symmetry

MDPI

Article

A Robust and Anonymous Three-Factor Authentication Scheme Based ECC for Smart Home Environments

Xiong Wang, Yuan Teng *, Yaping Chi and Hongbo Hu

Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
* Correspondence: tycamus@163.com; Tel.: +86-185-9202-2516

Abstract: With the rapid development of the Internet of Things (IoT) industry, the smart home is fully integrated with people's shelter and transportation, which facilitates people's daily life. A smart home without a security authentication mechanism will inevitably cause a series of security threats. This is essentially a problem of symmetry model worth solving. In fact, researchers have designed various authentication schemes to verify the identity of users and to ensure smart devices can be legally accessed through authorization in the smart home. In 2021, Yu proposed a three-factor anonymous authentication scheme for smart homes using lightweight symmetric encryption primitives and stated that their scheme is resistant to various known security attacks. However, after careful analysis, we found that Yu's scheme needs further improvement in node capture attack and offline password guessing attack and that forward security cannot be guaranteed. Therefore, we first design a robust three-factor anonymous authentication scheme for smart homes based on asymmetric encryption Elliptic Curve Cryptography (ECC). Then, we perform formal and informal security analysis in which the formal analysis tools include Burrows-Abadi-Needham (BAN) logic and Scyther simulation tool to prove that the proposed scheme can achieve user anonymity, untraceability, and session key forward security. Meanwhile, mutual authentication is performed, and the scheme is resistant to all known attacks described in this article. Finally, a performance comparison is made in terms of efficiency, which shows that our scheme can have certain advantages with those newly designed schemes, achieve a delicate balance in performance and safety, and is more practical for the real smart home environment.

Keywords: smart home; authentication; elliptic curve cryptography; robust; privacy protection

Citation: Wang, X.; Teng, Y.; Chi, Y.; Hu, H. A Robust and Anonymous Three-Factor Authentication Scheme Based ECC for Smart Home Environments. *Symmetry* **2022**, *14*, 2394. https://doi.org/10.3390/sym14112394

Academic Editors: Chin-Ling Chen, Jeng-Shyang Pan and Sergei D. Odintsov

Received: 27 September 2022
Accepted: 9 November 2022
Published: 12 November 2022

1. Introduction

With the rapid growth of 5G communication technology and the IoT ecosystem, the smart home and its device networks are gradually integrating with people's lives. The smart home itself is a new concept [1]. Whether in academia or industry, the smart home has attracted the attention of many researchers.

A smart home can be an intelligent communication network composed of some commonly used smart devices, such as smart curtains, node sensors, smart TVs, and smart lights [2–4]. Smart devices in smart homes provide people with convenience in life through human–computer interaction. The home automation system reduces operating costs and improves user comfort. In smart home environments, users can utilize electronic portable devices to enjoy new smart functions. For example, before returning home, users can remotely turn on heating or cooling devices to control the indoor temperature to maintain a comfortable state. In addition, users can remotely monitor home electricity safety and power consumption during working hours. At the same time, users can use smart wearable devices to check the health and life status of the elderly at all times so as to accurately provide life support services for patients with chronic diseases, middle-aged and elderly people and the disabled [5]. Unfortunately, despite the various significant advantages of

smart homes, it is vulnerable to various privacy and security issues due to the transmission interaction of information in wireless public network channels [6–8].

If the data collected in smart devices is leaked, malicious attackers can obtain various sensitive information and identity characteristics of legitimate users, including daily life habits and home movement trajectories, etc. [9]. Therefore, it is very necessary to ensure user safety and strengthen communication confidentiality for smart homes.

A typical smart home network [4] consists of user, gateway, smart device and registration authority (RA). Various types of smart devices are installed in the home environment, and their resources, such as computing power, communication power, and battery power, are limited in actual operation [5]. The RA is a trusted device that provides registration services for users and smart devices through a secure channel. Therefore, all data sent and received for registration cannot be tampered with by an attacker. The gateway node is a transit station for communication between users and smart devices, and it also connects smart devices to the world with the help of the Internet. While the information of these channels is public, it is essential to protect these sensitive real-time data from unauthorized access, an authentication mechanism [10,11] is needed to identify the user and establish the session key.

Designing a secure negotiation protocol is difficult because of the balance between security and efficiency. Due to some of the above problems and reasons, traditional cryptosystems cannot be used to provide lightweight authentication in smart home networks. ECC can be used as an efficient scheme for smart home because it requires less computing resources and has a smaller bit space compared to them [12].

At present and in the future, the most promising work is aimed to improve the existing schemes. Yu et al. [13] proposed a three-factor privacy anonymity scheme for smart home environments. They claim that their scheme is lightweight, privacy-anonymous, and resistant to attacks such as session key leakage. However, after a comprehensive analysis of Yu et al.'s scheme [13], we found security vulnerabilities in their schemes, including offline node capture attack, password guessing attack and session key leakage attack. Therefore, we propose a three-factor authentication scheme for smart homes based on ECC, hash, and XOR operation, which can overcome the above problems and can achieve multiple security properties. Actually, these attacks are extremely common and harmful in smart homes. For example, node capture attack is often used by malicious thieves as the first choice for obtaining confidential information in multi-node environments. Hence, our proposed scheme is a huge improvement over the scheme of Yu et al., and is more applicable to practical smart home environments. At the same time, our performance sacrifices are negligible in reasonable ranges.

1.1. Motivation and Contributions

A smart home environment that lacks an authentication mechanism will inevitably suffer from security threats from malicious attackers. However, the existing security authentication protocols based on identity privacy have more or less room for improvement as far as security properties and efficiency are concerned, which stimulates us to design an authentication scheme for the smart home. With superior security properties, the proposed scheme achieves a more balanced effect in terms of efficiency. Our contributions are summarized below:

- Three security threats discovered by Yu et al.'s scheme analysis: Through detailed security analysis, we demonstrate that Yu et al.'s [13] scheme cannot resist node capture attack and offline password guessing attack, and at the same time, cannot achieve forward security.
- A robust three-factor authentication scheme designed for a smart home: On the basis of Yu et al.'s scheme [13], we propose a three-factor authentication scheme based on ECC to provide security services for legitimate users in smart home, which can perform mutual authentication among the three entities, and at the same time generate a session key established by the user and the smart device. Additionally, our scheme

enables changing user passwords and biometrics, as well as adding smart devices, anytime, anywhere;

- Security and efficiency: In terms of security properties, the proposed protocol is proven to resist node capture attack, offline password guessing attack and achieve forward security. Complete formal proofs and informal security analysis demonstrate that our scheme can not only generate secure session keys but also achieve more security features and resist various known security attacks. Then, we compare the performance of the proposed scheme with related authentication schemes published in recent years, and the results demonstrate that the scheme achieves a delicate balance between security and efficiency and is suitable for real-world environments. This also illustrates that our scheme is more suitable.

1.2. Organization

The article is organized as follows. Section 2 describes related works and Section 3 generalizes preliminary works. In Sections 4 and 5, we briefly introduce Yu et al.'s scheme and analyze the flaws and vulnerabilities of his scheme. Our scheme is presented in Section 6. In Sections 7 and 8, the security and performance analyses of the proposed scheme are carried out. Finally, Section 9 concludes the article and prospects for the future of related works.

2. Related Works

In recent years, researchers have proposed to ensure communication security in the smart home environment by constructing a safe and effective AKA scheme. In 2008, in order to realize the authorized access of home users to smart devices, Jeong et al. [14] proposed a lightweight AKA protocol suitable for the home network environment, which is based on two factors password and smart card. However, the scheme cannot protect the privacy of the user's identity. At the same time, it only focuses on the mutual authentication between the user and the gateway, and lacks the mutual authentication process between the gateway and the smart device or between the user and the smart device. In addition, the scheme of Jeong et al. [14] is also vulnerable to attacks such as smart card loss attack, node capture attack, and privileged insider attack. In 2011, Vaidya et al. [15] proposed a password-based lightweight remote authentication scheme. The scheme adopts the hash-based one-time password operation to realize the authentication between the user and the server, and realizes the mutual authentication between the user and the gateway through the one-way hash chain technology. In the same year, Kim et al. [16] analyzed the scheme of Vaidya et al. [15] and proved that the protocol not only cannot resist offline password guessing attacks, but also cannot achieve forward security and user privacy security. In addition, the scheme of Vaidya et al. [15] also lacks mutual authentication between the gateway node and the smart device. Nevertheless, the scheme proposed by Kim et al. [16] also lacks the indispensable mutual authentication function between the three entities. In 2017, Kumar et al. [4] proposed an anonymous security framework suitable for smart home environments based on lightweight encryption primitives. The framework enables mutual authentication and key negotiation between the smart device and the gateway node, and ensures that devices are anonymous and unlinkable. In 2019, Poh et al. [17] proposed a privacy protection authentication scheme PrivHome for smart home secure communication and data storage. The scheme is constructed from two protocols: the first protocol is a lightweight authentication protocol that can provide mutual authentication for users and smart devices; the second protocol is a searchable encryption protocol for smart device authentication privacy-preserving encrypted queries. Unfortunately, the scheme of Poh et al. [17] is still not resistant to potential desynchronization attack.

Different from the above schemes based on lightweight encryption primitives, researchers have also tried to build AKA schemes using asymmetric encryption algorithms. These schemes have better security performance and can be more suitable for adversary attack environments of smart home. In 2015, Santoso and Vun [18] proposed an AKA proto-

col suitable for smart home environment based on ECC technology. However, the scheme cannot realize the privacy protection of the user's identity. Additionally, their scheme is vulnerable to smart card loss attack and privileged insider attack. In 2019, Yu and Li [19] proposed another user authentication scheme for smart home. Their scheme does not require users and devices to be in a secure environment during the registration process, but uses bilinear pairing operation, which is computationally expensive and not practical in smart home environments. In order to improve the efficiency of designing the authentication scheme, Shuai [20] proposed an ECC-based smart home identity authentication scheme in the same year. However, Xu et al. [21] pointed out [20] that there are security vulnerabilities such as offline password guessing attack and insider privilege attack. In 2021, Kaur and Kumar [22] proposed an enhanced scheme based on two-factor authentication to overcome the security problems of the scheme of Shuai et al. [20]. They claim their scheme is resistant to potential security attacks and also guarantees user anonymity, privacy, and mutual authentication. However, in the same year, Yu et al. [13] proved that the scheme proposed by Kaur and Kumar is prone to several weaknesses, including the exposure risk of session keys and the inability to resist impersonation attacks. Furthermore, Yu et al. [13] also claim that Kaur and Kumar's scheme [22] cannot provide mutual authentication. Thus, in the paper, we will analyze the security issues of Yu et al.'s [13] protocol and explore the strengths, weaknesses, and efficiency performance of various schemes. At the same time, compared with these schemes [13,19,20,22–24], we will propose a robust smart home three-factor authentication scheme to ensure security while guaranteeing efficiency.

3. Preliminaries

This section mainly introduces the indispensable models and notions to enhance the readability.

3.1. System Model

The system model of smart home is shown in Figure 1. In a smart home environment with wireless sensors, the system model typically consists of four entities. The specific details are as follows:

- Registration Authority (RA): RA is an absolute trusted third entity that must be responsible for the participants in communications;
- Gateway: As an intermediary for users and device nodes to pass information, the gateway assumes the responsibility for communication security. Meanwhile, the gateway also provides users with many convenient interactive services;
- User: User can use the various functions of the smart home anywhere by registering with the RA as legitimate users;
- Smart Device: Smart devices, as the nerve endings of smart homes to collect information, can pass real-time dynamic information through the gateway to legitimate users, including various sensor nodes and smart home appliances.

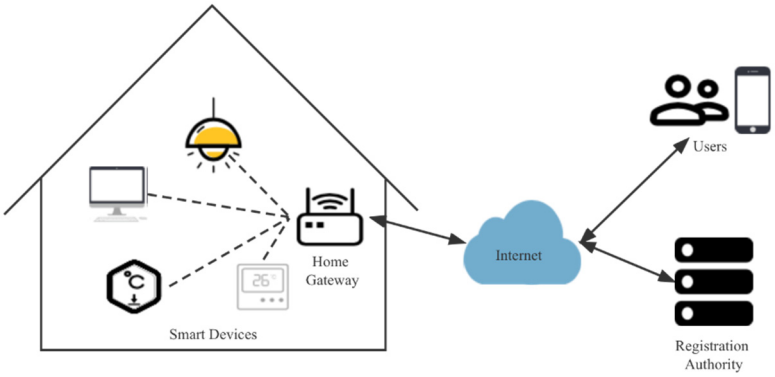

Figure 1. System model for smart home.

3.2. Threat Model

The Dolev–Yao [25] threat model is the most widely accepted attacker model in security protocol analysis. According to the model, if any two parties communicate on an insecure channel, the endpoint entity is not regarded as a trusted entity, and its transmission information is not in a secure channel. Based on this threat model and improved attacker capabilities, the capabilities of adversary $\mathcal{A}$ are summarized as follows:

- $\mathcal{A}$ may be a legitimate but malicious actor [26];
- $\mathcal{A}$ may be a legitimate but malicious sensor node that can obtain all the information of a limited number of sensor nodes [27,28];
- $\mathcal{A}$ can easily intercept, modify, destroy and delete information transmitted over insecure public communication channels;
- $\mathcal{A}$ can obtain all secret values stored in the smart terminal through side-channel attacks [26];
- $\mathcal{A}$ can obtain the system long-term key when evaluating forward security [29];
- $\mathcal{A}$ can guess and steal passwords and identifying information over polynomial time.
- In the n-factor protocol, $\mathcal{A}$ can obtain any (n − 1) factor information [27];
- In particular, when forward security is not evaluated, the gateway and base station of the system are trusted, and the information such as long-term keys stored by the gateway is safe.

3.3. Notions

For ease of notation and understanding by researchers, some of the shorthand notations used in our scheme are described in Table 1.

Table 1. Notions and descriptions.

Symbol	Description
U_a	User
GWN	Gateway Node
SD_j	Smart Device
RA	Registration Authority
SID_j, GID_k	Identity of SID_j and GWN
Ts_i	Timestamp
r	Nonce
ID_i, PW_i	U_a's identity and password
K	Master key of GWN
K_{GU}	Secret key between U_a and GWN
K_{GS}	Secret key between GWN and SD_j
SK	Session key
$\|\|, \oplus$	Join, XOR operations
$h(\cdot)$	Hash Function

4. Review of Yu et al.'s Scheme

The Section shows review of Yu et al.'s scheme [13]. Their scheme consists of registration phase, login and mutual authentication phase, and password update phase.

4.1. Registration Phase

4.1.1. User Registration Phase

In the user registration phase, the user U_a registers with RA.

- **Step 1:** In order to send a registration request, the user generates a random number r_i, selects the identity ID_i, the password PW_i, computes $Gen(Bio_i) = \langle \gamma_i, \beta_i \rangle$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$, and transmits $\{RID_i, RPW_i, r_i\}$ to RA via a secure channel;
- **Step 2:** RA computes $K_{GU} = h(RID_i||K||r_i)$, $C_1 = K_{GU} \oplus h(RPW_i||r_i)$, then RA transmits the secret key K_{GU} to the gateway GWN via the secure channel. Upon receiving

K_{GU} from RA, GWN computes $L_k = h(GID_i||K) \oplus K_{GU}$, stores it in the gateway GWN, and transmits C_1 to the smart card which saves it;

- **Step 3:** U_a computes $K_i = h(ID_i||PW_i||\gamma_i)$, $C_2 = E_{Ki}(C_1)$, $C_3 = r_i \oplus h(RID_i||RPW_i)$, $C_4 = h(RID_i||RPW_i||r_i) \mod v$, where $v \in [2^4, 2^8]$. After that, U_a deletes C_1 in the smart card, and stores $\{C_2, C_3, C_4\}$ secret parameter into the smart card.

4.1.2. Smart Device Registration Phase

- **Step 1:** In order to send a registration request, the user generates a random number r_i, selects the identity ID_i, the password PW_i, computes $Gen(Bio_i) = \langle \gamma_i, \beta_i \rangle$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$, and transmits $\{RID_i, RPW_i, r_i\}$ to RA via a secure channel;
- **Step 2:** RA computes $K_{GU} = h(RID_i||K||r_i)$, $C_1 = K_{GU} \oplus h(RPW_i||r_i)$, then RA transmits the secret key K_{GU} to the gateway GWN via the secure channel. Upon receiving K_{GU} from RA, GWN computes $L_k = h(GID_i||K) \oplus K_{GU}$, stores it in the gateway GWN, and transmits C_1 to the smart card which saves it;
- **Step 3:** U_a computes $K_i = h(ID_i||PW_i||\gamma_i)$, $C_2 = E_{Ki}(C_1)$, $C_3 = r_i \oplus h(RID_i||RPW_i)$, $C_4 = h(RID_i||RPW_i||r_i) \mod v$, where $v \in [2^4, 2^8]$. After that, U_a deletes C_1 in the smart card, and stores $\{C_2, C_3, C_4\}$ secret parameter into the smart card.

4.2. Login and Mutual Authentication Phase

- **Step 1:** The user U_a enters ID_i, PW_i and fingerprints biometric information Bio_i. Then the smart card computes $\gamma_i = Rep(Bio_i, \beta_i)$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$, $K_i = h(ID_i||PW_i||\gamma_i)$ and extracts C_2 from the memory, to compute $C_1 = D_{Ki}(C_2)$, $K_{GU} = C_1 \oplus h(RPW_i||r_i)$, $r_i = C_3 \oplus h(RID_i||RPW_i)$, $C_4^* = h(RID_i||RPW_i||r_i) \mod v$, where $v \in [2^4, 2^8]$, and check whether $C_4^* = C_4$. If the equation is valid, the smart card generates a random numbers r_a, $w \in Z_n^*$, the timestamp Ts_1. U_a selects the target smart device SD_j, and the smart card starts to compute $M_1 = (SID_j||r_a) \oplus K_{GU} \oplus Ts_1$, $M_2 = RID_i \oplus h(K_{GU}||r_a||Ts_1)$, $V_1 = h(RID_i||K_{GU}||r_a||Ts_1)$. Afterwards, the smart card sends $\{M_1, M_2, V_1, Ts_1\}$ to GWN;
- **Step 2:** After receiving the message from U_a, GWN extracts L_k from the database, and first computes $K_{GU} = h(GID_k||K) \oplus L_k$, $(SID_j||r_a) = M_1 \oplus K_{GU} \oplus Ts_1$, $RID_i = M_2 \oplus h(K_{GU}||r_a||Ts_1)$, $V_1^* = h(RID_i||K_{GU}||r_a||Ts_1)$, and verify if $V_1^* = V_1$. If it is equal, it means that the verification is completed, and then a random number r_b and the timestamp Ts_2 is generated by GWN. Furthermore, GWN computes $K_{GS} = h(TID_j||K||r_j)$, $M_3 = (RID_i||GID_k||r_a||r_b) \oplus h(SID_j||K_{GS}||Ts_2)$, $V_2 = h(RID_i||GID_k||K_{GS}||r_a||r_b||Ts_2)$, and transmits $\{M_3, V_2, Ts_2\}$ to SD_j;
- **Step 3:** On receiving the message from the gateway GWN, SD_j extracts $\{B_1, B_2\}$ from the memory, computes $r_j = B_1 \oplus h(K_{SD}||SID_j)$, $K_{GS} = B_2 \oplus h(K_{SD}||r_j)$, $(RID_i||GID_k||C_4||r_a||r_b) = M_3 \oplus h(SID_j||K_{GS}||Ts_2)$, $V_2^* = h(RID_i||GID_k||K_{GS}||r_a||r_b||Ts_2)$, verify whether $V_2^* = V_2$ is established. If so, then certification passed. After that, SD_j generates a random number r_c, the timestamp Ts_3, and computes a session key $SK = h(r_a||r_b||r_c||RID_i||GID_k||SID_j))$, $M_4 = r_c \oplus h(K_{GS}||RID_i||GID_k||Ts_3)$, $V_3 = h(SID_j||r_c||K_{GS}||SK||Ts_3)$. Finally, SD_j transmits $\{M_4, V_3, Ts_3\}$ to GWN;
- **Step 4:** After receiving the message sent by the smart device SD_j, GWN computes $r_c = M_4 \oplus h(K_{GS}||RID_i||GID_k||Ts_3)$, $SK = h(r_a||r_b||r_c||RID_i||GID_k||SID_j)$, $V_3^* = h(SID_j||r_c||K_{GS}||SK||Ts_3))$, and verify if V_3^*=V_3. If the equation holds, the authentication is completed. Then GWN generates the timestamp Ts_4 and computes $M_5 = (GID_k||r_b||r_c) \oplus h(RID_i||K_{GU}||r_a||Ts_4)$, $V_4 = h(RID_i||GID_k||r_a||r_b||SK||Ts_4)$. Lastly, GWN transmits the message $\{M_5, V_4, Ts_4\}$ to U_a;
- **Step 5:** On receiving the message from GWN, U_a first computes $(GID_k||r_b||r_c) = M_5 \oplus h(RID_i||K_{GU}||r_a||Ts_4)$, $SK = h(r_a||r_b||r_c||RID_i||GID_k||SID_j)$, $V_4^* = h(RID_i||GID_k||r_a||r_b||SK||Ts_4)$, and then verify if $V_4^* = V_4$. If the equation holds, U_a accept this response. At this point, the mutual authentication between the user and

the smart device entity is completed, and the three entities of communication have generated the session key.

4.3. Password Update Phase

- **Step 1:** U_a firstly enters the identity ID_i, the password PW_i, and fingerprints the biometric information Bio_i;
- **Step 2:** The smart card begins to compute $\gamma_i = Rep(Bio_i, \beta_i)$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$, $K_i = h(ID_i||PW_i||\gamma_i)$, $C_1 = D_{Ki}(C_2)$, $K_{GU} = C_1 \oplus h(RPW_i||r_i)$, $r_i = C_3 \oplus h(RID_i||RPW_i)$, $C_4^* = h(RID_i||RPW_i||r_i) \mod v$, where $v \in [2^4, 2^8]$, and verify if $C_4^* = C_4$. If the equation does not hold, the smart card rejects the session request. Otherwise, U_a is allowed to enter a new password and biometric feature;
- **Step 3:** U_a enters a new password PW_i^{new} and a new biometric feature Bio_i^{new} into the smart card. Then, the smart card computes $Gen(Bio_i^{new}) = \langle \gamma_i^{new}, \beta_i^{new} \rangle$, $RID_i^{new} = h(ID_i||\gamma_i^{new})$, $RPW_i^{new} = h(PW_i^{new}||\gamma_i^{new})$, $K_i^{new} = h(ID_i||PW_i^{new}||\gamma_i^{new})$, $C_2^{new} = E_{K_i^{new}}(C_1)$, $C_3^{new} = r_i \oplus h(RID_i^{new}||RPW_i^{new})$, $C_4^{new} = h(RID_i^{new}||RPW_i^{new}||r_i) \mod v$, where $v \in [2^4, 2^8]$. Finally, the smart card stores $\{C_2^{new}, C_3^{new}, C_4^{new}\}$ into the memory instead of $\{C_2, C_3, C_4\}$.

5. Cryptanalysis of Yu et al.'s Scheme

In this section, we perform cryptanalysis on Yu et al.'s scheme [13]. Yu claims that their scheme is resistant to various security attacks and implements multiple security properties, and also provides secure session keys. Unfortunately, we prove that their scheme is not resistant to potential security attacks, such as node capture attacks, offline password guessing attacks, and cannot achieve forward security.

5.1. Node Capture Attack

Node capture attack is an attacker who physically captures a sensor node and steals stored information to obtain a secret value calculated by the system. The attack is common and easy to implement in smart home multi-sensor node environments. Wang [30] listed various types of node capture attacks in detail and comprehensively of which the node capture attack in this paper is Type-I. In addition, Type-I has the following target and capability.

- $\mathcal{A}$ attack target: get the session key SK;
- $\mathcal{A}$'s unique capability: $\mathcal{A}$ can capture the node, get the long-term private key K_{SD}, and steal its stored information $\{B_1, B_2, SID_j\}$.

Step 1: Compute $b_j = B_1 \oplus h(K_{SD}||SID_j)$, $X_{GS} = B_2 \oplus h(K_{SD}||b_j)$;
Step 2: Compute $(RID_i||GID_i||r_U||r_{GW}) = M_3 \oplus h(SID_j||X_{GS}||T_2)$;
Step 3: Compute $r_{SD} = M_4 \oplus h(X_{GS}||RID_i||GID_i||T_3)$;
Step 4: Compute $SK = h(r_U||r_{GW}||r_{SD}||RID_i||GID_i||SID_j)$.

Through the above steps, attacker $\mathcal{A}$ successfully obtains the session key, and the forwarding security cannot be guaranteed.

5.2. Offline Password Guessing Attack

In authentication phase, offline password guessing attack requires an attacker to steal the secret value stored offline as well as the authentication parameters. Authentication parameters can be used to verify that the user's password is correct until the password is obtained. Yu et al.'s scheme [13] is not resistant to offline password guessing attack, and we have two attack methods to steal user's password. Next, we will introduce the steps of two attack in detail.

5.2.1. Offline Password Guessing Attack in Smart Cards

Attacker $\mathcal{A}$ can obtain the biometric *Bio* through a malicious scanner, and acquire the information $\{A_2, A_3, A_4, h(.), \beta_i, Gen(.)\}$ in the smart card through the side channel. $\mathcal{A}$ can perform password guessing attacks through the following steps.

Step 1: Guess (ID_i, PW_i) from the user space D_{id} and the password space D_{pw};
Step 2: Compute $Rep(Bio, \beta_i) = \gamma_i$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$;
Step 3: Extract A_3 from the memory of smart card, calculate $a_i = A_3 \oplus h(RID_i||RPW_i)$, $A_4^* = h(RID_i||RPW_i||a_i)$;
Step 4: Verify if $A_4^* = A_4$, and if it is established, the guess is successful. If it fails, repeat Steps 1–4 until it succeeds.

5.2.2. Offline Password Guessing Attacks on Open Channels

Once attacker $\mathcal{A}$ obtains $\{A_2, A_3, A_4, h(.), \beta_i, Gen(.)\}$ and eavesdrops on the public channel information transmitted by the user to the gateway, which includes the authentication factor, the *password* of users can be obtained by the following steps.

Step 1: Guess (ID_i, PW_i) from the user space D_{id} and the password space D_{pw};
Step 2: Compute $Rep(Bio, \beta_i) = \gamma_i$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$;
Step 3: Compute $a_i = A_3 \oplus h(RID_i||RPW_i)$, $K_i = h(ID_i||PW_i||\gamma_i)$, $A_1 = D_{K_i}(A_2)$, $X_{GU} = A_1 \oplus h(RPW_i||a_i)$, $(SID_j||r_U) = M_1 \oplus X_{GU} \oplus T_1$. At this time, $M_{UG}^* = h(RID_i||X_{GU}||r_U||T_1)$ can be computed as the verification factor, or $M_2^* = RID_i \oplus (X_{GU}||r_U||T_1)$ can be computed as the factor in the same way;
Step 4: Verify whether $M_{UG}^* = M_{UG}$ is established, and the establishment guess is successful. In addition, verify whether $M_2^* = M_2$ holds, which can be performed password guessing. If it fails, repeat Steps 1–4 until it succeeds.

5.3. No Forward Security

Implementing forward security means that past sessions including past session keys are still secure, even if the long-term session keys and the system long-term keys are exposed. However, the following steps can be used to attack the system of Yu et al. [13], and forward security will not be guaranteed due to the exposure of session keys.

- $\mathcal{A}$ attack target: get the session key *SK*;
- $\mathcal{A}$'s unique capability: obtain the long-term master key K_G of GWN, and its stored information $\{b_j, PID_j\}$.

Step 1: Compute $X_{GS} = h(PID_j||K_G||b_j)$;
Step 2: Compute $(RID_i||GID_i||r_U||r_{GW}) = M_3 \oplus h(SID_j||X_{GS}||T_2)$;
Step 3: Compute $r_{SD} = M_4 \oplus h(X_{GS}||RID_i||GID_i||T_3)$;
Step 4: Compute $SK = h(r_U||r_{GW}||r_{SD}||RID_i||GID_i||SID_j)$.

The attacker $\mathcal{A}$ successfully obtains the session key, and forward security cannot be guaranteed.

6. The Proposed Scheme

In this section, we design a robust three-factor authentication scheme for smart home. On the basis of Yu et al.'s scheme [13], we propose an authentication and key agreement scheme based on ECC to overcome the weakness of Yu et al.'s scheme, which provides various security features for legitimate users in smart home. Our proposed scheme includes the following four phases: initialization phase, registration phase, login and authentication phase, and password update phase.

6.1. System Initialization

The RA system administrator firstly selects the elliptic curve E over a prime finite field F_q, and a base point Q based on E. Furthermore, RA selects a system private key $y \in F_q$, calculates the system public key $P = y \cdot Q$, and generates an identity GID_k for GWN. Then,

RA generates a master key K to GWN, and stores it in GWN together with the system private key y. Finally, RA generates an identity SID_j for SID_j and generate long-term key K_{SD} gives SD_j.

6.2. Registration Phase

6.2.1. User Registration Phase

- **Step 1:** In order to send a registration request, the user generates a random number r_i, selects an identity ID_i, a password PW_i, enter the biometric information Bio_i, computes $Gen(Bio_i) = \langle \gamma_i, \beta_i \rangle$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$, and transmits $\{RID_i, RPW_i, r_i\}$ to RA via a secure channel;
- **Step 2:** RA computes $K_{GU} = h(RID_i||K||r_i)$, $C_1 = K_{GU} \oplus h(RPW_i||r_i)$, then RA transmits the secret key K_{GU} to the gateway GWN via the secure channel. Upon receiving K_{GU} from RA, GWN computes $L_k = h(GID_i||K) \oplus K_{GU}$, stores it in the gateway GWN, and transmits C_1 to the smart card which saves it;
- **Step 3:** U_a computes $C_2 = r_i \oplus h(RID_i||RPW_i)$, $C_3 = h(RID_i||RPW_i||r_i) \bmod v$, where $v \in [2^4, 2^8]$. After that, U_a stores $\{C_1, C_2, C_3\}$ secret parameter into the smart card.

6.2.2. Smart Device Registration Phase

- **Step 1:** The smart device SD_j generates a random number r_j, computes $TID_j = h(SID_j||r_j)$, and then transmits $\{r_j, TID_j\}$ to RA via a secure channel;
- **Step 2:** Upon receiving the message from SD_j, RA computes $K_{GS} = h(TID_j||K||r_j)$, stores $\{r_j, TID_j\}$ in the secure database of GWN, and transmits K_{GS} to SD_j via the secure channel;
- **Step 3:** SD_j computes $B_1 = r_j \oplus h(K_{SD}||SID_j)$, $B_2 = K_{GS} \oplus h(K_{SD}||r_j)$. Finally, SD_j stores $\{B_1, B_2\}$ in the memory.

6.3. Login and Mutual Authentication Phase

As shown in Figure 2, the procedure of login and mutual authentication is described as follows:

- **Step 1:** The user U_a enters ID_i, PW_i and fingerprints the biometric information Bio_i. Then, the smart card computes $\gamma_i = Rep(Bio_i, \beta_i)$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$, $K_{GU} = C_1 \oplus h(RPW_i||r_i)$, $r_i = C_2 \oplus h(RID_i||RPW_i)$, $C_3^* = h(RID_i||RPW_i||r_i) \bmod v$, where $v \in [2^4, 2^8]$, and check whether $C_3^* = C_3$. If the equation is valid, the smart card generates a random number r_a, $w \in Z_n^*$, the timestamp Ts_1. U_a selects the target smart device SD_j, and the smart card starts to compute $M_1 = (SID_j||r_a) \oplus K_{GU} \oplus Ts_1$, $C_4 = w \cdot Q$, $C_5 = w \cdot P$, $V_1 = h(RID_i||K_{GU}||r_a||C_5||Ts_1)$, $S_1 = RID_i \oplus C_5$. Afterward, the smart card sends $\{C_4, M_1, V_1, S_1, Ts_1\}$ to GWN;
- **Step 2:** After receiving the message from U_a, GWN extracts L_k from the database, and first computes $RID_i = S_1 \oplus C_5$, $K_{GU} = h(GID_k||K) \oplus L_k$, $(SID_j||r_a) = M_1 \oplus K_{GU} \oplus Ts_1$, $V_1^* = h(RID_i||K_{GU}||r_a||C_5||Ts_1)$, and verify if $V_1^* = V_1$. If it is equal, it means that the verification is completed, and then a random number r_b and the timestamp Ts_2 is generated by GWN. What's more, GWN computes $K_{GS} = h(TID_j||K||r_j)$, $M_2 = (RID_i||GID_k||C_4||r_a||r_b) \oplus h(SID_j||K_{GS}||Ts_2)$, $V_2 = h(RID_i||GID_k||K_{GS}||r_a||r_b||Ts_2)$, and transmits $\{M_2, V_2, Ts_2\}$ to SD_j;
- **Step 3:** On receiving the message from the gateway GWN, SD_j extracts $\{B_1, B_2\}$ from the memory, computes $r_j = B_1 \oplus h(K_{SD}||SID_j)$, $K_{GS} = B_2 \oplus h(K_{SD}||r_j)$, $(RID_i||GID_k||C_4||r_a||r_b) = M_2 \oplus h(SID_j||K_{GS}||Ts_2)$, $V_2^* = h(RID_i||GID_k||K_{GS}||r_a||r_b||Ts_2)$, verify whether $V_2^* = V_2$ is established. If so, then certification passed. After that, SD_j generates a random number r_c, the timestamp Ts_3, and computes $C_6 = r_c \cdot Q$, $C_7 = r_c \cdot C_4 = w \cdot C_6$, a session key $SK = h(RID_i||GID_k||SID_j||C_4||C_6||C_7)$, $M_3 = C_6 \oplus h(K_{GS}||RID_i||GID_k||Ts_3)$, $V_3 = h(SID_j||GID_k||C_6||K_{GS}||Ts_3)$. Finally, SD_j transmits $\{M_3, V_3, Ts_3\}$ to GWN;

- **Step 4:** After receiving the message sent by the smart device SD_j, GWN computes $C_6 = M_3 \oplus h(K_{GS}||RID_i||GID_k||Ts_3)$, $V_3^* = h(SID_j||GID_k||C_6||K_{GS}||Ts_3)$, and verify if V_3^*=V_3. If the equation holds, the authentication is completed. Then GWN generates the timestamp Ts_4 and computes $M_4 = (GID_k||r_a||r_b||C_6) \oplus h(RID_i||K_{GU}||r_a||Ts_4)$, $V_4 = h(RID_i||GID_k||r_a||r_b||C_6||Ts_4)$. Lastly, GWN transmits the message $\{M_4, V_4, Ts_4\}$ to U_a;
- **Step 5:** On receiving the message from GWN, U_a first computes $(GID_k||r_a||r_b||C_6) = M_4 \oplus h(RID_i||K_{GU}||r_a||Ts_4)$, $C_7 = w{\cdot}C_6$, $V_4^* = h(RID_i||GID_k||r_a||r_b||C_6||Ts_4)$, and then verify if $V_4^* = V_4$. If the equation holds, U_a accept this response and compute $SK = h(RID_i||GID_k||SID_j||C_4||C_6||C_7)$. At this point, the mutual authentication between the user and the smart device entity is completed, and the two entities of communication have generated the session key.

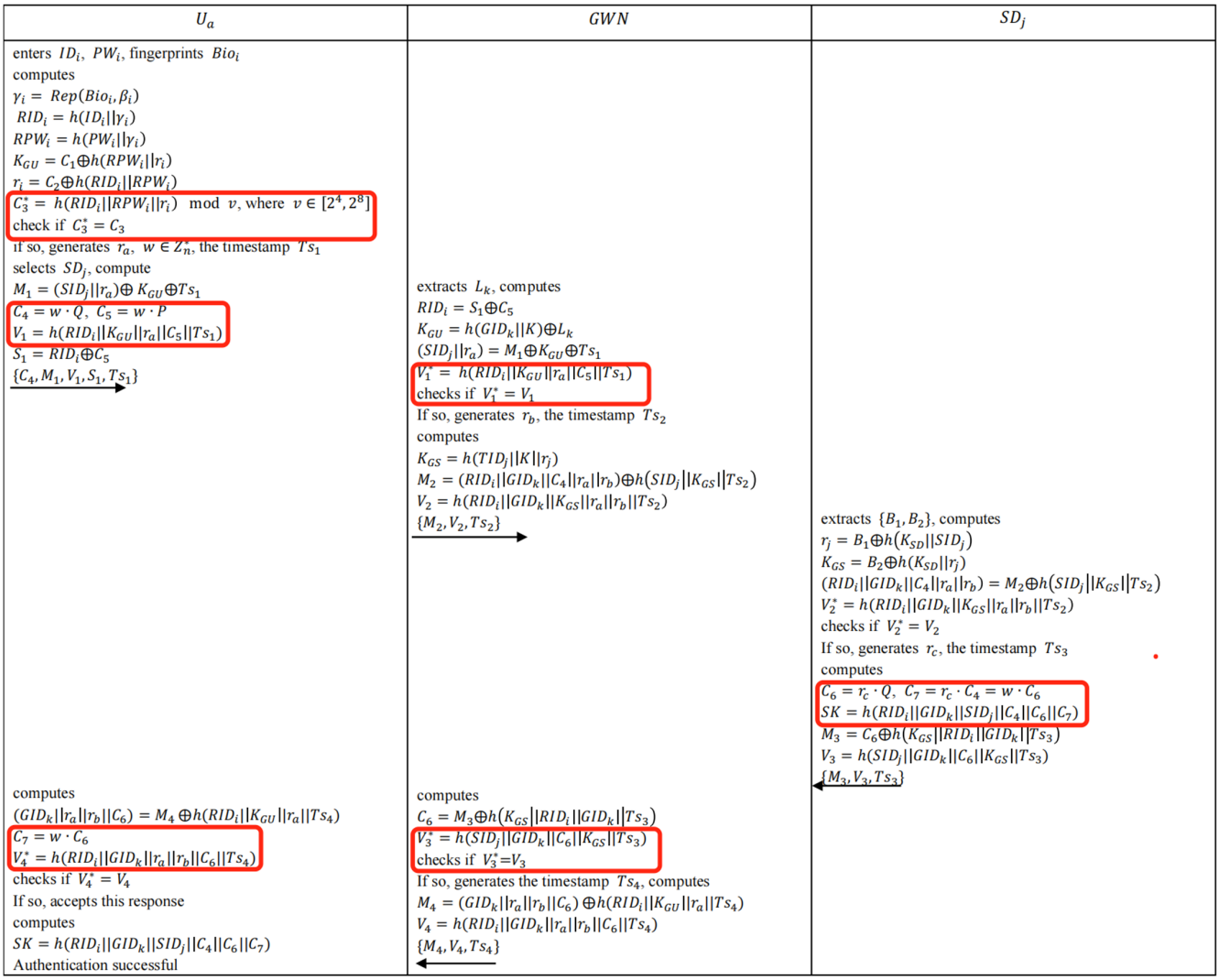

Figure 2. Authentication and key agreement phase of the proposed scheme. Red boxs mark the main improvements of our scheme.

6.4. Password Update Phase

- **Step 1:** U_a firstly enters the identity ID_i, the password PW_i, and fingerprints the biometric information Bio_i;
- **Step 2:** The smart card begins to compute $\gamma_i = Rep(Bio_i, \beta_i)$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$, $K_{GU} = C_1 \oplus h(RPW_i||r_i)$, $r_i = C_2 \oplus h(RID_i||RPW_i)$, $C_3^* = h(RID_i||RPW_i||r_i) \mod v$, where $v \in [2^4, 2^8]$, and verify if $C_3^* = C_3$. If the equa-

tion does not hold, the smart card rejects the session request. Otherwise, U_a is allowed to enter a new password and biometric feature;

- **Step 3:** U_a enters a new password PW_i^{new} and a new biometric feature Bio_i^{new} into the smart card. Then, the smart card computes $Gen\left(Bio_i^{new}\right) = \left\langle \gamma_i^{new}, \beta_i^{new} \right\rangle$, $RID_i^{new} = h(ID_i||\gamma_i^{new})$, $RPW_i^{new} = h(PW_i^{new}||\gamma_i^{new})$, $C_1^{new} = K_{GU} \oplus h(PW_i^{new}||r_i)$, $C_2^{new} = r_i \oplus h(RID_i^{new}||RPW_i^{new})$, $C_3^{new} = h(RID_i^{new}||RPW_i^{new}||r_i) \mod v$, where $v \in \left[2^4, 2^8\right]$. Finally, the smart card stores $\{C_1^{new}, C_2^{new}, C_3^{new}\}$ into the memory instead of $\{C_1, C_2, C_3\}$.

7. Security Analyses of the Proposed Scheme

In this section, we first show that the proposed scheme is resistant to various known attacks and provides the desired security properties through heuristic analysis [31]. Then, we formalize the proposed scheme by using BAN logic [32,33] to prove that the proposed scheme successfully achieves mutual authentication, including establishing a secure session key between users and smart devices. Furthermore, we demonstrate that the proposed scheme provides mutual authentication and resists man-in-the-middle attacks and replay attacks confidentiality using an automatic cryptographic scheme verifier tool Scyther [34,35].

7.1. Informal Security Analysis

7.1.1. Mutual Authentication

The user U_a and the smart device SD_j achieve mutual authentication with the help of the intermediate GWN. Particularly, U_a and GWN realize mutual authentication by verifying whether $V_1^* = V_1$ and $V_4^* = V_4$ are established. Similarly, GWN and SD_j achieve mutual authentication by verifying whether $V_2^* = V_2$ and $V_4^* = V_4$ are established, respectively. Therefore, the proposed protocol is able to successfully achieve three-party mutual authentication.

7.1.2. Session Key Agreement

$SK = h(RID_i||GID_k||SID_j||C_4||C_6||C_7)$ is negotiated between U_a and smart device SD_j in which the attacker $\mathcal{A}$ cannot calculate the parameters $\{C_6, C_7\}$ through public information, which is based on the hardness of the discrete logarithm problem on the ECC. Hence, SK cannot be obtained by the attacker $\mathcal{A}$. At the same time, GWN does not generate SK, and does not associate SK with the generation of the authentication factor, which increases the robustness of the system.

7.1.3. User Anonymity

In fact, $\mathcal{A}$ cannot get the identity ID_i directly from the transmitted message, since ID_i is not directly included in any public channel message. Meanwhile, $RID_i = h(ID_i||\gamma_i)$ is calculated during the registration and login phases, which need to use biometric information. Furthermore, in public channels, RID_i is also communicated under the protection of ECC, and will be $S_1 = RID_i \oplus C_5$ protection. Without knowing the system key y, $\mathcal{A}$ cannot obtain the user's RID_i from the communication message, based on the hardness of the discrete logarithm problem on the ECC of the public key technology, which further enhances user anonymity.

7.1.4. Untraceability

When an attacker $\mathcal{A}$ can distinguish between multiple users, then the user can be considered to be trackable. Obviously, in each session, the random number w is randomly generated, and the message S_1 sent by the current session is also different from the S_1 of others. By computing $RID_i = h(ID_i||\gamma_i)$ and the encryption protection of parameter C_5, the scheme can achieve the untraceability of user behavior.

7.1.5. Offline Password Guessing Attack

Regarding offline password guessing attack, $\mathcal{A}$ can obtain the parameters in the smart card, construct the authentication factor with the guessed password and identity, and

verify the guessed password by comparing the constructed authentication factor with the value of the real one. On one hand, the password is protected by $C_3^* = h(RID_i||RPW_i||r_i) \bmod v$, $v \in [2^4, 2^8]$ through the "fuzzy-verifier" technique. Meanwhile, since the "honey-list" records the number of authentication failures, $\mathcal{A}$ has a limited number of online attempts. Even if under the premise of biometric leakage, $\mathcal{A}$ cannot successfully guess the password. On the other hand, for the authentication factor transmitted in the open channel, in order to perform the offline password guessing attack, $\mathcal{A}$ needs to construct and compute $V_1 = h(RID_i||K_{GU}||r_a||C_5||Ts_1)$. However, only the gateway and users who have the secret private key y can calculate the parameter C_5, which is based on the hardness of ECC. All in all, the proposed scheme can resist offline password guessing attacks not only against smart card but also against open channels.

7.1.6. Smart Card Loss Attack

In the smart card loss attack, $\mathcal{A}$ can obtain the information stored in the smart device through side-channel attack. In the proposed scheme, the smart card stores $\{C_1, C_2, C_3\}$, where $C_1 = K_{GU} \oplus h(RPW_i||r_i)$, $C_2 = r_i \oplus h(RID_i||RPW_i)$, $C_3 = h(RID_i||RPW_i||r_i)$. After stealing $\{C_1, C_2, C_3\}$, it is impossible for $\mathcal{A}$ to forge the identity without knowing the random number r_i generated by U_a and the gateway key K, thus impersonating the user. At the same time, in the sending request $V_1 = h(RID_i||K_{GU}||r_a||C_5||Ts_1)$, C_5 cannot be computed by $\mathcal{A}$ based on the hardness of ECDLP, and thus $\mathcal{A}$ is unable to construct the request. Therefore, the proposed scheme is resistant to smart card loss attack and has a higher robustness.

7.1.7. Node Capture Attack

The attacker $\mathcal{A}$ can steal the stored information by capturing the node. The sensor node of the smart device sends $\{M_3, V_3, Ts_3\}$ to GWN, where $M_3 = C_6 \oplus h(K_{GS}||RID_i||GID_k||Ts_3)$, $V_3 = h(SID_j||GID_k||C_6||K_{GS}||Ts_3)$. Since, the parameter C_6 is calculated from the random number r_c generated by the node, $\mathcal{A}$ cannot calculate $\{M_3, V_3\}$. Moreover, when the attacker steals the session key, the generation of $SK = h(RID_i||GID_k||SID_j||C_4||C_6||C_7)$ needs to compute the parameters C_6 and C_7, where $C_7 = w \cdot C_6$. However, $\mathcal{A}$ cannot calculate C_7 based on the hardness of ECDLP, and only the user and the smart device can compute the session key SK. Therefore, the proposed scheme is resistant to node capture attack.

7.1.8. Replay Attack

Replay attack is one of the most common attack means. In the proposed scheme, timestamp and random number mechanisms are used to resist replay attack. The messages passed between the communicating entities contain timestamps $\{Ts_1, Ts_2, Ts_3, Ts_4\}$ and random numbers $\{r_a, r_b\}$. The freshness of these parameters is verified in the authentication factor, and even if the attacker $\mathcal{A}$ replays the communication message, the authentication of entities cannot be realized. Therefore, replay attack is impossible in our scheme.

7.1.9. Forward Security

When implementing forward security, it is necessary to consider whether the attacker can guarantee the security of the session key under the condition that the attacker can obtain the long-term key of the system. In fact, in the proposed protocol $SK = h(RID_i||GID_k||SID_j||C_4||C_6||C_7)$, $\mathcal{A}$ steals the long-term secret K of GWN, and further computes K_{GS}, K_{GU} and C_6. However, the parameter C_7 is still unable to be obtained based on the hardness of ECDLP, only the two entities of the user and the smart device can calculate the session key SK. Thus, our scheme achieves forward security.

7.1.10. Desynchronization Attack

After the session key is established, U_a, GWN and SD_j do not need to update any parameters, and the three entities do not store the same secret value. Therefore, the proposed scheme is resistant to desynchronization attack.

7.1.11. Smart Device Impersonation Attack

In the designed scheme, SD_j sends a message $\{M_3, V_3, Ts_3\}$ to GWN, where $M_3 = C_6 \oplus h(K_{GS}||RID_i||GID_k||Ts_3)$, $V_3 = h(SID_j||GID_k||C_6||K_{GS}||Ts_3)$. To calculate these values, $\mathcal{A}$ needs to calculate K_{GS} and C_6, but $\mathcal{A}$ cannot construct M_3 and V_3 without knowing the gateway key K and random number r_c. Furthermore, in the process of forging the session key SK, $\mathcal{A}$ cannot compute C_7 based on the hardness of ECDLP. Therefore, no attacker can impersonate himself as a legitimate smart device, and our scheme has a strong resistant-smart device impersonation attack ability.

7.1.12. Privileged Insider Attack

During the registration phase of the protocol, U_a sends a registration request message to RA. $\mathcal{A}$ cannot obtain the identity and password of U_a from the sent message, because the identity and password values are protected by the biometric information parameter γ_i and calculated by a one-way hash function. Therefore, the scheme is resistant to privileged insider attack.

7.1.13. Man-in-the-Middle Attack

Obviously, each message sending and receiving realizes mutual authentication, including under the protection of the secret values K_{GU} and K_{GS}. More importantly, the message consists of the three important parameters $\{C_5, C_6, C_7\}$. Since, the calculation of parameters can only be done by both communicating parties, no one can construct a legitimate message without knowing the secret value and important parameters. Therefore, the proposed scheme is resistant to man-in-the-middle attack.

7.2. BAN Logic

BAN logic is a very well-known formal proof to verify the mutual authentication properties of a scheme and the security of the session key. As a result, we demonstrate that the mutual authentication of the proposed scheme can be realized.

7.2.1. Rules

The basic notions and implications are shown in Table 2.

Table 2. Notions of BAN Logic.

Notions	Implications
$P\|\equiv X$	P believes X
$P \lhd X$	P receives X
$P\| \sim X$	P once said X
$P\|\Rightarrow X$	P has jurisdiction over X
$P \overset{K}{\leftrightarrow} Q$	K is a shared key between P and Q
$\#(X)$	X is fresh
$\{X\}_K$	X is encrypted with the key K
$(X)_h$	hash of X
(X, Y)	X and Y is one part of message (X, Y)
$< X >_Y$	X combines with Y, Y is secret value

The basic rules of BAN logic are as follows

1. Message-meaning rule:

$$\frac{P| \equiv \left(P \overset{K}{\leftrightarrow} Q\right), P \lhd \{X\}_K}{P| \equiv (Q| \sim X)}$$

2. Nonce-verification rule:

$$\frac{P| \equiv \#(X), P| \equiv (Q| \sim X)}{P| \equiv (Q| \equiv X)}$$

3. Jurisdiction rule:

$$\frac{P| \equiv (Q| \Rightarrow X), P| \equiv (Q| \equiv X)}{P| \equiv X}$$

4. Message-freshness rule:

$$\frac{P| \equiv \#(X)}{P| \equiv \#(X, Y)}$$

5. Belief rule:

$$\frac{P| \equiv X, P| \equiv Y}{P| \equiv (X, Y)}$$

6. Session key rule:

$$\frac{P| \equiv \#(X), P| \equiv Q| \equiv X}{P| \equiv P \overset{K}{\leftrightarrow} Q}$$

7.2.2. Goals

The proposed scheme needs to achieve the following goals:

- G_1: $U_a| \equiv SD_j| \equiv \left(U_a \overset{SK}{\leftrightarrow} SD_j\right)$
- G_2 : $U_a| \equiv \left(U_a \overset{SK}{\leftrightarrow} SD_j\right)$
- G_3 : $SD_j| \equiv U_a| \equiv \left(U_a \overset{SK}{\leftrightarrow} SD_j\right)$
- G_4 : $SD_j| \equiv \left(U_a \overset{SK}{\leftrightarrow} SD_j\right)$

7.2.3. Idealized Forms

First of all, the messages communicated in the proposed scheme can be transformed into idealized forms as follows:

$$Msg1: \{C_4, M_1, V_1, S_1, Ts_1\}:$$

$$< SID_j, RID_i, r_a, Ts_1, w \cdot Q >_{U_a \overset{K_{GU}}{\leftrightarrow} GWN}$$

$$Msg2: \{M_2, V_2, Ts_2\}:$$

$$< RID_i, GID_k, r_a, r_b, w \cdot Q, Ts_2 >_{GWN \overset{K_{GS}}{\leftrightarrow} SD_j}$$

$$Msg3: \{M_3, V_3, Ts_3\}:$$

$$< SID_j, GID_k, r_c \cdot Q, Ts_3 >_{SD_j \overset{K_{GS}}{\leftrightarrow} GWN}$$

$$Msg4: \{M_4, V_4, Ts_4\}:$$
$$< RID_i, GID_k, r_a, r_b, r_c \cdot Q, Ts_4 >_{GWN \overset{K_{GU}}{\leftrightarrow} U_a}$$

7.2.4. Assumptions

Then, some initial assumptions are given below:
$N1$: $GWN| \equiv \#r_a$
$N2$: $SD_j| \equiv \#r_b$
$N3$: $GWN| \equiv \#Ts_3$
$N4$: $U_a| \equiv U_a \overset{K_{GU}}{\leftrightarrow} GWN$
$N5$: $GWN| \equiv GWN \overset{K_{GU}}{\leftrightarrow} U_a$
$N6$: $GWN| \equiv GWN \overset{K_{GS}}{\leftrightarrow} SD_j$
$N7$: $SD_j| \equiv SD_j \overset{K_{GS}}{\leftrightarrow} GWN$
$N8$: $U_a| \equiv SD_j| \Rightarrow \{SID_j, Ts_3, SK, r_c \cdot Q\}$
$N9$: $U_a| \equiv GWN| \Rightarrow \{GID_k, r_b, Ts_2, wy.Q\}$
$N10$: $GWN| \equiv U_a| \Rightarrow \{RID_i, r_a, Ts_1, yw.Q\}$
$N11$: $GWN| \equiv SD_j| \Rightarrow \{Ts_3, SID_j, r_c \cdot Q\}$
$N12$: $SD_j| \equiv U_a| \Rightarrow \{RID_i, r_a, SK, wr_c \cdot Q\}$
$N13$: $SD_j| \equiv GWN| \Rightarrow \{GID_k, r_b, Ts_2\}$

7.2.5. Proof

Next, based on the BAN logic rules and assumptions, the main proofs are given below:
According to the $Msg1$, we get $B1$: $GWN \lhd < SID_j, RID_i, r_a, Ts_1, \ w \cdot Q >_{U_a \overset{K_{GU}}{\leftrightarrow} GWN}$
From $N5$, $B1$ and Message-meaning rule, we obtain $B2$:

$$GWN| \equiv U_a| \sim (SID_j, RID_i, r_a, Ts_1, \ w \cdot Q)$$

From $N1$ and Message-freshness rule, we get $B3$:

$$GWN| \equiv \#(SID_j, RID_i, r_a, Ts_1, \ w \cdot Q)$$

From $B2$, $B3$ and Nonce-verification rule, we have $B4$:

$$GWN| \equiv U_a| \equiv (SID_j, RID_i, r_a, Ts_1, \ w \cdot Q)$$

According to the $Msg2$, we get $B5$:

$$SD_j \lhd < RID_i, GID_k, r_a, r_b, w \cdot Q, Ts_2 >_{GWN \overset{K_{GS}}{\leftrightarrow} SD_j}$$

From $N7$, $B5$ and Message-meaning rule, we obtain $B6$:

$$SD_j| \equiv GWN| \sim (RID_i, GID_k, r_a, r_b, w \cdot Q, Ts_2)$$

From $N2$ and Message-freshness rule, we get $B7$:

$$SD_j| \equiv \#(RID_i, GID_k, r_a, r_b, w \cdot Q, Ts_2)$$

From $B6$, $B7$ and Nonce-verification rule, we have $B8$:

$$SD_j| \equiv GWN| \equiv (RID_i, GID_k, r_a, r_b, w \cdot Q, Ts_2)$$

According to the $Msg3$, we get $B9$:

$$GWN \lhd < SID_j, GID_k, r_c \cdot Q, Ts_3 >_{SD_j \overset{K_{GS}}{\leftrightarrow} GWN}$$

From $N6$, $B9$ and Message-meaning rule, we obtain $B10$:

$$GWN|\equiv SD_j|\ \sim (SID_j, GID_k, r_c{\cdot}Q, Ts_3)$$

From $N3$ and Message-freshness rule, we get $B11$:

$$GWN|\equiv \#(SID_j, GID_k, r_c{\cdot}Q, Ts_3)$$

From $B10$, $B11$ and Nonce-verification rule, we have $B12$:

$$GWN|\equiv SD_j| \equiv (SID_j, GID_k, r_c{\cdot}Q, Ts_3)$$

According to the $Msg4$, we get $B13$:

$$U_a \lhd < RID_i, GID_k, r_a, r_b, r_c{\cdot}Q, Ts_4 > {}_{GWN}{}^{K_{GU}}_{\leftrightarrow} U_a$$

From $N4$, $B13$ and Message-meaning rule, we obtain $B14$:

$$U_a|\equiv GWN|\ \sim (RID_i, GID_k, r_a, r_b, r_c{\cdot}Q, Ts_4)$$

From $N1$, $N2$, $N3$ and Message-freshness rule, we get $B15$:

$$U_a|\equiv \#(RID_i, GID_k, r_a, r_b, r_c{\cdot}Q, Ts_4)$$

From $B14$, $B15$ and Nonce-verification rule, we have $B16$:

$$U_a|\equiv GWN| \equiv (RID_i,\ GID_k, r_a, r_b,\ r_c{\cdot}Q,\ Ts_4)$$

From $B4$, $B8$, we get $B17$:

$$SD_j|\equiv U_a| \equiv (RID_i, r_a, w{\cdot}Q)$$

From $B7$, $B17$ and Session key rule, we have $B18$:

$$SD_j|\equiv U_a| \equiv U_a \overset{SK}{\leftrightarrow} SD_j\ (Goal3)$$

From $N12$, $B18$ and Jurisdiction rule, we get $B19$:

$$SD_j| \equiv U_a \overset{SK}{\leftrightarrow} SD_j\ (Goal4)$$

From $B12$, $B16$, we get $B20$:

$$U_a|\equiv SD_j| \equiv (SID_j, GID_k, r_c{\cdot}Q)$$

From $B15$, $B120$ and Session key rule, we have $B21$:

$$U_a|\equiv SD_j| \equiv U_a \overset{SK}{\leftrightarrow} SD_j\ (Goal1)$$

From $N8$, $B21$ and Jurisdiction rule, we get $B22$:

$$U_a| \equiv U_a \overset{SK}{\leftrightarrow} SD_j\ (Goal2)$$

All in all, the above BAN logic analysis proves that U_a, GWN and SD_j can perform mutual authentication successfully. In particular, with the assistance of GWN, the secure session key SK is established between U_a and SD_j.

7.3. Scyther Simulation

In this section, the proposed scheme will be formally analyzed by the Scyther tool, in the environment (CPU: 2.7 GHz Intel Core i5; RAM: 8 GB 1867 MHz DDR3). Scyther is an automated security scheme verification tool [34] that can be used to capture potential attacks and security threats. In previous related work, it has been used by many researchers to evaluate various security schemes. In this paper, we employ Scyther Tool to evaluate the properties of the proposed scheme, mainly focusing on confidentiality, resistance to replay attack, and resistance to a man-in-the-middle attack. Scyther provides a graphical user interface, which includes the Scyther command line tool and Python scripting interface, and the description of the scheme is written in Security Protocol Description Language(SPDL). Security properties are schemaless as declarative events. The adversary model used by Scyther is predefined and based on the Dolev–Yao model. The simulation results use Scyther to ensure that the private information used by the proposed scheme is safe from attackers during scheme execution. Compared to other emulators, such as AVISPA, ProVerif, etc., Scyther emulation tools are now very popular for authentication-based schemes. If it is analyzed that the scheme is secure, it means that the scheme is protected from man-in-the-middle attack and replay attack, achieving important security properties, such as confidentiality.

To analyze the proposed scheme, we model our scheme in SPDL, and various claims are made on the scheme. The specific claims and codes are found in Appendix A. Figure 3 accurately illustrates the results obtained in Scyther's simulation of the login and authentication scheme, which clearly shows that the proposed scheme is secure.

We repeated the Scyther verification thirty times with the same experimental results, using a combination of manually defined claims and Scyther's automatically generated claims. The results of the analysis for the proposed scheme are as follow:

Scyther results : verify

Claim				Status		Comments
home	Ua	home,Ua1	Niagree	Ok	Verified	No attacks.
		home,Ua2	Weakagree	Ok	Verified	No attacks.
		home,Ua3	Nisynch	Ok	Verified	No attacks.
		home,Ua4	Alive	Ok	Verified	No attacks.
		home,Ua5	Secret ra	Ok	Verified	No attacks.
		home,Ua6	Secret C5	Ok	Verified	No attacks.
		home,Ua7	Secret C7	Ok	Verified	No attacks.
		home,Ua8	Secret C6	Ok	Verified	No attacks.
		home,Ua9	Secret RID	Ok	Verified	No attacks.
		home,Ua10	Secret GID	Ok	Verified	No attacks.
		home,Ua11	Secret SID	Ok	Verified	No attacks.

(**a**)

Figure 3. *Cont.*

Gwn	home,Gwn1	Niagree	Ok	Verified	No attacks.
	home,Gwn2	Weakagree	Ok	Verified	No attacks.
	home,Gwn3	Nisynch	Ok	Verified	No attacks.
	home,Gwn4	Alive	Ok	Verified	No attacks.
	home,Gwn5	Secret ra	Ok	Verified	No attacks.
	home,Gwn6	Secret C5	Ok	Verified	No attacks.
	home,Gwn7	Secret C6	Ok	Verified	No attacks.
	home,Gwn8	Secret RID	Ok	Verified	No attacks.
	home,Gwn9	Secret SID	Ok	Verified	No attacks.
	home,Gwn10	Secret rb	Ok	Verified	No attacks.
	home,Gwn11	Secret GID	Ok	Verified	No attacks.

(**b**)

SD	home,SD1	Niagree	Ok	Verified	No attacks.
	home,SD2	Weakagree	Ok	Verified	No attacks.
	home,SD3	Nisynch	Ok	Verified	No attacks.
	home,SD4	Alive	Ok	Verified	No attacks.
	home,SD5	Secret rc	Ok	Verified	No attacks.
	home,SD6	Secret C6	Ok	Verified	No attacks.
	home,SD7	Secret RID	Ok	Verified	No attacks.
	home,SD8	Secret SID	Ok	Verified	No attacks.
	home,SD9	Secret SK	Ok	Verified	No attacks.
	home,SD10	Secret GID	Ok	Verified	No attacks.

Done.

(**c**)

Figure 3. Analysis results using Scyther tool for the proposed scheme: (**a**) Role of User; (**b**) Role of Smart Device; (**c**) Role of Gateway Node.

8. Performance and Security Analysis

In this section, we show the results of the comparison results of the proposed protocol with similar protocols [13,19,20,22–24], including computational costs, communication costs, security features [36], and storage costs.

8.1. Computation Costs Comparison

Completely, for computation cost analysis in these schemes, we denote T_p, T_{ED}, T_e and T_h as the time needed for computing "bilinear pairing", "encryption and decryption", "ECC multiplication", and "hashing" operations, respectively. According to the experimental data of [37], the running time for bilinear pairing is $T_p \approx 32.713$ ms (milliseconds), for an ECC multiplication is $T_e \approx 13.405$ ms, for hash function computation is Th ≈ 0.056 ms, and for encryption and decryption is $T_{ED} \approx 1.657$ ms. In Table 3, we show the compared results of computation cost analysis. We can see that the computation costs of the proposed scheme is slightly greater than that of Yu et al. [13]. However, as the informal analysis and Table 3 show, our proposed scheme has more security features and is able to overcome the weaknesses of Yu et al.' scheme [13]. Therefore, these sacrifices of computational overhead are acceptable, and our proposed scheme achieves a high-level balance in terms

of security and efficiency, which is more suitable for the practical application environments of smart home.

Table 3. Computation Costs Comparison.

Scheme	Naoui [23]	Shuai [20]	Yu & Li [19]	Kumar [22]	Nasib [24]	Yu [13]	Ours
U_a	$12T_h+2T_e+3T_{ED}$	$6T_h+2T_e$	$7T_h+14T_e$	$6T_h+2T_e$	$7T_h+2T_e$	$12T_h+T_{ED}$	$9T_h+3T_e$
GWN	$13T_h+2T_e+4T_{ED}$	$7T_h+T_e$	$12T_h+19T_e+4T_p$	$8T_h+T_e$	$5T_h+T_e$	$11T_h$	$9T_h+T_e$
SD_j	T_e+T_{ED}	$3T_h$	$7T_h+14T_m$	$3T_h$	$6T_h$	$7T_h$	$7T_h+2T_e$
Total costs	81.681	27.604	762.343	41.167	41.223	3.337	68.425

8.2. Communication Costs

For the communication cost comparison, it is assumed that the ECC point is 320 bits, the hash digest is 160 bits, the encryption and decryption are 256 bits, the timestamp is 32 bits, and the nonce or identity are 128 bits long. In Table 4, We show the comparison results of the communication cost in bytes between the proposed scheme and previous schemes. It can be concluded that the proposed scheme provides better communication costs compared to related schemes.

Table 4. Communication Costs Comparison.

Scheme	Total Costs (Byte)	Number Messages
Naoui [23]	(228 + 136 + 96) = 460	3
Shuai [20]	(192 + 80 + 80 + 80) = 432	4
Yu & Li [19]	(84 + 124 + 164 + 164) × 2 = 1072	8
Kumar [22]	(200 + 88 + 88 + 88) = 464	4
Nasib [24]	(352 + 184 + 112 + 184) = 832	4
Yu [13]	(144 + 80 + 80 + 80) = 384	4
Ours	(192 + 80 + 80 + 112) = 464	4

8.3. Security Comparisons

This section evaluates the security properties of the proposed scheme compared to previous schemes [13,19,20,22–24]. Table 5 shows that previous schemes suffer from various security attacks, such as smart card loss attack, insider privilege attack, and offline password guessing attack, etc., and fail to provide user anonymity, forward security, and mutual authentication. In contrast, the proposed scheme resists various security attacks. In particular, forward secrecy, user anonymity, etc. are also provided in Table 5. Therefore, it can be concluded that our proposed scheme provides more security properties than previous schemes [13,19,20,22–24].

8.4. Storage Costs

Comparing storage costs is based on the size of the data storage in the smart card. Table 6 shows how many bits are stored in the smart card for each scheme, where the length of the secret parameters is described in Section 8.2. Obviously, we can see the advantages of the proposed scheme in storage costs, and our scheme overhead is in a reasonable range, which can be well adapted to the practical remote control system.

Table 5. Security Features.

Feature	Naoui [23]	Shuai [20]	Yu & Li [19]	Kumar [22]	Nasib [24]	Yu [13]	Ours
S1	✓	✓	✓	✓	✓	✓	✓
S2	✓	✓	✓	✓	✓	✓	✓
S3	✓	✗	✓	✗	✗	✓	✓
S4	✓	✓	✓	✓	✓	✗	✓
S5	✗	✗	✓	✓	✗	✗	✓
S6	✗	✓	✓	✓	✗	✗	✓
S7	✗	✗	✓	✗	✗	✗	✓
S8	✓	✓	✓	✓	✓	✓	✓
S9	✗	✗	✓	✗	✗	✗	✓
S10	✓	✓	✗	✓	✓	✓	✓
S11	✗	✗	✓	✗	✗	✗	✓
S12	✓	✓	✓	✓	✗	✓	✓
S13	✓	✓	✓	✓	✓	✓	✓
S14	✗	✗	✓	✗	✓	✓	✓
S15	✗	✓	✗	✓	✗	✓	✓

S1: mutual authentication; S2: session key agreement; S3: user anonymity; S4: untraceability; S5: anti-offline password guessing attack; S6: anti-smart card loss attack; S7: anti-node capture attack; S8: anti-reply attack; S9: forward security; S10: anti-desynchronization attack; S11: anti-smart device impersonation attack; S12: anti-privileged insider attack; S13: anti-man-in-the-middle attack; S14: three-factor security; S15: no password verification table.

Table 6. Storage Costs Comparison.

Scheme	Total Costs (Bit)
Naoui [23]	320
Shuai [20]	512
Yu & Li [19]	480
Kumar [22]	384
Nasib [24]	640
Yu [13]	480
Ours	480

9. Conclusions

The security issue of smart homes has been a serious challenge to the growing demand. In related research, a large number of authentication schemes have been designed to adapt to the unique communication environment of smart homes. However, previous schemes do not make a good job of guaranteeing the privacy of transmitted information and the anonymity of users. Fortunately, in this paper, we first prove that Yu et al.'s [13] scheme is insecure to offline password guessing attack, node capture attack, and cannot achieve forward secrecy. Hence, in order to overcome these security threats, we propose a robust three-factor anonymous authentication scheme. Next, we demonstrate that the scheme is resistant to various known attacks through formal and informal proofs. Moreover, we compared the scheme with the recently related schemes in terms of computation consumption time and communication overhead, and demonstrated the efficiency and superior performance of the proposed scheme, which can adapt to the actual environment of a smart home. After comparing the security properties of these protocols, it can be proved that our scheme can better ensure the applicability of smart home systems. Looking to the future, the schemes designed for the future smart home will continue to focus on security, privacy and anonymity, which is also in line with people's pursuit of a safe life. It should be pointed out that the existing scheme models have high requirements for trusted third parties. However, in practice, we need to think further about how to reduce the pre-safety conditions of the system and still achieve the same safety effect.

Author Contributions: Conceptualization, Y.T.; methodology, X.W.; software, Y.T.; validation, X.W., Y.T. and H.H.; formal analysis, Y.T.; investigation, X.W.; resources, X.W. and Y.C. data curation, H.H.; writing—original draft preparation, Y.T.; writing—review and editing, H.H. project administration, Y.C.; funding acquisition, Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Key R & D Program of China, grant number 2018YFB1004100.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Claims and Code of Scyther for login and authentication scheme:

```
usertype Sessionkey, Timestamp;
usertype String;
const XOR: Function;

hashfunction h;
protocol home(Ua, Gwn, SD) {
role Ua {

fresh RID,SID,GID : String;
fresh ra: Nonce;
fresh Ts1 :Timestamp;
fresh C4,C5 ,C6,C7:Nonce;
var SK:Sessionkey;
var V1,V4 :String;
var Ts4:Timestamp;
var rb: Nonce;
match(V1,h(RID,k(Ua,Gwn),ra,Ts1, C5));
match(SK,h(RID,GID,SID,C4,C6,C7));
send_1(Ua, Gwn,Ts1,C4,V1,XOR(RID,C5),XOR(XOR((SID,ra),C5),Ts1));
recv_4(Gwn, Ua, Ts4, V4,XOR( (GID,ra,rb,C6),h(RID,k(Ua,Gwn),ra,Ts4 ) ) );

claim(Ua, Niagree);
claim(Ua, Weakagree);
claim(Ua, Nisynch);
claim(Ua, Alive);
claim(Ua, Secret, ra);
claim(Ua, Secret, C5);
claim(Ua, Secret, C7);
claim(Ua, Secret, C6);
claim(Ua, Secret, RID);
claim(Ua, Secret, GID);
claim(Ua, Secret, SID);
}

role Gwn {
fresh GID:String;
fresh rb : Nonce;
fresh Ts2 ,Ts4:Timestamp;
fresh RID, SID :String;
var V1,V2 ,V3,V4:String;
fresh ra ,C4,C5,C6: Nonce;
var Ts1,Ts3:Timestamp;
```

```
match(V2,h(GID,SID,k(Gwn,SD),ra,rb,Ts2));
match(V4,h(RID,GID,ra,rb,C6,Ts4));
recv_1(Ua, Gwn,Ts1,C4,V1,XOR(RID,C5),XOR(XOR((SID,ra),C5),Ts1));
send_2(Gwn, SD, Ts2,V2,XOR((RID,GID,C4,ra,rb),h(SID,k(Gwn,SD),Ts2)) );
recv_3(SD, Gwn, Ts3, V3,XOR(C6,h(k(Gwn,SD),RID,GID,Ts3)));
send_4(Gwn, Ua, Ts4, V4,XOR( (GID,ra,rb,C6),h(RID,k(Ua,Gwn),ra,Ts4 ) ) );

claim(Gwn, Niagree);
claim(Gwn, Weakagree);
claim(Gwn, Nisynch);
claim(Gwn, Alive);
claim(Gwn, Secret, ra);
claim(Gwn, Secret, C5);
claim(Gwn, Secret, C6);
claim(Gwn, Secret, RID);
claim(Gwn, Secret, SID);
claim(Gwn, Secret, rb);
claim(Gwn, Secret, GID);
}

role SD {
fresh rc ,C6: Nonce;
fresh SK:Sessionkey;
fresh Ts3:Timestamp;
fresh RID, SID ,GID:String;
var ra,rb,C4: Nonce;
fresh Ts2 :Timestamp;
var V2,V3 :String;

match(V3,h(SID,GID,k(Gwn,SD),C6,Ts2));
recv_2(Gwn, SD, Ts2,V2,XOR((RID,GID,C4,ra,rb),h(SID,k(Gwn,SD),Ts2)) );
send_3(SD, Gwn, Ts3, V3,XOR(C6,h(k(Gwn,SD),RID,GID,Ts3)));

claim(SD, Niagree);
claim(SD, Weakagree);
claim(SD, Nisynch);
claim(SD, Alive);
claim(SD, Secret, rc);
claim(SD, Secret, C6);
claim(SD, Secret, RID);
claim(SD, Secret, SID);
claim(SD, Secret, SK);
claim(SD, Secret, GID);
}
}
```

References

1. Mart Homes in Easy Steps: Master Smart Technology for Your Home. Available online: https://b-ok.org/book/3704507/a67507 (accessed on 15 July 2018).
2. Han, K.; Shon, T.; Kim, K. Efficient mobile sensor authentication in smart home and WPAN. *IEEE Trans. Consum. Electron.* **2010**, *56*, 591–596. [CrossRef]
3. Mendes, T.D.P.; Godina, R.; Rodrigues, E.M.G. Smart home communication technologies and applications: Wireless protocol assessment for home area network resources. *Energies* **2015**, *8*, 7279–7311. [CrossRef]
4. Kumar, P.; Gurtov, A.; Iinatti, J.; Ylianttila, M.; Sain, M. Lightweight and secure session-key establishment scheme in smart home environments. *IEEE Sens. J.* **2015**, *16*, 254–264. [CrossRef]

5. Gomez, C.; Paradells, J. Wireless home automation networks: A survey of architectures and technologies. *IEEE Commun. Mag.* **2010**, *48*, 92–101. [CrossRef]
6. Vanhoef, M.; Ronen, E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020; pp. 517–533.
7. Krawczyk, H.; Paterson, K.G.; Wee, H. On the Security of the TLS Protocol: A Systematic Analysis. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; p. 8042.
8. Balakrishnan, S.; Vasudavan, H.; Murugesan, R.K. Smart Home Technologies: A preliminary Review. In Proceedings of the 6th International Conference on Information Technology: IoT and Smart City, Hong Kong, China, 29–31 December 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 120–127.
9. Shin, S.; Kwon, T. A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart homes. *Sensors* **2019**, *19*, 2012. [CrossRef] [PubMed]
10. Andola, N.; Yadav, V.K.; Venkatesan, S.; Verma, S. SpyChain: A lightweight blockchain for authentication and anonymous authorization in IoD. *Wirel. Pers. Commun.* **2021**, *119*, 343–362. [CrossRef]
11. Yadav, V.K.; Verma, S.; Venkatesan, S. Linkable privacy-preserving scheme for location-based services. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 7998–8012. [CrossRef]
12. Wang, D.; Wang, P.; Wang, C. Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs. *ACM Trans. Cyber-Phys. Syst.* **2020**, *4*, 1–26. [CrossRef]
13. Yu, S.; Jho, N.; Park, Y. Lightweight three-factor-based privacy-preserving authentication scheme for IoT-enabled smart homes. *IEEE Access* **2021**, *9*, 126186–126197. [CrossRef]
14. Jeong, J.; Chung, M.Y.; Choo, H. Integrated OTP-based user authentication scheme using smart cards in home networks. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 7–10 January 2008; p. 294.
15. Vaidya, B.; Park, J.H.; Yeo, S.S.; Rodrigues, J.J. Robust one-time password authentication scheme using smart card for home network environment. *Comput. Commun.* **2011**, *34*, 326–336. [CrossRef]
16. Kim, H.J.; Kim, H.S. $AUTH_{HOTP}$-HOTP based authentication scheme over home network environment. In Proceedings of the International Conference on Computational Science and Its Applications, Santander, Spain, 20–23 June 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 622–637.
17. Poh, G.S.; Gope, P.; Ning, J. PrivHome: Privacy-preserving authenticated communication in smart home environment. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 1095–1107. [CrossRef]
18. Santoso, F.K.; Vun, N.C.H. Securing IoT for smart home system. In Proceedings of the 2015 international symposium on consumer electronics, Madrid, Spain, 24–26 June 2015; pp. 1–2.
19. Yu, B.; Li, H. Anonymous authentication key agreement scheme with pairing-based cryptography for home-based multi-sensor Internet of Things. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1–11. [CrossRef]
20. Shuai, M.; Yu, N.; Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security. *Comput. Secur.* **2019**, *86*, 132–146. [CrossRef]
21. Xu, M.; Dong, Q.; Zhou, M.; Wang, C.; Liu, Y. Security Analysis on "Anonymous Authentication Scheme for Smart Home Environment with Provable Security". *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8838363. [CrossRef]
22. Kaur, D.; Kumar, D. Cryptanalysis and improvement of a two-factor user authentication scheme for smart home. *J. Inf. Secur. Appl.* **2021**, *58*, 102787. [CrossRef]
23. Naoui, S.; Elhdhili, M.H.; Saidane, L.A. Novel Smart Home Authentication Protocol LRP-SHAP. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'19), Marrakech, Morocco, 15–18 April 2019; pp. 1–6.
24. Abdi Nasib Far, H.; Bayat, M.; Kumar Das, A.; Fotouhi, M.; Pournaghi, S.M.; Doostari, M.A. LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT. *Wirel. Netw.* **2021**, *27*, 1389–1412. [CrossRef]
25. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
26. Messerges, T.S.; Dabbish, E.A.; Sloan, R.H. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.* **2002**, *51*, 541–552. [CrossRef]
27. Li, W.; Wang, D.; Wang, P. Insider attacks against multi-factor authentication protocols for wireless sensor networks. *J. Softw.* **2019**, *30*, 2375–2391.
28. Wang, D.; Li, W.; Wang, P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4081–4092. [CrossRef]
29. Wang, C.; Xu, G.; Sun, J. An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks. *Sensors* **2017**, *17*, 2946. [CrossRef] [PubMed]
30. Wang, C.; Wang, D.; Tu, Y.; Xu, G.; Wang, H. Understanding node capture attacks in user authentication schemes for wireless sensor networks. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 507. [CrossRef]
31. Wang, C.; Xu, G.; Li, W. A secure and anonymous two-factor authentication protocol in multiserver environment. *Secur. Commun. Netw.* **2018**, *2018*, 9062675. [CrossRef]
32. Burrows, M.; Abadi, M.; Needham, R.M. A logic of authentication. ACM Trans. *Comput. Syst.* **1990**, *8*, 18–36.

33. Lee, J.; Yu, S.; Park, K.; Park, Y.; Park, Y. Secure three-factor authentication protocol for multi-gateway IoT environments. *Sensors* **2019**, *19*, 2358. [CrossRef]
34. Cremers, C.J.F. The Scyther Tool: Verification, falsification, and analysis of security protocols. In Proceedings of the International Conference on Computer Aided Verification, Princeton, NJ, USA, 7–14 July 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 414–418.
35. Elbaz, H.A.; Abd-Elaziz, M.H.; Nazmy, M.T. Analysis and verification of a key agreement protocol over cloud computing using scyther tool. *Int. J. Distrib. Cloud Comput.* **2014**, *2*, 1–7.
36. Wang, K.; Chen, C.M.; Tie, Z.; Shojafar, M.; Kumar, S.; Kumari, S. Forward Privacy Preservation in IoT-Enabled Healthcare Systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1991–1999. [CrossRef]
37. Wu, L.; Wang, J.; Choo, K.R.; He, D. Secure Key Agreement and Key Protection for Mobile Device User Authentication. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 319–330. [CrossRef]