IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 August 2022, accepted 17 September 2022, date of publication 21 September 2022,
date of current version 29 September 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3208347*

RESEARCH ARTICLE

# A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF

**YEONGJAE CHO[1], JIHYEON OH[1], DEOKKYU KWON[1], SEUNGHWAN SON[1], JOONYOUNG LEE[1], (Student Member, IEEE), AND YOUNGHO PARK[1,2], (Member, IEEE)**
[1]School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea
[2]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

Corresponding author: Youngho Park (parkyh@knu.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) through the Ministry of Education under Grant 2020R1I1A3058605; and in part by the Korean Government through the Electronics and Telecommunications Research Institute (ETRI), Core Technology Research on Trust Data Connectome, under Grant 22ZR1330.

**ABSTRACT** With the continuous development of Internet of Things (IoT) technology, research on smart home environments is being conducted by many researchers. In smart home environments, home users can remotely access and control a variety of home devices such as smart curtains, lights, and speakers placed throughout the house. Despite providing convenient services, including home monitoring, temperature management, and daily work assistance, smart homes can be vulnerable to malicious attacks because all messages are transmitted over insecure channels. Moreover, home devices can be a target for device capture attacks since they are placed in physically accessible locations. Therefore, a secure authentication and key agreement scheme is required to prevent such security problems. In 2021, Zou *et al.* proposed a two-factor-based authentication and key agreement scheme using elliptic curve cryptography (ECC) in smart home environments. They claimed that their scheme provides user anonymity and forward secrecy. However, we prove that their scheme suffers from forgery, ephemeral secret leakage, and session key disclosure attacks. To overcome the security vulnerabilities of Zou *et al.*'s scheme and provide home users with secure communication in smart home environments, we propose a secure user authentication scheme using physical unclonable functions (PUF). We utilize Real-or-Random (ROR) model and Burrows-Abadi-Needham (BAN) logic to verify the session key security and mutual authentication of the proposed scheme, respectively. Furthermore, we use the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool to simulate the resistance of our scheme to security attacks. After that, we analyze and compare the communication costs, computational consumption, and security functionalities along with related schemes.

**INDEX TERMS** Internet of Things, smart home, authentication, physical unclonable functions, ROR model, BAN logic, AVISPA.

## I. INTRODUCTION

With the development of Internet of Things (IoT) technology over the past few years, the smart home has attracted various interests from researchers [1]. The smart home is a system architecture utilizing a wireless sensor network (WSN) of multiple sensors interacting via IoT technology. Smart home environments provide users with various home services, including daily work support, house monitoring, and energy management [2]. As shown in Figure 1, entities in smart home environments consist of home devices, gateway, and home users (i.e., residents). Home devices are placed in the user's home to collect and transmit various data such as brightness, temperature, and humidity to the home user. The

The associate editor coordinating the review of this manuscript and approving it for publication was Chakchai So-In.

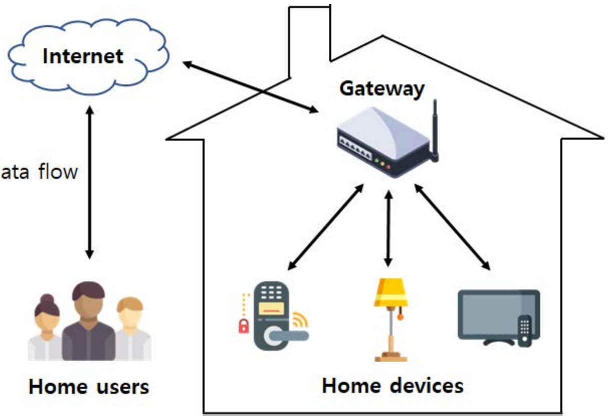


**FIGURE 1.** Architecture of smart home environments.

gateway acts as a relay for the exchange of messages between users and home devices. As a resident, users can access and control their home devices remotely via the Internet to use home services. Recently, the smart home environment has been studied from various aspects such as interoperability and energy consumption, thereby efficient smart home services are provided to home users [3].

Despite these efforts, there are several security issues that need to be considered for secure smart home environments. In smart home environments, entities communicate over public channels where messages can be eavesdropped, inserted or deleted by malicious adversary. This allows the adversary to attempt a variety of security attacks, including man-in-the-middle (MITM), user impersonation, and replay attacks [4], [5], [6], [7]. Through these attacks, the adversary can threaten the anonymity and privacy of users by obtaining the user's real identity and information. Furthermore, the adversary can perform a device capture attack that compromises the entire system by capturing physically accessible home devices [8]. In the past few years, various security threats such as monitoring electricity consumption and malicious control of home appliances are occurring in the actual smart home environments [9]. These security threats can negatively affect user's anonymity and the reliability of smart home environments. Therefore, a secure and anonymous authentication scheme is essential to resist various security problems and use smart home services securely.

In 2021, Zou *et al.* [10] suggested user authentication scheme utilizing elliptic curve cryptography (ECC) for secure smart home environments in IoT. They claimed that their scheme provides user anonymity and forward secrecy. However, we prove that their scheme is vulnerable to forgery, ephemeral secret leakage, and session key disclosure attacks. Then, we demonstrate that their scheme does not guarantee mutual authentication between home users and home devices. To overcome the security vulnerabilities of Zou *et al.*'s scheme, we suggest a secure and anonymous authentication scheme. Moreover, we use physical unclonable functions (PUF) [11] to prevent device capture attacks in smart home environments.

### A. OUR CONTRIBUTIONS

The contributions of this paper are summarized below:

- We prove that Zou *et al.*'s scheme is vulnerable to forgery, ephemeral secret leakage, and session key disclosure attacks. Then, we propose a secure and anonymous PUF-based authentication scheme to overcome the security vulnerabilities of Zou *et al.*'s scheme. We demonstrate that our scheme guarantees user anonymity and resistance to various security attacks.
- We conduct informal security analysis to verify the resistance for well-known security attacks and Real-or-Random (ROR) model [12] to prove the session key security in the proposed scheme.
- We use Burrows-Abadi-Needham (BAN) logic [13] to validate that the proposed scheme performs mutual authentication and key agreement correctly. We also simulate Automated Validation of Internet Security Protocols and Applications (AVISPA) [14] to verify that our scheme is resistant to replay and MITM attacks.
- We compare the security property of the proposed scheme with existing related schemes. Furthermore, we evaluate the communication cost and computational consumption of our scheme and compare them with other authentication schemes.

### B. ORGANIZATION

The remainder of this paper is organized as follows. Section II describes existing related works. Section III introduces our scheme's system model, PUF, fuzzy extractor, notations, and threat model. In Section IV and Section V, we briefly review and analyze Zou *et al.*'s scheme. Then, we present the proposed scheme in Section VI. In Section VII, we evaluate security analysis using BAN logic, ROR model, and AVISPA simulation along with informal analysis. Section VIII demonstrates the security and efficiency performance of our scheme, and Section IX is the conclusion.

## II. RELATED WORK

User authentication schemes for secure smart home environments have been proposed over the past few years. In 2015, Chen *et al.* [15] argued that user authentication is a significant security issue for WSNs due to sensors are placed in locations where an adversary can easily access them. Therefore, they suggested a user authentication scheme using symmetric key cryptography to provide users with secure communication. However, Jung *et al.* [16] pointed out that their scheme cannot provide anonymity because Chen *et al.*'s scheme transmits the user identity in plaintext to the gateway. Thus, Jung *et al.* proposed an enhanced authentication and key agreement scheme that guarantees user anonymity. However, Xiang *et al.* [17] analyzed that their scheme [16] does not provide the perfect forward secrecy. In 2016, Kumar *et al.* [18] suggested an authentication scheme for the smart home using cipher block chaining message authentication code (CBC-MAC). Unfortunately, Fakroon *et al.* [19] analyzed that Kumar *et al.*'s scheme is vulnerable to impersonation and password guessing attacks. Moreover, Fakroon *et al.* argued that the design of an efficient authentication scheme is necessary in the smart home because the home device has limited resources. Therefore, Fakroon *et al.* proposed a hash-based user authentication scheme utilizing physical context awareness and transaction history. Although their scheme [19] achieves an efficient computational cost, they suffer from a variety of security attacks, including offline password guessing and insider attacks [20].

Recently, user authentication schemes based on ECC and user biometric information have been proposed. In 2018, Li *et al.* [21] suggested a user authentication scheme using ECC and fuzzy extractor. They claimed that their scheme ensures the legality of data access. In 2019, Naoui *et al.* [22] suggested a user authentication scheme using symmetric key cryptography and ECC for smart home environments. They argued that their scheme is suitable for resource-constrained devices because the gateway computes a large part of the key agreement phase between the user and the home device. In the same year, Shuai *et al.* [23] argued that the authentication scheme that stores a verification table in the gateway can be compromised from the verifier stolen attack by the adversary. Therefore, they proposed an ECC-adopted authentication scheme without verification table. However, their schemes [21], [22], [23] have a high computational consumption because they used elliptic curve scalar multiplication. Furthermore, their schemes does not resist device capture attacks [10].

In smart home environments, device capture attack is a significant security issue since an adversary can compromise the entire system by physically accessing the home device. Therefore, PUF-adopted authentication schemes have been proposed to prevent this security vulnerability. In 2020, Liu *et al.* [24] suggested authentication and key agreement scheme using PUF. They claim that their scheme prevents device capture attack because each sensor in their PUF-based scheme has a unique challenge-response pair. In 2021, Chen and Chen [25] proposed a PUF-based authentication and key agreement scheme. They asserted that MITM and tampering attacks are powerless against their scheme due to the proposed scheme performs mutual authentication based on the secret key generated by the PUF response. Xia *et al.* [26] proposed a PUF-assisted group authentication scheme for the smart home that establishes a group session key between the home user and the home device by utilizing the chinese remainder theorem. Although their schemes [24], [25], [26] resist device capture attack utilizing PUF, they does not consider the verifier stolen attack, which can compromise all user communications by exploiting the verification table stored on the gateway.

In 2021, Zou *et al.* [10] suggested a user authentication and key agreement scheme utilizing ECC for the smart home. They claimed that their scheme is secure against various security problems, including user impersonation and device capture attacks. However, we conduct a careful analysis to prove that their scheme is vulnerable to forgery, ephemeral secret leakage, and session key disclosure attacks. Moreover, their scheme does not succeed in providing mutual authentication. Therefore, we propose a PUF-based user authentication scheme that overcomes the vulnerabilities of Zou *et al.*'s scheme and considers the security problems in smart home environments.

## III. PRELIMINARIES

In this section, we describe the system model, PUF, fuzzy extractor, notations, and threat model to review the Zou *et al.*'s scheme and to help the understanding of our proposed scheme.

### A. SYSTEM MODEL

The entities in our system model are composed of the registration center, home users, gateway, and home devices. In our scheme, home users store secret credentials on a smart card by registering in the registration center. Similarly, home devices register with the registration center to generate a unique secret key using PUF. The gateway maintains a verification table to authenticate home users and home devices. Afterword, home users and home devices perform mutual authentication with each other using the secret credentials and secret key generated during the registration phase. If mutual authentication succeeds, home users, gateway, and home devices compute a shared session key and use it to communicate with each other. Descriptions of each entity are as follows.

- **Registration center:** The registration center registers the home users and home devices in the smart home. In our system model, the registration center is regarded as a fully trusted entity.
- **Home users:** These are residents of the smart home. Before using the smart home service, home users register with the registration center. Home users can authenticate with home devices using a smart card obtained from the registration center.
- **Gateway:** The gateway oversees public channel communication of entities. The gateway supports mutual authentication between home users and home devices.
- **Home devices:** Before home devices are deployed in the smart home, they register with the registration center to obtain secret credentials. Using these secret credentials, home devices authenticate with home users during the login and verification phase.

### B. PHYSICAL UNCLONABLE FUNCTION (PUF)

PUF is built into the hardware and operates as a one-way function. When a PUF is embedded in an integrated circuit, it can use the physical uniqueness of a device as an arbitrary source [11]. This arbitrary source is utilized to generate the output value of the PUF. Therefore, a unique response value is an output when a random challenge value is an input to the PUF device (i.e., a challenge-response pair). Because PUF is based on the physical properties of the device, it is impossible to replicate and predict even if the manufacturing process is reproduced. The characteristics of PUF used in our paper are summarized below.

- When $C$ is the challenge and $R$ is the response, $PUF(C) = R$.
- Even if the challenge value is known, it is impossible to predict the response value of a specific device.
- All PUF devices output different response values even if the same challenge value is input.

To utilize the characteristics of PUF for authentication, it is necessary to stabilize the noise that occurs when the response is generated. We use a fuzzy extractor to remove the noise of the PUF and extract a constant output.

### C. FUZZY EXTRACTOR

Fuzzy extractor [27] is a technology that generates a fixed secret key when a noise-containing value is input. When the fuzzy extractor receives an input value, it generates a bit string $s$ as a secret key and a helper bit string $h$ for error correction. Even if there is a slight error in the input value, the fuzzy extractor can extract the same secret key with the help of helper bit string. In our scheme, we use the generation and reproduction functions of the fuzzy extractor. The description of each function is as follows.

- $Gen(Y) = (h, s)$: Generation function generates helper bit string $h$ and secret bit string $s$ by inputting a random value $Y$ including noise.
- $Rep(Y', h) = s'$: Reproduction function extracts the secret bit string $s'$ using a random value $Y'$ containing noise and the helper bit string $h'$. The generated $s'$ is the same as the generated $s$ in $Gen(Y)$.

### D. NOTATIONS

The notations used in our paper are listed in Table 1.

### E. THREAT MODEL

We consider Dolev-Yao (DY) model [28] for security analysis of our scheme. DY model is a popular analysis tool used for security analysis of multiple authentication schemes. Under the DY model, a malicious adversary can control all messages exchanged in public channels. Furthermore, we apply Canetti-Krawczyk (CK) model [29] to validate the security of our scheme on a more robust adversary assumption. In the CK model, the adversary can corrupt the session state and obtain the short-term key or long-term key. According to the DY model and the CK model, we assume that the adversary's capabilities are as follows:

- The adversary can completely control communications over public channels by interfering with, modifying, or deleting messages. Then, the adversary can attempt passive or active security attacks.
- The adversary can conduct offline password guessing attack within the polynomial time using dictionary attack [30].
- Under the CK model assumption, the adversary can obtain session-specific temporary information, such as a random nonce generated in each session. Thereafter, the adversary tries to compute the session key [31].
- The adversary can extract the sensitive information stored in the user smart card or the home device using a power analysis attack [32]. The adversary can use this information to attempt to generate a valid authentication message.
- The adversary can register as a legitimate user of the smart home. The adversary then attempts to impersonate another legitimate user with his/her secret credentials.

**TABLE 1. Notations.**

| Symbol | Description |
|---|---|
| $ID_i$, $PW_i$ | Identity and password of home user |
| $PID_i$ | Temporary identity of home user |
| $SID_j$ | Identity of home device |
| $RID_i$, $DID_j$ | Pseudo identity of home user and home device |
| $K_{GU}$, $K_{GS}$ | Secret key of home user and home device |
| $K_{UG_i}$, $K_{HD_j}$ | Long-term key of home user and home device |
| $s$, $t$, $b$ | Master key of registration center, gateway, and home device |
| $C_j$, $R_j$ | Challenge and response of PUF |
| $n_0$, $w$ | Fuzzy verifier |
| $PUF(.)$ | PUF operation |
| $SK$ | Session key |
| $a_1$, $a_2$, $a_3$ | Random nonce |
| $Gen(.)/Rep(.)$ | Generation/reproduction function |
| $h(.)$ | One-way hash function |
| $\oplus$ | Exclusive-OR (XOR) operation |
| $\|\|$ | Message concatenation operarion |

## IV. REVIEW OF ZOU *et al.*'s SCHEME

In this section, we quickly review Zou *et al.*'s user authentication scheme. Zou *et al.*'s scheme has system setup, home device registration, home user registration, login and verification, and password update phases. A detailed description of each phase is as follows.

### A. SYSTEM SETUP PHASE

In the system setup phase, the gateway chooses an elliptic curve $E(F_p)$ and a base point $P$ on the finite field. Then, the gateway generates long-term key $x \in F_p$ and computes $h(GID||x)$ as secret parameter. The gateway publishes $X = x \cdot P$ as an open parameter of the system.

### B. HOME DEVICE REGISTRATION PHASE

Before deploying the home device to the smart home, the home device registers to the gateway as shown in Figure 2.

- HDR 1: The home device selects $SID_j$ and sends it to the gateway.

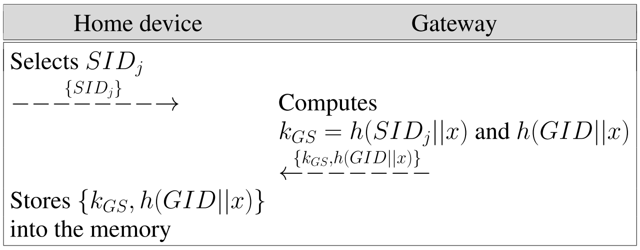


**FIGURE 2.** Home device registration phase of Zou *et al.*'s scheme.

- HDR 2: After receiving $SID_j$, the gateway computes $k_{GS} = h(SID_j||x)$ and transmits to the home device.
- HDR 3: Then, the home device stores $\{k_{GS}, h(GID||x)\}$ into the home device's memory.

### C. HOME USER REGISTRATION PHASE

Figure 3 shows the home user registration phase of Zou *et al.*'s scheme. In this phase, the home user registers with the gateway to use the smart home service.

- HUR 1: The home user selects $ID_i, PW_i$ and random number $r$. Then, the home user computes $HID_i = h(ID_i||PW_i)\ mod\ n_0$, $A_0 = HPW_i \oplus r$ and sends $A_0$ to the gateway.
- HUR 2: After receiving $A_0$, the gateway computes $K_{GU} = h(A_0||x)$, $A_1 = k_{GU} \oplus A_0$ and sends $\{A_1, SUM = 0\}$ to the home user. $SUM$ is the number of allowed login attempts, and is discarded when $SUM$ exceeds the threshold.
- HUR 3: Upon receiving $\{A_1, SUM = 0\}$, home user computes $k_{GU} = A_0 \oplus A_1$, $A_2 = h(ID_i||PW_i||k_{GU})\ mod\ n_0$ and stores $\{A_1, A_2, SUM = 0\}$ into home user's smart card.

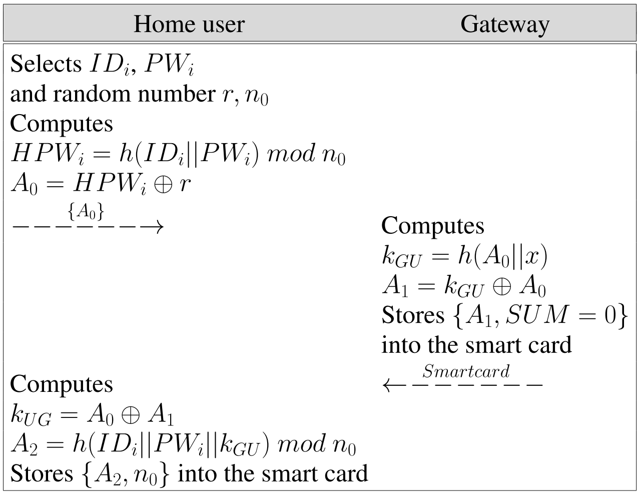

Home user
Gateway
Selects $ID_i$, $PW_i$
and random number $r$, $n_0$
Computes
$HPW_i = h(ID_i||PW_i)\ mod\ n_0$
$A_0 = HPW_i \oplus r$
$\{A_0\}$
Computes
$k_{GU} = h(A_0||x)$
$A_1 = k_{GU} \oplus A_0$
Stores $\{A_1, SUM = 0\}$
into the smart card
$Smartcard$
Computes
$k_{UG} = A_0 \oplus A_1$
$A_2 = h(ID_i||PW_i||k_{GU})\ mod\ n_0$
Stores $\{A_2, n_0\}$ into the smart card

**FIGURE 3.** Home user registration phase of Zou *et al.*'s scheme.

### D. LOGIN AND VERIFICATION PHASE

As shown in Figure 4, the home user and the home device authenticate each other using their secret credentials and establish a shared session key.

- LAV 1: The home user enters $ID_i$, $PW_i$ into the smart card. Then, home user computes $HPW_i' = h(ID_i'||PW_i')$ $mod\ n_0$, $k_{GU}' = HPW_i' \oplus A_1$, $A_2' = h(ID_i'||PW_i'||k_{GU}')$ $mod\ n_0$. If $A_2'$ is not the same as $A_2$ stored in the smart card, the session is terminated and $SUM = SUM + 1$. Otherwise, home user selects random numbers $a$, $r_1$, $r_1^+$ and timestamp $T_u$. Then, home user computes $A_4 = r_1 \cdot P$, $w = r_1 \cdot X$, $DID_i = h(r_1||a) \oplus w$, $M_1 = (r_1^+||SID_j) \oplus h(r_1||a)$, $V_1 = h(h(r_1||a)||r_1^+||M_1||SID_j||T_u)$ and transmits $\{DID_i, A_4, M_1, V_1, T_u\}$ to the gateway via public channels.
- LAV 2: After receiving the message, the gateway verifies the freshness of timestamp and calculates $h(r_1'||a') = DID_i \oplus x \cdot A_4$, $(r_1^{+'}||SID_j') = M_1 \oplus h(r_1'||a')$, $V_1' = h(h(r_1'||a')||r_1^{+'}||M_1||SID_j'||T_u)$. When $V_3'$ is valid, the gateway selects random nonce $r_2$ and timestamp $T_g$. After that, the gateway computes $k_{GS} = h(SID_j||x)$, $M_2 = (h(r_1||a)||GID||A_4||r_2||SID_j) \oplus k_{GS}$, $V_2 = h(SID_j||h(r_1||a)||GID||k_{GS}||A_4||r_2||T_g)$ and sends the message $\{M_2, V_2, T_g\}$ to the home device via public channels.
- LAV 3: Upon receiving the message from the gateway, the home device verifies $|T_g' - T_g| < \triangle T$. If the condition is satisfied, the home device calculates $(h(r_1'||a')||GID'||A_4'||r_2'||SID_j') = M_2 \oplus k_{GS}$, $V_2' = h(SID_j||h(r_1'||a')||GID'||k_{GS}||A_4'||r_2'||T_g)$. If $V_2'$ equals $V_2$, the home device generates $r_3$ as a random nonce and $T_d$ as a timestamp. Then, the home device computes $A_5 = r_3 \cdot P$, $A_6 = r_3 \cdot A_4$, $SK = h(h(r_1||a)||A_6)$, $M_3 = SID_j \oplus h(GID||x)$, $N_3 = (A_5||h(SK||r_2)) \oplus k_{GS}$, $V_3 = h(A_5||h(SK||r_2)||k_{GS}||T_d)$, $Y_3 = h(SK||A_5) \oplus h(SK||r_2) \oplus k_{GS}$ and transmits $\{M_3, N_3, V_3, Y_3, T_d\}$ to the gateway.
- LAV 4: Upon getting $\{M_3, N_3, V_3, Y_3, T_d\}$, the gateway verifies the timestamp's validation and calculates $SID_j' = M_3 \oplus h(GID||x)$, $k_{GS}' = h(SID_j'||x)$, $(A_5'||h(SK'||r_2')) = N_3 \oplus k_{GS}'$, $V_3' = h(A_5'||h(SK'||r_2')||k_{GS}'||T_d)$. If $V_3'$ is same as $V_3$, the gateway computes $h(SK||A_5) = Y_3 \oplus h(SK||r_2) \oplus k_{GS}$, $M_4 = A_5 \oplus x \cdot A_4$, $V_4 = h(h(SK||A_5)||x \cdot A_4)$ and transmits $\{M_4, V_4\}$ to the home user.
- LAV 5: After receiving the message from the gateway, home user computes $A_5' = M_4 \oplus w$, $A_6' = r_1 \cdot A_5'$, $SK' = h(h(r_1||a)||A_6')$, $V_4' = h(h(SK'||A_5')||w)$. If $V_4'$ is valid, session key agreement is completed.

### E. PASSWORD UPDATE PHASE

In this phase, the home user changes their password. The home user inputs his/her $ID_i'$, $PW_i'$ into the smart card. Then, the home user computes $HPW_i' = h(ID_i'||PW_i')$ $mod$ $n_0$, $k_{GU}' = HPW_i' \oplus A_1$, $A_2' = h(ID_i'||PW_i'||k_{GU}')$ $mod$ $n_0$. If $A_2'$ is invalid, this phase is terminated. Otherwise, the home user enters new password $PW_i^{new}$ and computes $HPW_i' = h(ID_i'||PW_i^{new})$ $mod$ $n_0$, $A_1^{new} = k_{GU}' \oplus HPW_i'$,

<table>
<tr><th>Home user/smart card</th><th>Gateway</th><th>Home device</th></tr>
<tr><td>Enters $ID_i^{'}$ and $PW_i^{'}$<br>Computes<br>$HPW_i^{'} = h(ID_i^{'}||PW_i^{'})\ mod\ n_0$<br>$k_{GU}^{'} = HPW_i^{'} \oplus A_1$<br>$A_2^{'} = h(ID_i^{'}||PW_i^{'}||k_{UG}^{'})\ mod\ n_0$<br>Checks $A_2^{'} \overset{?}{=} A_2$<br>If $A_2^{'} \neq A_2$, $SUM = SUM + 1$<br>Generates random nonces $a$, $r_1$, $r_1^{+} \in Z_p^*$<br>and timestamp $T_u$<br>Computes<br>$A_4 = r_1 \cdot P$<br>$w = r_1 \cdot X$<br>$DID_i = h(r_1||a) \oplus w$<br>$M_1 = (r_1^{+}||SID_j) \oplus h(r_1||a)$<br>$V_1 = h(h(r_1||a)||r_1^{+}||M_1||SID_j||T_u)$<br>$\xrightarrow{\{DID_i, A_4, M_1, V_1, T_u\}}$</td><td></td><td></td></tr>
<tr><td></td><td>Checks if $|T_u^{'} - T_u| < \triangle T$<br>Computes<br>$h(r_1^{'}||a^{'}) = DID_i \oplus x \cdot A_4$<br>$(r_1^{+'}||SID_j^{'}) = M_1 \oplus h(r_1^{'}||a^{'})$<br>$V_1^{'} = h(h(r+1^{'}||a^{'})||r_1^{+'}||M_1||SID_j^{'}||T_u)$<br>Checks $V_1^{'} \overset{?}{=} V_1$<br>Generates a random nonce $r_2$<br>and timestamp $T_g$<br>Computes<br>$k_{GS} = h(SID_j||x)$<br>$M_2 = (h(r_1||a)||GID||A_4||r_2||SID_j) \oplus k_{GS}$<br>$V_2 = h(SID_j||h(r_1||a)||GID||k_{GS}||A_4||r_2||T_g)$<br>$\xrightarrow{\{M_2, V_2, T_g\}}$</td><td></td></tr>
<tr><td></td><td></td><td>Checks if $|T_g^{'} - T_g| < \triangle T$<br>Computes<br>$(h(r_1^{'}||a^{'})||GID^{'}||A_4^{'}||r_2^{'}||SID_j^{'}) = M_2 \oplus k_{GS}$<br>$V_2^{'} = h(SID_j||h(r_1^{'}||a^{'})||GID^{'}||k_{GS}||A_4^{'}||r_2^{'}||T_g)$<br>Checks $V_2^{'} \overset{?}{=} V_2$<br>Generates a random nonce $r_3$<br>and timestamp $T_d$<br>Computes<br>$A_5 = r_3 \cdot P$<br>$A_6 = r_3 \cdot A_4$<br>$SK = h(h(r_1||a)||A_6)$<br>$M_3 = SID_j \oplus h(GID||x)$<br>$N_3 = (A_5||h(SK||r_2)) \oplus k_{GS}$<br>$V_3 = h(A_5||h(SK||r_2)||k_{GS}||T_d)$<br>$Y_3 = h(SK||A_5) \oplus h(SK||r_2) \oplus k_{GS}$<br>$\xleftarrow{\{M_3, N_3, V_3, Y_3, T_d\}}$</td></tr>
<tr><td></td><td>Checks if $|T_d^{'} - T_d| < \triangle T$<br>Computes<br>$SID_j^{'} = M_3 \oplus h(GID||x)$<br>$k_{GS}^{'} = h(SID_j^{'}||x)$<br>$(A_5^{'}||h(SK^{'}||r_2)) = N_3 \oplus k_{GS}^{'}$<br>$V_3^{'} = h(A_5^{''}||h(SK^{'}||r_2^{'})||k_{GS}^{'}||T_d)$<br>Checks $V_3^{'} \overset{?}{=} V_3$<br>Computes<br>$h(SK||A_5) = Y_3 \oplus h(SK||r_2) \oplus k_{GS}$<br>$M_4 = A_5 \oplus x \cdot A_4$<br>$V_4 = h(h(SK||A_5)||x \cdot A_4)$<br>$\xleftarrow{\{M_4, V_4\}}$</td><td></td></tr>
<tr><td>Computes<br>$A_5^{'} = M_4 \oplus w$<br>$A_6^{'} = r_1 \cdot A_5^{'}$<br>$SK^{'} = h(h(r_1||a)||A_6^{'})$<br>$V_4^{'} = h(h(SK^{'}||A_5^{'})||w)$<br>Checks $V_4^{'} \overset{?}{=} V_4$</td><td></td><td></td></tr>
</table>

**FIGURE 4.** Login and verification phase of Zou *et al.*'s scheme.

$A_2^{new} = h(ID_i^{\prime}||PW_i^{new}||k_{GU}^{\prime})\ mod\ n_0$. After that, the home user replaces $\{A_1, A_2\}$ with $\{A_1^{new}, A_2^{new}\}$.

## V. SECURITY ANALYSIS OF ZOU *et al.*'s SCHEME

As reviewed in Section IV, Zou *et al.*'s scheme is designed for secure communication between home users and home devices using ECC. However, Zou *et al.*'s scheme has several security vulnerabilities. We prove in this section that their scheme is vulnerable to forgery, ephemeral secret leakage, and session key disclosure attacks. Subsequently, we explain that their scheme cannot achieve mutual authentication.

### A. FORGERY ATTACK

According to the threat model assumptions in Section III-E, the adversary can attempt a power analysis attack on the home device to extract $h(GID||x)$. Using $h(GID||x)$ and $M_3$, the adversary can compute $SID_j = M_3 \oplus h(GID||x)$ of any home device because $h(GID||x)$ is the same for all home devices. After that, the adversary generates random nonces $a^A, r_1^A, r_1^{+A}$ and computes $A_4^A = r_1^A \cdot P$, $w^A = r_1^A \cdot X$, $DID_i^A = h(r_1^A||a^A) \oplus w^A$, $M_1^A = (r_1^{+A}||SID_j) \oplus h(r_1^A||a^A)$, $V_1^A = h(h(r_1^A||a^A)||r_1^{+A}||M_1^A||SID_j||T_u^A)$. Then, the adversary can transmits valid authentication request message $\{DID_i^A, A_4^A, M_1^A, V_1^A, T_u^A\}$ to the gateway. Thus, Zou *et al.*'s scheme is vulnerable to forgery attack.

### B. EPHEMERAL SECRET LEAKAGE ATTACK

In this attack, the adversary can compute a session key by obtaining a random nonce generated in each session. If the adversary obtains $a, r_1, r_1^+$, he can compute $w = r_1 \cdot X$, $A_5 = M_4 \oplus w$, $A_6 = r_1 \cdot A_5$ where $X$ and $M_4$ is a system parameter and public message, respectively. Using these information, the adversary can successfully calculates the session key $SK = h(h(r_1||a)||A_6)$. Therefore, Zou *et al.*'s scheme cannot resist ephemeral secret leakage attack.

### C. SESSION KEY DISCLOSURE ATTACK

The session key of Zou *et al.*'s scheme consists only of short-term keys. Under the CK model, a malicious adversary can corrupt the session state or acquire short-term keys. As described in section V-B, if a malicious adversary obtains a public channel message and a short-term key, it can easily compute the current session key. Therefore, Zou *et al.*'s scheme is vulnerable to session key disclosure attack.

### D. LACK OF MUTUAL AUTHENTICATION

Zou *et al.* argued that their scheme provides mutual authentication between home users and home devices. However, as demonstrated in Section V-A, the adversary can use $h(GID||x)$ stored in the home devices to authenticate with any home device. Furthermore, Section V-B showed that the current session key is calculated when the short-term key is leaked to the adversary. Therefore, Zou *et al.*'s scheme does not achieve mutual authentication.

## VI. PROPOSED SCHEME

In this section, we propose a PUF-based user authentication scheme for smart home that overcomes the security vulnerabilities of Zou *et al.*'s scheme. The proposed scheme consists of system setup, home device registration, home user registration, login and verification, and password update phases. The following subsections describe each phase.

### A. SYSTEM SETUP PHASE

Before the gateway and home device are deployed in the smart home, the registration center generates $t$ as the gateway's master key and $C_j$ as the home device's challenge value. After that, the registration center stores it securely in each entity's memory. The registration center selects one-way hash function $h(.) : \{0, 1\}^* \rightarrow \{0, 1\}^l$ as system parameter and the master key of the home device $b$ is deployed during the device production process.

### B. HOME DEVICE REGISTRATION PHASE

In this phase, the home device stores secret credentials in its memory by registering with the registration center. Messages in this phase are exchanged on a secure channel. As shown in Figure 5, the detailed process is as follows.

- HDR 1: The home device computes $X_j = h(SID_j||b)$, $R_j = PUF(C_j)$, $Gen(R_j) = (D_j, HS_j)$, where $SID_j$ is the unique identity of the home device, and sends $\{SID_j, C_j, X_j\}$ to the registration center.
- HDR 2: The registration center verifies that $HDC_j = h(SID_j||s)$ is stored in its database. If $HDC_j$ exists in the database, the registration center terminates this phase. Otherwise, the registration center stores it into the database and computes $K_{HD_j} = h(h_j||SID_j||s)$,$DID_j = h(SID_j||h_j||K_{HD_j})$, $PD_j = h(K_{HD_j}||X_j)$, $B_j = h_j \oplus h(DID_j||t)$. After that, the registration center stores $\{DID_j, C_j, PD_j, B_j\}$ into the memory of $GW$ and transmits $\{DID_j, K_{HD_j}, h_j\}$ to the home device.
- HDR 3: Upon receiving them, the home device computes $H_j = D_j \oplus h_j$ and deletes $D_j$. Finally, the home device stores $\{HS_j, H_j, K_{HD_j}\}$ into the its memory.

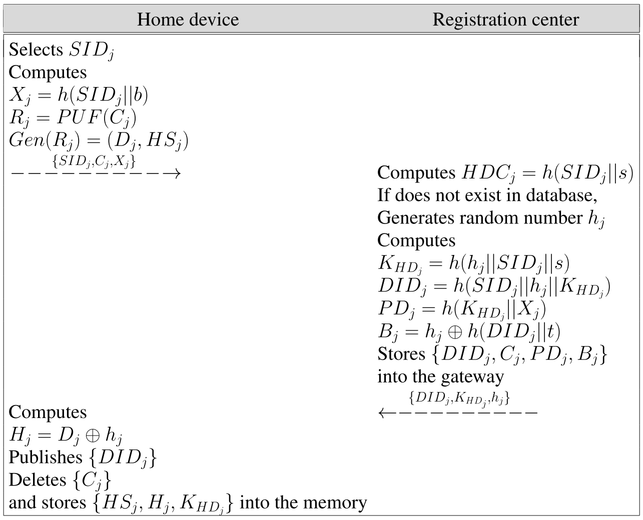
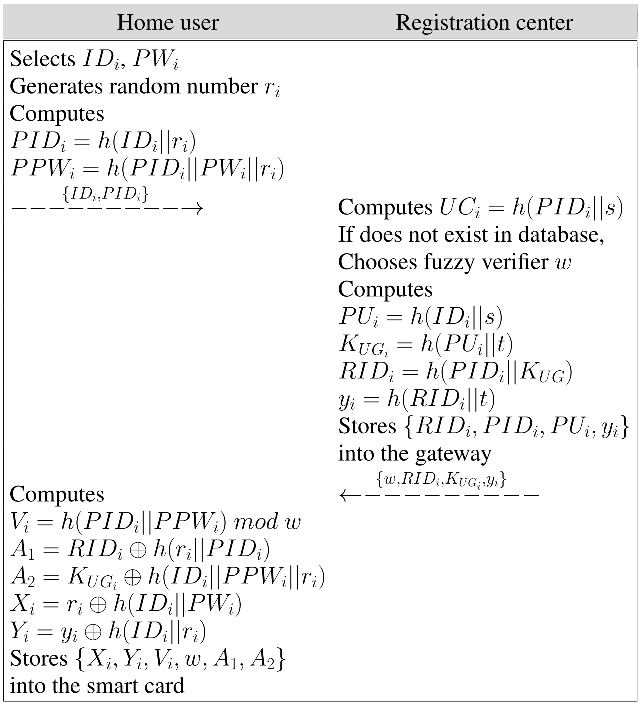

Home device
Registration center
Selects $SID_j$
Computes
$X_j = h(SID_j||b)$
$R_j = PUF(C_j)$
$Gen(R_j) = (D_j, HS_j)$
$\xrightarrow{\{SID_j, C_j, X_j\}}$
Computes $HDC_j = h(SID_j||s)$
If does not exist in database,
Generates random number $h_j$
Computes
$K_{HD_j} = h(h_j||SID_j||s)$
$DID_j = h(SID_j||h_j||K_{HD_j})$
$PD_j = h(K_{HD_j}||X_j)$
$B_j = h_j \oplus h(DID_j||t)$
Stores $\{DID_j, C_j, PD_j, B_j\}$
into the gateway
$\xleftarrow{\{DID_j, K_{HD_j}, h_j\}}$
Computes
$H_j = D_j \oplus h_j$
Publishes $\{DID_j\}$
Deletes $\{C_j\}$
and stores $\{HS_j, H_j, K_{HD_j}\}$ into the memory

FIGURE 5. **Home device registration phase of proposed scheme.**

### C. HOME USER REGISTRATION PHASE

Home users register with the registration center to use home services by securely authenticating with home devices. All messages in this phase are transmitted on a secure channel and the detailed process is shown in Figure 6.

- HUR 1: The home user selects $ID_i, PW_i$, and generates random number $r_i$. Then, the home user computes $PID_i = h(ID_i||r_i)$, $PPW_i = h(PID_i||PW_i||r_i)$, and sends $\{ID_i, PID_i\}$ to the registration center via secure channels.
- HUR 2: After receiving that, the registration center verifies that $UC_i = h(PID_i||s)$ existed in its database. If $UC_i$



Home user | Registration center

Selects $ID_i$, $PW_i$
Generates random number $r_i$
Computes
$PID_i = h(ID_i||r_i)$
$PPW_i = h(PID_i||PW_i||r_i)$
$\xrightarrow{\{ID_i, PID_i\}}$

Computes $UC_i = h(PID_i||s)$
If does not exist in database,
Chooses fuzzy verifier $w$
Computes
$PU_i = h(ID_i||s)$
$K_{UG_i} = h(PU_i||t)$
$RID_i = h(PID_i||K_{UG})$
$y_i = h(RID_i||t)$
Stores $\{RID_i, PID_i, PU_i, y_i\}$
into the gateway
$\xleftarrow{\{w, RID_i, K_{UG_i}, y_i\}}$

Computes
$V_i = h(PID_i||PPW_i)\ mod\ w$
$A_1 = RID_i \oplus h(r_i||PID_i)$
$A_2 = K_{UG_i} \oplus h(ID_i||PPW_i||r_i)$
$X_i = r_i \oplus h(ID_i||PW_i)$
$Y_i = y_i \oplus h(ID_i||r_i)$
Stores $\{X_i, Y_i, V_i, w, A_1, A_2\}$
into the smart card

**FIGURE 6.** **Home user registration phase of proposed scheme.**

stores in the database, registration center terminates this phase. Otherwise, the registration center stores it into the database and computes $PU_i = h(ID_i||s)$, $K_{UG_i} = h(PU_i||t)$, $RID_i = h(PID_i||K_{UG})$, $y_i = h(RID_i||t)$ $y_i = h(RID_i||t)$. Then, the registration center stores $\{RID_i, PID_i, PU_i, y_i\}$ into the gateway's memory and transmits $\{w, RID_i, K_{UG_i}, y_i\}$ to the home user.

- HUR 3: Upon receiving the message, the home user computes $V_i = h(PID_i||PPW_i)\ mod\ w$, $A_1 = RID_i \oplus h(r_i||PID_i)$, $A_2 = K_{UG_i} \oplus h(ID_i||PPW_i||r_i)$, $X_i = r_i \oplus h(ID_i||PW_i)$, $Y_i = y_i \oplus h(ID_i||r_i)$ and stores $\{X_i, Y_i, V_i, w, A_1, A_2\}$ into the smart card.

### *D. LOGIN AND VERIFICATION PHASE*

After the registration phase, the home user and the home device perform mutual authentication with the cooperation of the gateway. If authentication is successful, the home user and the home device agree on a session key as shown in Figure 7.

- **LAV 1:** The home user enters $ID_i'$, $PW_i'$ into the smart card. Then, the smart card calculates $r_i = X_i \oplus h(ID_i'||PW_i')$, $PID_i' = h(ID_i'||r_i)$, $PPW_i' = h(PID_i'||PW_i'||r_i)$, $V_i' = h(PID_i'||PPW_i')\ mod\ w$ and verifies that $V_i'$ is equal to $V_i$. If the condition is satisfied, the home user generates random nonce $a_1$, and computes $y_i = Y_i \oplus h(ID_i||r_i)$, $RID_i = A_1 \oplus h(r_i||PID_i)$, $K_{UG_i} = A_2 \oplus h(ID_i||PPW_i||r_i)$, $M_1 = DID_j \oplus h(K_{UG_i}||PID_i)$, $M_2 = a_1 \oplus h(K_{UG_i}||DID_j)$, $V_1 = h(a_1||DID_j||PID_i)$. Then, the home user transmits $\{RID_i, M_1, M_2, V_1\}$ to the gateway.
- LAV 2: After receiving that, the gateway retrieves $\{PID_i, PU_i\}$ corresponding to $RID_i$ and computes $DID_j = M_1 \oplus h(h(PU_i||t)||PID_i)$, $a_1 = M_2 \oplus h(h(PU_i||t)||DID_j)$, $V_1' = h(a_1||DID_j||PID_i)$. If $V_1'$ equal to $V_i$, the gateway retrieves $\{C_j, PD_j, B_j\}$ corresponding to $DID_j$ and generates $a_2$. Then, the gateway computes $h_j = B_j \oplus h(DID_j||t)$, $M_3 = (a_1||a_2||C_j) \oplus PD_j$, $M_4 = h(PU_t||t) \oplus h_j$, $V_2 = h(a_1||a_2||C_j||RID_i)$ and sends $\{RID_i, M_3, M_4, V_2\}$ to the home device.
- LAV 3: Upon receiving the message, the home device calculates $(a_1||a_2||C_j) = M_3 \oplus h(K_{HD_j}||h(SID_j||b))$, $V_2' = h(a_1||a_2||C_j||RID_i)$. If $V_2'$ equal to $V_2$, the home device generates $a_3$. Then, the home device computes $R_j = PUF(C_j)$, $D_j = Rep(R_j, HS_j)$, $h_j = D_j \oplus H_j$, $h(PU_i||t) = M_4 \oplus h_j$, $SK = h(h(PU_i||t)||a_1||a_2||a_3)$, $M_5 = a_3 \oplus h(h(K_{HD_j}||h(SID_j||b))||h_j)$, $V_3 = h(SK||a_3||h(PU_i||t))$ and transmits $\{M_5, V_3\}$.
- LAV 4: After receiving the message, the gateway calculates $a_3 = M_5 \oplus h(PD_j||h_j)$, $SK = h(h(PU_i||t)||a_1||a_2||a_3)$, $V_3' = h(SK||a_3||h(PU_i||t))$ and verifies that $V_3'$ and $V_3$ are the same. If the condition is satisfied, the gateway computes $RID_i^{new} = h(a_2||RID_i)$, $M_6 = (a_2||a_3) \oplus h(h(PU_i||t)||y_i)$, $V_4 = h(SK||RID_i^{new}||a_2||a_3)$ and transmits $\{M_6, V_4\}$ to the home user.
- LAV 5: After receiving $\{M_6, V_4\}$, the home user calculates $(a_2||a_3) = M_6 \oplus h(K_{UG_i}||y_i)$, $RID_i^{new} = h(a_2||RID_i)$, $SK = h(K_{UG_i}||a_1||a_2||a_3)$, $V_4' = h(SK||RID_i^{new}||a_2||a_3)$. If $V_4'$ is equal to $V_4$, the home user computes $A_1^{new} = RID_i^{new} \oplus h(r_i||PID_i)$ and replaces $A_1$ with $A_1^{new}$. If session key agreement is successful, the gateway replaces $RID_i$ with $RID_i^{new}$. All messages in login and verification phase are exchanged in public channels.

### *E. PASSWORD UPDATE PHASE*

Home users can change their passwords and update information stored in the smart card through this phase. the home user enters his/her $ID_i'$, $PW_i'$ into the smart card. Then, the smart card calculates $r_i = X_i \oplus h(ID_i'||PW_i')$, $PID_i' = h(ID_i'||r_i)$, $PPW_i' = h(PID_i'||PW_i'||r_i)$, $V_i' = h(PID_i'||PPW_i')$ $mod\ w$. IF $V_i'$ is equal to $V_i$, the home user can select new password $PW_i^{new}$. After the home user enters $PW_i^{new}$, smart card computes $K_{UG_i} = A_2 \oplus h(ID_i||PPW_i||r_i)$, $X_i^{new} = r_i \oplus h(ID_i||PW_i^{new})$, $PPW_i^{new} = h(PID_i||PW_i^{new}||r_i)$, $A_2^{new} = K_{UG_i} \oplus h(ID_i||PPW_i^{new}||r_i)$, $V_i = h(PID_i||PPW_i^{new})\ mod\ w$ and replaces $\{X_i, V_i, A_2\}$ with $\{X_i^{new}, V_i^{new}, A_2^{new}\}$.

## VII. SECURITY ANALYSIS

In this section, we perform informal and formal security analysis to validate that the proposed scheme achieves the resistance to security attacks. In our paper, we use the ROR model to evaluate the security of the session key. We utilize BAN logic to verify that our scheme performs mutual authentication correctly. Moreover, we simulate AVISPA to evaluate security under the DY threat model.

<table>
<tr><th>Home user/smart card</th><th>Gateway</th><th>Home device</th></tr>
<tr><td>Enters $ID_i^{'}$ and $PW_i^{'}$<br>Computes<br>$r_i = X_i \oplus h(ID_i^{'}||PW_i^{'})$<br>$PID_i^{'} = h(ID_i^{'}||r_i)$<br>$PPW_i^{'} = h(PID_i^{'}||PW_i^{'}||r_i)$<br>$V_i^{'} = h(PID_i^{'}||PPW^{'})\ mod\ w$<br>Checks $V_i^{'} \overset{?}{=} V_i$<br>Generates random nonces $a_1$<br>Computes<br>$y_i = Y_i \oplus h(ID_i||r_i)$<br>$RID_i = A_1 \oplus h(r_i||PID_i)$<br>$K_{UG_i} = A_2 \oplus h(ID_i||PPW_i||r_i)$<br>$M_1 = DID_j \oplus h(K_{UG_i}||PID_i)$<br>$M_2 = a_1 \oplus h(K_{UG_i}||DID_j)$<br>$V_1 = h(a_1||DID_j||PID_i)$<br>$\xrightarrow{\{RID_i, M_1, M_2, V_1\}}$</td><td></td><td></td></tr>
<tr><td></td><td>Retrieves $\{PID_i, PU_i\}$ corresponding to $RID_i$<br>Computes<br>$DID_j = M_1 \oplus h(h(PU_i||t)||PID_i)$<br>$a_1 = M_2 \oplus h(h(PU_i||t)||DID_j)$<br>$V_1^{'} = h(a_1||DID_j||PID_i)$<br>Checks $V_1^{'} \overset{?}{=} V_1$<br>Retrieves $\{C_j, PD_j, B_j\}$ corresponding to $DID_j$<br>Generates a random nonce $a_2$<br>Computes<br>$h_j = B_j \oplus h(DID_j||t)$<br>$M_3 = (a_1||a_2||C_j) \oplus PD_j$<br>$M_4 = h(PU_i||t) \oplus h_j$<br>$V_2 = h(a_1||a_2||C_j||RID_i)$<br>$\xrightarrow{\{RID_i, M_3, M_4, V_2\}}$</td><td></td></tr>
<tr><td></td><td></td><td>Computes<br>$(a_1||a_2||C_j) = M_3 \oplus h(K_{HD_j}||h(SID_j||b))$<br>$V_2^{'} = h(a_1||a_2||C_j||RID_i)$<br>Checks $V_2^{'} \overset{?}{=} V_2$<br>Generates a random nonce $a_3$<br>Computes<br>$R_j = PUF(C_j)$<br>$D_j = Rep(R_j, HS_j)$<br>$h_j = D_j \oplus H_j$<br>$h(PU_i||t) = M_4 \oplus H_j$<br>$SK = h(h(PU_i||t)||a_1||a_2||a_3)$<br>$M_5 = a_3 \oplus h(h(K_{HD_j}||h(SID_j||b))||h_j)$<br>$V_3 = h(SK||a_3||h(PU_i||t))$<br>$\xleftarrow{\{M_5, V_3\}}$</td></tr>
<tr><td></td><td>Computes<br>$a_3 = M_5 \oplus h(PD_j||h_j)$<br>$SK = h(h(PU_i||t)||a_1||a_2||a_3)$<br>$V_3^{'} = h(SK||a_3||h(PU_i||t))$<br>Checks $V_3^{'} \overset{?}{=} V_3$<br>Computes<br>$RID_i^{new} = h(a_2||RID_i)$<br>$M_6 = (a_2||a_3) \oplus h(h(PU_i||t)||y_i)$<br>$V_4 = h(SK||RID_i^{new}||a_2||a_3)$<br>If session key agreement is successful,<br>replaces $\{RID_i\}$ with $\{RID_i^{new}\}$<br>$\xleftarrow{\{M_6, V_4\}}$</td><td></td></tr>
<tr><td>Computes<br>$(a_2||a_3) = M_6 \oplus h(K_{UG_i}||y_i)$<br>$RID_i^{new} = h(a_2||RID_i)$<br>$SK = h(K_{UG_i}||a_1||a_2||a_3)$<br>$V_4^{'} = h(SK||RID_i^{new}||a_2||a_3)$<br>Checks $V_4^{'} \overset{?}{=} V_4$<br>Computes<br>$A_1^{new} = RID_i^{new} \oplus h(r_i||PID_i)$<br>Replace $\{A_1\}$ with $\{A_1^{new}\}$</td><td></td><td></td></tr>
</table>

**FIGURE 7.** Login and verification phase of the proposed scheme.

### A. INFORMAL ANALYSIS

We demonstrate that the proposed scheme resists various security attacks, including smart card stolen, forgery, and ephemeral secret leakage attacks, and ensures perfect forward secrecy and mutual authentication using the informal analysis.

### 1) SMART CARD STOLEN ATTACK

Referring to Section III-E, an adversary $\mathcal{A}$ can extract $\{X_i, Y_i, V_i, A_1, A_2\}$ from a legitimate home user's smart card. $\mathcal{A}$ can attempt to compute an authentication request message $M_1 = DID_j \oplus h(K_{UG_i}||PID_i)$, $V_1 = h(a_1||DID_j||PID_i)$ based on this information. However, $\mathcal{A}$ cannot calculate $PID_i$ without the knowledge of the home user's real identity $ID_i$ and the random number $r_i$ generated at the home user registration phase. Thus, the proposed authentication scheme resists the smart card stolen attack.

### 2) FORGERY ATTACK

In this attack, an adversary $\mathcal{A}$ forges valid authentication request messages $RID_i = A_1 \oplus h(r_i||PID_i)$, $M_1 = DID_j \oplus h(K_{UG_i}||PID_i)$, $M_2 = a_1 \oplus h(K_{UG_i}||DID_j)$, and $V_1 = h(a_1||DID_j||PID_i)$ to impersonate the legitimate home user. If $\mathcal{A}$ acquires the home user's smart card and public channel messages, $\mathcal{A}$ can attempt to compute the valid authentication request messages $RID_i = A_1 \oplus h(r_i||PID_i)$, $M_1 = DID_j \oplus h(K_{UG_i}||PID_i)$, $M_2 = a_1 \oplus h(K_{UG_i}||DID_j)$, and $V_1 = h(a_1||DID_j||PID_i)$. However, $\mathcal{A}$ cannot calculate $M_1$ and $M_2$ without $K_{UG_i} = A_2 \oplus h(ID_i||PPW_i||r_i)$. Since $\mathcal{A}$ cannot compute the valid authentication request messages $\{RID_i, M_3, M_4, V_2\}$, the proposed scheme prevents the forgery attack.

### 3) OFFLINE PASSWORD ATTACK

As in section VII-A1, an adversary $\mathcal{A}$ can extract the parameters $\{X_i, Y_i, V_i, A_1, A_2\}$ stored in the smart card and use them for offline password guessing attack. In this attack, $\mathcal{A}$ chooses a random password and attempts to calculate $V_i' = h(PID_i'||PPW_i') \ mod \ w$, where $PPW_i = h(PID_i||PW_i||r_i)$. However, $\mathcal{A}$ cannot guess a valid password because $\mathcal{A}$ does not know $r_i$. Therefore, our authentication scheme is secure against the offline password guessing attack.

### 4) REPLAY ATTACK

In the login and verification phase of our scheme, $\{RID_i, M_1, M_2, V_1\}$, $\{RID_i, M_3, M_4, V_2\}$, $\{M_5, V_3\}$, and $\{M_6, V_4\}$ are exchanged over public channels. These messages are calculated by random nonces $a_1, a_2$, and $a_3$ generated every session. In our scheme, entities validate the freshness of the random nonce each time it receives these messages. Therefore, the proposed scheme is secure against the replay attack because $\mathcal{A}$ cannot attempt to authenticate using the previous message.

### 5) USER ANONYMITY

In our scheme, the home user transmits $RID_i = a_1 \oplus h(ID_i||r_i)$ to the gateway. According to Section III-E, a malicious adversary $\mathcal{A}$ can monitor this message. However, $\mathcal{A}$ cannot compute the real identity of the home user due to $ID_i$ is masked with $A_1$ and $r_i$. Moreover, $RID_i$ is updated every session in proposed scheme. Therefore, our scheme provides home user anonymity.

### 6) VERIFIER STOLEN ATTACK

If an adversary $\mathcal{A}$ obtains the verification table $\{(PID_i, PU_i, y_i), (C_j, PD_j, B_j)\}$ stored in the gateway, $\mathcal{A}$ can use it to calculate the session key $SK = h(K_{UG_i}||a_1||a_2||a_3)$. To compute the session key of the proposed scheme, $\mathcal{A}$ must have the home user's long-term key $K_{UG_i}$ and the random nonce of each entity. However, $\mathcal{A}$ cannot compute random nonce $a_1$ from the public channel message without the master key $t$. Thus, our scheme can resist the verifier stolen attack.

### 7) EPHEMERAL SECRET LEAKAGE ATTACK

Under the CK model, an adversary $\mathcal{A}$ can acquire a random nonce that is generated every session. Using this nonce along with public channel messages, $\mathcal{A}$ can attempt to compute the current session key. However, $\mathcal{A}$ cannot calculate correct session key $SK = h(K_{UG_i}||a_1||a_2||a_3)$ without $K_{UG_i}$ and $PU_i$. Conversely, even if $\mathcal{A}$ obtains a long-term key such as $K_{UG_i}$, $\mathcal{A}$ cannot calculate the session key without a random nonce such as $a_1, a_2$, and $a_3$. Thus, the proposed scheme prevents the ephemeral secret leakage attack because our session key is constructed using both long-term and short-term keys.

### 8) INSIDER ATTACK

According to the threat model in our paper, an adversary $\mathcal{A}$ can register as a legitimate home user in the smart home. In this case, $\mathcal{A}$ attempts to compute another legitimate home user's session key of using $\{X_a, Y_a, V_a, A_{a1}, A_{a2}\}$ stored on the $\mathcal{A}$'s smart card. However, it is difficult for $\mathcal{A}$ to calculate another home user's session key $SK = h(K_{UG_i}||a_1||a_2||a_3)$ based on these parameters because every home user has a different long-term key $K_{UG_i} = A_2 \oplus h(ID_i||PPW_i||r_i)$. Even if $\mathcal{A}$ uses the parameters stored in his smart card and $K_{UG_a}$, $\mathcal{A}$ cannot calculate another home user's long-term key $K_{UG_i}$. Therefore, the proposed scheme is resistant to the insider attack.

### 9) SESSION KEY DISCLOSURE ATTACK

In accordance with Section VII-A6 and Section VII-A7, an adversary $\mathcal{A}$ can obtain and use a verification table or short-term key to compute the session key. $\mathcal{A}$ use it to perform verifier stolen and ephemeral secret leakage attacks. However, it is difficult for the adversary to calculate the correct session key without knowing both the long-term key and the short-term key. As a result, the proposed scheme resists the session key disclosure attack.

### 10) DEVICE CAPTURE ATTACK

In our scheme, an adversary $\mathcal{A}$ can extract $\{HS_j, H_j, K_{HD_j}\}$ by capturing home devices deployed in smart homes. However, $\mathcal{A}$ cannot compromise the communication of another home device with the parameters of the captured home device due to all home devices use different secret credentials. Moreover, it is impossible for $\mathcal{A}$ to physically duplicate the home device because the home device of our scheme adopts PUF. Thus, our scheme prevents the device capture attack.

#### 11) PERFECT FORWARD SECRECY

An adversary $\mathcal{A}$ attempts to calculate the session key by acquiring the long-term key of the home user or home device. In our scheme, $\mathcal{A}$ knows the long-term key $K_{UG_i}$, $\mathcal{A}$ can only calculate $a_1$. Even if $\mathcal{A}$ obtains the master key $b$, it cannot compute the session key without the secret credentials of the home device. Therefore, our scheme provides perfect forward secrecy.

#### 12) MUTUAL AUTHENTICATION

In the login and verification phase of the proposed scheme, home users, gateway, and home devices verify messages exchanged with each other. The gateway verifies $V_1' \stackrel{?}{=} V_1$ transmitted by the home user. If $V_1'$ and $V_1$ are are equal, the gateway authenticates the home user. Similarly, the gateway and home devices verify $V_2' \stackrel{?}{=} V_2$, $V_3' \stackrel{?}{=} V_3$, and $V_4' \stackrel{?}{=} V_4$ in every session. When all verification is successful, they authenticate each other and compute a shared session key. Therefore, the proposed scheme provides mutual authentication between home users, gateway, home devices.

### B. ROR MODEL

The ROR model [12] is a method widely used by researchers to verify the semantic security of session key in authentication and key agreement schemes [33], [34], [35], [36]. We utilize the ROR model to prove that it is difficult for an adversary $\mathcal{A}$ to obtain the session key of our scheme. In our scheme, participants are denoted as $I_U^{a1}$, $I_{GW}^{a2}$, and $I_{HD}^{a3}$, which are instances of home user, gateway, and home device, respectively. In the ROR model, $\mathcal{A}$ can monitor and control all public channel message communication between entities. The queries that $\mathcal{A}$ can perform are $CorruptSC(I_U^{a1})$, $Send(I_x^{a_n}, Msg)$, $Execute(I_U^{a1}, I_{GW}^{a2}, I_{HD}^{a3})$, $Reveal(I_x^{a_n})$, and $Test(I_x^{a_n})$. Each of these queries is described in Table 2.

*Theorem 1:* The adversary $\mathcal{A}$ attempts to compute the session key between the legitimate home user and the home device in the proposed scheme. *Advantage*$(A)$ is a probability that $\mathcal{A}$ successfully computes the session key within polynomial time. *Advantage*$(A)$ of the proposed scheme is shown as (1), where $q_{puf}$, $q_{hash}$, and $q_{send}$ denote the number of times to perform PUF, hash, and send queries, respectively. Additionally, $C^*$ and $S^*$ are Zipf's law parameters [37], and $l$ is the length of the secret key.

$$Advantage(A) \leq \frac{q_{puf}^2}{|PUF|} + \frac{q_{hash}^2}{|Hash|} + 2max\{C^* \cdot q_{send}^{S^*}, \frac{q_{send}}{2^l}\} \quad (1)$$

*Proof:* We conduct several games to prove Theorem 1. There are four games in this proof, and detailed descriptions of each are below.

- *Game*$_0$: This game is an initial state, where $\mathcal{A}$ has not performed any queries. Therefore, we derive the following equation.

$$Advantage(A) = |2 \cdot Adv_{game_0} - 1| \quad (2)$$

**TABLE 2.** Queries in the ROR model.

| Query | Description |
|---|---|
| $CorruptSC(I_U^{a_1})$ | In this query, $\mathcal{A}$ obtains secret credentials of participant $I_U^{a_1}$'s smart card. |
| $Send(I_x^{a_n}, Msg)$ | This query sends message $Msg$ to participant $I_x^{a_n}$. If message $Msg$ is valid, then participant $I_x^{a_n}$ believes $\mathcal{A}$ is a legitimate participant and returns a response message. |
| $Execute(I_U^{a_1}, I_{GW}^{a_2}, I_{HD}^{a_3})$ | By performing this query, $\mathcal{A}$ can eavesdrop on messages exchanged on public channels between participants $I_U^{a_1}$, $I_{GW}^{a_2}$, and $I_{HD}^{a_3}$. $\mathcal{A}$ can use these messages to attempt passive or active attacks. |
| $Reveal(I_x^{a_n})$ | Under the $Reveal$ query, $\mathcal{A}$ can reveal the session key $SK$ established between each participant $I_x^{a_n}$. |
| $Test(I_x^{a_n})$ | $\mathcal{A}$ flips an unbiased coin $c$ to fulfill this query. Depending on the result of the coin toss, $\mathcal{A}$ obtains the following output from the messages exchanged between participants. If $c = 1$, $\mathcal{A}$ gets the correct session key. When $c = 0$, $\mathcal{A}$ gets a random nonce. If neither, $\mathcal{A}$ gets $NULL(\perp)$. |

- *Game*$_1$: In this game, $\mathcal{A}$ performs an *Execute* query to eavesdrop on messages on public channels. Afterward, $\mathcal{A}$ uses *Reveal* and *Test* queries to derive the session key shared between the home user and the home device. $\mathcal{A}$ cannot calculate the session key from the public channel message because the session key of our scheme consists of a masked long-term key and a short-term key. Thus, we obtain the following equation.

$$Adv_{game_1} = Adv_{game_0} \quad (3)$$

- *Game*$_2$: $\mathcal{A}$ performs *Hash* and *Send* queries to derive the session key of our scheme. Since $\mathcal{A}$ does not know any random nonces $\{a_1, a_2, a_3\}$, $\mathcal{A}$ attempts to find a hash collision using only the public channel messages $\{RID_i, M_1, M_2, V_1\}$,$\{RID_i, M_3, M_4, V_2\}$, $\{M_5, V_3\}$, $\{M_6, V_4\}$. Thus, we can obtain the following equation based on the birthday problem.

$$|Adv_{game_2} - Adv_{game_1}| \leq \frac{q_{hash}^2}{2|Hash|} \quad (4)$$

- *Game*$_3$: This game is an extension of *Game*$_2$. The probability of obtaining the secret key using *PUF* query is similar to *Hash* query, so we can get the following equation.

$$|Adv_{game_3} - Adv_{game_2}| \leq \frac{q_{puf}^2}{2|PUF|} \quad (5)$$

- *Game*$_4$: In this game, $\mathcal{A}$ conducts a $CorruptSC(P_U^{a_1})$ query to extract the $\{X_i, Y_i, V_i, A_1, A_2\}$ stored on the smart card. However, $\mathcal{A}$ cannot guess the correct session key using this information because the home user's secret credential is masked with a one-way hash function. Thus, we can derive the equation below, where $C^*$

and $S^*$ are the parameters of Zipf's law.

$$|Adv_{game_4} - Adv_{game_3}| \leq max\{C^* \cdot q_{send}^{S^*}, \frac{q_{send}}{2^l}\} \quad (6)$$

After completing all previous games, $\mathcal{A}$ guesses bit $c$. Therefore, we obtain the following equation.

$$Adv_{game_5} = \frac{1}{2} \quad (7)$$

By combining (2), (3), (4), (5), (6), (7), we can derive the following triangular inequality as a result.

$$\begin{aligned} \frac{1}{2}Advantage(A) &= |Adv_{game_0} - \frac{1}{2}| \\ &= |Adv_{game_1} - Adv_{game_5}| \\ &\leq |Adv_{game_1} - Adv_{game_2}| \\ &\quad + |Adv_{game_2} - Adv_{game_3}| \\ &\quad + |Adv_{game_3} - Adv_{game_4}| \\ &\quad + |Adv_{game_4} - Adv_{game_5}| \\ &\leq \frac{q_{puf}^2}{2|PUF|} + \frac{q_{hash}^2}{2|Hash|} \\ &\quad + max\{C^* \cdot q_{send}^{S^*}, \frac{q_{send}}{2^l}\} \qquad (8) \end{aligned}$$

Consequently, we can derive (9) by utilizing (8).

$$\begin{aligned} Advantage(A) \leq \frac{q_{puf}^2}{|PUF|} + \frac{q_{hash}^2}{|Hash|} \\ + 2max\{C^* \cdot que_{send}^{S^*}, \frac{q_{send}}{2^l}\} \qquad (9) \end{aligned}$$

Since (9) is equal to (1), we successfully prove theorem 1. Therefore, we have verified the semantic security of the session key.

### C. BAN LOGIC

BAN logic [13] is a widely used formal security analysis method for defining and analyzing authentication schemes [38], [39], [40], [41]. BAN logic is an axiomatic system, using rules and assumptions to verify the authenticity and security of information exchanged during authentication. We explain the rules, assumptions and proofs of BAN logic in this section. The symbols used in BAN logic and their meanings are shown in Table 3.

#### 1) RULES

BAN logic has several rules to validate session key sharing. The rules defined in BAN logic are as follows. 1) Message meaning rule (MMR):

$$\frac{r| \equiv r \overset{s}{\leftrightarrow} s, r \lhd \{w\}_s}{r| \equiv s| \sim w}$$

2) Nonce verification rule (NVR):

$$\frac{r| \equiv \#(w), r| \equiv s| \sim w}{r| \equiv s| \equiv w}$$

3) Jurisdiction rule (JR):

$$\frac{r| \equiv s \Rightarrow w, r| \equiv s| \equiv w}{r| \equiv w}$$

**TABLE 3.** Symbol of BAN logic.

| Symbol | Meaning |
|---|---|
| $r, s$ | Principals |
| $w, v$ | Statements |
| $s$ | Shared secret key |
| $r\| \equiv w$ | $r$ believes $w$ |
| $r\| \sim w$ | $r$ once said $w$ |
| $r \lhd w$ | $r$ sees $w$ |
| $\#(w)$ | $w$ is fresh |
| $r \Rightarrow w$ | $r$ controls $w$ |
| $r \overset{s}{\leftrightarrow} s$ | $r$ and $s$ communicate utilizing $s$ |
| $\{w\}_s$ | $w$ is encrypted by $s$ |

4) Freshness meaning rule (FR):

$$\frac{r| \equiv \#(w)}{r| \equiv \#(w, v)}$$

5) Belief rule (BR):

$$\frac{r| \equiv (w, v)}{r| \equiv w}$$

#### 2) GOALS OF THE PROPOSED SCHEME

The goal of our scheme is to successfully share session keys between entities. We denote home users, gateways, and home devices as $US$, $GW$, and $HD$, respectively. The detailed goal is as follows.

**Goal 1**: $US| \equiv (US \overset{SK}{\leftrightarrow} GW)$
**Goal 2**: $GW| \equiv (US \overset{SK}{\leftrightarrow} GW)$
**Goal 3**: $US| \equiv GW| \equiv (US \overset{SK}{\leftrightarrow} GW)$
**Goal 4**: $GW| \equiv US| \equiv (US \overset{SK}{\leftrightarrow} GW)$
**Goal 5**: $GW| \equiv (HD \overset{SK}{\leftrightarrow} GW)$
**Goal 6**: $HD| \equiv (HD \overset{SK}{\leftrightarrow} GW)$
**Goal 7**: $GW| \equiv HD| \equiv (HD \overset{SK}{\leftrightarrow} GW)$
**Goal 8**: $HD| \equiv GW| \equiv (HD \overset{SK}{\leftrightarrow} GW)$

#### 3) IDEALIZED FORMS OF MESSAGES

The idealized forms of authentication request and response messages exchanged in our scheme is as follows.

**Msg 1**: $US \rightarrow GW : \{DID_j, a_1\}_{K_{UG_i}}$
**Msg 2**: $GW \rightarrow HD : \{h(PU_i||t), a_1, a_2\}_{PD_j}$
**Msg 3**: $HD \rightarrow GW : \{a_3\}_{PD_j}$
**Msg 4**: $GW \rightarrow US : \{a_2, a_3\}_{K_{UG_i}}$

#### 4) ASSUMPTIONS

The following list is the assumptions for BAN logic analysis of our scheme.

**A1**: $GW| \equiv US \overset{K_{UG_i}}{\leftrightarrow} GW$
**A2**: $GW| \equiv \#(a_1)$
**A3**: $HD| \equiv GW \overset{PD_j}{\leftrightarrow} HD$
**A4**: $HD| \equiv \#(a_2)$
**A5**: $GW| \equiv HD \overset{PD_j}{\leftrightarrow} GW$

**A6**: $GW| \equiv \#(a_3)$
**A7**: $US| \equiv US \overset{K_{UG_i}}{\leftrightarrow} GW$
**A8**: $US| \equiv \#(a_3)$
**A9**: $GW| \equiv HD \Rightarrow (HD \overset{SK}{\leftrightarrow} GW)$
**A10**: $HD| \equiv GW \Rightarrow (HD \overset{SK}{\leftrightarrow} GW)$
**A11**: $US| \equiv GW \Rightarrow (US \overset{SK}{\leftrightarrow} GW)$
**A12**: $GW| \equiv US \Rightarrow (US \overset{SK}{\leftrightarrow} GW)$

### 5) PROOF

We prove the mutual authentication of our scheme by deriving the above-mentioned goals using the rules of BAN logic, idealized forms of messages, and assumptions. Detailed descriptions are as follows.

- **Step 1**: We can obtain $S_1$ from *Msg* 1.

$$S_1 : GW \triangleleft \{DID_j, a_1\}_{K_{UG_i}}$$

- **Step 2**: Consider $S_1$ and $A_1$ with MMR, we can obtain $S_2$.

$$S_2 : GW| \equiv US| \sim (DID_j, a_1)$$

- **Step 3**: Consider $S_2$ and $A_2$ with FR, we can obtain $S_3$.

$$S_3 : GW| \equiv \#(DID_j, a_1)$$

- **Step 4**: We can obtain $S_4$ from $S_2$ and $S_3$ with NVR.

$$S_4 : GW| \equiv US| \equiv (DID_j, a_1)$$

- **Step 5**: We can obtain $S_5$ from $S_4$ with BR.

$$S_5 : GW| \equiv US| \equiv (a_1)$$

- **Step 6**: We can obtain $S_6$ from *Msg* 2.

$$S_6 : HD \triangleleft \{h(PU_i||t), a_1, a_2\}_{PD_j}$$

- **Step 7**: Consider $S_6$ and $A_3$ with MMR, we can obtain $S_7$.

$$S_7 : HD| \equiv GW| \sim (h(PU_i||t), a_1, a_2)$$

- **Step 8**: Consider $S_7$ and $A_4$ with FR, we can obtain $S_8$.

$$S_8 : HD| \equiv \#(h(PU_i||t), a_1, a_2)$$

- **Step 9**: We can obtain $S_9$ from $S_7$ and $S_8$ with NVR.

$$S_9 : HD| \equiv GW| \equiv (h(PU_i||t), a_1, a_2)$$

**Step 10**: We can obtain $S_{10}$ from *Msg* 3.

$$S_{10} : GW \triangleleft \{a_3\}_{PD_j}$$

- **Step 11**: Consider $S_{10}$ and $A_5$ with MMR, we can obtain $S_{11}$.

$$S_{11} : GW| \equiv HD| \sim (a_3)$$

- **Step 12**: We can obtain $S_{12}$ from $S_{11}$ and $A_6$ with NVR.

$$S_{12} : GW| \equiv HD| \equiv (a_3)$$

- **Step 13**: We can obtain $S_{13}$ from *Msg* 4.

$$S_{13} : US \triangleleft \{a_2, a_3\}_{K_{UG_i}}$$

- **Step 14**: Consider $S_{13}$ and $A_7$ with MMR, we can obtain $S_{14}$.

$$S_{14} : US| \equiv GW| \sim (a_2, a_3)$$

- **Step 15**: Consider $S_{14}$ and $A_8$ with FR, we can obtain $S_{15}$.

$$S_{15} : US| \equiv \#(a_2, a_3)$$

- **Step 16**: We can obtain $S_{16}$ from $S_{14}$ and $S_{15}$ with NVR.

$$S_{16} : US| \equiv GW| \equiv (a_2, a_3)$$

- **Step 17**: Because GW and HD can establish the session key $SK = h(h(PU_i||t)||a_1||a_2||a_3)$, we can obtain $S_{17}$ and $S_{18}$ from $S_9$ and $S_{12}$.

$$S_{17} : GW| \equiv HD| \equiv (HD \overset{SK}{\leftrightarrow} GW) \quad (Goal\ 7)$$
$$S_{18} : HD| \equiv GW| \equiv (HD \overset{SK}{\leftrightarrow} GW) \quad (Goal\ 8)$$

- **Step 18**: Because US and GW can establish the session key $SK = h(K_{UG_i}||a_1||a_2||a_3)$, we can obtain $S_{19}$ and $S_{20}$ from $S_5$ and $S_{16}$.

$$S_{19} : US| \equiv GW| \equiv (US \overset{SK}{\leftrightarrow} GW) \quad (Goal\ 3)$$
$$S_{20} : GW| \equiv US| \equiv (US \overset{SK}{\leftrightarrow} GW) \quad (Goal\ 4)$$

- **Step 19**: We can obtain $S_{21}$ and $S_{22}$ from $S_{17}$ and $S_{18}$ with JR.

$$S_{21} : GW| \equiv (HD \overset{SK}{\leftrightarrow} GW) \quad (Goal\ 5)$$
$$S_{22} : HD| \equiv (HD \overset{SK}{\leftrightarrow} GW) \quad (Goal\ 6)$$

- **Step 20**: We can obtain $S_{23}$ and $S_{24}$ from $S_{19}$ and $S_{20}$ with JR.

$$S_{23} : US| \equiv (US \overset{SK}{\leftrightarrow} GW) \quad (Goal\ 1)$$
$$S_{24} : GW| \equiv (US \overset{SK}{\leftrightarrow} GW) \quad (Goal\ 2)$$

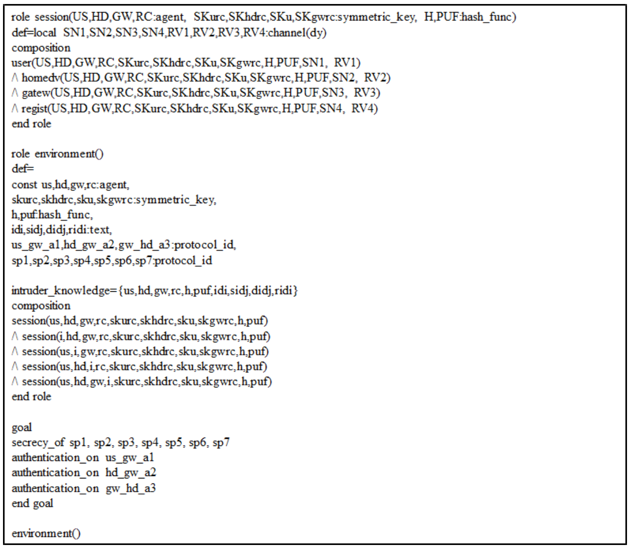
As a result, we prove that our scheme provides correct mutual authentication because our scheme achieves all the goals in BAN logic.

## D. AVISPA SIMULATION

In this section, we perform AVISPA [14] simulation to verify the resistance of the proposed scheme to security attacks such as MITM and replay. AVISPA is an analysis tool that implements and simulates an authentication scheme based on High-Level Protocols Specification Language (HLPSL) [42], [43], [44]. AVISPA contains backends called SAT-based Model Checker (SATMC), Constraint Logic-based Attack Searcher (CL-AtSE), Tree automata based on Automatic Approximations for Analysis of Security Protocol (TA4SP), and On-the-fly ModelChecker (OMFC). The HLPSL2IF translator converts the HLPSL code to an Intermediate Format (IF) and enters it into the backend. The backend evaluates the security of the proposed scheme and outputs the Output Format (OF) as a result. Since XOR operation is used in the proposed scheme, we only use CL-AtSE and OMFC backends.

### 1) SPECIFICATIONS OF HLPSL

In the proposed method, roles are composed of the home user, gateway, home device, and registration center. The HLPSL code for threat model capabilities and goals are shown in Figure 8. Referring to Figure 9, state 0 is the start of the registration phase, and the home user transmits $\{ID_i, PID_i\}$ to the registration center in state 1. After receiving that in state 1, the registration center calculates $\{w, RID_i, K_{UG_i}, y_i\}$ and sends it to the home user. Upon receiving messages from the registration center, the home user updates the state and stores $\{X_i, Y_i, V_i, w, A_1, A_2\}$ into the smart card. After the registration phase, the home user computes an authentication message $\{RID_i, M_1, M_2, V_1\}$ and transmits it to the gateway in state 2. When the home user receives a response message from the gateway, the home user updates the state from 2 to 3 and computes the session key $SK = h(K_{UG_i}||a_1||a_2||a_3)$.

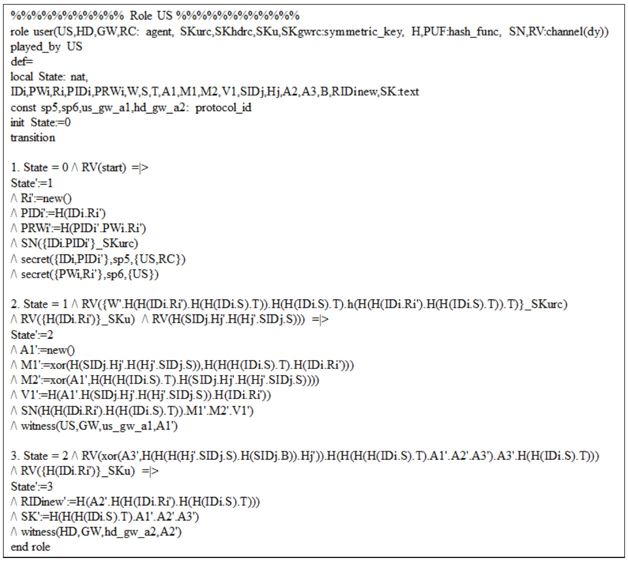


```
role session(US,HD,GW,RC:agent,  SKurc,SKhdrc,SKu,SKgwrc:symmetric_key,  H,PUF:hash_func)
def=local  SN1,SN2,SN3,SN4,RV1,RV2,RV3,RV4:channel(dy)
composition
user(US,HD,GW,RC,SKurc,SKhdrc,SKu,SKgwrc,H,PUF,SN1,  RV1)
/\ homedv(US,HD,GW,RC,SKurc,SKhdrc,SKu,SKgwrc,H,PUF,SN2,  RV2)
/\ gatew(US,HD,GW,RC,SKurc,SKhdrc,SKu,SKgwrc,H,PUF,SN3,  RV3)
/\ regist(US,HD,GW,RC,SKurc,SKhdrc,SKu,SKgwrc,H,PUF,SN4,  RV4)
end role

role environment()
def=
const us,hd,gw,rc:agent,
skurc,skhdrc,sku,skgwrc:symmetric_key,
h,puf:hash_func,
idi,sidj,didj,ridi:text,
us_gw_a1,hd_gw_a2,gw_hd_a3:protocol_id,
sp1,sp2,sp3,sp4,sp5,sp6,sp7:protocol_id

intruder_knowledge={us,hd,gw,rc,h,puf,idi,sidj,didj,ridi}
composition
session(us,hd,gw,rc,skurc,skhdrc,sku,skgwrc,h,puf)
/\ session(i,hd,gw,rc,skurc,skhdrc,sku,skgwrc,h,puf)
/\ session(us,i,gw,rc,skurc,skhdrc,sku,skgwrc,h,puf)
/\ session(us,hd,i,rc,skurc,skhdrc,sku,skgwrc,h,puf)
/\ session(us,hd,gw,i,skurc,skhdrc,sku,skgwrc,h,puf)
end role

goal
secrecy_of sp1, sp2, sp3, sp4, sp5, sp6, sp7
authentication_on  us_gw_a1
authentication_on  hd_gw_a2
authentication_on  gw_hd_a3
end goal

environment()
```

**FIGURE 8.** Role of the session and environment.

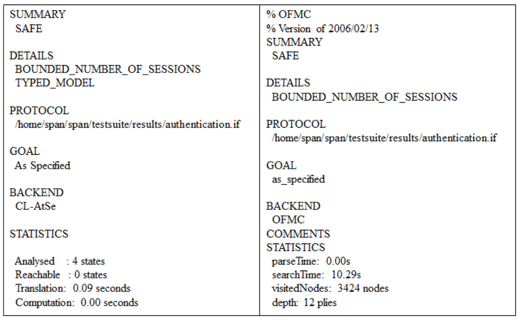
### 2) RESULT OF SIMULATION

The AVISPA backend outputs simulation results for the safety of the authentication scheme against the security attack by the adversary model. Figure 10 shows the results of CL-AtSE and OFMC for the proposed authentication scheme, respectively. Since both outputs are SAFE, our scheme is secure from MITM and replay attacks.



```
%%%%%%%%%%%%%% Role US %%%%%%%%%%%%%%%
role user(US,HD,GW,RC:  agent,  SKurc,SKhdrc,SKu,SKgwrc:symmetric_key,  H,PUF:hash_func,  SN,RV:channel(dy))
played_by  US
def=
local  State: nat,
IDi,PWi,Ri,PIDi,PRWi,W,S,T,A1,M1,M2,V1,SIDj,Hj,A2,A3,B,RIDinew,SK:text
const  sp5,sp6,us_gw_a1,hd_gw_a2:  protocol_id
init  State:=0
transition

1. State = 0 /\ RV(start)  =|>
State':=1
/\ Ri':=new()
/\ PIDi':=H(IDi.Ri')
/\ PRWi':=H(PIDi'.PWi.Ri')
/\ SN({IDi.PIDi'}_SKurc)
/\ secret({IDi,PIDi'},sp5,{US,RC})
/\ secret({PWi,Ri'},sp6,{US})

2. State = 1 /\ RV({W'.H(H(IDi.Ri').H(H(IDi.S).T)).H(H(IDi.S).T).h(H(H(IDi.Ri').H(H(IDi.S).T)).T)}_SKurc)
/\ RV({H(IDi.Ri')}_SKu)  /\ RV(H(SIDj.Hj'.H(Hj'.SIDj.S)))  =|>
State':=2
/\ A1':=new()
/\ M1':=xor(H(SIDj.Hj'.H(Hj'.SIDj.S)),H(H(H(IDi.S).T).H(IDi.Ri')))
/\ M2':=xor(A1',H(H(H(IDi.S).T).H(SIDj.Hj'.H(Hj'.SIDj.S))))
/\ V1':=H(A1'.H(SIDj.Hj'.H(Hj'.SIDj.S)).H(IDi.Ri'))
/\ SN(H(H(IDi.Ri').H(H(IDi.S).T)).M1'.M2'.V1')
/\ witness(US,GW,us_gw_a1,A1')

3. State = 2 /\ RV(xor(A3',H(H(H(Hj'.SIDj.S).H(SIDj.B)).Hj')).H(H(H(H(IDi.S).T).A1'.A2'.A3').A3'.H(H(IDi.S).T)))
/\ RV({H(IDi.Ri')}_SKu)  =|>
State':=3
/\ RIDinew':=H(A2'.H(H(IDi.Ri').H(H(IDi.S).T)))
/\ SK':=H(H(H(IDi.S).T).A1'.A2'.A3')
/\ witness(HD,GW,hd_gw_a2,A2')
end role
```

**FIGURE 9.** Role of the home user.



```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/authentication.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed    : 4 states
 Reachable   : 0 states
 Translation:  0.09 seconds
 Computation:  0.00 seconds
```

```
% OFMC
% Version  of 2006/02/13
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS

PROTOCOL
 /home/span/span/testsuite/results/authentication.if

GOAL
 as_specified

BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime:  0.00s
 searchTime:  10.29s
 visitedNodes:  3424 nodes
 depth:  12 plies
```

**FIGURE 10.** AVISPA result.

## VIII. PERFORMANCE ANALYSIS

In this section, we estimate the computational consumption and communication cost to evaluate the performance of the proposed authentication scheme. Furthermore, we compare the security functionality of our scheme with related authentication schemes [10], [19], [21], [22], [23], [24], [25], [26].

### A. COMPUTATIONAL CONSUMPTION

We evaluate the computation cost to prove the computational efficiency of the proposed authentication scheme. We denote the consumption time of one-way hash function, fuzzy extractor, elliptic curve scalar multiplication, PUF, and symmetric cryptography operation as $T_h$, $T_f$, $T_{mul}$, $T_p$ and $T_s$, respectively. According to [26], each time is defined as $T_h = 0.0026$ *ms*, $T_f = 1.989$ *ms*, $T_{mul} = 1.989$ *ms*, $T_p = 0.12$ *ms* and $T_s = 0.00325$ *ms*. Table 4 compares the computaional consumption of our scheme with the existing related schemes. The proposed scheme has a higher computational consumption than Fakroon *et al.*'s [19] authentication scheme, which uses only the one-way hash function. However, their scheme is vulnerable to offline-password guessing and insider attacks. We can achieve better security characteristics by using PUF and fuzzy extractor, and our scheme is more efficient than

**TABLE 4.** Computational consumption.

| Scheme | Home user | Gateway | Home device | Total | Cost |
|---|---|---|---|---|---|
| Fakroon *et al.* [19] | $4T_h$ | $5T_h$ | $3T_h$ | $12T_h$ | 0.0312ms |
| Li *et al.* [21] | $T_f + 2T_{mul} + 2T_s + 7T_h$ | $T_{mul} + 4T_s + 8T_h$ | $2T_s + 4T_h$ | $T_f + 3T_{mul} + 8T_s + 19T_h$ | 8.0314ms |
| Naoui *et al.* [22] | $2T_{mul} + 2T_{sym} + 7T_h$ | $T_{mul} + 3T_s + 8T_h$ | $T_s + 2T_h$ | $3T_{mul} + 6T_s + 17T_h$ | 6.0307ms |
| Shuai *et al.* [23] | $2T_{mul} + 6T_h$ | $T_{mul} + 7T_h$ | $3T_h$ | $3T_{mul} + 16T_h$ | 6.0086ms |
| Liu *et al.* [24] | $T_f + 2T_s + 8T_h$ | $T_f + 5T_s + 11T_h$ | $2T_p + T_f + 2T_s + 6T_h$ | $2T_p + 3T_f + 9T_s + 25T_h$ | 6.2850ms |
| Chen and Chen [25] | $T_p + 2T_f + 14T_h$ | $8T_h$ | $T_f + 8T_h$ | $T_p + 3T_f + 30T_h$ | 6.1650ms |
| Xia *et al.* [26] | $T_f + T_s + 10T_h$ | $4T_s + 9T_h$ | $T_f + T_p + 3T_s + 5T_h$ | $T_p + 2T_f + 8T_s + 24T_h$ | 4.1864ms |
| Zou *et al.* [10] | $3T_{mul} + 6T_h$ | $T_{mul} + 6T_h$ | $2T_{mul} + 6T_h$ | $6T_{mul} + 6T_h$ | 11.9496ms |
| Ours | $15T_h$ | $12T_h$ | $T_p + T_f + 7T_h$ | $T_p + T_f + 34T_h$ | 2.1974ms |

**TABLE 5.** Communication costs.

| Scheme | Messages | Total cost |
|---|---|---|
| Fakroon *et al.* [19] | 4 | 2720 bits |
| Li *et al.* [21] | 4 | 2816 bits |
| Naoui *et al.* [22] | 3 | 1920 bits |
| Shuai *et al.* [23] | 4 | 2880 bits |
| Liu *et al.* [24] | 4 | 2848 bits |
| Chen and Chen [25] | 5 | 2880 bits |
| Xia *et al.* [26] | 6 | 3648 bits |
| Zou *et al.* [10] | 4 | 2976 bits |
| Ours | 4 | 2368 bits |

**TABLE 6.** Security properties.

| Property | [19] | [21] | [22] | [23] | [24] | [25] | [26] | [10] | Ours |
|---|---|---|---|---|---|---|---|---|---|
| S1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| S2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ |
| S3 | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| S4 | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| S5 | ✓ | ✓ | - | - | - | - | - | ✓ | ✓ |
| S6 | - | × | - | - | ✓ | ✓ | ✓ | × | ✓ |
| S7 | × | - | ✓ | - | - | ✓ | - | ✓ | ✓ |
| S8 | - | × | × | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| S9 | ✓ | ✓ | × | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| S10 | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| S11 | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | × | ✓ |
| S12 | ✓ | × | × | × | × | × | × | × | ✓ |

✓: Achieved, × : Does not achieved, - : Does not considered

related schemes that utilize ECC and symmetric cryptography.

### B. COMMUNICATION COST

To evaluate the communication cost of the proposed scheme, we calculate the length of messages exchanged during authentication and key agreement. Referring to [24], the length of the identity, random nonce, and one-way hash output, timestamp, elliptic curve point, PUF, and symmetric cryptography block sizes are 160, 160, 160, 32, 320, 128, and 128 bits, respectively. In our scheme, messages exchanged on public channels are $\{RID_i, M_1, M_2, V_1\}$, $\{RID_i, M_3, M_4, V_2\}$, $\{M_5, V_3\}$, and $\{M_6, V_4\}$. Therefore, communication costs are 160+160+160+160=640 bits, 160+448+160+160=928 bits, 160+160=320 bits, and 320+160=480 bits. The total communication cost of related schemes and our scheme are summarized in Table 5. Our scheme has a higher communication cost compared to [22]. However, our scheme is more efficient than other related schemes. Therefore, our scheme is sufficiently efficient in smart home environments.

### C. SECURITY FUNCTIONALITY

To evaluate the security functionality of the proposed authentication scheme, we compare the security characteristics between the related schemes and ours in Table 6. In this paper, we denote each security property as follows. S1: “Resists smart card stolen attack”, S2: “Resists forgery attack”, S3: “Resists offline password guessing attack”, S4: “Resists replay attack”, S5: “Resists verifier stolen attack”, S6: “Resists ephemeral secret leakage attack”, S7: “Resists insider attack”, S8: “Resists device capture attack”, S9: “Provides user anonymity”, S10: “Provides perfect forward secrecy”, S11: “Provides mutual authentication”, S12: “Conducts AVISPA simulation”. As shown in Table 6, the proposed scheme is more secure against various security attacks than the related schemes and guarantees user anonymity and mutual authentication. Therefore, our scheme provides secure communication in smart home environments.

## IX. CONCLUSION

In this paper, we proved that Zou *et al.*’s authentication and key agreement scheme proposed in smart home environments using IoT is vulnerable to forgery, ephemeral secret leakage, and session key disclosure attacks and does not guarantee mutual authentication. We proposed an improved authentication scheme to provide secure communication and achieve various security functions in smart home systems. Furthermore, our scheme utilized PUF and fuzzy extractors to overcome device capture attack on home devices. We demonstrated that our scheme is secure from various security vulnerabilities by performing informal security analysis and AVIPA simulation. In addition, we verified the validity of our authentication scheme using BAN logic and ROR model. Finally, the performance of the proposed scheme was analyzed by comparing the previously proposed authentication scheme with communication cost, computational consumption, and security properties. In the future, we will estimate the packet delay rate, end-to-end delay, and throughput of the proposed scheme by additional simulations to evaluate the efficiency. Then, we will improve the proposed scheme to design a user authentication scheme suitable for IoT environments including practical smart home environments.

## REFERENCES

[1] W. Yan, Z. Wang, H. Wang, W. Wang, J. Li, and X. Gui, "Survey on recent smart gateways for smart home: Systems, technologies, and challenges," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e4067, Jun. 2022.

[2] D. Bouchabou, S. M. Nguyen, C. Lohr, B. LeDuc, and I. Kanellos, "A survey of human activity recognition in smart Homes based on IoT sensors algorithms: Taxonomies, challenges, and opportunities with deep learning," *Sensors*, vol. 21, no. 18, p. 6037, Sep. 2021.

[3] Z. A. Almusaylim and Z. Noor, "A review on smart home present state and challenges: Linked to context-awareness Internet of Things (IoT)," *Wireless Netw.*, vol. 25, no. 6, pp. 3193–3204, Aug. 2019.

[4] D. K. Kwon, S. J. Yu, J. Y. Lee, S. H. Son, and Y. H. Park, "WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks," *Sensors*, vol. 21, no. 3, p. 936, Jan. 2021.

[5] A. K. Sutrala, M. S. Obaidat, S. Saha, A. K. Das, M. Alazab, and Y. Park, "Authenticated key agreement scheme with user anonymity and untraceability for 5G-enabled softwarized industrial cyber-physical systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2316–2330, Mar. 2022.

[6] G. Abbas, M. Tanveer, Z. H. Abbas, M. Waqas, T. Baker, and D. Al-Jumeily, "A secure remote user authentication scheme for 6LoWPAN-based Internet of Things," *PLoS ONE*, vol. 16, no. 11, Nov. 2021, Art. no. e0258279.

[7] C.-M. Chen, X. Deng, S. Kumar, S. Kumari, and S. H. Islam, "Blockchain-based medical data sharing schedule guaranteeing security of individual entities," *J. Ambient Intell. Humanized Comput.*, Aug. 2021, doi: 10.1007/s12652-021-03448-7.

[8] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Netw.*, vol. 20, pp. 1–15, Sep. 2014.

[9] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Future Gener. Comput. Syst.*, vol. 56, pp. 719–733, Mar. 2016.

[10] S. Zou, Q. Cao, C. Wang, Z. Huang, and G. Xu, "A robust two-factor user authentication scheme-based ECC for smart home in IoT," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4938–4949, Sep. 2022, doi: 10.1109/JSYST.2021.3127438.

[11] F. Armknecht, R. Maes, A.-R. Sadeghi, B. Sunar, and P. Tuyls, "Memory leakage-resilient encryption based on physically unclonable functions," in *Proc. ASIACRYPT*, in Lecture Notes in Computer Science, vol. 5912, 2009, pp. 685–702.

[12] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. 8th Int. Theory Pract. Public Key Cryptograph. (PKC)*, 2005, pp. 65–84.

[13] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[14] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electron. Notes Theor. Comput. Sci.*, vol. 155, pp. 61–86, May 2006.

[15] L. Chen, F. Wei, and C. Ma, "A secure user authentication scheme against smart-card loss attack for wireless sensor networks using symmetric key techniques," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 4, Apr. 2015, Art. no. 704502.

[16] J. Jung, J. Kim, Y. Choi, and D. Won, "An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 8, p. 1299, Aug. 2016.

[17] L. Xiong, D. Peng, T. Peng, H. Liang, and Z. Liu, "A lightweight anonymous authentication protocol with perfect forward secrecy for wireless sensor networks," *Sensors*, vol. 17, no. 11, p. 2681, 2017.

[18] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and secure session-key establishment scheme in smart home environments," *IEEE Sensors J.*, vol. 16, no. 1, pp. 254–264, Jan. 2016.

[19] M. Fakroon, M. Alshahrani, F. Gebali, and I. Traore, "Secure remote anonymous user authentication scheme for smart home environment," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100158.

[20] M. Saqib, B. Jasra, and A. H. Moon, "A lightweight three factor authentication framework for IoT based critical applications," *J. King Saud Univ.-Comput. Inf. Sci.*, Aug. 2021, doi: 10.1016/j.jksuci.2021.07.023.

[21] 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 Things J.*, vol. 5, no. 3, pp. 1606–1615, Jun. 2018.

[22] S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Lightweight and secure password based smart home authentication protocol: LSP-SHAP," *J. Netw. Syst. Manage.*, vol. 27, no. 4, pp. 1020–1042, Oct. 2019.

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

[24] Z. Liu, C. Guo, and B. Wang, "A physically secure, lightweight three-factor and anonymous user authentication protocol for IoT," *IEEE Access*, vol. 8, pp. 195914–195928, 2020.

[25] Y. Chen and J. Chen, "An efficient mutual authentication and key agreement scheme without password for wireless sensor networks," *J. Supercomput.*, vol. 77, no. 12, pp. 13653–13675, Dec. 2021.

[26] Y. Xia, R. Qi, S. Ji, J. Shen, T. Miao, and H. Wang, "PUF-assisted lightweight group authentication and key agreement protocol in smart home," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–15, Mar. 2022.

[27] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptograph. Tech.*, Interlaken, Switzerland, 2004, pp. 523–540.

[28] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[29] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2002, pp. 337–351.

[30] A. K. Das, B. Bera, M. Wazid, S. S. Jamal, and Y. Park, "On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure," *IEEE Access*, vol. 9, pp. 71856–71867, 2021.

[31] S. Son, Y. Park, and Y. Park, "A secure, lightweight, and anonymous user authentication protocol for IoT environments," *Sustainability*, vol. 13, no. 16, p. 9241, Aug. 2021.

[32] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, and Y. Park, "Secure ECC-based three-factor mutual authentication protocol for telecare medical information system," *IEEE Access*, vol. 10, pp. 11511–11526, 2022.

[33] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May 2022.

[34] D. Kwon, S. Son, Y. Park, H. Kim, Y. Park, S. Lee, and Y. Jeon, "Design of secure handover authentication scheme for urban air mobility environments," *IEEE Access*, vol. 10, pp. 42529–42541, 2022.

[35] P. R. Babu, R. Amin, A. G. Reddy, A. K. Das, W. Susilo, and Y. Park, "Robust authentication protocol for dynamic charging system of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 11338–11351, Nov. 2021.

[36] M. Umar, S. H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar, and M. A. Saleem, "Provable secure identity-based anonymous and privacy-preserving inter-vehicular authentication protocol for VANETS using PUF," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 12158–12167, Nov. 2021.

[37] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.

[38] M. Kim, J. Lee, K. Park, Y. Park, K. H. Park, and Y. Park, "Design of secure decentralized car-sharing system using blockchain," *IEEE Access*, vol. 9, pp. 54796–54810, 2021.

[39] J. Lee, M. Kim, J. Oh, Y. Park, K. Park, and S. Noh, "A secure key aggregate searchable encryption with multi delegation in cloud data sharing service," *Appl. Sci.*, vol. 11, no. 19, p. 8841, Sep. 2021.

[40] I. U. Haq, J. Wang, and Y. Zhu, "Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, Art. no. 102660.

[41] C.-M. Chen, X. Deng, W. Gan, J. Chen, and S. K. H. Islam, "A secure blockchain-based group key agreement protocol for IoT," *J. Supercomput.*, vol. 77, no. 8, pp. 9046–9068, Aug. 2021.

[42] D. Chattaraj, B. Bera, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing fine-grained access control for software-defined networks using private blockchain," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1542–1559, Jan. 2022.

[43] J. Lee, G. Kim, A. K. Das, and Y. Park, "Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2412–2425, Sep. 2021.

[44] R. Amin, S. H. Islam, P. Gope, K.-K. R. Choo, and N. Tapas, "Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system," *IEEE J. Biomed. Health Inform.*, vol. 23, no. 4, pp. 1749–1759, Jul. 2019.

**YEONGJAE CHO** received the B.S. degree in electronics engineering from Kyungpook National University, Daegu, South Korea, in 2020, where he is currently pursuing the M.S. degree with the School of Electronic and Electrical Engineering. His research interests include cryptography and information security.

**JIHYEON OH** received the B.S. degree in electronics engineering and the M.S. degree in electronic and electrical engineering from Kyungpook National University, Daegu, South Korea, in 2020 and 2022, respectively, where she is currently pursuing the Ph.D. degree with the School of Electronic and Electrical Engineering. Her research interests include the Internet of Things and information security.

**DEOKKYU KWON** received the B.S. degree in electronics engineering and the M.S. degree in electronic and electrical engineering from Kyungpook National University, Daegu, South Korea, in 2020 and 2022, respectively, where he is currently pursuing the Ph.D. degree with the School of Electronic and Electrical Engineering. His research interests include the internet of drones, wireless sensor networks, and information security.

**SEUNGHWAN SON** received the B.S. degree in mathematics and M.S. degree in electronic and electrical engineering from Kyungpook National University, Daegu, South Korea, in 2019 and 2021, respectively, where he is currently pursuing the Ph.D. degree with the School of Electronic and Electrical Engineering. His research interests include blockchain, cryptography, and information security.

**JOONYOUNG LEE** (Student Member, IEEE) received the B.S. and M.S. degrees in electronics engineering from Kyungpook National University, Daegu, South Korea, in 2018 and 2020, respectively, where he is currently pursuing the Ph.D. degree with the School of Electronics Engineering. His research interests include authentication, the Internet of Things, blockchain, and information security.

**YOUNGHO PARK** (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. From 1996 to 2008, he was a Professor at the School of Electronics and Electrical Engineering, Sangju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar at the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor with the School of Electronic and Electrical Engineering, Kyungpook National University. His research interests include computer networks, multimedia, and information security.