Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8865158, 15 pages
https://doi.org/10.1155/2022/8865158

Research Article

PUF-Assisted Lightweight Group Authentication and Key Agreement Protocol in Smart Home

Yandong Xia,[1,2] Rongxin Qi,[1,2] Sai Ji,[1,2] Jian Shen,[1,2,3] Tiantian Miao,[1,2] and Huaqun Wang[4]

[1]*Nanjing University of Information Science and Technology, Nanjing, China*
[2]*Jiangsu Engineering Center of Network Monitoring, Nanjing, China*
[3]*Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen, China*
[4]*Jiangsu Key Laboratory of Big Data Security and Intelligent Processing, Nanjing University of Posts and Telecommunications, China*

Correspondence should be addressed to Jian Shen; s_shenjian@126.com

Received 11 August 2020; Revised 18 January 2021; Accepted 25 February 2022; Published 24 March 2022

Academic Editor: Yin Zhang

Various IoT-based applications such as smart home, intelligent medical, and VANETs have been put into practical utilization. The smart home is one of the most concerned environments, allowing users to access and control smart devices via the public network remotely. The smart home can provide many intelligent services for users through these smart devices. To securely access devices and obtain collected data over the public network, multifactor authentication protocols for smart home have gained wide attention. However, most of these protocols cannot withstand impersonation attack, smart device lost attack, privileged-insider attack, smart card lost attack, and so on. Besides, high communication and computational costs weaken the system performance, which leads to most authentication protocols are not suitable for resource-constrained smart devices. To mitigate the aforementioned drawbacks, we proposed a PUF-assisted lightweight group authentication and key agreement protocol to implement secure access to multiple devices in the smart home simultaneously using the Chinese Remainder Theorem and secret sharing technique. Our protocol also utilizes physical unclonable function (PUF) and fuzzy extractor technique to extract the digital fingerprint of the smart devices, which can uniquely validate smart devices and protect the secrets stored in their memory. Our protocol can support various security features and withstand the many well-known attacks in the smart home. The performance analysis indicates that the proposed protocol can efficiently reduce communication/computational costs when the user simultaneously accesses multiple devices.

1. Introduction

With the rapid development of the Internet of Things (IoT) technology, various IoT-based applications such as smart home, intelligent medical, and VANETs have emerged. In these applications, the smart home has gained wide attention in recent years due to its convenience, efficiency, and other properties, providing basic and practical home control services for users. The smart home is a dwelling that connects major appliances and services and permits them to be accessed via the public network [1]. In most existing schemes, the smart home is usually composed of user equipment (e.g., smartphone), home gateway (HG), and lots of smart devices (e.g., surveillance camera, lighting controller, and temperature sensors) [2]. The smart devices are interconnected to collect the data in the smart home and interact with users via the public network. HG acts as the communication medium between the user and smart devices.

Smart devices are generally easy to suffer from various attacks such as impersonation attack, physical device lost attack, and privileged-insider attack during the execution of the protocol. Once these devices are broken, user privacy will be compromised. For example, unauthorized users may access the surveillance cameras and control

them to monitor smart home residents. In addition, most of these IoT devices such as sensors have limited resources to execute complex computational operations [3, 4]. In recent years, many Elliptic Curve Cryptography- (ECC-) based schemes [5, 6] have been proposed to enhance authentication security. However, these schemes generally require to perform complex computational operations, which are not suitable for resource-constrained devices. Some schemes also cannot provide most security features and functionalities such as user anonymity, perfect forward secrecy, and dynamic device addition. To solve the security and privacy issues in IoT environments, a large number of authentication schemes have been proposed [7–9]. In most of the existing schemes, the computational and communication costs are too high to be suitable for resource-constrained [8] devices. If the user wants to access multiple smart devices simultaneously, it is necessary to verify the authenticity of user identity frequently and send access requests to correspond with smart devices in a short time, which may lead to network delay and even congestion. Therefore, it is crucial to design an efficient and lightweight authentication scheme to establish the secure session key between the user and smart devices in the smart home. Group authentication schemes are put forward to solve aforementioned issues. Group authentication schemes based on secret sharing can authenticate multiple smart devices belonging to the same group simultaneously.

Besides, the traditional read-only memory- (ROM-) based authentication techniques have the characteristic of expensive power consumption and nonvolatile memory, which are vulnerable to external attacks [10]. Physical unclonable function is a promising hardware primitive that can be utilized for lightweight authentication and secret key storage, which extracts the unique physical property from the integrated circuits (IC) [11]. Each IC has different physical characteristics even if they are identical in function. The secrets derived from IC through PUF are actually different due to the variability in manufacturing. PUF can handle the inherent weaknesses successfully existing in the traditional ROM-based authentication techniques. PUF technique can be utilized to distinguish the smart devices and prevent them from being attacked, cloned, and forged by the adversary. However, changes in the environment around smart devices may affect the digital circuit, which leads to errors in the output of the PUF function. In order to improve the fault tolerance rate of the PUF function, the fuzzy extractor has been widely used to correct errors in the PUF function [12].

Considering the security of the parameters stored in the smart devices, PUF is utilized to prevent stolen device attack. PUF can be utilized to assist smart devices to generate a biometric key, which efficiently protects the security smart devices [12]. Therefore, we propose a PUF-assisted lightweight group authentication and key agreement protocol in the smart home. Our protocol supports many well-known features such as untraceability, user anonymity, and forward secrecy. The smart devices are allowed to join or leave the group dynamically.

1.1. Our Contributions

(i) A PUF-assisted lightweight group authentication and key agreement protocol in the smart home is presented in our paper. Our protocol is suitable for the resource-constrained smart devices only using lightweight operation and symmetric cryptography. The secret sharing technique and Chinese Remainder Theorem are utilized to establish the group session key between the user and smart devices

(ii) The security of our protocol is proved under the widespread ROR model [13]. The formal security analysis shows that our protocol is semantically secure. Other discussions on security show that the proposed protocol can guarantee many security features such as untraceability and user anonymity and also can withstand most known attacks

(iii) The dynamic joining and leaving of smart devices from deployed network are both supported by the proposed protocol. The illegitimate smart devices fail to attain the group key without the secret share. The new smart device just registers itself before joining the deployed network

(iv) The physical security of smart devices is guaranteed by physical unclonable function technology. The output of PUF depends on the physical fingerprint of the physical device. PUF has the characteristics of tamper-resistant, unclonability, and unpredictability

(v) The issue of repeated authentication of the same user who accesses the multiple smart devices simultaneously is solved. The performance analysis indicates that the protocol effectively reduces resource costs compared with other protocols

1.2. Related Work

1.2.1. Authentication. Smart home allows the authorized users to remotely access devices and obtain information collected by these devices. To address security and privacy issues in IoT, a large number of researchers [14–16] have studied many authentication schemes for the smart home.

In 2011, Vaidya et al. proposed a novel authentication and key establishment mechanism based on ECC. Although their scheme satisfies more security requirements compared to previous schemes, their scheme is not suitable for resource-constrained home area networks. Therefore, many schemes focus on providing more security features while they are not suitable for resource-constrained devices. To solve communication security issues in WSNs, Xue et al. [14] utilized temporary credentials to implement authentication between the user and sensing nodes for WSNs in 2013. Their scheme is lightweight to be suitable for the sensing nodes using hash function and bit-wise XOR operations. However, He et al. [15] thought their scheme fails to resist offline password guessing attack, impersonation attack, and

tampering attack. In 2013, He et al. [17] proposed an improved authentication scheme that overcomes the security threats in Xue's scheme and only increases little computational cost. In 2014, Turkanovic et al. [17] focused on a scenario where the user accessing a single targeted sensor in WSNs does not need to interact with HG. Meanwhile, Kalra and Sood [18] found that Xue's scheme is vulnerable to smartcard lost attack. Kalra and Sood [18] proposed a novel authentication scheme based on password and smartcard, which can resist most known attacks and has a lower cost than other schemes. However, their scheme does not consider resisting sensing node capturing attack and privileged-insider attack. In 2018, Shen et al. [19] adopted the cloud to enhance the capabilities of devices and established a lightweight authentication scheme without certificates for WBANs.

The devices in the IoT environment have similar features to the sensing nodes in traditional WSNs. Due to the heterogeneity and dynamics of IoT devices, the higher security and privacy requirements need to be satisfied in the IoT environment. Kumar et al. [16] proposed an anonymous authentication framework for smart home only using hash function and symmetric cryptography. Kumar et al. firstly considered the features of anonymity and unlinkability for smart home, and their scheme can resist many known attacks. Challa et al. [20] proposed a novel signature-based authenticated key establishment scheme for the generic IoT environment. The user can not only communicate with smart devices but also with other users through HG. In 2018, Srinivas et al. [21] proposed an anonymous three-factor authentication and key agreement scheme which supports credentials update, user revocation, and new devices addition. However, Gope et al. [22] thought the sensitive information stored in the memory of smart devices may be compromised to the adversary by the side-channel attack. The adversary then obtains the sensitive information and traces all the access users in previous communications. Besides, most smart devices are not tamper-evident so that the adversary can intercept the communication messages and impersonate legitimate devices.

1.2.2. Group Authentication. The concept of group authentication is proposed to implement identity authentication among group members at a time. Many group-based authentication schemes are also proposed to improve the efficiency of group communication. In 2013, Harn [23] and Liu et al. [24] both proposed an improved group authentication protocol for group-oriented applications based on secret sharing. In 2016, Li et al. [25] thought that Harn's protocol fails to support key agreement during the authentication process and cannot resist replay attack and man-in-middle attack. They proposed an improved group authentication and key agreement protocol for MTC in LTE-A networks, which supports dynamical policy updating and provides strong security properties compared to previous work. In 2019, Cui et al. [26] proposed an efficient signature-based group authentication scheme for vehicular ad hoc networks (VANETs). RSU can efficiently update the group key generated by two hash chains to exclude malicious vehicles from the group. In 2020, Zhang and Lee [27] provided an efficient group authentication scheme based on the group signature technique, which protects the integrity of blockchain-based mobile-edge computing (BMEC). In this paper, we propose a secure and efficient group authentication protocol for smart home based on the PUF and secret sharing technique. Currently, most of these protocols cannot withstand smart device lost attack and smart card lost attack. Besides, high communication and computational cost leads to most authentication protocols are not suitable for resource-constrained smart devices.

1.2.3. PUF Technology. Recently, PUF technology is introduced to resist the aforesaid issues. Most existing authentication protocols are designed based on tamper-evident PUF [28–35] to prevent the physical attack. Wallrabenstein [28] proposed an ideal PUF-based authentication protocol to provide cost-effective tamper resistance for resource-constrained devices in IoT, which minimizes the probability of private key disclosure. To resist denial and masquerading attacks, Chatterjee et al. [31] used PUF's response to replace the public identity string used for message encryption and disabled the public key generator in the scheme, allowing the receiving node to generate its own public and private keys and the server to verify the public key. In order to solve the problems of man-in-the middle attack and replay attack under DY security model, Braeken [32] used elliptic curve addition and multiplication to replace bilinear pair operation and realized identity-based authentication. Chatterjee et al. [33] combined IBE, PUF, and message authentication code to propose a low-power, low-latency authentication, and key agreement protocol that solves the database storage overhead and successfully defies man-in-the-middle attacks. Gope et al. [29] proposed a lightweight anonymous authentication protocol based on ideal PUF. They subsequently took the effects of noise on PUF into account and enhanced the authentication protocol to support noisy PUF. They utilized other prestored pseudo identities and challenge-response pairs to ensure the security of the protocol when suffering from DoS attacks. Furthermore, Tiplea and Hristea [30] pointed that most existing PUF-based authentication protocols cannot protect security and privacy in IoT under corruption with temporary state disclosure, while some important temporary variables are not protected by PUF. Therefore, they proposed a general method to protect the temporary variables and utilized it to fix the flaws existing in the previous PUF-based authentication protocols. Li and Liu [34] optimized the existing RFID authentication protocol based on double PUF. They proposed a protocol that can meet the untraceable, successfully resist desynchronization attacks and tag impersonation attacks, and has better security and privacy. PUF-based authentication schemes are threatened by powerful machine learning attacks. Chen et al. [35] show that the "availability" and "reliability" features of Shamir's secret sharing (SSS) can be applied to address the security issue. They presented a mutual authentication protocol where no response is exposed to the adversary and can avoid the use of cryptographic algorithms and error correcting codes. The current PUF-based

authentication protocol can resist internal attacks, but it is still affected by external environment, resulting in PUF function output errors. How to improve the fault tolerance rate is an urgent problem to be solved.

2. Preliminaries

2.1. Chinese Reminder Theorem [36]. It is assumed that there are n prime positive integers $p_1, p_2, \cdots, p_n$. Let P be the product of n prime positive integers as $P = \prod_{i=1}^{n} p_i$ and $P_i = P/p_i$, where $i = 1, 2, \cdots n$. Let P_i^{-1} be the modular multiplicative inverse of $P_i \text{mod} p_i$ and satisfy $P_i P_i^{-1} \equiv 1 (\text{mod } p_i)$. Then, let $a_i, i = 1, 2, \cdots, n.$ be any n positive integers. Equation (1) has a unique general solution mod P.

$$\begin{aligned} X &\equiv a_1 \bmod p_1 \\ X &\equiv a_2 \bmod p_2 \\ &\vdots \\ X &\equiv a_n \bmod p_n \end{aligned} . \tag{1}$$

The general solution of Equation (1) is calculated in Equation (2).

$$\begin{aligned} X &= a_1 P_1^{-1} P_1 + a_2 P_2^{-1} P_2 + \cdots + \\ &\quad a_n P_n^{-1} P_n (\text{mod } P), \\ &= \sum_{i=1}^{n} a_i P_i^{-1} P_i (\text{mod } P), \\ &= a_1 + a_2 + \cdots + a_n (\text{mod } P). \end{aligned} \tag{2}$$

2.2. Physical Unclonable Function [28]. PUF which is based on complex physical system is a function $F : C \longrightarrow R$ $(C : \{0,1\}^{\lambda_1}, R : \{0,1\}^{\lambda_2})$. The challenges and their corresponding responses are called challenge-response pairs. PUF has the following properties:

(1) *Unclonable*. For all $c \in C$, there is no function F' satisfying $F'(c) = F(c)$. The probability of duplicating function F with a cloned function F' in probabilistic polynomial time (PPT) is negligible

(2) *Computable*. It is feasible to compute $r_i = F(c_i)$ in probabilistic polynomial time for all $c_i \in C$

(3) *Unpredictable*. For all $c \in C$, the probability of the adversary $\mathscr{A}$ correctly guessing response r of the function F corresponding to challenge c in probabilistic polynomial time is negligible. The output of the function F is a random string uniformly chosen from $\{0,1\}^{\lambda_1}$

(4) *Tamper-Proofing*. For all $c, c' \in C$, even the Hamming distance between c and c' is equal to t (t is sufficiently small) or less; the probability of outputting the similar results is negligible. Therefore, PUF is able to resist tampering attacks

2.3. Fuzzy Extractor [5]. The fuzzy extractor takes a low-entropy value containing noise as inputs and outputs the same uniform random value as long as inputs values are close. The fuzzy extractor is utilized to extract the user's biometric information and the smart device's information. It is assumed that fuzzy extractor is composed of two algorithms defined in a tuple $\langle M, l, t \rangle$.

Gen(): it is a probabilistic algorithm. The user takes his/her biometrics BIO_i from the metric space M as $\text{Gen}(\text{BIO}_i) = (\sigma_i, \tau_i)$, and the algorithm outputs the biometric key $\sigma_i \in \{0,1\}^l$ and the public parameter τ_i.

Rep(): it is a deterministic algorithm. Rep takes the biometrics $\text{BIO}_i' \in M$, reproduction parameter τ_i, and t as the input (t is the fault tolerance value and sufficiently small). The algorithm Rep can reproduce the biometric key σ_i as $\text{Rep}(\text{BIO}_i', \tau_i) = \sigma_i$, where the Hamming distance between twice inputs is t or less.

3. System Model and Definitions

3.1. System Model. The authentication protocol in the smart home consists of the user U_i, home gateway (HG), smart devices SD_j, and registration center (RC). All the entities are defined as shown in Figure 1.

(i) *RC*. RC is usually considered as a trusted registration center. It mainly has two functions including registering the user, HG, and smart devices and generating parameters for smart devices securely

(ii) *HG*. It is a trusted entity and cannot be compromised by the adversary $\mathscr{A}$. It acts as the communication medium between the user and smart devices in the smart home and is responsible for reconstructing secrets for smart devices during the authentication phase

(iii) U_i. The user U_i utilizes a smartphone or other smart devices which are referred to as user equipment UE_i. The user equipment has capability to extract U_i's biometrics and verify the authenticity of U_i's identity. U_i can access smart devices after registering at the RC

(iv) SD_j. Smart devices can execute the commands and collect all kinds of information in the smart home. It is assumed that $\mathscr{A}$ may attain authentication credentials stored in the smart devices through side-channel attack [21]. PUF technique can be utilized to identify the smart device due to the inherent physical characteristic. All the smart devices have the PUF module which protects them from device capturing attack. Therefore, each smart device cannot be forged physically by the adversary

3.2. Threat Model. It is assumed that the adversary $\mathscr{A}$ in our protocol has same capabilities as the adversary in Dolev-Yao (DY) threat model [37–39]. The capabilities of $\mathscr{A}$ in our protocol are enumerated as follows:

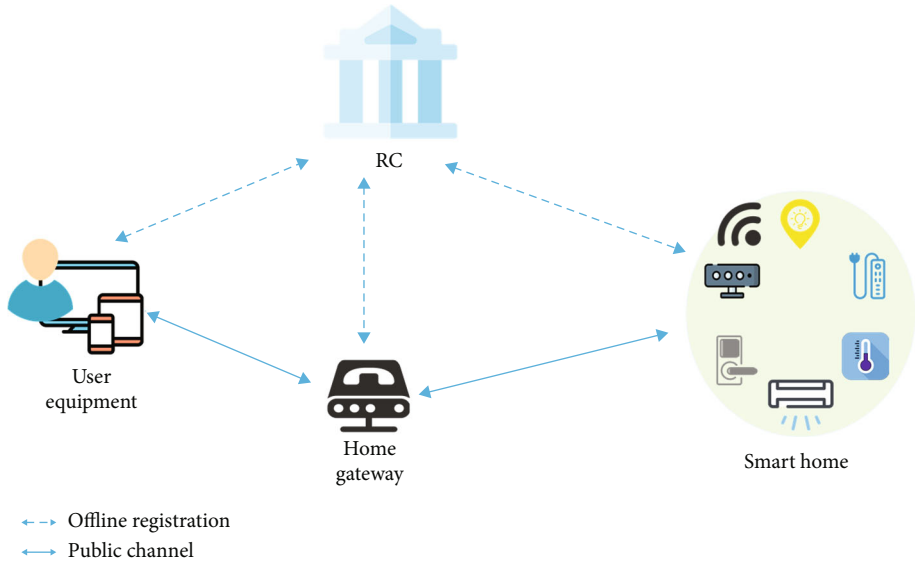

Figure 1: System model.

(i) $\mathcal{A}$ can eavesdrop, intercept, modify, inject, and delete all the messages transmitted via the public network

(ii) $\mathcal{A}$ can store or resend all the messages which are intercepted or forged

(iii) $\mathcal{A}$ can impersonate as the legitimate user or the smart device to participate in the authentication process during the execution of the protocol

(iv) $\mathcal{A}$ can obtain the credentials stored in the user equipment and launch various types of attacks on the protocol. However, the group session key cannot be compromised to the adversary during the execution of the protocol

In addition, the adversary $\mathcal{A}$ also has partial abilities in CK-adversary model proposed by Canetti and Krawczyk [40, 41]. Under the CK-adversary model, the reveal of ephemeral state information or other sensitive information has no influence on the security of sessions and long-term secrets. It is necessary to be guaranteed that the security of other sessions cannot be broken even though ephemeral secrets are compromised.

4. Our Proposed Protocol

We firstly introduce an overview of the protocol. A detailed description of the protocol is then presented in this section.

4.1. Overview of the Protocol. We propose a PUF-assisted lightweight group authentication and key agreement protocol in the smart home. The proposed protocol mainly includes four types of entities: RC, HG, user equipment, and smart devices.

In our protocol, RC plays the role of registration center. RC is responsible for registering other devices. HG acts as an intermediate device between the user equipment and smart devices and reconstructs the secret for a group of smart devices. Each user has a smartphone or terminal equipment that can read and verify a user's credential. During the login and authentication phase, the user sends the request to HG, and then, HG forwards the requests to a group of target smart devices. After a series of authentication, smart devices generate corresponding responses and send them to HG; HG encrypts the smart devices' responses and forwards them to the user. The user's shared group session key with a group of legal smart devices is securely established. Besides, the user has abilities to update personal password and biometrics locally. To resist replay attack, we assume that all the entities (i.e., users, HG, smart devices) are synchronized with the clock, and the maximum communication delay is ΔT.

The detailed notations and corresponding descriptions are summarized in Table 1.

4.2. Smart Device Registration Phase. The smart device registration is executed securely in the section. To prevent device capturing attack launched by the adversary, each smart device generates the physical fingerprint based on the physical unclonable function and fuzzy extractor to protect the credentials stored in its memory.

4.2.1. SDRP1. The smart device SD_j, $j = 1, 2, \cdots, n$. utilizes the PUF and fuzzy extractor to extract the information to register itself. The smart device SD_j firstly selects a random nonce c_j and compute $r_j = F(c_j)$. The digital circuits of the smart devices may be influenced by the changes in the external environment, which results in errors in the output of the PUF function. Therefore, the fuzzy extractor is utilized to reduce errors existing in the physical unclonable function. SD_j computes $(R_j, h_j) = \mathrm{Gen}(r_j)$ to generate secret R_j and sends R_j to RC securely.

Table 1: Notations and descriptions.

Notations	Descriptions
RC	Registration center
U_i, SD_j, and HG	i^{th} user, j^{th} smart device, and home gateway
UE_i	i^{th} user equipment
ID_i, ISD_j, and ID_{HG}	U_i's, SD_j, and HG's identity
PW_i	U_i's password
BIO_i	U_i's biometrics
Gen(·), Rep(·)	Generation and reproduction algorithm of fuzzy extractor
σ_i, R_j	U_i's biometrics key, SD_j's physical key
τ_i, x_i, h_j	Public parameters
T_i	Current timestamp
ΔT	Maximum communication delay
K_{HG}	HG's secret key
K_i	Symmetric key between U_i and HG
GSK	Group session key between the user and smart devices
s	Secret value utilized for secret sharing
s_j	SD_j's secret share
PUF	Physical unclonable function
$H(\cdot)$	One-way hash function
$\oplus$,$\|$	Concatenation and bit-wise XOR operation, respectively

4.2.2. SDRP2. When receiving the registration request from smart device SD_j, $j \in \{1, 2, \cdots, n\}$, RC chooses the identity ISD_j for each smart device and randomly selects a polynomial $f(x)$ of degree $t-1$: $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1} \bmod p$, such that all the coefficients $a_j, j \in \{1, 2, \cdots, t-1\}$., and $s = f(0)$ are in finite field GF(p). RC computes $H(s)$ and $s_j = f(x_j)$ (x_j is public system information related to the smart device SD_j). RC randomly selects a prime positive integer p_j, $j \in \{1, 2, \cdots, n\}$ corresponding to smart device SD_j. Then, RC computes $P = \prod_{j=1}^{n} p_j$, $P_j = P/p_j$, $j \in \{1, 2, \cdots, n\}$., and $\chi = \sum_{j=1}^{n} P_j P_j^{-1}$ ($P_j P_j^{-1} \equiv 1 \bmod p_j$, $\chi \bmod p_j \equiv 1$). Finally, RC calculates $RP_j = R_j \oplus p_j$, $share_j = R_j \oplus s_j$ and sends $\langle ISD_j, RP_j, share_j \rangle$ to corresponding smart device SD_j securely.

4.3. User Registration Phase. The user U_i must register himself at RC when he wants to access the smart home remotely through HG. As shown in Figure 2, the detailed registration process is executed in the following steps.

4.3.1. URP1. U_i firstly chooses an identity ID_i and high entropy password PW_i and imprints personal biometric information BIO_i using the fuzzy extractor in user equipment UE_i. UE_i adopts key generation algorithm Gen(·) to generate corresponding biometric key σ_i which acts as an element of three-factor authentication and public parameter τ_i as $Gen(BIO_i) = (\sigma_i, \tau_i)$. To protect the PW_i and σ_i, UE_i randomly generates a nonce a and takes personal credentials ID_i, PW_i, σ_i, and a as input to compute $RPW_i = H(ID_i \| PW_i \| \sigma_i) \oplus a$. Finally, UE_i securely sends request $\langle ID_i, RPW_i \rangle$ to RC.

4.3.2. URP2. When getting the request $\langle ID_i, RPW_i \rangle$ from U_i, RC firstly generates a 1024-bit long-term secret value K_{HG} and calculates $K_i = H(ID_i \| K_{HG})$, $TPW_i = K_i \oplus RPW_i$. Then, RC generates the anonymous identity TID_i corresponding to ID_i and securely sends the information $\langle TID_i, TPW_i \rangle$ to UE_i. Finally, RC deletes the information RPW_i and TPW_i from its database.

4.3.3. URP3. Upon receiving the response $\langle TID_i, TPW_i \rangle$ from RC, UE_i computes $A_i = H(PW_i \| \sigma_i \| a)$, $B_i = H(ID_i \| \sigma_i) \oplus a$, $rPW_i = TPW_i \oplus a$, $V_i = H(H(ID_i \| \sigma_i) \| A_i) \bmod \Omega$. Ω is a medium integer that defines the ability to withstand online guessing attack using "fuzzy-verifier" [42]. Then, UE_i stores $\langle TID_i, rPW_i, B_i, V_i, \tau_i, Gen(\cdot), Rep(\cdot), H(\cdot), t \rangle$ in its memory. Finally, UE_i deletes TPW_i, RPW_i, A_i from UE_i so as to prevent user equipment from compromising sensitive information.

4.4. Home Gateway Registration Phase. HG chooses an identity ID_{HG} and sends the registration request to RC. Upon receiving the request from HG, RC issues a long-term secret key K_{HG}, the user identity ID_i, corresponding temporal identity TID_i, $H(s)$, and other public parameters $h_j, x_j, j \in \{1, 2, \cdots, n\}$ to HG securely.

4.5. Login and Authentication Phase. Figure 3 gives the summary of login and authentication phase which could be divided into seven steps.

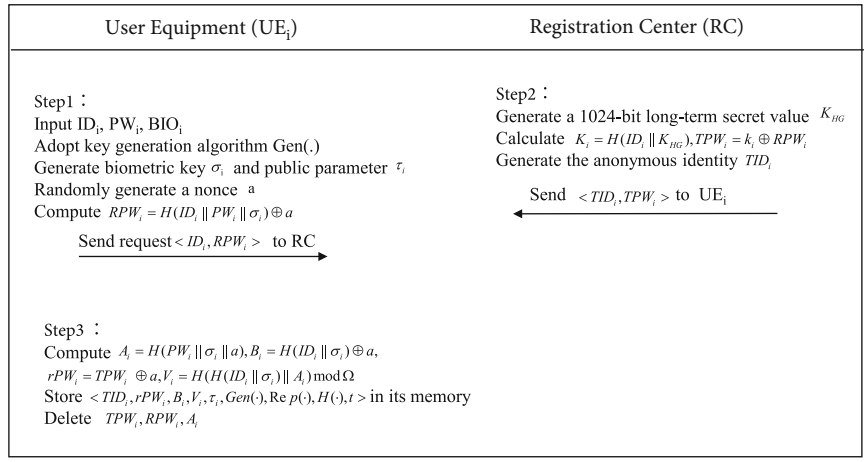

Figure 2: Summary of user registration phase.

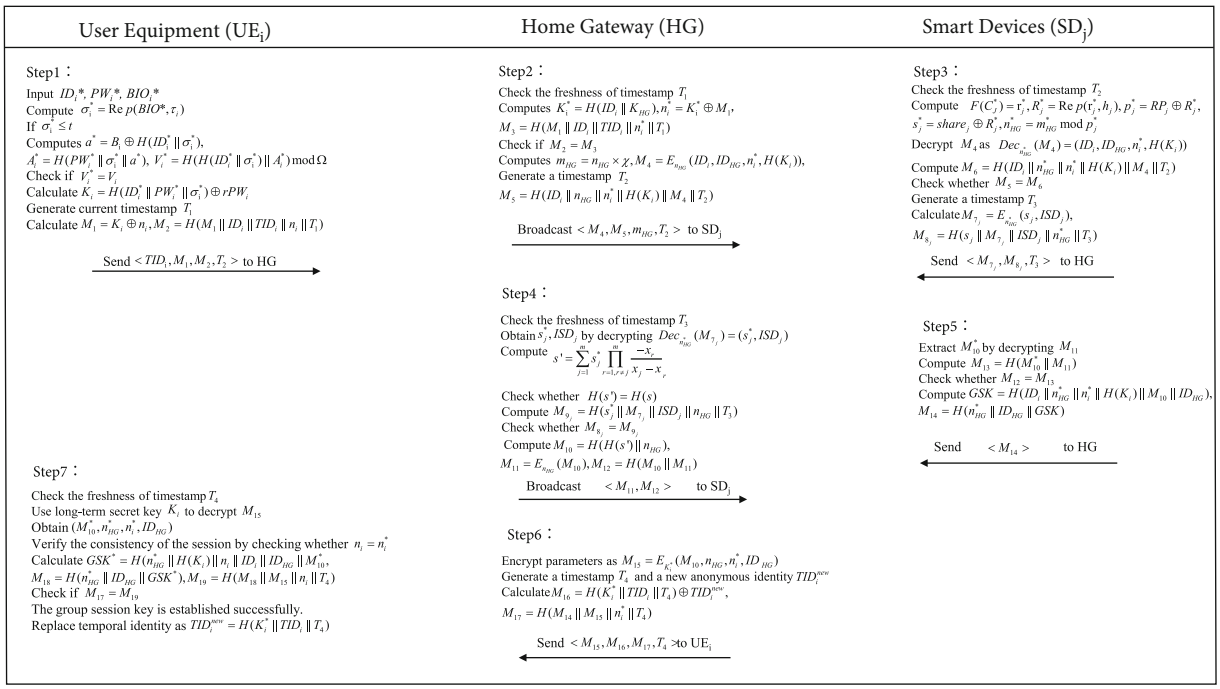

Figure 3: Summary of login and authentication phase.

4.5.1. LAP1. U_i firstly inputs ID_i^* and high entropy password PW_i^* and imprints personal biometrics BIO_i^* into U E_i. UE_i computes $\sigma_i^* = \mathrm{Rep}(\mathrm{BIO}_i^*, \tau_i)$ by the reproduction algorithm if the hamming distance between two biometrics is t or less. Then, UE_i calculates $a^* = B_i \oplus H(\mathrm{ID}_i^* \| \sigma_i^*)$, $A_i^* = H(\mathrm{PW}_i^* \| \sigma_i^* \| a^*)$, $V_i^* = H(H(\mathrm{ID}_i^* \| \sigma_i^*) \| A_i^*) \bmod \Omega$. UE_i verifies the authenticity of the inputs ID_i, PW_i^*, and BIO_i^* by checking whether V_i^* is equal to the stored V_i. After verifying the user's identity successfully, UE_i calculates symmetric key $K_i = H(\mathrm{ID}_i^* \| \mathrm{PW}_i^* \| \sigma_i^*) \oplus r\mathrm{PW}_i$. UE_i randomly generates a nonce n_i and the current timestamp T_1. UE_i then calculates $M_1 = K_i \oplus n_i$, $M_2 = H(M_1 \| \mathrm{ID}_i \| \mathrm{TID}_i \| n_i \| T_1)$. UE_i sends $\langle \mathrm{TID}_i, M_1, M_2, T_1 \rangle$ to HG via an open channel.

4.5.2. LAP2. Upon receiving the login request, HG firstly checks the freshness of the timestamp T_1. If it is true, HG retrieves ID_i and K_{HG}; computes $K_i^* = H(\mathrm{ID}_i \| K_{\mathrm{HG}}) = K_i$, $n_i^* = K_i^* \oplus M_1$, and $M_3 = H(M_1 \| \mathrm{ID}_i \| TID_i \| n_i^* \| T_1)$; and checks if $M_2 = M_3$. If it is invalid, the session is terminated immediately. Then, HG randomly generates a nonce n_{HG} and a timestamp T_2 and computes $m_{\mathrm{HG}} = n_{\mathrm{HG}} \times \chi$. HG calculates $M_4 = Enc_{n_{\mathrm{HG}}}(\mathrm{ID}_i, \mathrm{ID}_{\mathrm{HG}}, n_i^*, H(K_i))$, $M_5 = H(\mathrm{ID}_i \| n_{\mathrm{HG}} \| n_i^* \| H(K_i) \| M_4 \| T_2)$. Finally, HG broadcasts the message $\langle M_4, M_5, m_{\mathrm{HG}}, T_2 \rangle$ to a group of smart devices via the open channel.

4.5.3. LAP3. Upon receiving the message, SD_j firstly checks the freshness of the message by timestamp T_2. If it is valid, SD_j calculates $F(c_j^*) = r_j^*$, $R_j^* = \mathrm{Rep}(r_j^*, h_j)$, $p_j^* = \mathrm{RP}_j \oplus R_j^*$, $s_j^* = \mathrm{share}_j \oplus R_j^*$, $n_{\mathrm{HG}}^* = m_{\mathrm{HG}} \bmod p_j^*$ ($\chi \bmod p_j^* \equiv 1$, n_{HG}^* is called as a shared key of a group of legitimate smart devices).

Then, SD_j decrypts M_4 as $\mathrm{Dec}_{n^*_{HG}}(M_4) = (ID_i, ID_{HG}, n_i^*, H(K_i))$ using shared group key n^*_{HG} and computes $M_6 = H(ID_i \| n^*_{HG} \| n_i^* \| H(K_i) \| M_4 \| T_2)$. Then, SD_j checks whether $M_5 = M_6$. If it is invalid, SD_j terminates the session immediately. Otherwise, SD_j generates a timestamp T_3 and calculates $M_{7_j} = E_{n^*_{HG}}(s_j, ISD_j)$, $M_{8_j} = H(s_j \| M_{7_j} \| ISD_j \| n^*_{HG} \| T_3)$. Finally, SD_j sends message $\langle M_{7_j}, M_{8_j}, T_3 \rangle$ to HG.

4.5.4. LAP4. After receiving $\langle M_{7_j}, M_{8_j}, T_3 \rangle$ from smart devices $SD_j, j \in \{1, 2, \cdots, m\}$. HG checks the freshness of timestamp T_3. If it is valid, HG can obtain s_j^*, ISD_j by decrypting $\mathrm{Dec}_{n^*_{HG}}(M_{7_j}) = (s_j^*, ISD_j)$ and compute $s' = \sum_{j=1}^{m} s_j^* \prod_{r=1, r\neq j}^{m} (-x_r/(x_j - x_r))$. HG also checks whether $H(s') = H(s)$. If it is true, continues the session. Otherwise, HG computes $M_{9_j} = H(s_j^* \| M_{7_j} \| ISD_j \| n_{HG} \| T_3)$ and verifies the authenticity of corresponding SD_j by checking whether $M_{8_j} = M_{9_j}$. If it matches, the message is from valid SD_j. Otherwise, HG marks SD_j as invalid smart devices and terminates the session. Then, HG computes $M_{10} = H(H(s') \| n_{HG}), M_{11} = E_{n_{HG}}(M_{10}), M_{12} = H(M_{10} \| M_{11})$. Finally, HG sends $\langle M_{11}, M_{12} \rangle$ to all legitimate smart devices in the group.

4.5.5. LAP5. Upon receiving the message $\langle M_{11}, M_{12} \rangle$, each smart device SD_j firstly extracts M_{10}^* by decrypting the M_{11} using shared group key n^*_{HG}, computes $M_{13} = H(M_{10}^* \| M_{11})$, and checks whether $M_{12} = M_{13}$. If it is valid, each SD_j computes $GSK = H(n^*_{HG} \| H(K_i) \| n_i^* \| ID_i \| ID_{HG} \| M_{10})$, $M_{14} = H(n^*_{HG} \| ID_{HG} \| GSK)$. Finally, each SD_j sends the message $\langle M_{14} \rangle$ to HG.

4.5.6. LAP6. HG encrypts parameters as $M_{15} = E_{K_i^*}(M_{10}, n_{HG}, n_i^*, ID_{HG})$ and generates a timestamp T_4, a new anonymous identity TID_i^{new}. HG calculates $M_{16} = H(K_i^* \| TID_i \| T_4) \oplus TID_i^{new}, M_{17} = H(M_{14} \| M_{15} \| n_i^* \| T_4)$. Finally, HG sends the message $\langle M_{15}, M_{16}, M_{17}, T_4 \rangle$ to UE_i.

4.5.7. LAP7. UE_i firstly checks the freshness of timestamp T_4 when receiving the message $\langle M_{15}, M_{16}, M_{17}, T_4 \rangle$. UE_i then utilizes long-term secret key K_i to decrypt M_{15} and obtains $(M_{10}^*, n^*_{HG}, n_i^*, ID_{HG})$. UE_i verifies the consistency of the session by checking whether $n_i = n_i^*$. If it matches, U_i calculates $GSK^* = H(n^*_{HG} \| H(K_i) \| n_i \| ID_i \| ID_{HG} \| M_{10}^*), M_{18} = H(n^*_{HG} \| ID_{HG} \| GSK^*), M_{19} = H(M_{18} \| M_{15} \| n_i \| T_4)$. UE_i checks if $M_{17} = M_{19}$. If it matches, the group session key is established successfully. Finally, UE_i replaces temporal identity as $TID_i^{new} = H(K_i^* \| TID_i \| T_4) \oplus M_{16}$.

4.6. Biometrics and Password Update Phase. In this section, U_i can update the password and biometrics in the following steps.

4.6.1. BPUP1. U_i provides personal credentials ID_i, PW_i^{old}, and BIO_i^{old} to UE_i. UE_i computes biometrics key σ_i^{old} as $\mathrm{Gen}(BIO_i^{old}) = (\sigma_i^{old}, \tau_i^{old})$ and calculates $D_i^{old} = H(ID_i \| \sigma_i^{old})$, $a^* = B_i \oplus D_i^{old}$, $A_i^{old} = H(PW_i^{old} \| \sigma_i^{old} \| a^*)$, and $V_i^{old} = H(D_i^{old} \| A_i^{old}) \bmod \Omega$. UE_i validates the authenticity of U_i by checking whether $V_i^{old} = V_i$. If it matches, the user U_i can update personal password and biometrics. Otherwise, UE_i terminates the update phase.

4.6.2. BPUP2. U_i enters new password PW_i^{new} and imprints biometrics BIO_i^{new} into the user equipment UE_i. UE_i computes σ_i^{new} as $\mathrm{Gen}(BIO_i^{new}) = (\sigma_i^{new}, \tau_i^{new})$ and calculates $D_i^{new} = H(ID_i \| \sigma_i^{new})$, $B_i^{new} = B_i \oplus D_i^{old} \oplus D_i^{new}$, $A_i^{new} = H(PW_i^{new} \| \sigma_i^{new} \| a^*)$, $rPW_i^{new} = rPW_i \oplus H(ID_i \| PW_i^{old} \| \sigma_i^{old}) \oplus H(ID_i \| PW_i^{new} \| \sigma_i^{new})$, and $V_i^{new} = H(D_i^{new} \| A_i^{new}) \bmod \Omega$. Finally, UE_i replaces B_i, V_i, rPW_i, and τ_i^{old} with $B_i^{new}, V_i^{new}, rPW_i^{new}$, and τ_i^{new} without the help of RC, respectively.

4.7. Dynamic Smart Devices Joining and Revoking Phase. Some new smart devices may be added to the smart home after the initial deployment or some deployed smart devices may leave the smart home for some reasons. Therefore, to revoke the defunct device or add the new device into the smart home, it is necessary to update the status of smart devices in real-time. The detailed joining and leaving process is executed in the following steps.

4.7.1. Joining. When joining the smart home, a new smart device SD_j^{new} must firstly register itself as RC. SD_j^{new} randomly chooses a challenge value c_j^{new} and generates its physical fingerprint R_j^{new} based on PUF and fuzzy extractor technique. Then, a new smart device sends R_j^{new} to RC securely. RC generates a unique identity ISD_j^{new} and legitimate share (s_j^{new}, p_j^{new}) and computes Var_j^{new}. Then, RC adds $Var_j^{new} = P_j P_j^{-1}$ to χ as $\chi^{new} = \chi + Var_j^{new}$. During the execution of authentication and key agreement phase, only the legitimate smart devices can calculate secret n_{HG}^{new} as $m_{HG}^{new} \bmod s_j^{new} = n_{HG}^{new}$ $(m_{HG}^{new} = n_{HG}^{new} \times \chi^{new}, \chi^{new} \bmod p_j^{new} \equiv 1, n_{HG}^{new} < p_j^{new})$. Finally, the new smart devices can be accessed by user U_i.

4.7.2. Revoking. To protect the session security, HG should update the status of smart devices. A smart device that wants to leave the group or is marked as an illegal device will be revoked by HG. The HG subtracts corresponding $Var_j^{revoking}$ from χ as $\chi^{new} = \chi - Var_j^{revoking}$. The HG generates a new temporal secret and broadcasts it to a group of smart devices. The revoked smart device will fail to compute secret and decrypt the message due to the update of χ^{new}.

5. Security Analysis

The widespread Real-or-Random (ROR) model proposed by Abdalla et al. [13] is adopted to establish our security model in this section.

5.1. Formal Security Analysis

(1) *Participants.* Let $\prod_{U_i}^{u}$, $\prod_{SD_j}^{v}$, and $\prod_{HG}^{t}$ represent instances u, v, and t of participant U_i, SD_j, and HG, respectively

(2) *Partnering*. If the following conditions are satisfied, the instances $\prod_{U_i}^{u}$ and $\prod_{\mathrm{SD}_j}^{v}$ are said to be partners [37].

(i) Both instances $\prod_{U_i}^{u}$ and $\prod_{\mathrm{SD}_j}^{v}$ are accepted

(ii) Both instances $\prod_{U_i}^{u}$ and $\prod_{\mathrm{SD}_j}^{v}$ authenticate each other

(iii) The instance $\prod_{U_i}^{u}$ and the instance $\prod_{\mathrm{SD}_j}^{v}$ are only partners each other

(3) *Freshness*. The instance $\prod_{U_i}^{u}$ or $\prod_{\mathrm{SD}_j}^{v}$ is fresh if the session key SK is not compromised to $\mathscr{A}$

(4) *Adversary*. $\mathscr{A}$ has all the capabilities as the adversary in Dolev-Yao (DY) threat model [37–39] and also has some capabilities defined in CK-adversary model [40, 41]. Moreover, $\mathscr{A}$ can make queries as Execute $(\prod_u, \prod_v)$, Reveal$(\prod)$, Send$(\prod, m)$, CorruptUserEquipment$(\prod_{U_i}^{t})$, CorruptSmartDevice$(\prod_{\mathrm{SD}_j}^{t})$, and Test$(\prod)$ to challenger to obtain the sensitive information. These queries are utilized to construct a series of games. After games, $\mathscr{A}$ guesses a bit b' and wins the game only if $b' = b$. Succ represents that $\mathscr{A}$ wins the game. The advantage of $\mathscr{A}$ in breaking the IND-CPA of our protocol $\mathscr{P}$ in probabilistic polynomial time is $\mathrm{Adv}_{\mathscr{P},\mathscr{A}}^{\mathrm{IND-CCA}}(\mathscr{K}) = |2 \cdot \Pr[\mathrm{Succ}] - 1|$. The proposed protocol $\mathscr{P}$ is secure under the ROR model when $\mathrm{Adv}_{\mathscr{P},\mathscr{A}}^{\mathrm{IND-CPA}}(\mathscr{K})$ is negligible

Theorem 1. *Let $\mathscr{A}$ be the adversary running in the polynomial time t against our authentication protocol $\mathscr{P}$ in the random oracle. Let Dic, q_h, q_{send}, q_e, $|Hash|$, $|Dic|$, m, and l^r represent the a uniformly distributed password dictionary, the number of Hash oracles, the number of Send oracle, the number of Execute oracles, the space of hash function, the size of Dic, the bit length of biometrics key σ_i, and the bit length of the random nonce, respectively. The advantage of $\mathscr{A}$ in breaking protocol $\mathscr{P}$ in probabilistic polynomial time is defined as follows:*

$$Adv_{\mathscr{P},\mathscr{A}}^{AKA}(\mathscr{K}) \le \frac{q_h^2}{|Hash|} + \frac{(q_{send} + q_e)^2}{2^{l^r}} + 2\max\left(\frac{q_{send}}{2^m}, C' \cdot q_{send}^{s'}\right) + \frac{2}{q} \cdot Adv_{\mathscr{P},\mathscr{A}}^{IND-CPA}(\mathscr{K}). \tag{3}$$

Proof. The games Game_i, where $i = [0, 4]$ is defined in this section. Let Succ_i represent the event that $\mathscr{A}$ succeeds in guessing b in the Game_i.

Game_0 : the game Game_0 simulates the real attack in our protocol by $\mathscr{A}$ in ROR sense. At the beginning of Game_0, $\mathscr{A}$ guesses b. By definition, it follows

$$\mathrm{Adv}_{\mathscr{P},\mathscr{A}}^{\mathrm{AKA}}(\mathscr{K}) = |2 \Pr[\mathrm{Succ}_0] - 1|. \tag{4}$$

Game_1 : the game Game_1 simulates the adversary's eavesdropping attack by asking Execute$(\prod, \prod)$ oracle. At the end of the game, $\mathscr{A}$ queries Test oracle and then distinguishes whether the output of Test oracle is either a real session key SK or a random string in the same domain. The group session key is calculated as $\mathrm{GSK} = H(n_{\mathrm{HG}} \| H(K_i) \| n_i \| \mathrm{ID}_i \| \mathrm{ID}_{\mathrm{HG}} \| H(H(\mathrm{s}) \| n_{\mathrm{HG}}))$ in our protocol. To calculate the GSK, $\mathscr{A}$ has to obtain $H(K_i)$ and $H(H(s) \| n_{\mathrm{HG}})$. Additionally, $\mathrm{ID}_i, \mathrm{ID}_{\mathrm{HG}}, n_i$, and n_{HG} are not compromised to $\mathscr{A}$. Therefore, the probability of winning Game_1 for $\mathscr{A}$ is not increased by launching eavesdropping attacks. It is clear that

$$\Pr[\mathrm{Succ}_0] = \Pr[\mathrm{Succ}_1]. \tag{5}$$

Game_2 : there exists some differences between Game_2 and Game_1; the simulations of Send and Hash oracles are added to the Game_2. The game simulates an active attack in which $\mathscr{A}$ tries to fool the participant into accepting the forged messages. $\mathscr{A}$ is able to query Hash oracle many times to find collisions. Since all the exchanged messages are associated with participant's identity, random nonce, and timestamps, the probability of finding the collision of secret key for symmetric cryptography is $q_h^2/2 \cdot |\mathrm{Hash}|$ according to the birthday paradox. Besides, the probability of finding the collision of random nonce is defined as $(q_{\mathrm{send}} + q_e)^2 / 2^{l^r+1}$. It is clear that

$$|\Pr[\mathrm{Succ}_1] - \Pr[\mathrm{Succ}_2]| \le \frac{q_h^2}{2 \cdot |\mathrm{Hash}|} + \frac{(q_{\mathrm{send}} + q_e)^2}{2^{l^r+1}}. \tag{6}$$

Game_3 : by adding the simulation of querying the CorruptSmartPhone oracle and smartphone lost attack, the Game_2 is transformed into Game_3. $\mathscr{A}$ may obtain password PW_i and the biometrics key σ_i using online, offline dictionary attack, and physical device attack, respectively. The fuzzy extractor is utilized to extract the b bits of biometric information, and the probability of guessing the $\sigma_i \in \{0, 1\}^m$ for $\mathscr{A}$ is approximately $1/2^m$. Additionally, it is supposed that the number of password inputs is strictly limited. The user-chosen passwords tend to be low entropy and are far different distribution from uniform distribution. The size of the password space is limited in practical, and users usually only use a part of the password space. The probability of guessing the password is defined as $C' \cdot q_{\mathrm{send}}^{s'}$ [43]; C' and s' are the parameters of the Zipf model. Therefore, it is clear that

$$|\Pr[\mathrm{Succ}_2] - \Pr[\mathrm{Succ}_3]| \le \max\left(\frac{q_{\mathrm{send}}}{2^m}, C' \cdot q_{\mathrm{send}}^{s'}\right). \tag{7}$$

Game_4 : this game adds the simulation of CorruptSmartDevice oracle compared to Game_3. $\mathscr{A}$ can physically capture the smart devices and obtain the information prestored into the memory of smart device in the registration phase. However, this information is encrypted by the physical fingerprint R_j based on PUF and fuzzy extractor

technique. It is hard to obtain the secret share s_j and forge the device even if $\mathcal{A}$ grabs the device. Let $\mathcal{A}$ can eavesdrop all the exchanged messages. $\mathcal{A}$ tries to obtain the sensitive information $\{\mathrm{ID}_i, \mathrm{ID}_{\mathrm{HG}}, n_i, M_{10}, H(K_i)\}$ by decrypting the message M_4. Due to the Chinese Remainder Theorem, any illegitimate participant is unable to obtain the temporary group key n_{HG} and $H(K_i)$ without the secret share s_j. Even if $\mathcal{A}$ wants to reconstruct secret, it is hard for $\mathcal{A}$ to capture at least t legal smart devices. The probability of forging the appropriate pair of values is $1/q$. Additionally, it is difficult for $\mathcal{A}$ to decrypt the M_{15} as $\mathcal{A}$ is unknown to K_i. $\mathcal{A}$ can not compute $\mathrm{GSK} = H(n_{\mathrm{HG}} \| H(K_i) \| n_i \| \mathrm{ID}_i \| \mathrm{ID}_{\mathrm{HG}} \| H(H(s) \| n_{\mathrm{HG}}))$ due to the lacking of $H(H(s) \| n_{\mathrm{HG}})$ and $H(K_i)$. The proposed protocol is IND − CPA secure. It is concluded that

$$\left|\Pr\left[\mathrm{Succ}_3\right] - \Pr\left[\mathrm{Succ}_4\right]\right| \leq \frac{1}{q} \cdot \mathrm{Adv}^{\mathrm{IND-CPA}}_{\mathcal{P},\mathcal{A}}(\mathcal{K}). \tag{8}$$

All the oracles have been simulated in the game. $\mathcal{A}$ guesses b after querying Test oracle. It is clear that $\Pr[\mathrm{Succ}_4] = 1/2$.

Therefore, from formulas (4) to (8), we have

$$\begin{aligned}
\mathrm{Adv}^{\mathrm{AKA}}_{\mathcal{P},\mathcal{A}}(\mathcal{K}) &= 2 \cdot \left|\Pr\left[\mathrm{Succ}_0\right] - \frac{1}{2}\right| = 2 \cdot \left|\Pr\left[\mathrm{Succ}_1\right] - \Pr\left[\mathrm{Succ}_4\right]\right| \\
&\leq 2 \cdot \left(\left|\Pr\left[\mathrm{Succ}_1\right] - \Pr\left[\mathrm{Succ}_2\right]\right| + \left|\Pr\left[\mathrm{Succ}_2\right] - \Pr\left[\mathrm{Succ}_4\right]\right|\right) \\
&\leq 2 \cdot \left(\left|\Pr\left[\mathrm{Succ}_1\right] - \Pr\left[\mathrm{Succ}_2\right]\right| + \left|\Pr\left[\mathrm{Succ}_2\right] - \Pr\left[\mathrm{Succ}_3\right]\right| + \left|\Pr\left[\mathrm{Succ}_3\right] - \Pr\left[\mathrm{Succ}_4\right]\right|\right) \\
&\leq 2 \cdot \left(\frac{q_h^2}{2 \cdot |\mathrm{Hash}|} + \frac{(q_{\mathrm{send}} + q_e)^2}{2^{l'+1}} + \max\left(\frac{q_{\mathrm{send}}}{2^m}, C' \cdot q_{\mathrm{send}}^{s'}\right) + \frac{1}{q} \cdot \mathrm{Adv}^{\mathrm{IND-CPA}}_{\mathcal{P},\mathcal{A}}(\mathcal{K})\right) \\
&\leq \frac{q_h^2}{|\mathrm{Hash}|} + \frac{(q_{\mathrm{send}} + q_e)^2}{2^{l'}} + 2 \max\left(\frac{q_{\mathrm{send}}}{2^m}, C' \cdot q_{send}^{s'}\right) \\
&\quad + \frac{2}{q} \cdot \mathrm{Adv}^{\mathrm{IND-CPA}}_{\mathcal{P},\mathcal{A}}(\mathcal{K}).
\end{aligned} \tag{9}$$

□

5.2. Other Discussions on Security Features

5.2.1. Untraceability and User Anonymity. It is assumed that $\mathcal{A}$ has capability of intercepting all the messages during the execution of the authentication phase over the public channel. The user's identity ID_i is protected by hash function $H(\cdot)$ and symmetric cryptography. It is computationally infeasible for $\mathcal{A}$ to attain identity without secret parameters $n_{\mathrm{HG}}, n_i, V_i, \sigma_i$. Therefore, our protocol guarantees the feature of user anonymity. Moreover, the transmitted message generally involves the current timestamp and random nonce, and U_i temporary identity TID_i is updated when the session is completed successfully. Therefore, it is also computationally infeasible for $\mathcal{A}$ to track the user's activity in each session. In conclusion, the untraceability and user anonymity are both guaranteed in our protocol.

5.2.2. Replay Attack. It is assumed that $\mathcal{A}$ is capable of intercepting all the messages between the user, HG, and smart devices. The transmitted messages usually involve random nonces and timestamps. Even if $\mathcal{A}$ intercepts the messages and replays these messages shortly after, they can not pass the verification of timestamps due to maximum communication delay ΔT. Thus, our protocol can resist replay attack.

5.2.3. Smart Device Impersonation Attack. It is supposed that $\mathcal{A}$ intercepts the transmitted message during the execution of the protocol. $\mathcal{A}$ needs to generate valid information. However, $\mathcal{A}$ does not know the sensitive parameters to obtain the authentication parameters. Furthermore, the smart device is protected by PUF, which cannot be forged on hardware. It is computationally infeasible to impersonate the smart device in probabilistic polynomial time. Therefore, our protocol can withstand smart device impersonation attack.

5.2.4. HG Impersonation Attack. It is supposed that $\mathcal{A}$ intercepts the message during the execution of the protocol and tries to generate other messages to impersonate HG. However, without the knowledge of the secret parameters $\chi, n_i, \mathrm{ID}_i, K_{\mathrm{HG}}$, it is computationally infeasible to impersonate HG in probabilistic polynomial time. Thus, our protocol can withstand HG impersonation attack.

5.2.5. Smartphone Lost Attack. Supposed that the U_i's smartphone is lost or stolen by $\mathcal{A}$. By the threat model, $\mathcal{A}$ is capable of extracting all the information $\{\mathrm{TID}_i, r\mathrm{PW}_i, B_i, V_i, \tau_i, \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot), H(\cdot), t\}$ stored in the memory of UE_i using the power analysis attack [44]. In order to retrieve $\mathrm{ID}_i, \mathrm{PW}_i$ from the extracted information $\mathcal{A}$ needs to attain the secrets K_i, σ_i, n_i. The possibility of guessing the user's biometrics key σ_i as well as n_i, K_i is negligible. The adversary $\mathcal{A}$ may launch the password guessing attack. The password guessing attack is mainly divided into online and offline password guessing attack [45]. The online password guessing attack can be effectively prevented by limiting the number of illegal requests from users. In our paper, the "fuzzy verifier" is utilized to guarantee the security under offline password guessing attack. The password verifier V_i is computed $V_i = H(H(\mathrm{ID}_i \| \sigma_i) \| H(\mathrm{PW}_i \| \sigma_i \| a) \bmod \Omega$. Even if other two authentication factors are compromised, the adversary $\mathcal{A}$ has to guess ID_i, PW_i, and a. Furthermore, it is assumed that $\mathcal{A}$ has got the ID_i^*, PW_i^*, and a^* which satisfying $V_i = V_i^*$; the login request will be rejected due to the "fuzzy verifier." Therefore, our protocol can effectively withstand online and offline guessing attack. The user's identity credentials $\mathrm{ID}_i, \mathrm{PW}_i$ are not compromised to $\mathcal{A}$. So, our protocol can resist smartphone lost attack.

5.2.6. Privileged-Insider Attack. It is assumed that $\mathcal{A}$ is a privileged-insider user of trusted RC. $\mathcal{A}$ tries to attain the credentials of the authorized user and all the information from UE_i. $\mathcal{A}$ obtains the registration information $\{\mathrm{ID}_i, \mathrm{RPW}_i\}$ of U_i which is sent to RC. Meanwhile, $\mathcal{A}$ is able to extract all the information $\{\mathrm{TID}_i, r\mathrm{PW}_i, B_i, V_i, \tau_i, \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot), H(\cdot), t\}$ stored in the UE_i. Without knowing of random nonce a and biometrics key σ_i, it is computationally infeasible to retrieve PW_i in probabilistic polynomial time due to $\mathrm{RPW}_i = H(\mathrm{ID}_i \| \mathrm{PW}_i \| \sigma_i)$. Thus, our protocol can withstand privileged-insider attack.

5.2.7. Ephemeral Secret Leakage Attack. In our protocol, a secure group session key $\mathrm{GSK}^* = H(n_{\mathrm{HG}}^* \| H(K_i) \| n_i \| \mathrm{ID}_i \| \mathrm{I}$

Table 2: Security feature comparison.

Feature	[20]	[8]	[9]	[46]	[47]	[48]	Our protocol
User anonymity	√	√	√	√	√	√	√
Untraceability	√	√	√	√	√	√	√
Mutual authentication	√	√	√	√	√	√	√
Perfect forward secrecy	×	×	√	√	√	√	√
Dynamically devices joining	√	√	×	×	√	√	√
Device revocation	√	×	×	×	√	√	√
The number of factors used	Three	Three	Two	N/A	Two	Three	Two
Password/biometrics update	√	√	√	×	×	√	√
Smartphone/smartcard lost attack	√	√	√	N/A	×	√	√
Smart device lost attack	√	√	√	N/A	√	×	√
User impersonation attack	√	√	√	√	√	√	√
Device impersonation attack	√	√	√	N/A	√	√	√
HG impersonation attack	N/A	√	N/A	√	√	√	√
Session key security	√	√	√	√	√	√	√
Replay attack	√	√	√	√	√	√	√
Privileged-insider attack	√	√	√	√	√	√	√
Ephemeral secret leakage attack	N/A	N/A	N/A	×	×	√	√

[1]N/A means not considered. [2]√ means the scheme supports the functionality/security feature. [3]× means the scheme does not support the functionality/security feature.

Table 3: Communication cost comparison.

Scheme	Single device cost	n devices cost	The no. of message
Challa et al. [20]	2016	$2016n$	4
Wazid et al. [8]	2592	$2592n$	4
Li et al. [9]	2048	$2048n$	4
Yu and Li [46]	4096	$4096n$	8
Shuai et al. [47]	2272	$2272n$	4
Banerjee et al. [48]	2048	$2048n$	4
Our protocol	3296	$1376 + 1920n$	6

$D_{HG}\|M_{10}$) is established between a user and smart devices during the login and authentication phase. M_{10} is composed of long-term secret $H(s)$ and short-term secret n_{HG}. In particular, the secret s is computed by secret reconstruction algorithm of secret sharing technology. In addition, ID_{HG}, I D_i, $H(K_i)$ are the long-term secrets, and n_i is a short-term secret. On the one hand, it is assumed that the short-term secrets n_{HG}, n_i are revealed to $\mathcal{A}$. However, it is computationally infeasible to compute the GSK due to the lack of long-term secrets. On the other hand, it is assumed that $\mathcal{A}$ can obtain the long-term secrets. Even though $\mathcal{A}$ obtains some secret shares s_j from the smart devices, it is computationally infeasible to construct the secret S and then calculate the message M_{10}. The short-term secrets n_{HG}, n_i are randomly generated by the HG and U_i. It is also hard for $\mathcal{A}$ to compute GSK without the short-term secrets n_{HG}, n_i. Therefore, $\mathcal{A}$ cannot compute the current session key unless both all the long-term secrets and short-term secrets are compromised simultaneously. Our protocol can thwart the ephemeral secret leakage attack.

5.2.8. Perfect Forward Secrecy. It is supposed that the adversary obtains the secret keys of a user and the smart devices. Furthermore, the adversary intercepts all the messages transmitted among them during the group authentication process. The adversary computes $GSK = H(n_{HG}\|H(K_i)\|n_i\|ID_i\|ID_{HG}\|M_{10}) = H(n_{HG}\|H(ID_i\|K_{HG})\|n_i\|ID_i\|ID_{HG}\|H(H(s)\|n_{HG}))$ to get the group session key. However, the adversary cannot obtain the parameters n_{HG}, K_{HG} and reconstruct correctly the secret s with given shares to compute the group session key. Therefore, the proposed protocol can provide the perfect forward secrecy.

5.2.9. Session Key Security. The session key GSK is calculated by both all the authenticated smart devices and the user U_i. The message M_{14} contains the session key. Supposed that $\mathcal{A}$ intercepts the message and tries to forge GSK′ by random nonces $n_{i'}, n_{HG}{}'$. However, $\mathcal{A}$ does not know the parameters $ID_i, H(K_i), M_{10}$; it is impossible for $\mathcal{A}$ to compute GSK due to the collision resistance property of $H(\cdot)$. Thus, our protocol guarantees session key security successfully.

6. Performance Analysis

We analyze the performance of our protocol from three aspects, including computational cost, communication cost,

Table 4: Computational cost comparison.

Protocol	Single device accessing cost (ms)	n devices accessing cost (ms)
Challa et al. [20]	$T_{fe} + 16T_H + 13T_{ecm}$	$(T_{fe} + 16T_H + 13T_{ecm})n$
Wazid et al. [8]	$T_{fe} + 21T_H + 8T_{E/D}$	$(T_{fe} + 21T_H + 8T_{E/D})n$
Li et al. [9]	$T_{fe} + 19T_H + 8T_{E/D} + 3T_{ecm}$	$(T_{fe} + 19T_H + 8T_{E/D} + 3T_{ecm})n$
Yu and Li [46]	$4T_B + 26T_H + 47T_{ecm}$	$(4T_B + 26T_H + 47T_{ecm})n$
Shuai et al. [47]	$16T_H + 8T_{ecm}$	$(16T_H + 8T_{ecm})n$
Banerjee et al. [48]	$T_{fe} + 24T_H$	$(T_{fe} + 24T_H)n$
Our protocol	$T_{puf} + 2T_{fe} + 22T_H + 8T_{E/D}$	$T_{fe} + 9T_H + 4T_{E/D} + (T_{puf} + T_{fe} + 4T_{E/D} + 13T_H)n$

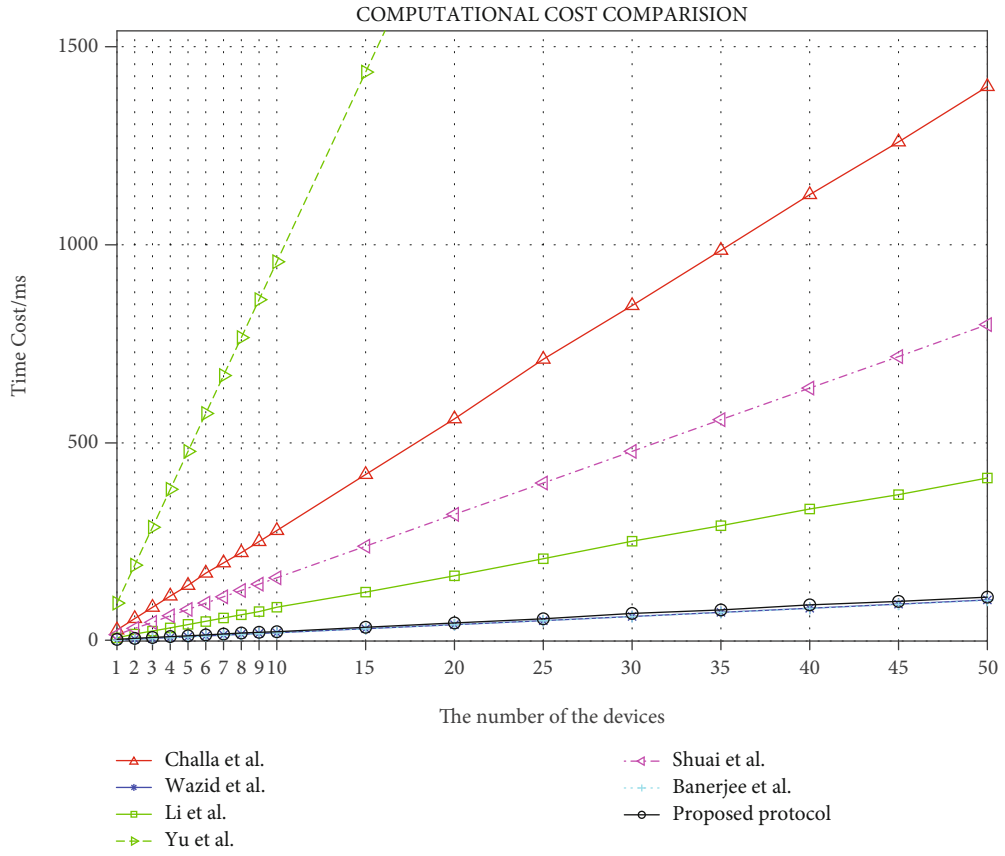

Figure 4: Computational cost comparison.

functionality, and security features, respectively. We also compare our protocols with other related protocols in the section.

6.1. Functionality and Features. We compare the functionality and security features of our protocol with other related protocols in Table 2. From Table 2, most protocols generally adopt a multifactor authentication mechanism to verify the authenticity of the user. Challa et al. [20] and Li et al. [9]'s protocol are insecure against HG impersonation attack and do not provide perfect forward secrecy. Although most authentication and key agreement protocols for the smart home declare they can resist many known attacks such as replay attack, privileged-insider attack, and man-in-the-middle attack, most protocols do not support all above features. It is obvious that the proposed protocol still provides more security functionalities and security features than other related protocols [46–48]. Yu and Li [46], Shuai et al. [47], and Banerjee et al. [48] all lack the security protection for the smart devices. The sensitive information stored in the smart devices may be compromised to the adversary while the adversary launch attacks on smart devices. Additionally, Yu and Li [46] and Shuai et al. [47] utilize pairing-based cryptography and ECC-based to implement authentication and establish session key between users and devices, respectively, which are not great for resource-constrained devices.

6.2. Communication Cost. We evaluate the communication and computational cost in our authentication protocol compared to other protocols [8, 9, 20, 46–48].

It is defined that the length of identity, random nonces, timestamps, and hash function operation is 128 bits, 128 bits, 32 bits, and 160 bits, respectively. It is also assumed that $|\lambda_1| = 128$ bits, $|\lambda_2| = 160$ bits, and AES-128 are adopted for symmetric cryptography, where λ_1, λ_2 denote the length of input and output of physical unclonable function, respectively. The messages in our protocol include $\text{msg}_1 = \{\text{TID}_i, M_1, M_2, T_1\}$, $\text{msg}_2 = \{M_4, M_5, m_{\text{HG}}, T_2\}$, $\text{msg}_3 = \{M_{7-\text{SD}_j}, M_{8-\text{SD}_j}, T_3\}$, $\text{msg}_4 = \{M_{11}, M_{12}\}$, $\text{msg}_5 = \{M_{14}\}$, and $\text{msg}_6 = \{M_{15}, M_{16}, M_{17}, T_4\}$; the corresponding bit length of messages is 480 bits, 864 bits, 576 bits, 320 bits, 160 bits, and 896 bits, respectively. Table 3 summarizes the proposed protocol and other existing authentication protocols in terms of communication cost. The proposed protocol requires second highest communication cost among all the protocols when users launch the access request to single device in the smart home. However, it is obvious that the proposed protocol effectively reduces the communication cost when accessing multiple devices compared to other protocols.

6.3. Computational Cost. The proposed protocol is simulated using Pair-Based Cryptography (PBC) library and GNU Multiple Precision Arithmetic (GMP) library. C language is utilized on Ubuntu 16.04 with 2.50 GHz Intel(R) Core(TM) i5-4200M CPU and 8 GB of RAM.

We compare the total execution time with other protocols [8, 9, 20, 46–48] during the login and authentication phase. It is assumed that T_B, T_H, $T_{E/D}$, T_{fe}, T_{xor}, T_{ecm}, T_{mm}, T_{puf}, T_{mac}, and T_{hmac} denote the computational cost required for a bilinear pairing, hash function, a symmetric cryptography using AES-128, a fuzzy extraction operation, a XOR operation, a point multiplication operation using ECC, a modular multiplication operation, a physical unclonable function operation, a message authentication code (MAC) operation, and a hashed MAC operation, respectively. As the computational cost of bit-wise XOR operation is much less than other operations, it is not considered in the evaluation. Besides, it is assumed that $T_H \approx T_{mac} \approx T_{hmac}$, $T_{fe} \approx T_{ecm}$ in our experiment according to [8]. The above operations are performed one hundred times and take its average value. Based on the experimental results reported in [49], we have the computational cost of T_B, T_H, $T_{E/D}$, T_{fe}, T_{mm}, T_{ecm}, and T_{puf} which is 0.544 ms, 0.0026 ms, 0.00325 ms, 1.989 ms, 0.171 ms, 1.989 ms, and 0.12 ms (ms is the abbreviation of milliseconds), respectively. The computational cost of accessing single and multiple devices for the related protocol and our protocol is described in Table 4. It is clear that the proposed protocol has significantly reduced the computational cost compared to Challa et al. [20] and Shuai et al. [47]. By introducing the Chinese residual theorem and secret sharing, although the copu is performance in the case of single device access, the performance is significantly better in the case of multiple devices access.

Figure 4 shows the comparison of computational cost in the login and authentication phase. Viewed from Figure 4, the X-axis represents the numbers of smart devices that users access simultaneously. The Y-axis represents the time cost to establish session key with n smart devices, simultaneously. It is obvious that the computational cost of Yu and Li [46] is much more than that of other protocols. Compared to protocols of Challa et al. [20], Li et al. [9], and Shuai et al. [47], the protocols of Wazid et al. [8] and Banerjee et al. [48] and our proposed protocol have the similar computational cost when accessing smart devices. Obviously, according to Table 4, the computational complexity of previous schemes increases linearly according to the number of devices. In this scenario, the computation cost is $T_{fe} + 9T_H + 4T_{E/D} + (T_{puf} + T_{fe} + 4T_{E/D} + 13T_H)n$. When n is large, we believe that the constant term can be ignored, so our computation time also increases linearly with the number of devices. However, our protocol effectively supports more functionalities and security features at the cost of slightly increasing the communication and computational cost compared to Wazid et al. [8] and Banerjee et al. [48]'s protocols.

7. Conclusion

In this paper, we proposed a PUF-assisted lightweight group authentication and key agreement protocol in the smart home based on secret sharing technique and Chinese Remainder Theorem. The proposed protocol can withstand most of several known attacks, which is proved under the ROR model and other security discussions. Compared with other related protocols, our protocol can effectively reduce the resource cost during the login and authentication phase. In addition, our smart devices protected by the physical unclonable function are secure against smart device lost attack. Our protocol supports dynamic smart device joining and leaving, password, and biometrics update without the involvement of HG. Overall, the performance of our authentication protocol is better than other related protocols only using lightweight operations. Therefore, our protocol is more suitable for resource-constrained smart devices in the smart home. In future work, we will take tools such as AVISPA for further security analysis and verify the performance of the protocol in the smart home.

Data Availability

The related data used to support the findings of this study are included within the article.

Disclosure

The paper is extended from the one that is accepted in SPNCE 2020. The previous version can be found at the SPNCE 2020 proceedings.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant No. 61922045, No. U21A20465, No. 62172292, and No.61877034.

References

[1] V. Ricquebourg, D. Menga, D. Durand, B. Marhic, L. Delahoche, and C. Loge, "The smart home concept: our immediate future," in *2006 1ST IEEE International Conference on E-Learning in Industrial Electronics*, pp. 23–28, Hammamet, Tunisia, 2006.

[2] L. Jiang, D. Liu, and B. Yang, "Smart home research," in *Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.04EX826)*, vol. 2, pp. 659–663, Shanghai, China, 2004.

[3] M. Chiang and T. Zhang, "Fog and IoT: an overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, 2016.

[4] L. Jiang, C. Wang, and J. Shen, "Stereo storage structure assisted one-way anonymous auditing protocol in e-health system," *Journal of Surveillance, Security and Safety*, vol. 1, pp. 61–78, 2020.

[5] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1953–1966, 2015.

[6] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[7] X. Ye and J. Huang, "A framework for cloud-based smart home," in *Proceedings of 2011 International Conference on Computer Science and Network Technology*, vol. 2, pp. 894–897, Harbin, 2011.

[8] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269–282, 2018.

[9] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo, "A robust and energy efficient authentication protocol for industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606–1615, 2018.

[10] Y. Wen and Y. Lao, "Efficient fuzzy extractor implementations for PUF based authentication," in *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*, pp. 119–125, IEEE Computer Society, Los Alamitos, CA, USA, 2017.

[11] C. Herder, M. D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: a tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[12] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park, "Physically secure lightweight anonymous user authentication protocol for Internet of Things using physically unclonable functions," *IEEE Access*, vol. 7, pp. 85627–85644, 2019.

[13] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," *IEE Proceedings-Information Security*, vol. 153, no. 1, pp. 27–39, 2006.

[14] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316–323, 2013.

[15] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," in *International Symposium on Wireless and pervasive Computing (ISWPC)*pp. 1–6, Taipei, Taiwan, 2013.

[16] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 968–979, 2017.

[17] M. Turkanovic, B. Brumen, and M. Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[18] S. Kalra and S. K. Sood, "Advanced password based authentication scheme for wireless sensor networks," *Journal of information security and applications*, vol. 20, pp. 37–46, 2015.

[19] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[20] S. Challa, M. Wazid, A. K. Das et al., "Secure signature-based authenticated key establishment scheme for future IoT applications," *Ieee Access*, vol. 5, pp. 3028–3043, 2017.

[21] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for Industrial Internet of Things," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1133–1146, 2018.

[22] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.

[23] L. Harn, "Group authentication," *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1893–1898, 2013.

[24] Y. Liu, C. Cheng, J. Cao, and T. Jiang, "An improved authenticated group key transfer protocol based on secret sharing," *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2335-2336, 2013.

[25] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408–417, 2016.

[26] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2972–2986, 2019.

[27] S. Zhang and J. Lee, "A group signature and authentication scheme for blockchain-based mobile-edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4557–4565, 2020.

[28] J. R. Wallrabenstein, "Practical and secure IoT device authentication using physical unclonable functions," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 99–106, Vienna, Austria, 2016.

[29] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 4957–4968, 2019.

[30] F. L. Tiplea and C. Hristea, "PUF protected variables: a solution to RFID security and privacy under corruption with temporary state disclosure," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 999–1013, 2021.

[31] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-based secure communication protocol for IoT," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 3, pp. 1–25, 2017.

[32] A. Braeken, "PUF based authentication protocol for IoT," *Symmetry*, vol. 10, no. 8, p. 352, 2018.

[33] U. Chatterjee, V. Govindan, R. Sadhukhan et al., "Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 3, pp. 424–437, 2019.

[34] T. Li and Y. Liu, "A double PUF-based RFID authentication protocol," *Journal of Computer Research and Development*, vol. 58, no. 8, pp. 1801–1810, 2021.

[35] S. Chen, B. Li, Z. Chen, Y. Zhang, C. Wang, and C. Tao, "Novel strong-PUFbased authentication protocols leveraging Shamir's secret sharing," *IEEE Internet of Things Journal*, 2021.

[36] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.

[37] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[38] M. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: a decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[39] M. Shariq, K. Singh, M. Y. Bajuri, A. Pantelous, A. Ahmadian, and M. Salimi, "A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario," *Sustainable Cities and Society*, vol. 75, article 103354, 2021.

[40] R. Canetti and H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels," in *Advances in Cryptology|EUROCRYPT 2001*, B. Pfitzmann, Ed., pp. 453–474, Springer, Berlin Heidelberg., 2001.

[41] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *Advances in Cryptology|EURO-CRYPT 2002*, L. R. Knudsen, Ed., pp. 337–351, Springer, Berlin Heidelberg, 2002.

[42] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K. K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.

[43] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. P. C. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 457–468, 2019.

[44] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE transactions on computers*, vol. 51, no. 5, pp. 541–552, 2002.

[45] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smartcard- based password-authenticated key agreement in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1767–1775, 2014.

[46] B. Yu and H. Li, "Anonymous authentication key agreement scheme with pairingbased cryptography for home-based multi-sensor Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.

[47] M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Computers and Security*, vol. 86, pp. 132–146, 2019.

[48] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, and Y. Park, "An efficient, anonymous and robust authentication scheme for smart home environments," *Sensors*, vol. 20, no. 4, p. 1215, 2020.

[49] J. Zhao, W. Bian, D. Xu et al., "A secure biometrics and PUFs-based authentication scheme with key agreement for multiserver environments," *IEEE Access*, vol. 8, pp. 45292–45303, 2020.