4.2 Security analysis of the inlayer authentication

In the inlayer authentication scheme, after the sensor node initiates an authentication request, the sink node should request the selection and challenge signals that are used for authentication and the response signal for comparison to the cloud. The cloud is considered as a TTP throughout the authentication process. It stores the selection signal of the sensor node and the mapping relationship of challenges and responses. For each sink node, only the selection, the challenge, and the corresponding response output are required, and the mapping relation with other nodes should not be stored. However, to unify the storage forms, the cloud still stores the mapping relations. The responses generated by these additional mappings can be used for intermediate values between the sensor nodes to verify the shared-key.

When accessing data from the cloud, the sink node should provide its own ID and sensor ID. We assume that the process of requesting access to data is secure and an attacker has the following capabilities.

(1) The attacker is capable of intercepting the information during the communication between the nodes; examples of such information include the data returned by the cloud to the sink node, and the data exchanged between the sink node and the sensor node.

(2) The attacker model is based on the intercepted information. For instance, it can build a corresponding mapping model based on the challenge-response information.

(3) An attacker can imitate the ID of a sink node or sensor node, and launch common attacks, such as denial of service attack and middleman attack.

In the inlayer scheme, there are two main information interactions. The first one is between the cloud and the sink node, whereby the cloud returns the challenge-

response information to the sink node. The second one is the information interaction process between the sink node and the sensor node. According to the above assumption, data in the two information interactions are likely to be intercepted.

The proposed authentication scheme is capable of preventing the above attacks effectively. The main reasons are as follows.

(1) In the above attack scenario, the challenge intercepted by the malicious attacker is the signal that has been generated by the true value and the response signal being XORed, instead of the true challenge information that can directly act on the RO PUF in the sensor node. After the sensor node initiates the request, the trusted sink node still has no response, because the sink node does not get the challenge-response signal from the cloud on time, and it is yet in a waiting state. Then, if the attacker directly sends the obtained challenge-response signal and the Trust to the crossover RO PUF, which is embedded in sensor nodes, the obtained output response would be found to be inconsistent with the received response signal. The sensor node believes that the sink node is not trusted and will voluntarily give up this authentication. Thus, it is infeasible for an attacker to defraud the trust of the sensor node by simply obtaining cloud data.

(2) If a malicious attacker compromises the sensor node by consuming its resources and introduces unfriendly sensor nodes to the network after exhausting the resources, the attacker can employ these sensor nodes to deliver malicious parameters or provide wrong treatment to patients, thereby leading to serious consequences. Accordingly, in the scheme design, when the sensor node does not receive the response of the sink node for three consecutive authentication requests, the sensor node will send an ATK$=1$ field to the sink node. This field indicates the network is abnormal or has been maliciously attacked. The sink node will check the network status. If the network status is abnormal, ACK$=1$ is sent to the sensor node, indicating that a malicious attack occurs. Subsequently, the sensor node will no longer initiate an authentication request, and the data collection will be suspended. When the sink node sends a signal to the outer layer server via the network, the data collected by the node is revealed to be temporarily not trusted. Thus, it is unpractical for an attacker to compromise the sensor node by exhausting the sensor node resources.

The above discussion illustrates that the proposed inlayer authentication scheme can implement mutual authentication between the sink node and the sensor node. Even if an attacker intercepts crucial authentication information, the scheme can ensure that the sensor node is not compromised. The data required in the authentication process are not directly transmitted in the form of plain text. Even if the attacker acquires the information, acquiring the corresponding plain text takes a long time. The flexibility of the crossover RO PUF configuration makes the modeling attack for the PUF more difficult and ensures the security of the inlayer authentication.

4.3 Security analysis of authentication between sensor nodes

The outer sensor node selects the similar node close to itself to transmit the data. The multi-hop makes it possible that the next hop node is not the inlayer node. Besides, it possibly remains an outer node. In the case of only two hops, if the inlayer node is deemed trustworthy by the sink node, it is necessary for outer sensor node to be authenticated by the inlayer node.

The mapping relation among the challenges of the adjacent nodes is not stored inside the sensor node. Accordingly, the attacker cannot directly obtain the challenge-response signal from the sensor node. In our authentication scheme, the selection signal S and the challenge C of the node that initiated the authentication are encrypted by the shared-key between the node that initiated the authentication and the sink node. Although the attacker has derived the message, the attacker cannot extract the selection signal and the challenge from the message without K_{AS}. Moreover, K_{AS} can be encrypted by the bijective function during the transmission process. It is virtually unlikely for attackers to derive it. Thus, the attacker cannot obtain the challenge and the selection signal by intercepting the transmitted data.

In the proposed authentication scheme, the authenticator derives the required data by decrypting, and then sends the rest of the data to the initiator, and selects a value of MidNum. Afterward, the MidNum is transmitted to the initiator through the bijective function encryption. After the initiator decrypts, this value will be XORed with the response generated by itself to get the Result. The Result should also be encrypted by the bijective function and sent to the authenticator. After receiving the message, the authenticator will XOR the Result and its own Response. Subsequently, it compares whether the value of the MidNum is the

same as the result of the XOR, and it finally completes the authentication. Even if the attacker intercepts the encrypted MidNum value and the Result sent to the authenticator, the value generated by XOR will not be the shared-key.

Suppose that the attacker derives the data passed between the nodes during the authentication process. In this case, if the data sent each time complies with a certain rule, the attacker is likely to discover this rule and forge the identity of the node to send the same data to gain trust. However, this problem can be effectively solved duce to the randomness of the MidNum value.

If the attacker can derive the encrypted MidNum from the authenticator and the data generated by the true value of MidNum and Response, the shared-key between the two sensor nodes cannot still be obtained. The shared-key can be obtained only when the MidNum value and the information sent to the authenticator are simultaneously acquired. In the authentication scheme, the initiator verifies whether the authenticator is trusted by comparing the random number Rand_A, and the authenticator authenticates the sensor node by comparing the MidNum. Accordingly, the outer authentication scheme implements mutual authentication between sensor nodes. Furthermore, it is necessary to control the frequency of consecutive authentications of the sensor nodes rigorously. If more than three authentication failures occur, it is necessary to confirm whether the network has been attacked. The authentication frequency counter can be set to implement this function.

In summary, the outer layer authentication ensures the lightweight and secure mutual authentication of sensor nodes.

5 Experiment

Two major experiments were performed to evaluate the effectiveness of the proposed authentication mechanism. First, the crossover RO PUF was implemented on the zynq7000, and its uniqueness and stability were evaluated. Second, the network topology was implemented in OMNET++ to make the communication among nodes more random, and in this process, the relevant parameters were counted. The experimental results revealed that after the authentication interval was set in the tree multi-hop network, the conflict rate was lower, the data packets received per unit time increased in amount, and the channel usage rate became more stable.

5.1 Performance evaluation of crossover RO PUF

5.1.1 Uniqueness

Uniqueness is used to evaluate the PUF quality[21]. During the experiment, the frequency of each RO link in the data was considered as the frequency of an inverter because the delay of a single inverter cannot be accurately obtained. According to the dataset, 100 pairs of a 256-bit response output were tested. The ambient temperature was 25℃, and the voltage was 1.2 V. The result showed that the average Hamming distance between any two pairs was very close to 50% (ideal value). The response outputs at different temperatures and voltages were yielded separately, and one of the variables was set to a fixed value. The average Hamming Distances (HDs) of the response produced on five FPGAs at different temperatures with a constant voltage of 1.2 V are listed in Table 1.

Table 2 shows the average Hamming distance of the response outputs in different FPGA development boards with a constant outside temperature of 25℃.

Figure 6 illustrates the frequency distribution of the average Hamming distance of the crossover RO PUF.

Table 1 Average HD of five FPGAs outputs at U = 1.2 V.

Mode	25℃	35℃	45℃	55℃	65℃
Crossover RO[7]	0.489	0.490	0.491	0.492	0.491
RO PUF[29]	0.467	0.168	0.467	0.462	0.462
Neighborhood	0.466	0.465	0.464	0.463	0.460

Table 2 Average HD of five boards outputs at T = 25℃.

Mode	0.96 V	1.08 V	1.20 V	1.32 V	1.44 V
Neighborhood	0.500	0.491	0.490	0.499	0.491
RO PUF[29]	0.450	0.454	0.465	0.471	0.470
Crossover RO[7]	0.457	0.461	0.466	0.473	0.472

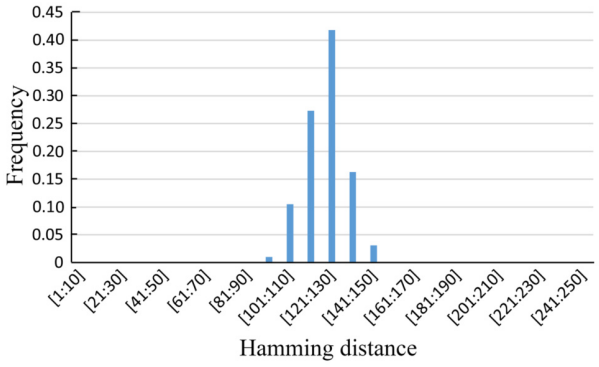


Fig. 6 Frequency distribution of the average HD of the crossover RO PUF.

Tables 1 and 2 and Fig. 6 indicate that the crossover RO PUF had good uniqueness. Thus, it is basically impossible for two PUFs to produce the same response.

5.1.2 Reliability

Reliability is another metric to evaluate the PUF quality. For a PUF, the response with the same challenge should be always identical in repeated experiments. However, the external environmental factors (e.g., temperature and supply voltage) may change the delay of the circuit and cause the PUF output to be unstable.

Temperature and voltage are critical factors affecting the delay of the PUF circuit. Therefore, for the 256-bit PUF on each board, the hamming distances between responses under different temperatures and voltages are calculated. Firstly, we conduct the experiments when the voltage is 1.2 V and the temperatures are 25℃, 35℃, 45℃, 55℃, and 65℃, respectively. Secondly, we conduct the experiments when the temperature is 25℃ and the voltages are 0.96 V, 1.08 V, 1.20 V, 1.32 V, and 1.4 V, respectively. According to the results of two experiments, 90% of hamming distances is less than 10, and no hamming distance is larger than 20.

5.2 Construction of network topology

Network simulators NS2, OPNET, and OMNET++ are three major types of wireless sensor network simulation software. NS2 is primarily used for discrete time research, OPNET refers to a commercial communication network simulation platform, and OMNET++ is a popular discrete event simulation platform in science and industry. In addition, OMNET++ has a powerful graphical interface and node definition capabilities. Hence, it was employed as the experimental platform in this study.

In the OMNET++ network topology description NED files, *outerSensorNode.ned*, *SensorNode.ned*, and *SinkNode.ned* are defined, representing the outer sensor node, the inner sensor node, and the sink node, respectively. *WBAN.ned* is defined as the description file of the entire network. The parameter configuration is shown in Table 3.

Table 3 Simulation environment parameters.

Parameter	Corresponding value
Number of nodes	3–12
Simulation duration	300 s
Data length	512 bit
Transmission rate	9.6 kbps
Transmission delay	10 ms
Signal channel	Wireless channel

After configuring the above parameters, the .cc file will get the corresponding parameter information from the nodes according to the parameters defined in .h for loading and processing operations.

We establish the network to exclusively contain the sensor nodes through the configuration file. Figure 7 shows the data conflicts at the sink node within the simulation time of 300 s in a network of 10 nodes.

Figure 8 is the data conflicts at the sink node in a network of five nodes within the simulation time of 300 s. In the figure, the state of the channel is represented by three values of 0, 1, and 2. The value 2 reflects the conflict state. The comparison of the legend reveals that when there are 10 nodes, the number of channel collisions at the sink node is significantly more than that when they are only five sensor nodes. Since the sensor nodes and the sink nodes randomly communicate, the number of sensor nodes directly affects the probability of conflicts at the sink nodes. If the signals are directly retransmitted without waiting for a period, the communication time will be longer, and considerable re-transmission data will also increase the overhead of energy consumption. Accordingly, for the body area network, direct communication between all nodes and the sink node results in greater energy consumption.

Without setting the authentication waiting time, we continuously increased the number of sensor nodes by

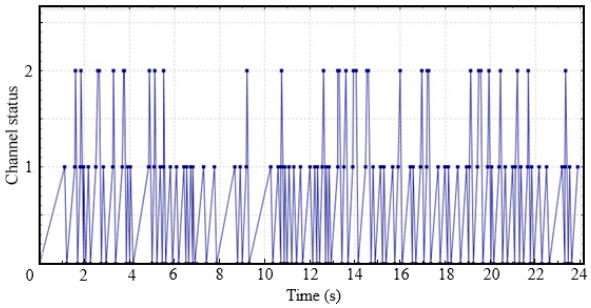


Fig. 7 Channel state of 10 sink nodes in 300 s.

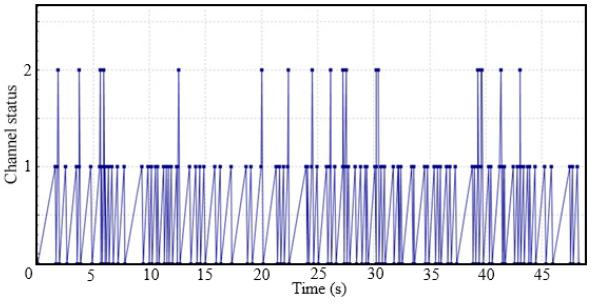


Fig. 8 Channel state of 5 sink nodes in 300 s.

setting variables in the NED file. It was found that when the number of nodes is 13, continuous conflict will occur after a period, as shown in Fig. 9. To detect whether that is an exception, the number of nodes was increased to more than 13. Experimental results show that the continuous conflict will occur after communication for a period. The main reason is that when two transmission points are set to transmit data to the channel at the same time, a conflict is triggered; thus, with the increase of nodes, the conflict frequency increases. Increasing the number of nodes to a certain extent may cause the sink node to be in a conflict state all the time.

In this experiment, the waiting time for the node to resend the authentication request after the collision is set to 100 ms, and the number of inner sensor nodes, i.e., the number of interactions between the sensor node and the sink node, was reduced. The number of received data packets, channel utilization, and packet loss rate were compared in the two network topologies.

Figure 10 demonstrates that in the case where only the number of inlayer nodes was changed without setting the retransmission time interval, the packet loss rate was high; if the number of inlayer nodes was reduced, and the retransmission time of the post-conflict data packet was set, the package loss rate would drop significantly.

With the increase of nodes, conflicts will increase during data transmission, and the number of packets received by the sink node per unit time will decrease. As shown in Fig. 11, the average values of packets received by the sink node per unit time between two different

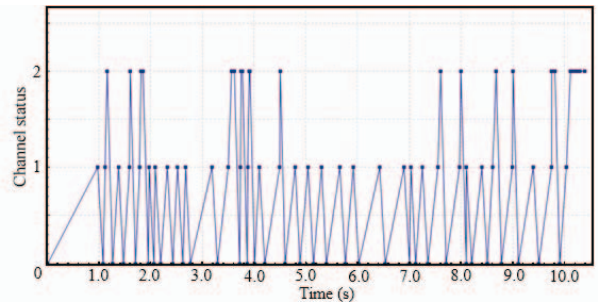


Fig. 9 Consecutive conflict.

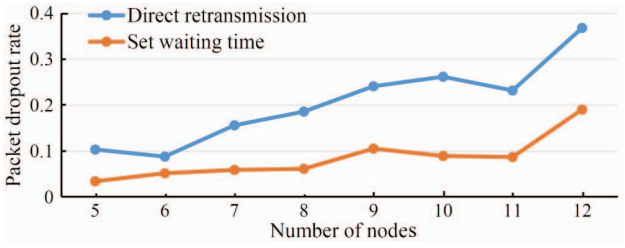


Fig. 10 Comparison of data packet dropout rate.

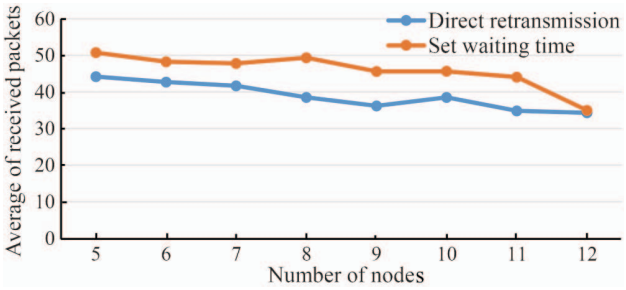


Fig. 11 Average number of received packets by the sink node per unit time.

network configurations are compared. As described above, the direct retransmission means that the sensor node retransmits the last sent message immediately after receiving the conflict message returned by the sink node. The waiting time we set was the same as that of the previous experiment to ensure fairness.

Figure 11 demonstrates that with the increase of nodes in the network topology, the number of packets received by the sink node gradually decreased. The average number of packets received by the sink node was higher than the previous one when the retransmission waiting time was set and the topology was changed.

Figure 12 shows the comparison of channel utilization in two different scenarios. It can be seen that with the increase of nodes, the channel utilization at the sink node grows stably after the waiting time was set and the topology was changed. However, the channel utilization in the direct retransmission scenario fluctuated significantly. This indicates that the network becomes more stable after a waiting time was set and outer nodes were added.

6 Conclusion

Authentication is especially important for network security[31,32]. In this paper, a PUF-based and cloud-assisted lightweight authentication mechanism is proposed for multi-hop body area network. In the tree multi-hop network, the crossover RO PUF is pre-embedded in the sensor node, and sufficient CRPs of the

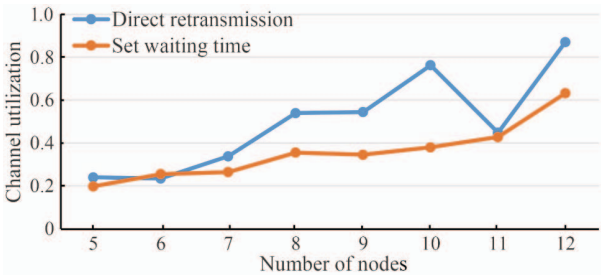


Fig. 12 Comparison of channel utilization rate.

inner node are stored in the cloud, thereby reducing the storage overhead on the nodes in the body area network. Experimental results show that after the authentication interval was set in the tree multi-hop network, the conflict rate was lower, the data packets received per unit time increased in amount, and the channel usage rate became more stable. Therefore, the lightweight authentication scheme is more suitable for multi-hop topology networks.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Nos. 61874042 and 61602107), the Key Research and Development Program of Hunan Province (No. 2019GK2082), the Hu-Xiang Youth Talent Program (No. 2018RS3041), the Peng Cheng Laboratory Project of Guangdong Province (No. PCL2018KP004), the Fundamental Research Funds for the Central Universities, and the Program for Lianning Innovative Research. We would like to thank Mr. Lele Liu's contributions to the experiments of this paper.

References

[1] Y. Ding, X. Yu, J. Zhang, and X. Xu, Application of linear predictive coding and data fusion process for target tracking by Doppler through-wall radar, *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 3, pp. 1244–1254, 2019.

[2] X. Lin, Y. Ding, X. Xu, and Y. Sun, A multi-target detection algorithm using high-order differential equation, *IEEE Sensors Journal*, vol. 19, no. 13, pp. 5062–5069, 2019.

[3] S. Zhang, Y. Lin, Q. Liu, J. Jiang, B. Yin, and K.-K. R. Choo, Secure hitch in location-based social networks, *Computer Communications*, vol. 100, pp. 65–77, 2017.

[4] S. Zhang, X. Li, H. Liu, Y. Lin, and A. K. Sangaiah, A privacy-preserving friend recommendation scheme in online social networks, *Sustainable Cities and Society*, vol. 38, pp. 275–285, 2018.

[5] M. Kumar, Security issues and privacy concerns in the implementation of wireless body area network, in *Proceedings of International Conference on Information Technology*, Singapore, 2015, pp. 58–62.

[6] M. Kumar and P. Samundiswary, Wireless body area network security issues-survey, in *Proceedings of International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, Kuala Lumpur, Malaysia, 2016, pp. 190–194.

[7] Z. Pang, J. Zhang, Z. Qiang, S. Gong, and B. Tang, Crossover ring oscillator PUF, in *Proceedings of International Symposium on Quality Electronic Design*, Santa Clara, CA, USA, 2017, pp. 237–243.

[8] J. Zhang and G. Qu, Physical unclonable function-based key sharing via machine leaning for IoT security, *IEEE Transactions on Industrial Electronics*, DOI:10.1109/TIE.2019.2938462.

[9] K. Pardeep and L. Hoon-Jae, Security issues in healthcare applications using wireless medical sensor networks: A survey, *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[10] C. Karlof, N. Sastry, and D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, in *Proceedings of International Conference on Embedded Networked Sensor Systems*, Hangzhou, China, 2004, p. 162.

[11] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, The tesla broadcast authentication protocol, *CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.

[12] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, MiniSec: A secure sensor network communication architecture, in *Proceedings of International Symposium on Information Processing in Sensor Networks*, Berkeley, CA, USA, 2007, pp. 479–488.

[13] S. M. Almheiri and H. S. Alqamzi, Data link layer security protocols in wireless sensor networks: A survey, in *Proceedings of IEEE International Conference on Networking*, Xi'an, China, 2013, pp. 312–317.

[14] P. Chuchaisri and R. Newman, Fast response PKC-based broadcast authentication in wireless sensor networks, *Mobile Networks and Applications*, vol. 17, no. 4, pp. 508–525, 2012.

[15] N. Zhao, A. Ren, F. Hu, Z. Zhang, M. U. Rehman, T. Zhu, X. Yang, and A. Alomainy, Double threshold authentication using body area radio channel characteristics, *IEEE Communications Letters*, vol. 20, no. 10, pp. 2099–2102, 2016.

[16] L. Ma, G. Yu, and Y. Zhu, TinyZKP: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks, *Wireless Personal Communications*, vol. 77, no. 2, pp. 1077–1090, 2014.

[17] Y. Liu, D. Liu, and G. Yue, A body gauss-markov-based mobility model for body area networks, *Tsinghua Science and Technology*, vol. 23, no. 3, pp. 277–287, 2018.

[18] M. H. Salama, S. Taha, and H. N. Elmahdy, PMAS: A proposed mutual authentication scheme for wireless body area networks, in *Proceedings of International Conference on Information and Communication Technology Convergence*, Jeju Island, Korea, 2015, pp. 636–641.

[19] J. Yuan, S. Lu, S. Yu, and L. Ming, Authenticated secret key extraction using channel characteristics for body area networks, in *Proceedings of ACM Conference on Computer and Communications Security*, Toronto, Canada, 2012, p. 1028.

[20] J. Zhang and G. Qu, Recent attacks and defenses on FPGA-based systems, *ACM Transactions on Reconfigurable Technology and Systems*, DOI: 10.1145/3340557.

[21] J. Zhang, G. Qu, Y. Q. Lv, and Q. Zhou, A survey on silicon PUFs and recent advances in ring oscillator PUFs, *Journal of Computer Science and Technology*, vol. 29, no. 4, pp. 664–678, 2014.

[22] J. Zhang, X. Tan, Y. Zhang, W. Wang, and Z. Qin, Frequency offset-based ring oscillator physical unclonable function, *IEEE Transactions on Multi-Scale Computing Systems*, vol. 4, no. 4, pp. 711–721, 2018.

[23] Q. Guo, J. Ye, Y. Gong, Y. Hu, and X. Li, PUF based

pay-per-device scheme for IP protection of CNN model, in *Proceedings of IEEE 27th Asian Test Symposium (ATS)*, Hefei, China, 2018, pp. 115–120.

[24] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, Transparent two-factor authentication, *IEEE Access*, vol. 6, pp. 32 677–32 686, 2015.

[25] J. Zhang, A practical logic obfuscation technique for hardware security, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 3, pp. 1193–1197, 2016.

[26] J. Zhang, Y. Lin, Y. Lyu, and Q. Gang, A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing, *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 6, pp. 1137–1150, 2017.

[27] J. Zhang, Y. Lin, and Q. Gang, Reconfigurable binding against FPGA replay attacks, *ACM Transactions on Design Automation of Electronic Systems*, vol. 20, no. 2, pp. 1–20, 2015.

[28] J. Zhang, B. Qi, and Q. Gang, HCIC: Hardware-assisted control-flow integrity checking, *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 458–471, 2019.

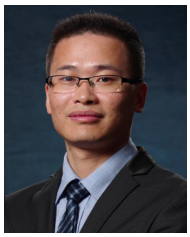
[29] G. Suh and S. Devadas, Physical unclonable functions for device authentication and secret key generation, in *Proceedings of 44th ACM/IEEE Des. Autom. Conf.*, San Diego, CA, USA, 2007, pp. 9–14.

[30] D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf, and G. Sigl, Localized electromagnetic analysis of RO PUFS, in *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust*, Austin, TX, USA, 2013, pp. 19–24.

[31] K. Fan, H. Li, W. Jiang, C. Xiao, and Y. Yang, Secure authentication protocol for mobile payment, *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 610–620, 2018.

[32] J. Liu, Y. Yu, J. Jia, S. Wang, P. Fan, H. Wang, and H. Zhang, Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular ad-hoc networks, *Tsinghua Science and Technology*, vol. 24, no. 5, pp. 575–584, 2019.

Xiao Tan received the MS degree from Hunan University, Changsha, China, in 2012. He is currently a PhD candidate in Hunan University. Her current research interests include hardware security and internet of things.



Jiliang Zhang received the PhD degree from Hunan University, Changsha, China, in 2015. From 2013 to 2014, he worked as a research scholar at the Maryland Embedded Systems and Hardware Security Lab, University of Maryland, College Park. From 2015 to 2017, he was an associate professor with Northeastern University, China. Since 2017, he has joined Hunan University. His current research interests include hardware/hardware-assisted security, artificial intelligence security, and emerging technologies.

Prof. Zhang is a recipient of the Hu-Xiang Youth Talent, and the best paper nominations in International Symposium on Quality Electronic Design 2017. He has been serving on the technical program committees of many international conferences, such as ASP-DAC, FPT, GLSVLSI, ISQED, and AsianHOST. He is a senior member of IEEE and a guest editor of the *Journal of Information Security and Applications* and *Journal of Low Power Electronics and Applications*.

Yuanjing Zhang is a visiting master student at Hunan University, China. She received the BS degree from Northeastern University in 2019. She is currently a master student in Beihang University. Her main current research interest is hardware security.

Zheng Qin received the PhD degree from Chongqing University, Chongqing, China, in 2001. He is currently a professor in the College of Computer Science and Electronic Engineering, Hunan University. His current research interests include network and data security, data analytics and applications, machine learning, and applied cryptography.

Yong Ding received the PhD degree from the School of Communication Engineering, Xidian University, China, in 2005. He is currently a professor at the School of Computer Science and Information Security, Guilin University of Electronic Technology, China. He was a research fellow of Computer Science at City University of Hong Kong from April 2008 to September 2009. His research interests include cryptography and information security.

Xingwei Wang received the PhD degree from the Northeastern University, Shenyang, China, in 1998. He is currently a professor at the College of Computer Science and Engineering, Northeastern University. His research interests include future internet and cloud computing.