PUF-Based Two-Factor Group Authentication in Smart Home

Sai Ji[1,3], Rongxin Qi[1,3(✉)], and Jian Shen[1,2,3]

[1] Nanjing University of Information Science and Technology, Nanjing, China
q_qirongxin@126.com
[2] Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen, China
[3] Jiangsu Engineering Center of Network Monitoring, Nanjing, China

Abstract. Various IoT-based applications such as smart home, intelligent medical and VANETs, have been put into practical utilization. Smart home is one of the most concerned environments, which allows users to remotely access and control smart devices via a public network. With development of the mobile network and smart devices, more services can be provided to users by smart devices. To securely access devices and obtain collected data over the public network, multi-factor authentication schemes for smart home have obtained wide attention. However, most of these schemes cannot withstand impersonation attack, physical device lost attack, privileged-insider attack, smart card lost attack and so on. Besides, high communication and computational costs weaken the system performance, which causes that most authentication schemes are not suitable for resource-constrained smart devices. To mitigate the aforementioned drawbacks, we proposed a two-factor anonymous group authentication scheme to implement secure access to multiple devices simultaneously using chinese remainder theorem and secret sharing technology. Our scheme also utilizes fuzzy extractor to extract personal biometric information, which helps uniquely validate authorized users in smart home. Our scheme can support various security features and withstand the most well-known attacks in smart home. Performance analysis indicates that the proposed scheme can efficiently reduce communication/computational costs when the user accesses multiple devices simultaneously.

Keywords: Smart home · Secret sharing · Authentication · Fuzzy extractor

1 Introduction

With the rapid development of IoT technology, various IoT-based applications such as smart home, intelligent medical and VANETs, have emerged. In these applications, smart home has obtained wide attention in recent years due to its convenience, efficiency and other properties, which provides basic and practical

D. Wang et al. (Eds.): SPNCE 2020, LNICST 344, pp. 209–222, 2021.
https://doi.org/10.1007/978-3-030-66922-5_14

home control services for the users. The smart home is a dwelling that connects major appliances and service, and permits them to be accessed via the public network [14]. In most existing schemes, 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, temperature sensors) [12]. The smart devices are interconnected to collect the data in smart home and exchange the collected data with the user 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, the unauthorized users may access the surveillance cameras and control them to monitor the resident in smart home. In addition, most of these IoT devices such as sensors, have the limited resources to execute complex computational operation [5]. In recent years, many Elliptic Curve Cryptography (ECC)-based schemes [10,13] have been proposed to enhance the authentication security. However, these schemes generally require to perform complex computational operations, which are not suitable for the resource-constrained devices. In addition, some schemes 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 [11,19,20]. In most of the existing schemes, the computational cost and communication cost too high to be suitable for resource-constrained [19]. If the user wants to access multiple smart devices simultaneously, it is necessary to frequently verify the authenticity of the user and send access request to corresponding 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 smart home. Group authentication schemes are put forward to solve aforementioned issues. Group authentication scheme based on secret sharing can authenticate multiple the smart devices belonging to the same group simultaneously. Considering the security of the parameters stored in the smart devices, physical unclonable function (PUF) is utilized to prevent stolen devices attack. PUF can be utilized to assist smart devices to generate biometric key, which efficiently protect the security smart devices [1]. Therefore, we propose a PUF-based two-factor group authentication scheme for smart home. Our scheme supports many well-known features such as un-traceability, user anonymity, forward secrecy. The smart devices are allowed to dynamically join or leave the group.

Our Contributions

– A PUF-based anonymous group authentication scheme is presented in our paper. Our scheme is suitable for the resource-constrained smart devices only using lightweight operation and symmetric cryptography. Furthermore, the proposed scheme meets many security requirements such as user anonymity, un-traceability and withstand many known attacks.

- The dynamic joining and leaving of smart devices from deployed network are both supported by our proposed scheme. The illegitimate smart devices fail to attain the group key without the secret share. The new smart device just register itself before joining the deployed network.
- The physical security of smart devices is guaranteed by physical unclonable function technology. The output of PUF depends on the physical microstructure of the physical device. PUF has the characteristics of tamper-resistant, unclonability, unpredictability.
- The issue of repeated user authentication is solved by utilizing secret sharing technology. The user can authenticate the multiple smart devices simultaneously and establish secure group session key, which effectively reduces communication and computational costs.

1.1 Related Work

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 [6,9,21] have studied many authentication schemes for smart home.

In 2011, Vaidya *et al.* proposed a novel authentication and key establishment mechanism which is based on ECC. Although their scheme satisfies more security requirements compared to schemes, their scheme is not suitable for resource-constrained home area networks. Therefore, many schemes focus on providing more security features while reducing resource cost of schemes. To solve communication security issue in WSNs, Xue *et al.* [21] 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 operation. However, He *et al.* [6] thought their scheme fails to resist offline password guessing attack, impersonation attack and tampering attack. In 2013, He *et al.* [6] proposed an improved authentication scheme which 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 *et al.* [8] found that Xue's scheme is vulnerable to smartcard lost attack. Kalra *et al.* [8] proposed a novel authentication scheme based on password and smartcard, which can resist most known attacks and has lower cost than other schemes. However, their scheme do not consider resisting sensing node capturing attack and privileged-insider attack. In 2018, Shen *et al.* [15] adopted the cloud to enhance the capabilities of devices and established a lightweight authentication scheme without certificates for WBANs.

The entity in IoT environment has similar features to the sensing nodes in traditional WSNs. Due to the heterogeneity and dynamics, the higher security and privacy requirements need to be satisfied in IoT environment. Kuma *et al.* [9] proposed an anonymous authentication framework for smart home using only 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.* [4] proposed a novel signature-based authenticated key establishment scheme for generic IoT environment. The user can not only communicate with smart devices but also with other users through *HG*. In 2018, Srinivas *et al.* [16] proposed an anonymous three-factor authentication and key agreement scheme which supports credentials update, user revocation and new devices addition.

2 Preliminaries

2.1 Chinese Reminder Theorem [22]

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 $P_i \ mod \ p_i$ and satisfy $P_i P_i^{-1} \equiv 1 \,(\mathrm{mod}\ p_i)$. Then, let $a_i, i = 1, 2, \cdots, n.$ be any n positive integers. The Eq. (1) has an 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 Eq. (1) is calculated in the Eq. (2).

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

2.2 Physical Unclonable Function [18]

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

1. **Unclonable:** For all $c \in C$, there is no function F' satisfing $F'(c) = F(c)$. 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 the $r_i = F(c_i)$ in probabilistic polynomial time for all $c_i \in C$.
3. **Unpredictable:** For all $c \in C$, the probability of adversary $\mathcal{A}$ correctly guessing response r of function F corresponding to challenge c in PPT is negligible. The output of 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 [13]

Fuzzy extractor takes a low-entropy value containing noise as input and outputs the same uniform random value as long as the inputs values are close. 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 the input of algorithm Gen, and it outputs the biometric key $\sigma_i \in \{0,1\}^l$ and the parameter τ_i.

Rep(): It is a deterministic algorithm. Rep takes the biometrics $BIO_i{}' \in M$, 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 $Rep\left(BIO_i{}', \tau_i\right) = \sigma_i$, where the Hamming distance between twice inputs is t or less.

3 Authentication Scheme Construction

Network Model. The authentication scheme in smart home consists of the user U_i, home gateway (HG), lots of smart devices SD_j and key generation center (KGC). All the entities are defined as follows.

- KGC : KGC is a trusted key generation center and is utilized to distribute sensitive parameters for the user, HG and lots of smart devices securely.
- HG : It is a trusted entity and cannot be compromised by the adversary $\mathcal{A}$.
- U_i : The user U_i is owner of the smartphone UE_i which has capabilities to extract U_i's biometrics and verify U_i's identity. U_i can access the smart devices after registering with the KGC. It is assumed that $\mathcal{A}$ may attain authentication credentials in the UE_i.
- SD_j : Smart devices can execute the commands and collect the information in smart home. Every smart device has a unique identity and cannot be forged physically by $\mathcal{A}$. All the smart devices have the PUF module which protects them from physically capturing attack.

Threat Model. Under the network model mentioned above, It is assumed that $\mathcal{A}$ in our scheme has same capabilities as the adversary in Dolev-Yao (DY) threat model [7]. The capabilities of $\mathcal{A}$ in our scheme are enumerated as follows:

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

Table 1. Notations and Descriptions

Notations	Descriptions
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
$Gen(\cdot)$, $Rep(\cdot)$	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

- $\mathcal{A}$ can store or resend the messages which are intercepted or forged.
- $\mathcal{A}$ can impersonate as the legitimate user or the smart device to participant during the running of the scheme.
- $\mathcal{A}$ can obtain the credentials stored in users' smartphones and smart devices, and launch various types of attacks on the protocol. However, it cannot compromise the group session key during the running of the scheme.

In addition, the adversary $\mathcal{A}$ also has some abilities in CK-adversary model proposed by Canetti *et al.* [2,3]. Under the CK-adversary model, the reveal of the ephemeral state information or other sensitive information have no influence on the session security and long-term secrets. Therefore, it is necessary to guarantee that the security of other sessions cannot be affected even through ephemeral secret is compromised (Table 1).

3.1 Smart Device Registration Phase

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 select random nonce c_j and compute $r_j = F(c_j)$. SD_j computes $(R_j, h_j) = Gen(r_j)$ to generate secret key R_j and sends R_j to KGC securely.

SDRP2. When receiving the registration from the smart device SD_j, $j = 1, 2, \cdots, n$. KGC 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 $a_j, j = 0, 1, 2, \cdots, t-1.$, and $s = f(0)$ are in finite field $GF(p)$. KGC computes $H(s)$ and $s_j = f(x_j)$ (x_j is public system information related to the smart device SD_j). KGC randomly selects a prime positive integer p_j, $j = 1, 2, \cdots, n.$ corresponding to smart device SD_j. Then, KGC computes $P = \prod_{j=1}^{n} p_j$, $P_j = P/p_j$, $j = 1, 2, \cdots, n.$ 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, KGC calculates $RP_j = R_j \oplus p_j$, $share_j = R_j \oplus s_j$ and sends ISD_j, RP_j, $share_j$ to corresponding smart device SD_j securely.

3.2 User Registration Phase

URP1. U_i firstly chooses a 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 $Gen(\cdot)$ to generates corresponding biometric key σ_i 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 take personal credentials ID_i, PW_i, σ_i and a as input to compute $RPW_i = h(ID_i \parallel PW_i \parallel \sigma_i) \oplus a$. Finally, UE_i securely sends request $\langle ID_i, RPW_i \rangle$ to KGC.

URP2. When getting the request $\langle ID_i, RPW_i \rangle$ from U_i, KGC firstly generates a 1024-bit long-term secret value K_{HG} and calculates $K_i = H(ID_i \parallel K_{HG})$, $TPW_i = K_i \oplus RPW_i$. Then, KGC 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, KGC deletes the information RPW_i and TPW_i from its database.

URP3. Upon receiving the response $\langle TID_i, TPW_i \rangle$ from KGC, UE_i computes $A_i = H(ID_i \parallel PW_i \parallel \sigma_i)$, $rPW_i = TPW_i \oplus a$, $B_i = H(ID_i \parallel A_i \parallel \sigma_i)$. Then, UE_i stores $\langle TID_i, rPW_i, B_i, \tau_i, Gen(\cdot), Rep(\cdot), H(\cdot), t \rangle$ 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.

3.3 Home Gateway Registration Phase

HG choose a identity ID_{HG} and sends the registration request to KGC. Upon receiving the request from HG, KGC issues a long-term secret key K_{HG}, the user identity ID_i, temporal identity TID_i, public parameters $h_j, x_j, j = 1, 2, \cdots, n$ and $H(s)$ to HG securely.

3.4 Login and Authentication Phase

LAP1. U_i firstly inputs ID_i and high entropy password PW_i^* and imprints personal biometrics BIO_i^* into UE_i. UE_i computes $\sigma_i^* = Rep(BIO_i^*, \tau_i)$ by the

reproduction algorithm if the Hamming distance between two biometrics is t or less. Then, UE_i calculates $A_i^* = H(ID_i \parallel PW_i^* \parallel \sigma_i^*)$, $B_i^* = H(ID_i \parallel A_i^* \parallel \sigma_i^*)$. UE_i utilized B_i^* to validate the user locally. After verifying the user's identity successfully, UE_i calculates symmetric key $K_i = A_i \oplus rPW_i^*$. UE_i randomly generates a nonce r_i and T_1. UE_i then calculates $M_1 = K_i \oplus r_i$, $M_2 = H(M_1 \parallel ID_i \parallel TID_i \parallel r_i \parallel T_1)$. UE_i sends $\langle TID_i, M_1, M_2, T_1 \rangle$ to HG via an open channel.

LAP2. Upon receiving the login request, HG firstly checks the freshness of the timestamp T_1. If it is true, HG retrieves ID_i, K_{HG} and computes $K_i^* = H(ID_i \parallel K_{HG}) = K_i$, $r_i^* = K_i^* \oplus M_1$, $M_3 = H(M_1 \parallel ID_i \parallel TID_i \parallel r_i^* \parallel T_1)$, and checks if $M_2 = M_3$. If valid, continue the session. Otherwise, HG terminates session immediately. Then, HG randomly generates a nonce r_{HG} and a timestamp T_2, and computes $m_{HG} = r_{HG} \times \chi$. HG calculates $M_4 = E_{r_{HG}}(ID_i, r_i^*, H(K_i))$, $M_5 = H(ID_i \parallel r_{HG} \parallel r_i^* \parallel H(K_i) \parallel M_4 \parallel T_2)$. Finally, HG broadcasts the message $\langle M_4, M_5, m_{HG}, T_2 \rangle$ to all the smart devices via an open channel.

LAP3. Upon receiving message, SD_j firstly checks the freshness of the message by timestamp T_2. If it is valid, SD_j calculates $F(c_j^*) = r_j^*$, $R_j^* = Rep(r_j^*, h_j)$, $p_j = RP_j \oplus R_j^*$, $s_j^* = share_j \oplus R_j^*$, $r_{HG}^* = m_{HG} \bmod p_j$ ($\chi \bmod p_j \equiv 1$, r_{HG} is a shared group key of all the legitimate smart devices). Then, SD_j decrypts M_4 as $ID_i, ID_{HG}, r_i^*, H(K_i)$ using shared group key r_{HG}^*, and compute $M_6 = H(ID_i \parallel r_{HG}^* \parallel r_i^* \parallel H(K_i) \parallel M_4 \parallel T_2)$ and check whether $M_5 = M_6$. If it is valid, SD_j terminates the request. Otherwise, SD_j generate a timestamp T_3 and calculates $M_{7_j} = E_{r_{HG^*}}(s_j, ISD_j)$, $M_{8_j} = H(s_j \parallel M_{7_j} \parallel ISD_j \parallel r_{HG}^* \parallel T_3)$. Finally, SD_j sends message $\langle M_{7_j}, M_{8_j}, T_3 \rangle$ to HG.

LAP4. After receiving $\langle M_{7_j}, M_{8_j}, T_3 \rangle$ from smart devices $SD_j, j = 1, 2, \cdots, m$. HG checks the freshness of timestamp T_3. If it is valid, HG can obtains s_j, ISD_j by using r_{HG} to decrypt M_{7_j}, and computes $s' = \sum_{j=1}^{m} s_j \prod_{r=1, r \neq j}^{m} \frac{-x_r}{x_j - x_r}$, HG also checks whether $H(s') = H(s)$. If it is true, continues the session. Otherwise, HG computes M_{9_j} and checks whether $M_{8_j} = M_{9_j}$ to verify SD_j. If it matches, the message is from valid SD_j. Otherwise, HG marks the invalid smart devices and terminates the session. Then, HG computes $M_{10} = H(H(s) \parallel r_{HG}), M_{11} = E_{r_{HG}}(M_{10}), M_{12} = H(M_{10} \parallel M_{11})$. Finally, HG sends $\langle M_{11}, M_{12} \rangle$ to smart devices.

LAP5. Each SD_j extracts M_{10} using shared group key r_{HG}^*, computes $M_{13} = H(M_{10} \parallel M_{11})$ and checks whether $M_{12} = M_{13}$. If it is valid, each SD_j computes $GSK = H(r_{HG}^* \parallel H(K_i) \parallel r_i^* \parallel ID_i \parallel M_{10})$, $M_{14} = H(r_{HG}^* \parallel ID_{HG} \parallel GSK)$. Finally, each SD_j sends message $\langle M_{14} \rangle$ to HG.

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

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 $(M_{10}, r^*_{HG}, r^*_i, ID_{HG})$. Then, UE_i checks whether $r_i = r^*_i$. If it matches, U_i calculates $GSK^* = H(r^*_{HG} \parallel H(K_i) \parallel r_i \parallel ID_i \parallel ID_{HG} \parallel M_{10}), M_{18} = H(r^*_{HG} \parallel ID_{HG} \parallel GSK^*), M_{19} = H(M_{18} \parallel M_{15} \parallel r_i \parallel T_4)$. UE_i checks if $M_{17} = M_{19}$. If it matches, the group session key is established successfully. Finally, UE_i replaces $TID^{new}_i = H(K^*_i \parallel TID_i \parallel T_4) \oplus M_{16}$ with new anonymous identity TID^{new}_i.

3.5 Biometrics and Password Update Phase

U_i provides personal credentials ID_i, PW^{old}_i and BIO^{old}_i to UE_i. UE_i utilizes these credentials validate the authenticity of U_i. If the credentials are valid, the credentials will be updated. When passing the validation, U_i enters the new credentials PW^{new}_i and biometrics BIO^{new}_i. UE_i utilizes these new credentials to compute new parameters and updates these parameters without the help of KGC.

4 Security Analysis

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

1. ***Participants:*** Let $\prod^u_{U_i}$, $\prod^v_{SD_j}$, $\prod^t_{HG}$ represent instances u, v and t of participant U_i, SD_j and HG, respectively.
2. ***Partnering:*** If the next conditions are satisfied, The instances $\prod^u_{U_i}$ and $\prod^v_{SD_j}$ are said to be partners [7].
   (i) both instance $\prod^u_{U_i}$ and $\prod^v_{SD_j}$ are accepted,
   (ii) both instances $\prod^u_{U_i}$ and $\prod^v_{SD_j}$ authenticate each other,
   (iii) the instance $\prod^u_{U_i}$ and the instance $\prod^v_{SD_j}$ are only partners each other.
3. ***Freshness:*** The instance $\prod^u_{U_i}$ or $\prod^v_{SD_j}$ is $fresh$ if the session key SK is not compromised to $\mathcal{A}$.
4. ***Adversary:*** $\mathcal{A}$ has all the capabilities as adversary in Dolev-Yao (DY) threat model [7] and also has some capabilities defined in CK-adversary model [2, 3]. Furthermore, $\mathcal{A}$ can make queries as $Execute(\prod_u, \prod_v)$, $Reveal(\prod^t)$, $Send(\prod^t, m)$, $CorruptUserEquipment(\prod^t_{U_i})$, $CorruptSmartDevice(\prod^t_{SD_j})$ and $Test(\prod^t)$ to challenger to obtain the sensitive information. These queries are utilized to construct a series of game. After games, $\mathcal{A}$ guesses a bit b' and wins the game only if $b' = b$. $Succ$ represents that $\mathcal{A}$ wins the game. The advantage of $\mathcal{A}$ in breaking the IND-CCA of our scheme $\mathcal{P}$ in PPT time is $Adv^{IND-CCA}_{\mathcal{P},\mathcal{A}}(\mathcal{K}) = |2 \cdot Pr[Succ] - 1|$. The proposed scheme $\mathcal{P}$ is secure under the ROR model when $Adv^{IND-CCA}_{\mathcal{P},\mathcal{A}}(\mathcal{K})$ is negligible.

Theorem 1. *Let $\mathcal{A}$ be the adversary running in the polynomial time t against our authentication scheme $\mathcal{P}$ 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 $\mathcal{A}$ in breaking scheme $\mathcal{P}$ in PPT is defined as follows*

$$Adv_{\mathcal{P},\mathcal{A}}^{AKA}(\mathcal{K}) \leq \frac{q_h^2}{|Hash|} + \frac{\left(q_{send} + q_e\right)^2}{2^{l^r}} + \frac{q_{send}}{2^{m-1} \cdot |Dic|} + \frac{2}{q} \cdot Adv_{\mathcal{P},\mathcal{A}}^{IND-CPA}(\mathcal{K}).$$

Un-traceability and User Anonymity. It is assumed that $\mathcal{A}$ has capabilities of intercepting all the message 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 r_{HG}, r_i, B_i, σ. Therefore, our scheme 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 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 un-traceability and user anonymity are both guaranteed in our scheme.

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. Suppose that $\mathcal{A}$ intercepts the message and tries to forge GSK' by random nonces r_i', r_{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 scheme guarantees session key security successfully.

Replay Attack. It is assumed $\mathcal{A}$ is capable to intercept all the message between the user, HG and smart devices. The transmitted messages usually involve the 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 scheme can resist replay attack.

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

Ephemeral Secret Leakage Attack. In our scheme, a secure group session key $GSK^* = H(r^*_{HG} \parallel H(K_i) \parallel r_i \parallel ID_i \parallel ID_{HG} \parallel M_{10})$ 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 r_{HG}. In particular, the secret S is computed by secret reconstruction algorithm of secret sharing technology. In addition, $ID_{HG}, ID_i, H(K_i)$ are the long-term secrets and r_i is a short-term secret. On the one hand, it is assumed that the short-term secrets r_{HG}, r_i are revealed to $\mathcal{A}$. However, it is computationally infeasible to compute the GSK due to lack of the long-term secrets. On the other hand, it is assumed that $\mathcal{A}$ can obtain the long-term secrets. Even through $\mathcal{A}$ obtain some secret shares s_j from the smart devices, it is computationally infeasible to construct the secret S and then calculate the M_{10}. The short-term secrets r_{HG}, r_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 r_{HG}, r_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 scheme can thwart ephemeral secret leakage attack.

5 Performance Analysis

We evaluate the communication and computational cost in our authentication scheme compared to other schemes [4,11,19]. The proposed scheme 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 suppose that the bit length of identities, random nonces, timestamps, hash function operation are 128bits, 128 bits, 32bits, 160 bits, respectively. It is also assumed that $|\lambda_1| = 128$, $|\lambda_2| = 160$ and AES-128 is adopted for symmetric cryptography, where λ_1, λ_2 denote the length of input and output of physical unclonable function, respectively. Table 2 show the total communication cost of our scheme and associated three schemes [4,11,19].

Table 2. Communication cost comparison.

Scheme	One device accessing cost (bits)	n devices accessing cost (ms)
[4]	2016	$2016n$
[11]	2048	$2048n$
[19]	2592	$2592n$
Our scheme	3296	$1376+1920n$

We compare the total execution time with other schemes [4,11,19] during the login and authentication phase. It is assumed that T_h, $T_{E/D}$, T_{fe}, T_{xor}, T_{ecm}, T_{mm}, T_{mac} and T_{hmac} denote the computational cost required for a 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 message authentication code (MAC) operation and a hashed MAC operation, respectively. The bit-wise XOR operation is not considered in the evaluation as the its computational cost is less than other operations. Besides, it is assumed that $T_h \approx T_{mac} \approx T_{hmac}$, $T_{fe} \approx T_{ecm}$ in our experiment according to [19]. The computational cost of T_h, $T_{E/D}$, T_{fe}, T_{mm} and T_{ecm} is 0.0026 ms, 0.00325 ms, 1.989, 0.171 ms and 1.989 ms (ms is the abbreviation of milliseconds), respectively. The computational cost of accessing a single and multiple devices for the related scheme and our scheme is described in the Table 3.

Table 3. Computational cost Comparison.

Scheme	One device accessing cost (ms)	n devices accessing cost (ms)
[4]	$T_{fe} + 16T_h + 13T_{ecm}$	$(T_{fe} + 16T_h + 13T_{ecm})n$
[11]	$T_{fe} + 19T_h + 8T_{E/D} + 3T_{ecm}$	$(T_{fe} + 19T_h + 8T_{E/D} + 3T_{ecm})n$
[19]	$T_{fe} + 21T_h + 8T_{E/D}$	$(T_{fe} + 21T_h + 8T_{E/D})n$
Our scheme	$T_{fe} + 20T_h + 8T_{E/D}$	$T_{fe} + 8T_h + 4T_{E/D} + (4T_{E/D} + 12T_h)n$

6 Conclusion

In this paper, we proposed a PUF-based two-factor anonymous group authentication scheme for smart home based on secret sharing technique and Chinese Remainder Theorem. The proposed scheme can withstand most of several known attacks, which is proved under ROR model and security discussion. Compared with other related schemes, our scheme can effectively reduce the resource cost during the login and authentication phase. In addition, our smart devices protected by physical unclonable function are secure against device capturing attack.

References

1. Banerjee, S., Odelu, V., Das, A.K., Chattopadhyay, S., Rodrigues, J.J.P.C., Park, Y.: Physically secure lightweight anonymous user authentication protocol for Internet of Things using physically unclonable functions. IEEE Access **7**, 85627–85644 (2019)
2. Canetti, R., Krawczyk, H.: Analysis of key-exchange protocols and their use for building secure channels. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 453–474. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_28. http://dl.acm.org/citation.cfm?id=647086.715688
3. Canetti, R., Krawczyk, H.: Universally composable notions of key exchange and secure channels. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 337–351. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_22
4. Challa, S., et al.: Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access **5**, 3028–3043 (2017)

5. Chiang, M., Zhang, T.: Fog and IoT: an overview of research opportunities. IEEE Internet of Things J. **3**(6), 854–864 (2016)
6. He, D., Kumar, N., Chilamkurti, N.: 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, November 2013
7. Dolev, D., Yao, A.: On the security of public key protocols. IEEE Trans. Inf. Theory **29**(2), 198–208 (1983)
8. Kalra, S., Sood, S.K.: Advanced password based authentication scheme for wireless sensor networks. J. Inf. Secur. Appl. **20**, 37–46 (2015). Security, Privacy and Trust in Future Networks and Mobile Computing
9. Kumar, P., Braeken, A., Gurtov, A., Iinatti, J., Ha, P.H.: Anonymous secure framework in connected smart home environments. IEEE Trans. Inf. Forensics Secur. **12**(4), 968–979 (2017)
10. Li, X., Niu, J., Bhuiyan, M.Z.A., Wu, F., Karuppiah, M., Kumari, S.: A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things. IEEE Trans. Ind. Inf. **14**(8), 3599–3609 (2018)
11. Li, X., Peng, J., Niu, J., Wu, F., Liao, J., Choo, K.R.: A robust and energy efficient authentication protocol for industrial Internet of Things. IEEE Internet of Things J. **5**(3), 1606–1615 (2018)
12. Jiang, L., Liu, D.-Y., Yang, B.: Smart home research. In: Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 04EX826), vol. 2, pp. 659–663, August 2004
13. Odelu, V., Das, A.K., Goswami, A.: A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans. Inf. Forensics Secur. **10**(9), 1953–1966 (2015)
14. Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., Loge, C.: The smart home concept: our immediate future. In: 2006 1ST IEEE International Conference on E-Learning in Industrial Electronics, pp. 23–28, December 2006
15. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., Tang, Y.: Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J. Netw. Comput. Appl. **106**, 117–123 (2018)
16. Srinivas, J., Das, A.K., Wazid, M., Kumar, N.: Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. IEEE Trans. Dependable Secure Comput. 1 (2018)
17. Turkanović, M., Brumen, B., Hölbl, M.: A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Netw. **20**, 96–112 (2014)
18. Wallrabenstein, J.R.: 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, August 2016
19. Wazid, M., Das, A.K., Odelu, V., Kumar, N., Jo, M.: Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet of Things J. **PP**(99), 1 (2017)
20. Ye, X., Huang, J.: A framework for cloud-based smart home. In: Proceedings of 2011 International Conference on Computer Science and Network Technology, vol. 2, pp. 894–897, December 2011

21. Xue, K., Ma, C., Hong, P., Ding, R.: A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. J. Netw. Comput. Appl. **36**(1), 316–323 (2013). http://www.sciencedirect.com/science/ARTICLE/pii/S1084804512001403
22. Zhang, J., Cui, J., Zhong, H., Chen, Z., Liu, L.: PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. IEEE Trans. Dependable Secure Comput. 1 (2019). https://doi.org/10.1109/TDSC.2019.2904274