An Improved Three-Factor Remote User Authentication Protocol Using Elliptic Curve Cryptography

Wan-Rong Liu, Bin Li, and Zhi-Yong Ji
(Corresponding author: Zhi-Yong Ji)

Shanghai Jiao Tong University Affiliated Sixth People's Hospital
Shanghai 201306, China
Email: joyer99@126.com

(Received Aug. 30, 2021; Revised and Accepted Jan. 22, 2022; First Online Mar. 26, 2022)

Abstract

With the rapid development of the Internet, more and more users' private information, such as patients' vital signs, is maliciously obtained by attackers. Therefore, we analyzed some of the protocols. Based on the security problems existing in the protocols between Jiang *et al.* and Li *et al.*, we have proposed an improved three-factor remote user authentication protocol using elliptic curve cryptography. The improved protocol uses the knowledge of elliptic curve cryptography, which is an algorithm for establishing public key encryption. Its main advantage is that it provides equivalent or higher security than other methods using more minor keys in some cases. We construct our protocol by using discrete logarithm and computational Diffie-Hellman problem. The protocol uses only random numbers to ensure the freshness and security of the protocol and does not use timestamps, so clock asynchrony will not occur. We performed Burrows–Abadi–Needham logic analysis, security analysis, and comparative security analysis on the protocol. The analysis shows that the improved protocol has higher security and does not add much computation.

Keywords: Anonymity; Authentication; Elliptic Curve Cryptography

1 Introduction

With the rapid development of the Internet, positive progress has been made in the application of the Internet in all fields of our life, such as wearable medical devices, industry, and smart homes [1, 2]. The Internet has become an important auxiliary means in many fields [3]. It can not only improve work efficiency, but also actively promote us to change the way of life and make continuous progress towards a more advanced and intelligent way. However, with our increasing dependence on the network, network security has become one of the important factors restricting the development of the network. Telemedicine information system is rapid development, can be implanted and wearable devices to the patient's blood pressure, body temperature, electrocardiogram monitoring, information related to health care personnel can access the server to obtain patient vital signs of real-time data [4], especially can provide better medical care to patients in remote areas, However, when sensitive vital sign data of patients are transmitted to medical personnel through public channels, there will be information leakage [5]. Wazid *et al.* [6] proposed a mutual user authentication mechanism between a remote surgeon and the robotic arms. Whether in the medical field or in other fields, it is very important to continuously improve network security and build a safe and reliable network environment for users [7]. In essence, network security is the information security of Internet users, that is, the data flowing and interacting on the network system is not subject to accidental or malicious damage, disclosure, tampering, etc. Considering the importance of data information security, in network use, we should combine the characteristics of database use, the information in the database identity authentication and other technologies. At present, with the development of the researchers on the network security, authentication from the perspective of a user authentication on the number of factors, from the initial single factor authentication protocol development up to now the double factor and three factors of authentication protocol, our agreement is a kind of based on the users passwords, smart cards and biometric information of three factor authentication protocol [8]. Compared with the traditional two-factor authentication protocol based on smart card and user password, the advantage of three-factor authentication protocol with user biometric is that there is no problem of forgetting or losing the user's biometric information [9], and it is hard for attackers to guess. This information is unique to the user. Due to the extensive application of basic pattern recogni-

tion system, more and more authentication schemes based on biometrics are proposed [10]. The following is a brief introduction to the work of other researchers close to our work. In 2018, Wazid *et al.* [11] proposed a protocol for generic IoT networks.

In 2019, Lu *et al.* [7] proved that the protocol of Das *et al.* [13] had some security flaws. In 2020, Jabbari *et al.* [14] proposed a new scheme in order to provide mutual authentication between users and sensor devices directly. Xu *et al.* [15] proposed a patient healthcare monitoring authentication protocol. And Alzahrani *et al.* [16] demonstrated that Xu *et al.*' protocol has privacy issues and is vulnerable to attacks such as replay attacks. Merabet *et al.* [17] proposed some protocols for IoT-based healthcare applications in 2020. Garg *et al.* [18] pointed out that Merabet *et al.*'s protocol cannot resist strong replay attack. Sharma *et al.* [19] thought Merabet *et al.*'s protocol cannot support blockchain solution. In 2015, He *et al.* [20] proposed an improved authentication protocol based on time certificate. In 2016, Jiang *et al.* [21] pointed out that He *et al.* had interior attack, stolen smart card attack and other security risks in their protocol and proposed their own protocol. In 2018, Li *et al.* [22] pointed out that the agreements of Jiang *et al.* and He *et al.* had some common shortcomings, such as the lack of password change stage, clock synchronization and other security problems. In the same year, Li *et al.* proposed an improved agreement based on Jiang *et al.*, but we found that there were some problems with Li *et al.*'s improved agreement.

1) Failure to provide three-factor certification: authentication protocols that provide three-factor security mean that attackers can only launch impersonation attacks until he/she has mastered all three factors: password, biometrics, and smart cards. Li *et al.* claimed that their protocol can provide three-factor security. However, we find that if an attacker steals a user's smart and acquires the user's biometric, he/she can perform an offline identity and password guessing attack, in which case, Li *et al.*'s protocol fails to provide the privacy protection and security attributes they claim.

2) Failure to resist forgery attack: Forgery attack is a common type of attack. The attacker can impersonate either party of the scheme using the communication messages collected from the public channel and the information in the user's smart card.

3) Failure to resist smart card loss attack.

4) Failure to provide user anonymity.

5) Failure to resist forward secrecy and so on.

We believe that the agreement proposed by Jiang *et al.* has a good framework. Therefore, based on the security problems existing in the agreement between Jiang et al and Li et al, an improved three-factor remote user authentication protocol using elliptic curve cryptography is proposed. Our improved protocol uses the knowledge of elliptic curve cryptography [23, 24], which is an algorithm for establishing public key encryption. The use of elliptic curves in cryptography was independently proposed by Neal Koblitz and Victor Miller in 1985. Its main advantage is that in some cases it provides equivalent or higher security than other methods using smaller keys, such as the RSA encryption algorithm. Another advantage is that can define a group of bilinear mapping between the double linear mapping has found a lot of application in cryptography, the downside is the same length under the key than any other mechanism of encryption and decryption operations take a long time, but you can use a shorter keys to achieve at the same level of security, so the safety degree of speed at the relatively faster. The probability of solving mathematical problems on elliptic curves by using polynomial time algorithm is negligible, so we construct our protocol by using discrete logarithm and computational Diffie-Hellman problem.

1) Discrete logarithm problem: given $P, aP \in E/Fq$, for unknown $a \in Z_n^*$, the probability of success of finding the value of a is negligible.

2) Computational Diffie-Hellman problem: given $P, aP, bP, P \in E/Fq$, for unknown $a, b \in Z_n^*$, the probability of success of finding the value of abP is negligible.

In addition, considering the clock synchronization problem, in wireless sensor networks, the clock precision of each network node is limited due to the cost limitation, and the difference between each node clock will be larger and larger with the passage of time [25]. Many important basic functions of wireless sensor networks require nodes in the network to maintain a relatively uniform time scale. In order to ensure the freshness of information transmission, researchers usually use the method of adding random numbers or timestamps into the protocol to resist replay attacks and man-in-the-middle attacks. Using both timestamp and random numbers in Jiang *et al.*'s protocol may encounter clock asynchronization problem. Our protocol uses only random numbers to ensure the freshness and security of the protocol, and does not use timestamps, so clock asynchrony will not occur [26]. Furthermore, the protocols of Jiang *et al.* and Li *et al.* both have the situation that the user name is sent in clear text, which cannot guarantee the anonymity of users. Our improved protocol ensures that the user name and password are not sent in clear text. Finally, we performed Burrows–Abadi–Needham logic [27] analysis, random oracle model analysis, security analysis and security comparative analysis on the protocol. The schematic diagram of the authentication process is shown in Figure 1.

2 Review of Jiang *et al.*'s Scheme

Jiang *et al.* put forward an untraceable two-factor authentication scheme for wireless sensor networks in 2016.

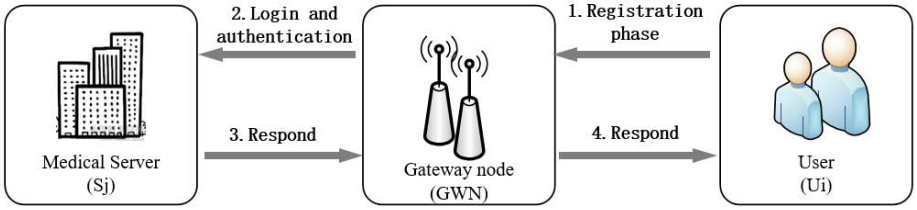

Figure 1: Schematic diagram of authentication process

Jiang *et al.*'s scheme consists of three phases: registration, login and authentication. This section is to review the scheme of Jiang *et al.* The notations used in the paper are summarized in Table 1.

Table 1: Notationas

Symbol	Definition
U_i	User
S_j	Medical Server
ID_i	Identity of U_i
PW_i	Password of U_i
GWN	Gateway node
c, y, g	A random number
P	A point on the elliptic curve
$P \cdot x$	The value of on x-axis
P_{par}	the parameters choosed by GWN
G	The additive group
SC	The smart card
n	A large prime order
F_P	A finite field
$h(\cdot)$	One-way hash function
$\oplus$	Bitwise XOR operation
$\|$	Concatenation operation
T	The current time of system
SID_j	Sensor node identity
PTC_i	The protected temporal credential of U_i
SK	Session-key
TC_i, TC_j	The temporal credential of U_i and S_j
TE_i	The expiration time of a user's temporal credential
b_i	Biological characteristics

2.1 User Registration Phase

Firstly, GWN chooses the additive group G generated by a point P with a large prime order n over a finite field F_P on an elliptic curve. The GWN randomly selects a number x as its private key and calculates $y = xP$ as public key. Finally, GWN stores x and publishes the system parameters $\{E(F_P), G, P, y\}$. Next, users register according to the following steps.

Step 1. As is supposed in He *et al.*'s scheme, U_i has a password PW_i shared with GWN, which maintains the value $\{U_i, H(PW_i)\}$. U_i imputs the old password PW_i, and selects a new one PW_i^{new}. Next, U_i chooses two random number a, $r_i \in Z_{p-1}^*$, calculates $A = aP, A' = ay = axP$, $VI_i = H(TS_1 \| H(PW_i) \| A \| A' \| H(PW_i^{new} \| ID_i \| r_i)$, $TPW_i = H(PW_i^{new} \| ID_i \| r_i) \oplus H(TS_1 \| H(PW_i) \| A \| A')$, sends messages $\{ID_i, TS_1, VI_i, TPW_i, A\}$ to GWN.

Step 2. GWN checks TS_1. If true, GWN calculates $A'' = xA = xaP$, $H(PW_i^{new} \| ID_i \| r_i) = TPW_i \oplus H(TS_1 \| H(PW_i) \| A \| A'')$, checks $VI_i \stackrel{?}{=} H(TS_1 \| H(PW_i) \| A \| A'' \| H(PW_i^{new} \| ID_i \| r_i))$, calculates $TC_i = H(K_{GWN-U} \| ID_i \| TE_i)$, $PTC_i = TC_i \oplus H(PW_i^{new} \| ID_i \| r_i)$, stores $\{H(\cdot), TE_i, PTC_i\}$ into a smart card, sends smart card to U_i.

2.2 Sensor Node Registration Phase

Step 1. S_j generates $b \in Z_{p-1}^*$, calculates $B = bP$, $B' = by = bxP$, $VI_j = H(TS_2 \| H(PW_j) \| B \| B')$, sends messages $\{SID_j, TS_2, VI_j, B\}$ to GWN.

Step 2. GWN checks TS_2. If true, GWN calculates $B'' = xB = xbP$, checks $VI_j \stackrel{?}{=} H(TS_2 \| H(PW_j) \| B \| B'')$, $TC_j = H(K_{GWN-S} \| SID_j)$, $REG_j = TC_j \oplus H(TS_3 \| H(PW_j) \| B \| B'')$, $VI_{GWN} = H(TC_j \| H(TS_3 \| H(PW_j) \| B \| B''))$, sends messages $\{TS_3, REG_j, VI_{GWN}\}$ to S_j.

Step 3. S_j checks TS_3. If true, calculates $TC_j = REG_j \oplus H(TS_3 \| H(PW_j) \| B \| B')$, checks $VI_{GWN} \stackrel{?}{=} H(TC_j \| H(TS_3 \| H(PW_j) \| B \| B'))$. If these two value are unequal, S_j terminates the session; otherwise, it stops.

2.3 Login and Authentication Phase

Step 1. U_i inputs ID_i and PW_i, the smart card calculates $TC_i = PTC_i \oplus H(PW_i \| ID_i \| r_i)$, U_i randomly generates $c \in Z_{p-1}^*$. Then U_i computes $C_i = cP$, $D_i = cy = cxP$, generates K_i, calculates $DID_i = ID_i \oplus H(C_i \| D_i)$, $PKS_i = K_i \oplus H(TC_i \| TS_4 \| D_i)$, $E_i = H(H(ID_i \| TS_4) \oplus D_i \oplus PKS_i \oplus TC_i)$, sends

messages $\{DID_i, C_i, PKS_i, TS_4, E_i\}$ to GWN. TS_4 is the current timestamp.

Step 2. Once receiving the message from U_i. GWN checks TS_4. If true, GWN calculates $D_i = xC = xcP$, $ID_i = DID_i \oplus H(C_i \| D_i)$, checks ID_i and retrieves TE_i, $TC_i = H(K_{GWN-U} \| ID_i \| TE_i)$, checks $H(H(ID_i \| TS_4) \oplus D_i \oplus PKS_i \oplus TC_i) \stackrel{?}{=} E_i$, $K_i = PKS_i \oplus H(TC_i \| TS_4 \| D_i)$, $TC_j = H(K_{GWN-S} \| SID_j)$, $DID_{GWN} = ID_i \oplus H(DID_i \| TC_j \| TS_5)$, $C_{GWN} = H(ID_i \| TC_j \| TS_5)$, $PKS_{GWN} = K_i \oplus H(TC_j \| TS_5)$, sends messages $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ to S_j. TS_5 is the current timestamp.

Step 3. Once receiving the message from GWN. S_j checks TS_5. If true, S_j calculates $ID_i = DID_{GWN} \oplus H(DID_i \| TC_j \| TS_5)$, checks $C_{GWN} \stackrel{?}{=} H(ID_i \| TC_j \| TS_5)$, generates K_j, calculates $K_i = PKS_{GWN} \oplus H(TC_j \| TS_5)$, $SK_{ij} = H(K_i \oplus K_j)$, $C_j = H(K_j \| ID_i \| SID_j \| TS_6)$ $PKS_j = K_j \oplus H(K_i \| TS_6)$, sends messages $\{SID_j, TS_6, C_j, PKS_j\}$ to U_i. TS_6 is the current timestamp.

Step 4. Once receiving the message from S_j. U_i checks TS_6. If true, U_i calculates $K_j = PKS_j \oplus H(K_i \| TS_6)$, checks $C_j \stackrel{?}{=} H(K_j \| ID_i \| SID_j \| TS_6)$. Finally, U_i calculates the session key $SK_{ij} = H(K_i \oplus K_j)$.

3 Weaknesses of Jiang *et al.*'s Scheme

3.1 Weakness 1: No User Anonymity

In Jiang *et al.*'s scheme and Li *et al.*'s scheme, ID_i is sent in plaintext in the registration. Once the attacker as a co-worker in the same organization, he/she acquires the information $\{ID_i, RPW_i, b_i\}$ and has knowledge of ID_i.Jiang *et al.*'s protocol does not guarantee user anonymity.

3.2 Weakness 2: Failure to Defend Known Session-Specific Temporary Information Attack

Once the session-specific temporary information of the protocol is leaked, such as random numbers that make up the session password, the session key is still secure, which indicates that the protocol can resist the known session-specific temporary information attack. In Jiang *et al.*'s scheme, the session key $SK_{ij} = H(K_i \oplus K_j)$, where K_i is generated by U_i and K_j is generated by S_j in the login and authentication phase. If an attacker knows information K_i and K_j, the session key will be exposed to the attacker. So in that sense, Jiang *et al.*'s scheme cannot defend known session-specific temporary information temporary information attack.

3.3 Weakness 3: No Password Change Phase

At present, authentication protocols are vulnerable to offline password guessing attacks and online password guessing attacks. Moreover, most users habitually use some anniversaries or dates with special meanings, which will further reduce the security of passwords. Jiang *et al.*'s scheme has no password change phase, which not only prevents users from changing their password when they forget it, but also makes their protocol vulnerable to password-related attacks. Of course, we know that we need not only the password change phase, but also the user authentication in the password change stage. Otherwise any illegal user will be able to change the password of the legitimate user, which will also have security risks.

3.4 Weakness 4: Inapplicable to IoT Environments

Wireless sensor network is very different from the traditional wireless communication network. The primary design goal of the traditional wireless communication network is to provide the highest possible service quality, and node energy can be supplemented, so consumption is a secondary consideration. However, the nodes of wireless sensor networks cannot replenish energy, so extending the life cycle of the network system as far as possible has become the primary design goal of wireless sensor networks [25]. Sensor nodes use low-power devices as much as possible, and the research on energy consumption is also based on low-power devices. Communication module is the department with the largest energy consumption among nodes, and it is also the focus of the research on wireless sensor network nodes. In the login and authentication phase of Jiang *et al.*'s protocol, a part of the information is transmitted directly between the user and the server, rather than building a communication platform for the user and the server through a third party GWN, which is inconsistent with the wireless sensor network's need to extend the life cycle of the network system as far as possible.

3.5 Weakness 5: No Clock Synchronization Mechanism

In information transmission, we need to ensure the freshness of information transmission and ensure that the information transmitted by legitimate users will not be intercepted and utilized by attackers, such as replay attack and man-in-the-middle attack, etc. Generally, researchers solve this problem by two methods: timestamp mechanism and random numbers. However, in wireless sensor

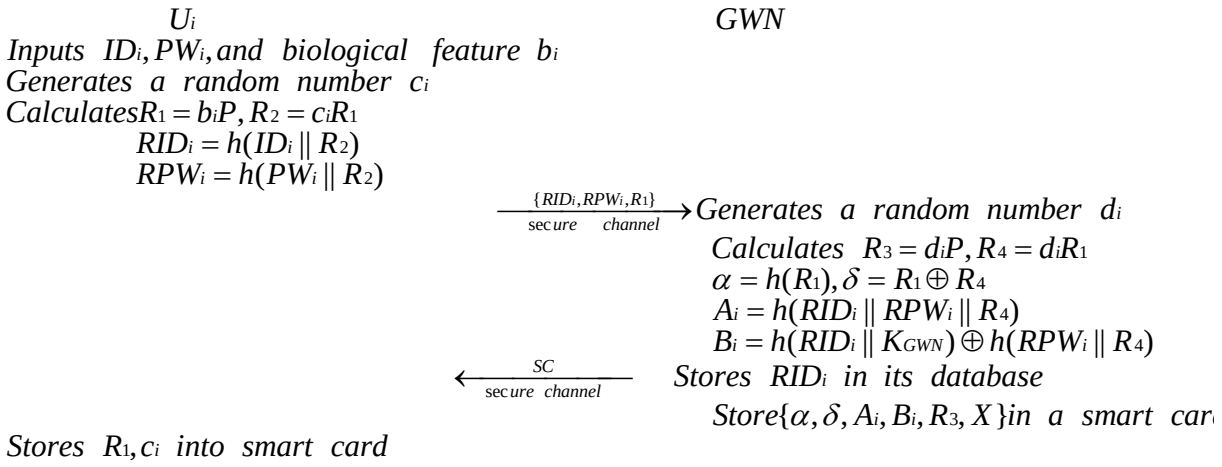

Figure 2: Registration phase of proposed protocol

networks, the clock precision of each network node is limited due to the cost limitation, and the difference between each node clock will be larger and larger with the passage of time. Many important basic functions of wireless sensor networks require nodes in the network to maintain a relatively uniform time scale. Using both timestamp and random numbers in Jiang *et al.* 's protocol may encounter clock asynchronization problem.

4 Proposed Protocol

At present, user biometric information is widely used in three-factor authentication protocols because of their uniqueness. We believe that Jiang *et al.* 's protocol has a good framework, so we propose an improved remote identity authentication protocol based on elliptic curve cryptography based on Jiang *et al.*' s two-factor authentication protocol. Our protocol not only improves the disadvantages of Jiang *et al.*'s protocol, but also adds user biometric to improve the security of the protocol.

Furthermore, we use elliptic curve cryptography, which provides equal or higher levels of security while using smaller keys than other methods.

4.1 Registration Phase

Firstly, GWN chooses the parameters $\{E(F_P), G, x, X, P_{par}, K_{GWN}\}$, $X = xP_{par}$, like Jiang *et al.*'s protocol in user registration phase. The registration phase of proposed protocol is shown in Figure 2.

During the registration phase, he/she will perform the following steps complete the registration.

4.2 Login and Authentication Phase

Once the user is registered, he/she will follow the steps below to begin the login and authentication phase. The login and authentication phase of proposed protocol is shown in Figure 3.

4.3 Password Change Phase

Compared with the protocol of Jiang *et al.*, our proposed improved protocol allows the user to change his/her password. Once the user wants to change his/her password, he/she will proceed as follows: U_i inserts smart card into a card reader, inputs biological feature b_i, SC calculates $R_4 = \delta \oplus R_1$, checks to see if the equation $R_4 = \delta \oplus R_1 \stackrel{?}{=} R_4' = b_i'R_3$ is true, and if so, SC continues to calculate the equation $A_i' = h(h(ID_i \| c_ib_i'P) \| h(PW_i \| c_ib_i'P) \| R_4') \stackrel{?}{=} A_i$ in its database. If they are equal, SC accepts $U_i's$ request to change passwords and sends U_i a request to enter a new password. Once U_i enters a new password, SC calculates $A_i^{new} = h(h(ID_i \| R_2) \| h(PW_i^{new} \| R_2) \| R_4')$, $B_i^{new} = h(h(ID_i \| R_2) \| K_{GWN}) \oplus h(h(PW_i^{new} \| R_2) \| R_4')$, updates A_i^{new} and B_i^{new} with A_i and B_i respectively. Following this step, the user makes a password change.

5 Security Analysis

In this section, we conducted a security analysis of our proposed protocol, and we demonstrated that our protocol can withstand all the major attacks.

User anonymity. In our improved protocol, either the user name U_i or the password PW_i is transmitted in plaintext. And U_i passes $RID_i = h(ID_i \| R_2), RPW_i = h(PW_i \| R_2)$ to GWN, where $R_2 = c_ib_iP$. According to DL and CDH problem, we can know that even if the attacker obtains the information R_1 in the channel, he/she cannot calculate R_2. So our protocol can guarantee user anonymity.

Resist known session-specific temporary information attack. In Jiang *et al.*'s scheme, the session key $SK_{ij} = H(K_i \oplus K_j)$, where K_i is generated by U_i and K_j is generated by S_j in the login and authentication phase. If an attacker knows information K_i and K_j, the session key will be exposed

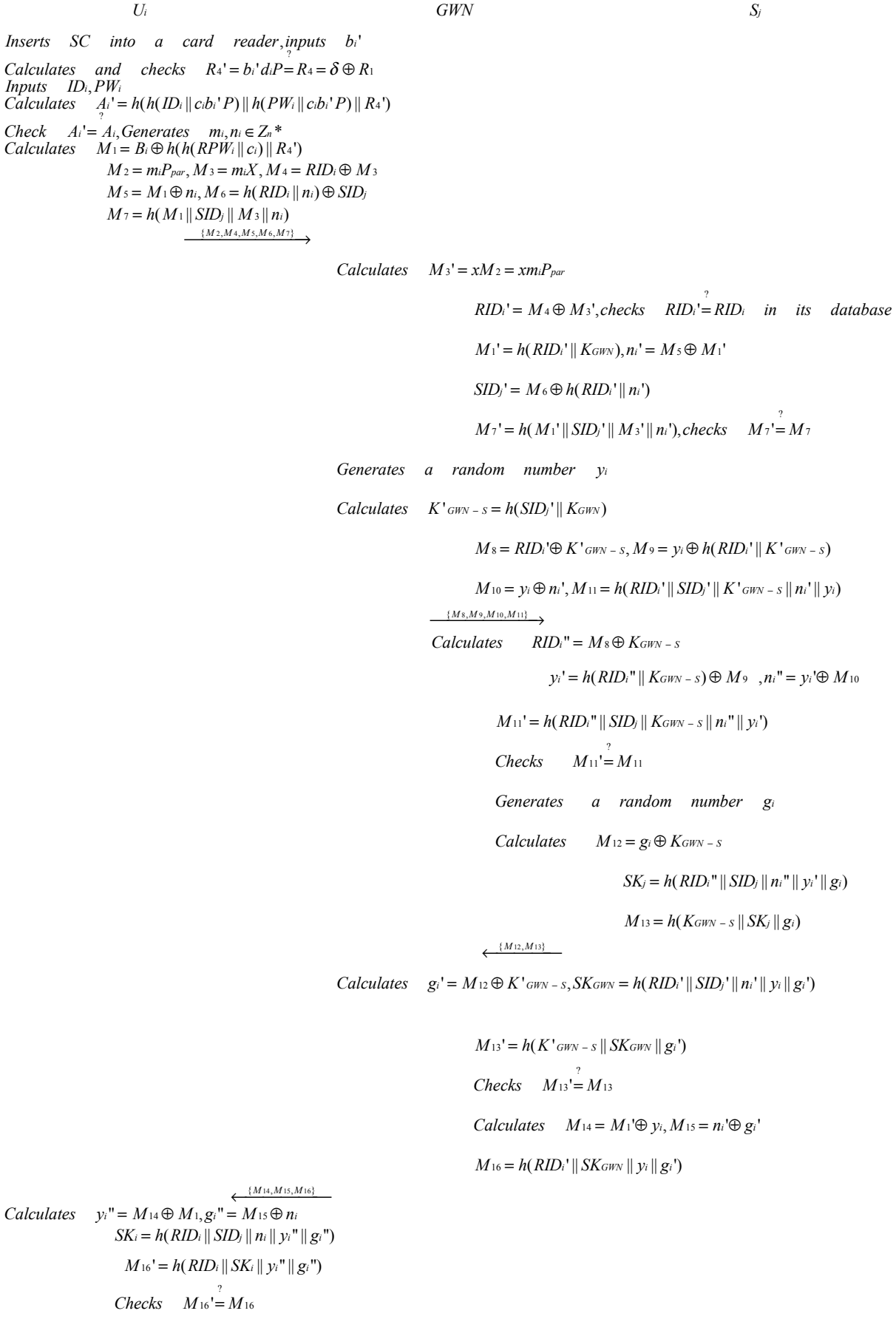

Figure 3: Login and authentication phase of proposed protocol

to the attacker. In our improved protocol, the session key $SK_i = h(RID_i \| SID_j \| n_i \| y_i'' \| g_i'')$, where $RID_i = h(ID_i \| R_2)$, $SID_j = M_6 \oplus h(RID_i \| n_i)$, $n_i \in Z_n^*$, y_i and g_i are random numbers. Even though an attacker knows the information y_i, g_i, it would not be able to calculate SK_i without the information SID_j.

Efficient password change. Jiang *et al.*'s protocol does not have a password change mechanism. Our proposed improved protocol has a password change mechanism, and once the user wants to change his/her password, the system will verify it first. The system will only let the user go through the password change phase if the authentication has passed.

Applicable to IoT environments. In the login and authentication phase of Jiang *et al.*'s protocol, a part of the information is transmitted directly between the user and the server, rather than building a communication platform for the user and the server through a third party, which is inconsistent with the wireless sensor network's need to extend the life cycle of the network system as far as possible. We modified this part of Jiang *et al.* 's protocol to ensure that the information transfer between the user and the server needs to be carried out through a third party GWN.This form of information transmission is more suitable for the Internet of Things environment

Clock synchronization mechanism. In order to resist replay attack or man-in-the-middle attack, scholars usually add timestamp mechanism or random number into the protocol. However, when both of these are used in the protocol, the clock asynchronous problem will be caused, so we only use random numbers in the improved protocol, without the use of timestamp mechanism, which ensures the protection against replay attacks or man-in-the-middle attacks, while keeping the clock synchronized.

Resist privileged insider attack. In general, users tend to register on different systems with the same password in order to remember the password more easily. Once a privileged internal staff member obtains the user's password, she/he can use the same password for access on other systems. However, our proposed protocol does not pass the user's username and password over the channel in clear text, and it also uses CDH mathematical puzzle to mask them.

Resist stolen smart attack. In our improved protocol, the massages $\{\alpha, \delta, A_i, B_i, R_3, X, f(\cdot)\}$ are stored on the smart card, where $A_i = h(RID_i \| RPW_i \| R_4)$, $B_i = h(RID_i \| K_{GWN}) \oplus h(RPW_i \| R_4)$. So given the CDH problem, even if the attacker knows c_i, d_i, R_1, he/she cannot compute R_4 or R_2. So attackers cannot get important information from smart cards even if they use side-channel attack such as strong analysis.

Provide mutual authentication. In Jiang et al,' protocol, the session key $SK_{ij} = H(K_i \oplus K_j)$. We think it failures to defend known session-specific temporary information attack. In our protocol, the session key $SK = h(RID_i \| SID_j \| n_i \| y_i \| g_i)$, where $RID_i = M_4 \oplus M_3$, $SID_j = M_6 \oplus h(RID_i \| n_i)$, y_i' and g_i are random numbers. The attacker cannot derive the correct RID_i without M_3. And we never send M_3 on the message channel. So our protocol can be safely authenticated to each other.

5.1 Security Analysis Using BAN Logic

The goals to be achieved by using BAN logic are mutual authentication among, GWN, and S_i. The goals are described by using BAN logic language as follows:

$G1 : S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$G2 : S_j| \equiv U_i| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$G3 : U_i| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$G4 : U_i| \equiv S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$G5 : GWN| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} U_i$

$G6 : GWN| \equiv U_i| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} U_i$

$G7 : GWN| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} S_j$

$G8 : GWN| \equiv S_j| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} S_j$

The messages that U_i, GWN, and S_i communicate with each other are described in BAN logic language as follows:

$M_1 : U_i \rightarrow GWN : \{M_2, M_4, M_5, M_6, M_7\}$
$\{miP_{par}, \langle RID_i \rangle_{miX}, \langle n_i \rangle_{h(RID_i \| K_{GWN})}, \langle SID_j \rangle_{h(RID_i \| n_i)},$
$(SID_j \| n_i) miX, h(RID_i \| K_{GWN})\}$
$M_2 : GWN \rightarrow S_j : \{M_8, M_9, M_{10}, M_{11}\}$
$\{\langle RID_i' \rangle_{K_{GWN-S}}, \langle y_i \rangle_{h(RID_i' \| K_{GWN-S}')}, \langle n_i \rangle_{y_i},$
$(RID_i \| SID_j)(n_i, y_i, K_{GWN-S}')\}$
$M_3 : S_j \rightarrow GWN : \{M_{12}, M_{13}\}$
$\{\langle g_i \rangle_{K_{GWN-S}}, (g_i)(SK_j, K_{GWN-S}')\}$
$M_4 : GWN \rightarrow U_i : \{M_{14}, M_{15}, M_{16}\}$
$\{\langle y_i \rangle_{h(RID_i \| K_{GWN})}, \langle g_i' \rangle_{n_i'}, (RID_i')(y_i, g_i', SK_{GWN})\}$

To demonstrate the security of our proposed protocol, we propose a number of hypotheses:

$A_1 : U_i| \equiv \#n_i$

$A_2 : GWN| \equiv y_i$

$A_3 : S_j| \equiv \#g_i$

$A_4 : U_i| \equiv U_i \overset{miX}{\longleftrightarrow} GWN$

$A_5 : U_i| \equiv U_i \overset{SK_j}{\longleftrightarrow} S_j$

$A_6 : GWN| \equiv GWN \overset{mixP}{\longleftrightarrow} U_i$

$A_7 : GWN| \equiv GWN \overset{K_{GWN-S}}{\longleftrightarrow} S_j$

$A_8 : S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$

$A_9 : S_j| \equiv S_j \overset{K_{GWN-S}}{\longleftrightarrow} GWN$

$A_{10} : U_i| \equiv S_j \Rightarrow g_i, SK_j$

$A_{11} : U_i| \equiv GWN \Rightarrow y_i, SK_{GWN}$

$A_{12} : GWN| \equiv U_i \Rightarrow n_i, SK_i, mixP$

$A_{13} : GWN| \equiv S_j \Rightarrow g_i \oplus K_{GWN-S}$

$A_{14} : S_j| \equiv GWN \Rightarrow y_i \oplus h(RID_i \| K_{GWN-S})$

$A_{15}: S_j| \equiv U_i \Rightarrow n_i, SK_i$

According to the above initial state and based on BAN logic inference rules, the properties of the protocol are analyzed and deduced as follows:

From $M_1: U_i \rightarrow GWN: \{M_2, M_4, M_5, M_6, M_7\}$, we have

$S_1: GWN \triangleleft \{miP_{par}, \langle RID_i\rangle miX, \langle n_i\rangle h(RID_i\|K_{GWN}), \langle SID_j\rangle h(RID_i\|n_i), (SID_j\|n_i)miX, h(RID_i\|K_{GWN})\}$.

According to S_1, A_6, and message meaning rule, we have

$S_2: GWN| \equiv U_i \sim \{miP_{par}, \langle RID_i\rangle miX, \langle n_i\rangle h(RID_i\|K_{GWN}), \langle SID_j\rangle h(RID_i\|n_i), (SID_j\|n_i) miX, h(RID_i\|K_{GWN})\}$.

According to S_2, A_1, and freshness conjucatenation and nonce verification rules, we have

$S_3: GWN| \equiv U_i| \equiv \{miP_{par}, \langle RID_i\rangle miX, \langle n_i\rangle h(RID_i\|K_{GWN}), \langle SID_j\rangle h(RID_i\|n_i), (SID_j\|n_i)miX, h(RID_i\|K_{GWN})\}$.

According to S_3, A_6, A_{12}, and jurisdiction rule, we have

$S_4: GWN| \equiv \{miP_{par}, \langle RID_i\rangle miX, \langle n_i\rangle h(RID_i\|K_{GWN}), \langle SID_j\rangle h(RID_i\|n_i), (SID_j\|n_i)miX, h(RID_i\|K_{GWN})\}$.

According S_4, and session key rule, we have

$S_5: GWN| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} U_i$. (G5)

According S_5, A_2, and nonce-verification rule, we have

$S_6: GWN| \equiv U_i| \equiv GWN \overset{SK_{GWN}}{\longleftrightarrow} U_i$. (G6)

According M_2, we have

$S_7: S_j \triangleleft \{\langle RID_i'\rangle K_{GWN-S}, \langle y_i\rangle h(RID_i'\|K'_{GWN-S}), \langle n_i\rangle y_i, (RID_i\|SID_j)(n_i, y_i, K'_{GWN-S})\}$.

According to S_7, A_9, and message meaning rule, we have

$S_8: S_j| \equiv GWN \sim \{\langle RID_i'\rangle K_{GWN-S}, \langle y_i\rangle h(RID_i'\|K'_{GWN-S}), \langle n_i\rangle y_i, (RID_i \|SID_j) (n_i, y_i, K'_{GWN-S})\}$.

According to S_8, A_2, A_{14}, and freshness conjucatenation and nonce verification rules, we have

$S_9: S_j| \equiv GWN| \equiv \{\langle RID_i'\rangle K_{GWN-S}, \langle y_i\rangle h(RID_i'\|K'_{GWN-S}), \langle n_i\rangle y_i, (RID_i\|SID_j) (n_i, y_i, K'_{GWN-S})\}$.

According M_4, we have

$S_{10}: U_i \triangleleft \{\langle y_i\rangle h(RID_i\|K_{GWN}), \langle g_i'\rangle n_i', (RID_i')(y_i, g_i', SK_{GWN})\}$.

According to S_{10}, A_4, and message meaning rule, we have

$S_{11}: U_i| \equiv GWN \sim \{\langle y_i\rangle h(RID_i\|K_{GWN}), \langle g_i'\rangle n_i', (RID_i')(y_i, g_i', SK_{GWN})\}$.

According to S_{11}, A_2, A_{11}, freshness conjucatenation and nonce verification rules, we have

$S_{12}: U_i| \equiv GWN| \equiv \{\langle y_i\rangle h(RID_i\|K_{GWN}), \langle g_i'\rangle n_i', (RID_i')(y_i, g_i', SK_{GWN})\}$.

According to S_9, A_9, A_{14}, and jurisdiction rule, we have

$S_{13}: S_j| \equiv \{\langle RID_i'\rangle K_{GWN-S}, \langle y_i\rangle h(RID_i'\|K'_{GWN-S}), \langle n_i\rangle y_i, (RID_i\|SID_j)(n_i, y_i, K'_{GWN-S})\}$.

According to S_{12}, A_4, A_{11}, and jurisdiction rule, we have

$S_{14}: U_i| \equiv \{\langle y_i\rangle h(RID_i\|K_{GWN}), \langle g_i'\rangle n_i', (RID_i')(y_i, g_i', SK_{GWN})\}$.

According to S_{13}, and the session key rules, we have

$S_{15}: S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} GWN, S_j| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$. (G1)

According to S_{13}, A_{14}, and the session key rules ,we have

$S_{16}: S_j| \equiv GWN| \equiv S_j \overset{SK_j}{\longleftrightarrow} GWN, S_j| \equiv U_i| \equiv S_j \overset{SK_j}{\longleftrightarrow} U_i$. (G2)

According to S_{14}, and the session key rules, we have

$S_{17}: U_i| \equiv U_i \overset{SK_i}{\longleftrightarrow} GWN, U_i| \equiv S_j \overset{SK_i}{\longleftrightarrow} U_i$. (G3)

According to S_{14}, A_{11}, A_5 and the session key rules ,we have

$S_{18}: U_i| \equiv GWN| \equiv U_i \overset{SK_i}{\longleftrightarrow} GWN, U_i| \equiv S_j| \equiv S_j \overset{SK_i}{\longleftrightarrow} U_i$. (G4)

According $M_3: S_j \rightarrow GWN: \{M_{12}, M_{13}\}$, we have

$S_{19}: GWN \triangleleft \{\langle g_i\rangle K_{GWN-S}, (g_i)(SK_j, K'_{GWN-S})\}$.

According S_{19}, A_7, and message meaning rule, we have

$S_{20}: GWN| \equiv S_j \sim \{\langle g_i\rangle K_{GWN-S}, (g_i) (SK_j, K'_{GWN-S})\}$.

According S_{20}, A_3, we have

$S_{21}: GWN| \equiv S_j| \equiv \{\langle g_i\rangle K_{GWN-S}, (g_i) (SK_j, K'_{GWN-S})\}$.

According S_{21}, A_7, A_{13}, and jurisdiction rule, we have

$S_{22}: GWN| \equiv \{\langle g_i\rangle K_{GWN-S}, (g_i)(SK_j, K'_{GWN-S})\}$.

According to S_{22}, A_{13}, A_{15}, we have

$S_{23}: GWN| \equiv S_j| \equiv S_j \overset{SK_{GWN}}{\longleftrightarrow} GWN$. (G8)

According to S_{22}, A_8, we have

$S_{24}: GWN| \equiv S_j \overset{SK_{GWN}}{\longleftrightarrow} GWN$. (G7)

According to the BAN logic proof, mutual authentication can be achieved between them.

5.2 Security Analysis Using Random Oracle Model

We conduct a security proof in the random oracle model. Through strict formal verification using random Oracle, it can be proved that the scheme is secure against an adversary.

Definition 1. *Reveal: Given a hash value $y = h(x)$, this random oracle unconditionally outputs the input x.*

Theorem 1. *Under the assumption that a one-way hash function $h(\cdot)$ behaves like an oracle, the proposed scheme is probably secure against an adversary A for deriving the identity ID_i, the password PW_i, the biometric key b_i of a legal user U_i and the secure key K_{GWN} of the GWN, even if user U_i's smart card is lost/stolen.*

Proof. For the proof, we assume that an adversary A is able to derive the identity ID_i, the password PW_i, the biometric key b_i of a legal user U_i, and the secret key K_{GWN} of the GWN. We assume that the adversary A has lost/stolen smart card of the user U_i and A can extract all the sensitive information stored in smart card using the power analysis attack. For this, A uses the Reveal oracle to run an experimental algorithm $EXP1^{3FAKA}_{HASH,A}$ shown in Algorithm 1for

the proposed three-factor authentication and key agreement(3FAKA). We define the success probability for $EXP1^{3FAKA}_{HASH,A}$ as $Succ1^{3FAKA}_{HASH,A} = |\Pr[EXP1^{3FAKA}_{HASH,A} = 1] - 1|$, where $\Pr[E]$ is the probability of an event E. The advantage function for this experiment becomes $Adv1^{3FAKA}_{HASA,A}(t_1, q_R) = \max A\{Succ1^{3FAKA}_{HASH,A}\}$ in which the maximum is taken over all A with execution time t_1 and the number of queries q_R made to the Reveal oracle. According to the attack experiment described in Algorithm 1, if the adversary A has the ability to invent the one-way hash function $h(\cdot)$, then A can directly obtain $U_i's$ ID_i, PW_i and b_i and $GWN's$ K_{GWN}, and win the game. However, it is computationally infeasible problem to invert $h(\cdot)$, i.e., $Adv1^{3FAKA}_{HASA,A}(t_1) < \varepsilon$, for any sufficiently small $\varepsilon > 0$. Then, we have $Adv1^{3FAKA}_{HASA,A}(t_1, q_R) \leq \varepsilon$, since $Adv1^{3FAKA}_{HASA,A}(t_1, q_R) \leq \varepsilon$ depends on $Adv1^{3FAKA}_{HASA,A}(t_1)$. Therefore, the proposed scheme is provably secure against the adversary A for deriving ID_i, PW_i, b_i and K_{GWN}, even if the smart card is lost/stolen by A. □

1: Extract the information $\{\alpha, \delta, A_i, B_i, R_3, X\}$ from smart card using the power analysis attack.
2: Call the Reveal oracle. Let $(RID_i^*, K_{GWN}*, RPW_i^*, R_4*) \leftarrow \mathrm{Re}\,veal(B_i)$
3: Call the Reveal oracle. Let $(R_1* = b_i^*P) \leftarrow \mathrm{Re}\,veal(\alpha)$
4: Compute $R_1' = R_4 * \oplus\delta$
5: **if** $(R_1' = R_1*)$ **then**
6: Call the Reveal oracle. Let $(ID_i^*, R_2*) \leftarrow \mathrm{Re}\,veal(RID_i)$
7: Call the Reveal oracle. Let $(PW_i^*, R_2*) \leftarrow \mathrm{Re}\,veal(RPW_i)$
8: Compute $A_i^* = h(h(ID_i^*\|R_2*)\|h(PW_i^*\|R_2*)\|R_4*)$
9: **if** $(A_i^* = A_i)$ **then**
10: Intercept the message $\{M_8, M_9, M_{10}, M_{11}\}$
11: Call the Reveal oracle. Let $(RID_i^*, SID_j*, K'_{GWN-S}*, n_i^*, y_i^*) \leftarrow \mathrm{Re}\,veal(M_{11})$
12: Call the Reveal oracle. Let $(SID_j **, K_{GWN} * *) \leftarrow \mathrm{Re}\,veal(K'_{GWN-S}*)$
13: Compute $M_8* = RID_i^* \oplus K'_{GWN-S}*$
14: Compute $B_i^* = h(RID_i^*\|K_{GWN} * *) \oplus h(RPW_i^*\|R_4*)$
15: **if** $(M_8* = M_8)$ and $(B_i^* = B_i)$ **then**
16: Accept ID_i^*, PW_i^* and b_i^* as the correct identity ID_i, PW_i and b_i of the user, an
17: $K_{GWN} **$ as the correct parameters of GWN.
18: **return** 1
19: **else**
20: **return** 0
21: **end if**
22: **else**
23: **return** 0
24: **end if**
25: **else**
26: return 0
27: **end if**

Algorithm 1 $EXP1^{3FAKA}_{HASH,A}$

Theorem 2. *Under the assumption that a one-way hash function $h(\cdot)$ behaves like an oracle, the proposed scheme is probably secure against an adversary A for deriving the session key SK_j/SK_i shared between U_i and S_j.*

Proof. We assume that an adversary A is able to derive the session key shared between a legal user and medical server S_j. For this, A user the Reveal oracle to run an experimental algorithm $EXP2^{3FAKA}_{HASH,A}$ shown in Algorithm 2. We define the success probability for $EXP2^{3FAKA}_{HASH,A}$ as $Succ2^{3FAKA}_{HASH,A} = |\Pr[EXP2^{3FAKA}_{HASH,A} = 1] - 1|$. The advantage function for this experiment becomes $Adv2^{3FAKA}_{HASA,A}(t_2, q_R) = \max A\{Succ2^{3FAKA}_{HASH,A}\}$ in which the maximum is taken over all A with execution time t_2 and the number of queries q_R made to the Reveal oracle. According to the attack experiment described in Algorithm 2, if the adversary A has the ability to invert the one-way hash function $h(\cdot)$, then A can easily derive SK_j/SK_i and win the game. However, it is computationally infeasible problem to invent $h(\cdot)$, i.e., $Adv2^{3FAKA}_{HASA,A}(t_2) \leq \varepsilon$, for any sufficiently small $\varepsilon > 0$. Then, we have $Adv2^{3FAKA}_{HASA,A}(t_2, q_R) \leq \varepsilon$ is also dependent on $Adv2^{3FAKA}_{HASA,A}(t_2)$. The proposed scheme is provably secure against the adversary A for deriving S_j. □

1: Extract the login request information $\{M_2, M_4, M_5, M_6, M_7\}$ during the login phase.
2: Call the Reveal oracle. Let $(M_1'\|SID_j'\|M_3'\|n_i') \leftarrow \mathrm{Re}\,veal(M_7)$
3: Compute $RID_i' = M_4 \oplus M_3'$
4: Compute $n1* = M_5 \oplus M_1'$
5: **if** $(n1* = n1')$ **then**
6: Intercept the message $\{M_8, M_9, M_{10}, M_{11}\}$, $\{M_{12}, M_{13}\}$
7: Call the Reveal oracle. Let $(K * GWN - S\|SK_j * \|g_i^*) \leftarrow \mathrm{Re}\,veal(M_{13})$
8: Compute $g_i^{*'} = M_{12} \oplus K * GWN - S$
9: **if** $(g_i^* = g_i^{*'})$ **then**
10: Compute $y_i^* = M_{10} \oplus n_i'$
11: Compute $SK_j*' = h(RID_i'\|SID_j'\|n_i'\|y_i^*\|g_i^{*'})$
12: **if** $(SK_j*' = SK_j')$ **then**
13: Accept SK_j*' as the correct session key shared between U_i and S_j.
14: **return** 1
15: **else**
16: **return** 0
17: **end if**
18: **else**
19: **return** 0
20: **end if**
21: **else**
22: **return** 0

Table 2: Comparison of security features

Performance	Jiang *et al.* (2016) [21]	Farash *et al.* (2016) [?]	Wazid *et al.* (2018) [11]	Amin *et al.* (2018) [?]	Li *et al.* (2018) [22]	Ours
F1	Yes	No	Yes	No	No	Yes
F2	Yes	Yes	Yes	Yes	No	Yes
F3	No	No	No	Yes	No	Yes
F4	No	Yes	Yes	Yes	Yes	Yes
F5	No	Yes	Yes	Yes	Yes	Yes
F6	No	Yes	Yes	Yes	Yes	Yes
F7	No	Yes	No	No	Yes	Yes
F8	No	No	Yes	Yes	Yes	Yes
F9	Yes	No	No	No	No	Yes
F10	Yes	Yes	Yes	Yes	Yes	Yes
F11	No	No	No	No	No	Yes

F1: Provide three-factor security; F2: Resist forgery attack; F3: User anonymity; F4: Defend known session-specific temporary information attack; F5: Password change phase; F6: Applicable to IoT environments; F7: Clock synchronization mechanism; F8: Resist offline guessing attack; F9: Resist forward secrecy; F10: session key agreement; F11: Smart card loss attack.

Table 3: Comparison of efficiency characteristcs

	U_i	S_i	GWN	Total
Jiang *et al.*(2016) [21]	8 $T1$ +2 $T3$	6 $T1$	9 $T1$ + $T3$	23 $T1$ +3 $T3$
Farash *et al.*(2016) [?]	11 $T1$	7 $T1$	14 $T1$	32 $T1$
Wazid *et al.*(2018) [11]	13 $T1$ +2 $T2$	4 $T1$ +2 $T2$	5 $T1$ +4 $T2$	21 $T1$ +8 $T2$
Amin *et al.*(2018) [?]	12 $T1$	6 $T1$	16 $T1$	34 $T1$
Li *et al.*(2018) [22]	8 $T1$ +2 $T3$	4 $T1$	9 $T1$ + $T3$	21 $T1$ +3 $T3$
Our	7 $T1$ +2 $T3$	4 $T1$	9 $T1$ + $T3$	20 $T1$ +3 $T3$

$T1$: The cost for executing the hash function operation; $T2$: The cost for symmetric encryption/decryption operation; $T3$: The ECC operation for the ECC operation

23: **end if**

Algorithm 2 $EXP2^{3FAKA}_{HASH,A}$

6 Comparison of Security Features and Efficiency Characteristics

Table 2 is the comparison of security features. Table 3 is the comparison of efficiency characteristics.

7 Conclusions

Based on the security problems existing in the protocols between Jiang et al and Li et al, we have proposed an improved three-factor remote user authentication protocol using elliptic curve cryptography. Our improved protocol uses the knowledge of elliptic curve cryptography, which is an algorithm for establishing public key encryption. Its main advantage is that in some cases it provides equivalent or higher security than other methods using smaller keys. We construct our protocol by using discrete logarithm and computational Diffie-Hellman problem. And our protocol uses only random numbers to ensure the freshness and security of the protocol, and does not use timestamps, so clock asynchrony will not occur. We performed BAN logic analysis, security analysis and security comparative analysis on the protocol. From the analysis, we can see that the improved protocol has higher security and does not add much computation.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments

References

[1] B. A. Alzahrani, A. Irshad, A. Albeshri, *et al*, "A Provably Secure and Lightweight Patient-Healthcare Authentication Protocol in Wireless Body Area Net-

works," *Wireless Personal Communications*, vol. 117, no. 1, pp. 47– 69, 2021.

[2] R. Amin, S. K. H. Islam, G. P. Biswas, *et al*, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483–495, 2018

[3] A. Angelucci, D. Kuller, A. Aliverti, "A home telemedicine system for continuous respiratory monitoring," *IEEE Journal of Biomedical and Health Informatics*, vol. 25, no. 4, pp. 1247– 1256, 2021.

[4] M. Burrows, M. Abadi, R. Needham, "A logic of Authentication," *ACM Transactions on Computer Systems (TOCS)*, vol. 8, no. 1, pp. 18–36, 1990.

[5] A. K. Das, "A Secure and Efficient User Anonymity-Preserving Three-Factor Authentication Protocol for Large-Scale Distributed Wireless Sensor Networks," *Wireless Personal Communications*, vol. 82, no. 3, pp. 1377–1404, 2015.

[6] M. L. Dow, S. R. Dugan, "Hypothesis: A wearable device may help COVID-19 patients improve lung function," *Medical Hypotheses*, vol. 146, 2021.

[7] M. S. Farash, M. Turkanovi´c, S. Kumari, *et al*, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016.

[8] N. Garg, M. Wazid, A. K. Das, *et al*, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[9] D. He, N. Kumar, N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, vol. 321, pp. 263–277, 2015.

[10] A. Jabbari , J. B. Mohasefi, "Usersensor mutual authenticated key establishment scheme for critical applications in wireless sensor networks," *Wireless Networks*, vol. 27, no. 1, pp. 227– 248, 2021.

[11] X. Y. Jia, D. B. He, N. Kumar, *et al*, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Networks*, vol. 25, no. 8, pp. 4737–4750, 2019.

[12] Q. Jiang, S. Zeadally, J. F. Ma, *et al*, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376– 3392, 2017.

[13] X. Li, J. W. Niu, S. Kumari, *et al*, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[14] S. G. Liu, X. Wang, Y. W. Liu, *et al*, "Fast scalar multiplication algorithms based on 5p+ q of elliptic curve over gf (3ˆ m)," *International Journal of Network Security*, vol. 23, no. 4, pp. 604–611, 2021.

[15] W. R. Liu, X. He, Z. Y. Ji, "An improved authentication protocol for telecare medical information system," *International Journal of Electronics and Information Engineering*, vol. 12, no. 4, pp. 170–181, 2020.

[16] W. R. Liu, X. He, Z. Y. Ji, "Security analysis and enhancements of a user authentication scheme," *International Journal of Network Security*, vol. 23, no. 5, pp. 895–903, 2021.

[17] Y. R. Lu, G. Q. Xu, L. X. Li, *et al*, "Anonymous three-factor authenticated key agreement for wireless sensor networks," *Wireless Networks*, vol. 25, no. 4, pp. 1461–1475, 2019.

[18] F. Merabet, A. Cherif, M. Belkadi, *et al*, "New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications," *Peer-to-Peer Networking and Applications*, vol. 13, no. 2, pp. 439–474, 2020.

[19] J. Q. Mo, W. Shen, and W. S. Pan, "An Improved Anonymous Authentication Protocol for Wearable Health Monitoring Systems," *Wireless Communications and Mobile Computing*, vol. 2020, 2020.

[20] R. Sharma, M. Wazid, P. Gope, "A blockchain based secure communication framework for community interaction," *Journal of Information Security and Applications*, vol. 58, 2021.

[21] S. Q. Cao, W. R. Liu, L. L. Cao, *et al*, "An Improved Authentication Protocol Using Smart Cards for the Internet of Things," *IEEE Access*, vol. 7, pp. 157284–157292, 2019.

[22] C. Wang, H. Y. Qi. "Visualising the knowledge structure and evolution of wearable device research," *Journal of Medical Engineering & Technology*, vol. 45, no. 3, pp.1-16, 2021.

[23] H. Wang, F. Yu, M. Li, *et al*, "Clock Skew Estimation for Timestamp-Free Synchronization in Industrial Wireless Sensor Networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 90–99, 2021.

[24] M. Wazid, A. K. Das, J. H. Lee, "User authentication in a tactile internet based remote surgery environment: Security issues, challenges, and future research directions," *Pervasive and Mobile Computing*, vol. 54, pp. 71–85, 2019.

[25] M. Wazid, A. K. Das, V. Odelu, *et al*, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269–282, 2018.

[26] F. Wu, X. Li, L. L. Xu, *et al*, "A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks with IoT Notion," *IEEE Systems Journal*, vol. 15, no. 1, pp. 1120–1129, 2021.

[27] Z. S. Xu, C. Xu, H. X. Chen, *et al*, "A lightweight anonymous mutual authentication and key agreement scheme for WBAN," in *Concurrency and Computation: Practice and Experience*, vol. 31, 2019.

[28] F. Yan, L. G. Xing, Z. C. Zhang, "An improved certificateless signature scheme for iot-based mobile

payment," *International Journal of Network Security*, vol. 23, no. 5, pp. 904–913, 2021.

Biography

Liu Wanrong received her master's degree from Shanghai Ocean University in 2021. At present, she has worked in Shanghai Jiao Tong University Affiliated Sixth People's Hospital. Her main research is communication security and Internet of things technology.

Li Bin received his master's degree in NMR Analysis Center from East China Normal University in 1990. From 1990 to 1996, he worked in hospital and global medical equipment manufacture, and has been trained on MRI and CT technology four times in Japan and United States of American. From 1997 he has been in charge of device management and quality control of medical equipment in Shanghai Sixth people's hospital for 20 years. He authorized and co-authorized six books, published over 60 articles in national statistical source journal. He is the Vice-director of east-campus of Shanghai Sixth People's Hospital Affiliated to Shanghai Jiao Tong University now. His research interests include regional medical equipment management and quality control, assessment and management of medical equipment suppliers, management of service and rating of customer satisfaction, evaluation of medical imaging equipment performance and service system, and IOT and communication safety in medical technology management. Mr. Li is Director of Shanghai Quality Control Centre of Management of Medical Equipment, Chairman of Clinical Engineering Society of Chinese Medical Association, Vice Chairman of Clinical Engineers branch of Chinese medical doctor association, Council Member of Chinese society of Biomedical engineering, and Committee member of medical device classification technology of China SFDA. Coopted Member of Clinical Engineering Division of IFMBE.

Ji Zhiyong received his bachelor's degree from Nanjing University of Aeronautics and Astronautics in 2012. He received his MS degree Jiangsu University in 2017. He is the master's supervisor of mechanical engineering of Shanghai Ocean University. He is also the medical equipment senior engineer and deputy director of Shanghai Sixth People's Hospital East. His research directions include the development and application of wearable medical devices based on the Internet of things and the information security of the medical Internet of things.