IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 24, 2019, accepted November 6, 2019, date of publication November 14, 2019, date of current version December 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2953532

An Enhanced Three-Factor Authentication Scheme With Dynamic Verification for Medical Multimedia Information Systems

DEMING MAO[1], **HUIHONG LIU**[2], **AND WEI ZHANG**[3]

[1]College of Cyberspace Security, Northwestern Polytechnical University, Xi'an 710072, China
[2]Southwest Institute of Telecommunication, Chengdu 610041, China
[3]China Electronic Technology Cyber Security Company, Ltd., Chengdu 610041, China

Corresponding author: Deming Mao (maodmnwpu@163.com)

This work was supported by the Science Fund for Distinguished Young Scholars of Sichuan Province under Grant 2019JDJQ0058.

ABSTRACT The medical multimedia information system (MMIS), which integrates all available multimedia sources (such as videos of endoscopes, CT scans) to support diagnosis, inspection, surgery, and reporting, has greatly facilitated users (including patients and healthcare providers). What's more, MMIS enables patients to obtain diagnostic information at home and eliminates geographical restrictions between patients and hospitals. However, a large amount of sensitive medical multimedia information in MMIS, such as surgical video, may be leaked during the transmission on the public channel. Therefore, authentication and key agreement (AKA) protocols are urgently needed to provide protection for MMIS. Specifically, authentication can prevent illegal users from accessing the MMIS, while key agreement can derive session keys to protect the sensitive data in transit from eavesdropping and interception. Recently, Zhang et al. presented a dynamic three-factor AKA scheme for privacy protection in the healthcare system which provides user untraceability by dynamic identity. However, we find that Zhang et al.'s scheme cannot withstand offline password guessing attacks and denial of service attacks. Besides, their scheme does not provide password and biometric change phase. To address these shortcomings, an enhanced scheme using Rabin cryptosystem and fuzzy verifier is proposed for MMIS. The analysis of both security and performance demonstrates that the enhanced AKA scheme is better than previous schemes proposed for MMIS.

INDEX TERMS Authentication, multimedia, healthcare, privacy protection, Rabin cryptosystem, dynamic verification.

I. INTRODUCTION

The adoption of information and communication technologies has brought tremendous reforms in the medical service industry, and medical multimedia information system (MMIS) comes into being. MMIS can eliminate the geographical distance between patients and hospitals, since patients can remotely access to medical resources, such as, electrocardiogram, disease diagnosis, video of inspection, etc. and even get medical service outside the hospital [1]. Specifically, after the examination, the patient does not need to wait for the result in the hospital for a long time, nor does he/she need to commute between hospitals and homes to obtain the diagnosis result. Moreover, MMIS can greatly save the time of both patients and healthcare providers, so that patients can get timely medical treatments before their condition worsens. Hence, MMIS can reduce the patient's time and transportation costs and significantly improve the healthcare provider efficiency and patient satisfaction.

In MMIS, as shown in Figure 1, a patient first registers his/her basic information on a mobile phone [2], [3] or personal computer with the medical multimedia server (MMS). After the patient has finished the examination and diagnosis in the hospital, various medical multimedia information will be uploaded to MMS by healthcare providers. Later, the patient will be able to obtain results from MMS at home or workplace remotely. In this process, the MMIS will process a large amount of sensitive data (such as medical multimedia information and personal information). In addition, these sensitive information must be transmitted via the Internet [4]–[6].

The associate editor coordinating the review of this manuscript and approving it for publication was Dapeng Wu.

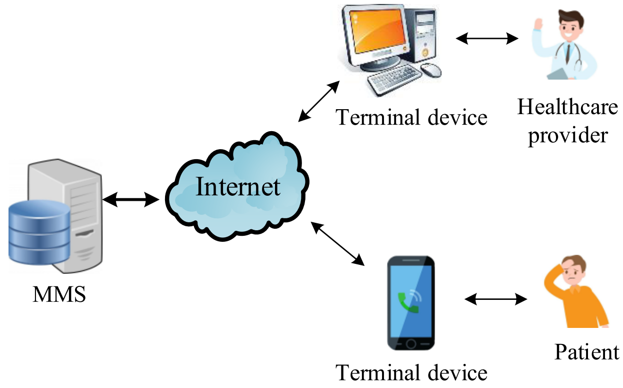


FIGURE 1. The system model of MMIS.

However, the Internet is vulnerable to attacks owing to its open nature [7]–[9], which leads to the MMIS running over the Internet becoming insecure. As a result, the sensitive medical multimedia information in MMIS may be acquired by an adversary [10]. Specifically, the adversary can intercept the medical multimedia information transmitted by patients through the open channel, then he/she performs data analysis or data mining, and obtains relevant sensitive information, such as the genetic history of the family disease. The disclosure of these private data will cause great trouble to the patients' daily life [11], [12]. Moreover, the adversary may interact with the healthcare provider by impersonating as a legitimate user to obtain private information, and make profit from it, or he/she can counterfeit a legitimate healthcare provider based on the information obtained, and defraud the patient. The adversary may also launch a tampering attack on the MMIS. He/she may alter symptoms submitted by a patient to the doctor, causing the doctor to obtain wrong patient information and thus make a wrong diagnosis; or he/she counterfeits the doctor's prescription for the patient. In either case, the patient's condition will not be diagnosed or treated correctly, and it will affect the recovery of the patient's physical condition and even endanger the patient's life.

Therefore, the provision of a protection scheme to ensure secure data transmission is crucial in MMIS [13]. Specifically, the first step is to prevent illegal users from logging into the system, accessing sensitive data or sending illegal messages. Secondly, it is essential to protect the transmitted information among parties and prevent the adversary from learning the content of the medical multimedia information. The first one can be solved by the authentication mechanism, which plays an important role in enforcing only authorized visitors to obtain access permission to the server [14], [15], [17]. There are several ways to achieve authentication: one-time password, public key encryption, and digital signatures [16]. The security of the transmitted data can be guaranteed by data encryption using the key negotiated from key agreement, thus realizing data confidentiality and integrity [17], [18]. Therefore, the proposal of an authentication and key agreement (AKA) for the MMIS is a necessity to provide security protection for sensitive medical multimedia information. However, the past works [19]–[29] have shown that designing a secure AKA protocol for MMIS is not trivial.

A. RELATED WORKS

Initially, the single-factor authentication protocol based on the password has been widely adopted to authenticate users. In this case, users enter their usernames and the corresponding passwords to prove their own identities to the system. After successful verification, they can access the data and enjoy the services provided by the system. However, user often prefers low-entropy password which is picked from a dictionary, which may be too weak to resist the exhaustive enumeration of the adversary. As a result, this type of protocols is subject to offline password guessing attacks. As for long and high-entropy passwords which may be selected randomly, their user friendliness is low in practice since users can only accurately remember and reliably enter relatively short password [34].

According to the above analysis, password-based schemes do not meet the security and user friendliness requirements at the same time. To overcome these issues, a mass of two-factor schemes which introduce the something the user owns (like smart card and security token) as the second factor have been proposed later [30]. Shiuh-Jeng and Jin-Fu [19] proposed a password authentication scheme using smart card in 1996. Then Li *et al.* [20] also gave a two-factor scheme for electronic healthcare (e-healthcare) which we mainly concern. Nevertheless, the smart card may be lost and stolen, and the secret data in it will be extracted by an adversary through side-channel attacks as long as he/she holds the smart card for enough time. The adversary can break the two-factor schemes based on the password and smart card with obtained information from the smart card. Thus, two-factor schemes need further enhancement.

To this end, three-factor authentication (3FA) schemes are put forward which combine what the user knows (password), what the user owns (the smart card, the security token) and what the users is (biometrics like iris, fingerprint and face) to provide satisfactory security attributes [31], [32]. To log in to a system, a user inserts the smart card into a terminal device and inputs his/her identity and password, then imprints biological data. Only all these three factors are valid can the user be validated as a legal one. In short, the 3FA scheme provides stronger security strength than previous two types of schemes.

In 2013, Das and Goswami put forward a 3FA scheme for healthcare [21] which is stated to be able to withstand many kinds of attacks. However, Amin *et al.* [22] indicated that Das et al.'s scheme is susceptible to offline password guessing attacks, smart card stolen attacks, server/user impersonation attacks, and doesn't provide session key privacy and user anonymity. To address flaws in [21], they introduced an anonymity preserving 3FA scheme. Though this scheme [22] is designed elaborately, Li *et al.* [24] pointed out Amin et al.'s scheme lacks the step of verifying passwords of users, which may cause denial of service (DoS) attacks when the user changes his/her password incautiously.

Since there are a large amount of data generated in e-healthcare, clouds are introduced to deal with the high volume of data. Accordingly, in 2016, Jiang *et al.* [23] came up with a privacy preserving 3FA scheme for electronic health (e-health) clouds, and the concept of fuzzy extractor is adopted to preserve the biometrics privacy. In 2015 Mir and Nikooghadam [25] proposed a 3FA protocol for Telecare Medicine Information System (TMIS) which uses lightweight operations and is claimed to be secure. However, in 2018, Chaudhry *et al.* [26] pointed Mir et al.'s scheme cannot resist smart card stolen attacks and anonymity violation attacks, and came up with an enhanced one. Ruhul *et al.* [27] presented a mutual authentication protocol in a single server scenario, and proved their scheme is immune to active and passive attacks. But later, Irshad *et al.* [28] revealed [27] has several security weaknesses which cannot counteract user phishing attacks and server masquerade attacks.

Most recently, Zhang *et al.* [29] presented a 3FA scheme for protecting the privacy of e-health system. They use the dynamic identity (ID) to achieve user untraceability and adopt 3FA to against adversaries. Nonetheless, after careful analysis, we found their scheme has several weaknesses.

B. OUR CONTRIBUTIONS

The above analyses indicate that designing a 3FA solution for MMIS that can withstand various known attacks while satisfying desired security attributes remains a huge challenge. In this paper, we present an enhanced 3FA scheme for MMIS. The following contributions are made in this paper.

- First, we review the 3FA scheme of Zhang *et al.* [29] and demonstrate its security flaws. To be specific, we find that the user's password can be guessed by an adversary via offline exhaustive enumeration if the adversary gets the sensitive information in the smart card and eavesdrops all messages transmitted in public channel. Additionally, the protocol suffers from DoS attacks if an adversary logs in to the device with a victim's information intercepted from the public channel. Besides, no local validation is provided in their scheme, so the scheme does not achieve efficiency and user friendliness.
- Second, we come up with an efficient and secure scheme which contains five phases for MMIS. The improved dynamic verification table and fuzzy verifier are adopted in the proposed scheme to prevent illegal access to the MMIS. The enhanced scheme is based on Rabin cryptosystem whose computation cost of encryption and decryption is asymmetric.
- Third, we present a formal verification by the automatic tool ProVerif and show that the proposed protocol is immune to multiple attacks including offline password attacks and DoS attacks which exist in Zhang et al.'s protocol. After that, we also analytically state that the proposed protocol can fulfill the expected security attributes. Additionally, efficiency analysis manifests that our improved protocol is a practical and efficient solution for MMIS.

The rest of this paper is organized as follows. Section II gives the basics of Biohash and Rabin cryptosystem. In Section III, we review Zhang et al.'s 3FA protocol [29] and discuss the security of it in Section IV. Section V introduces a novel 3FA protocol with dynamic verification for MMIS. In Section VI, both formal and informal verification are given. Section VII presents efficiency analysis of our protocol. In Section VIII, we conclude the paper.

II. PRELIMINARY

A. BIOHASH

As mentioned earlier, the factors in the 3FA protocol refer to passwords, smart cards, and biometrics. Biometric information has many advantages such as: uniqueness, portability. Besides, it is difficult to forge and guess correctly. So it can be used in authentication protocols. Many methods have been put forward constantly to protect the privacy of biometric data [33]–[36].

The basic idea of biohash is to convert the original biometrics into feature vectors, and then iterate the inner product to transform the feature vectors into a set of pseudo-random numbers stored in the user identity token. The result is binarized by selecting a threshold to obtain a set of binary sequences corresponding to a particular user. In the authentication phase, the legitimacy of the user is confirmed by comparing the binary sequences.

In this paper, biohash [36], [37] is adopted to protect the biometric privacy. At registration stage, the biohash $h_{Bio}(\cdot)$ takes a random secret key K and biometric template T imprinted by user as parameters to generate specific pseudo random coding $h_{Bio}(K \oplus T)$ for this user. Later the random result is transmitted to server rather than the single T to prevent server from obtaining the exact value about user's biometric information.

By mixing random numbers and user's biometric data (features vectors), biohash protects the privacy of user's biometric data via a very simple way. Because the user's biometric data and identity token cannot be obtained, the adversary has no way to get the specific user's binary sequence, biohash can be considered secure [36].

B. RABIN CRYPTOSYSTEM

The Rabin cryptosystem [38], [39] is based on the hard problem of large integer decomposition which is characterized by the fact that the same ciphertext may correspond to two or more plaintexts. It is mainly composed of key generation algorithm, encryption and decryption algorithms.

Key Generation: We select two large distinct primes p, q which satisfy $p \equiv q \equiv 3 \bmod 4$, and then compute $n = p \times q$. Then we keep n as the public key, and p, q as the private key.

TABLE 1. Notations.

Notation	Description
U_i	A user
S	The medical multimedia server
ID_i, PW_i	The identity and password of U_i
T_i, B_i	The biometric template and sample of U_i
s	The master key of S
SC	The smart card
ID_{SC}	The identifier of U_i 's smart card
r_x	The high-entropy random integer involved in this protocol
C_j	The j th message transmitted in this protocol
$h(\cdot)$	The one-way hash function
$h_{Bio}(\cdot)$	The secure biohash function
$E_k(\cdot)$	The symmetric encryption function with key k
$D_k(\cdot)$	The symmetric decryption function with key k
Δ	The matching algorithm
$\|\|$	The concatenation operation
$\oplus$	The exclusive-or operation

Encryption: The ciphertext c is produced by computing $c = m^2 \bmod n$ where m is the plaintext.

Decryption: To decrypt the ciphertext c, we should solve the equation $x^2 \equiv c \bmod n$ which is equivalent to

$$\begin{cases} x^2 \equiv c \bmod p \\ x^2 \equiv c \bmod q \end{cases}$$

If the equation $x^2 \equiv y \bmod n$ has a root x, then y is a quadratic residue mod n. The quadratic residue problem can be defined as: let QR_n be the set of all quadratic residues mod n, given $y \in QR_n$, it is computationally infeasible to find x without knowing p and q due to the hardness of factoring n [40].

With the knowledge of the private key p, q, four possible plaintexts $\{m_1, m_2, m_3, m_4\}$ with the Chinese remainder theorem can be derived. In order to determine the correct plaintext, additional information can be added to the plaintext, such as the identity of sender or recipient, date, and time.

III. REVIEW OF ZHANG ET AL.'S PROTOCOL

Now, we simply review Zhang et al.'s 3FA scheme [29]. It contains three phases which are registration phase, login phase and authentication phase. For ease of understanding, notations we used in this paper is similar to those in Zhang et al.'s protocol which are listed in Table 1.

A. REGISTRATION PHASE

A new user U_i needs to carry out the following steps to register with the medical server S to be a legal user.

Step R1: U_i chooses his/her own identity ID_i, password PW_i and imprints biometric template T_i into the terminal device, and then the terminal device computes $C_1 = h(ID_i||PW_i||h_{Bio}(T_i))$ and $C_2 = T_i \oplus r_1$. Finally, the device sends $\{C_1, C_2\}$ to the medical multimedia server S.

Step R2: S computes $M = h(h_{Bio}(C_2||s))$ with its master key s. Then, S selects a random integer r_2 and computes $W = h(h_{Bio}(C_2 \oplus r_2))$, $X = h(ID_{SC}||C_1||M)$ and $Y = M \oplus C_1$. Next, S writes $\{ID_{SC}, h(\cdot), h_{Bio}(\cdot), X, Y\}$ into a SC and distributes it to U_i. Finally, S stores the item $\{C_2, W_0, W\}$ into its database where W_0 is NULL.

Step R3: U_i writes $Z = r_1 \oplus h_{Bio}(T_i)$ into SC.

B. LOGIN PHASE

If U_i intends to get information or related service from S, U_i needs to execute following operations.

Step L1: U_i should insert SC into the terminal device, and inputs identity ID_i, password PW_i, and imprints the biometric data B_i.

Step L2: SC computes $C_1^* = h(ID_i||PW_i||h_{Bio}(B_i))$, $M^* = Y \oplus C_1^*$, $r_2^* = X \oplus h(ID_{SC}||C_1^*||M^*)$ and $r_1^* = Z \oplus h_{Bio}(B_i)$ using the secrets kept in it.

Step L3: SC computes $C_3 = h_{Bio}(B_i \oplus r_1^* \oplus r_2^*)$, $C_4 = B_i \oplus r_1^* \oplus h(M^*||r_3)$, and $C_5 = r_3 \oplus h_{Bio}(B_i \oplus r_1^*)$ then sends $\{C_3, C_4, C_5\}$ to the MMIS server S.

C. AUTHENTICATION PHASE

After U_i implements the login phase, S receives the login request and conducts following steps to authenticate the U_i and negotiates a shared session key with U_i.

Step A1: S calculates $W^* = h(C_3)$ and seeks W^* in the dynamic verification table to obtain the corresponding C_2.

Step A2: S computes $M' = h(h_{Bio}(C_2)||s)$, $r_3^* = C_5 \oplus h_{Bio}(C_2)$, $B_i \oplus r_1^* = C_4 \oplus h(M'||r_3^*)$. Then it examines if $\Delta(B_i \oplus r_1^*, C_2) \leq \tau$. If it holds, S computes $C_6 = r_4 \oplus h(B_i \oplus r_1^*)$, $C_7 = h((B_i \oplus r_1^*)||r_3^*||r_4)$ and sends $\{C_6, C_7\}$ to U_i, else, S terminates the session immediately.

Step A3: U_i computes $r_4^* = C_6 \oplus h(B_i \oplus r_1^*)$, and checks if $C_7 ?= h(h(B_i \oplus r_1^*)||r_3||r_4^*)$. If it holds, U_i computes the shared session key $SK = h(M'||r_3^*||r_4)$, $X_{new} = h(ID_{SC}||C_1^*||M^*) \oplus r_4^*$ and $C_8 = h(h_{Bio}(B_i \oplus r_1^* \oplus r_4^*) \oplus r_4^*)$. Then, U_i sends $\{C_8\}$ to S.

Step A4: S checks if $C_8 ?= h(h_{Bio}(B_i \oplus r_1^* \oplus r_4) \oplus r_4)$. If it holds, S admits the common session key $SK = h(M'||r_3^*||r_4)$, and calculates $W_{new} = h(h_{Bio}(C_2 \oplus r_4))$, $C_9 = h(SK||r_4)$. Then, S replaces (W_0, W) with (W, W_{new}). Finally, S sends $\{C_9\}$ to U_i.

Step A5: U_i checks $C_9 ?= h(SK||r_4^*)$. If it holds, U_i accepts SK and replaces X with X_{new}.

IV. WEAKNESSES OF THE PROTOCOL BY ZHANG ET AL.

This scheme is claimed to be not affected by man-in-the-middle attacks, offline password guessing attacks, de-synchronization attacks, and stolen verifier attacks, insider attacks as well as guaranteeing known key security, perfect forward secrecy, biometric protection and user anonymity including the untraceability. However, we observe that their scheme has some vulnerabilities.

Before demonstrating the Zhang et al.'s protocol's cryptanalysis, we first show the adversarial model [40].

1) The adversary A has the capability to offline enumerate the Cartesian product $D_{id} \times D_{pw}$ where D_{id}, D_{pw} represent the space of ID and PW respectively.
2) A can get one or two of three factors which are the sensitive data in the smart card, the legal user's password, and the biometric data of the legal user. But not all of them at the same time.
3) A can eavesdrop, block, intercept, modify, replay, and falsify all messages on the public channel.

A. OFFLINE PASSWORD GUESSING ATTACKS

Normally, it is thoughtful to have consideration for that the adversary A can obtain two of the three factors and then attacks the scheme when analyzing the security of a 3FA protocol. So, treating user's biometrics information as a known value is more feasible, and the adversary has got the victim's SC somehow and retrieves the secret data in card by side-channel attacks. Through the above hypotheses, after careful analysis, we found that the adversary can launch offline password guessing attacks through the following steps:

First, A computes $r_1' = Z \oplus h_{Bio}(B_i') = r_1 \oplus h_{Bio}(T_i) \oplus h_{Bio}(B_i')$ with the obtained biometric data B_i'.

Then, A computes $r_2' = X \oplus h(ID_{SC}||C_1'||M') = X \oplus h(ID_{SC}||h(ID_i'||PW_i'||h_{Bio}(B_i'))||(Y \oplus C_1'))$.

Next, A computes $C_3' = h_{Bio}(B_i' \oplus r_1' \oplus r_2') = h_{Bio}(B_i' = \oplus(Z \oplus h_{Bio}(B_i')) \oplus (X \oplus h(ID_{SC}||h(ID_i'||PW_i'||h_{Bio}(B_i'))||(Y \oplus h(IDsc||h(ID_i'||PW_i'||h_{Bio}(B_i')))$ where $\{ID_{SC}, X, Y, Z\}$ are retrieved from SC.

According to the above calculation, if B_i' and T_i are close enough, $r_1' = r_1 = r_1^*$. Then, $r_2' = r_2 = r_2^*$. Thus, A can guess ID_i', PW_i' by comparing $C_3'? = C_3$, where C_3 is intercepted from public channel.

B. DENIAL OF SERVICE ATTACKS

Zhang et al. proclaimed that their scheme can defend a lot of attacks, but we have discovered that after the user's authentication phase is completed, if the adversary sends the old message which intercepted during login phase of victim's, it will mislead the server to refuse service for the legal user when this user logs in with updated information. Since after this attempt of A, the server cannot find the corresponding fresh item in its dynamic verification table when the victim logs in next time. The details are as follows:

After completing the hole login-authentication phase, $X_{new} = h(ID_{SC}||C_1||M) \oplus r_4$, the user replaces X with X_{new}, the server updates its dynamic verification table simultaneously as shown in Table 2.

When the user logs in again, $r_2^* = X \oplus h(ID_{SC}||C_1||M) = r_4$, so $C_3 = h_{Bio}(B_i \oplus r_1 \oplus r_2^*) = h_{Bio}(B_i \oplus r_1 \oplus r_4)$, S can find $W^* = h(h_{Bio}(B_i \oplus r_1 \oplus r_4))$ in column W of Table 2. But when A uses the messages $\{C_3, C_4, C_5\}$ intercepted during the victim's last login to impersonate the victim, where $C_3 = h_{Bio}(B_i \oplus r_1 \oplus r_2^*) = h_{Bio}(B_i \oplus r_1 \oplus r_2)$, S can find $W^* = h(h_{Bio}(B_i \oplus r_1 \oplus r_2))$ in column W_0 of Table 2, and then S sets $W = W_0$ according to the update rules of Zhang et al.'s protocol. The updated dynamic verification table is shown in Table 3.

TABLE 2. The server's database after the authentication.

C_2	W_0	W
$T_i \oplus r_1$	$h(h_{Bio}(T_i \oplus r_1 \oplus r_2))$	$h(h_{Bio}(T_i \oplus r_1 \oplus r_4))$

TABLE 3. The server's database after the attack.

C_2	W_0	W
$T_i \oplus r_1$	$h(h_{Bio}(T_i \oplus r_1 \oplus r_2))$	$h(h_{Bio}(T_i \oplus r_1 \oplus r_2))$

Thus, when the victim wants to login again, S cannot find the entry according the receiving message $C_3 = h_{Bio}(B_i \oplus r_1 \oplus r_2^*) = h_{Bio}(B_i \oplus r_1 \oplus r_4)$. So, S confirms this user illegal and terminates this session. In a word, Zhang et al.'s scheme cannot resist DoS attacks.

C. NO LOCAL VERIFICATION

In Zhang et al.'s protocol, since SC doesn't verify the information which user input, it's not effcient or user friendliness. Regardless of whether the password entered by the user is correct, SC will send it to server without consideration to let the server perform the calculation and then determination about whether the password is legitimate or not is performed by S. This will definitely cause useless calculation of S and add the S's burden.

V. THE PROPOSED AUTHENTICATION PROTOCOL

We enhance Zhang et al.'s protocol from the following aspects:

(1) The public key primitive Rabin cryptosystem and the fuzzy verifier are introduced to avoid offline password guessing attacks;
(2) The dynamic verification table is improved and simplified to avoid DoS attacks and de-synchronization attacks;
(3) The password change phase and biometric change phase are added to complete the protocol.

Therefore, the proposed protocol contains five phases: registration phase, login phase, authentication phase, password change phase and biometric change phase.

A. REGISTRATION PHASE

U_i performs following steps with the medical server S to be a legitimate member of MMIS, as shown in Figure 2.

Step R1: U_i chooses the identity ID_i, password PW_i, and imprints his/her biometric data T_i into the terminal device as a biometric template. Then the terminal device computes $C_1 = h(ID_i||PW_i||h_{Bio}(T_i))$, $C_2 = T_i \oplus r_1$ with a high-entropy

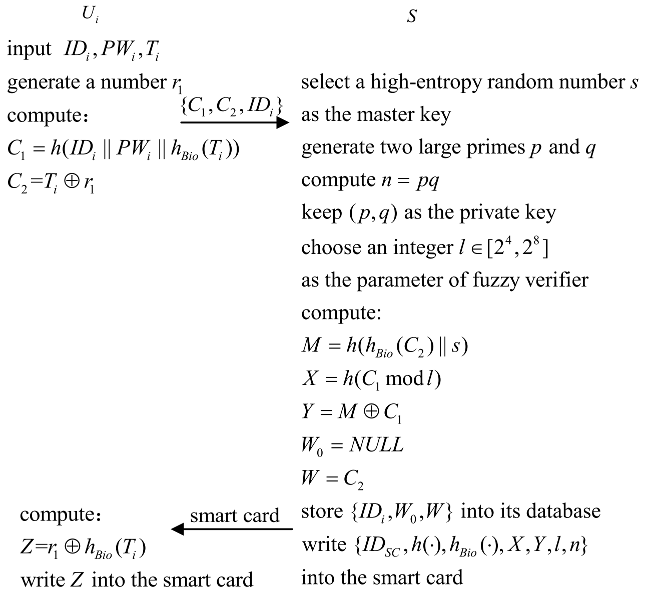

U_i
S
input ID_i, PW_i, T_i
generate a number r_1
compute:
$C_1 = h(ID_i \| PW_i \| h_{Bio}(T_i))$
$C_2 = T_i \oplus r_1$
$\{C_1, C_2, ID_i\}$
select a high-entropy random number s
as the master key
generate two large primes p and q
compute $n = pq$
keep (p, q) as the private key
choose an integer $l \in [2^4, 2^8]$
as the parameter of fuzzy verifier
compute:
$M = h(h_{Bio}(C_2) \| s)$
$X = h(C_1 \bmod l)$
$Y = M \oplus C_1$
$W_0 = NULL$
$W = C_2$
store $\{ID_i, W_0, W\}$ into its database
write $\{ID_{SC}, h(\cdot), h_{Bio}(\cdot), X, Y, l, n\}$
into the smart card
smart card
compute:
$Z = r_1 \oplus h_{Bio}(T_i)$
write Z into the smart card

FIGURE 2. Registration phase of the proposed protocol.

random number r_1. Finally, the device sends $\{C_1, C_2, ID_i\}$ to S through the secure channel.

Step R2: After receiving the message from U_i, S selects a high-entropy random number s as its master key, and produces two large primes p and q to compute $n = pq$. S takes (p, q) as the private key and selects an integer $l \in [2^4, 2^8]$ as the parameter of fuzzy verifier. Then, S computes $M = h(h_{Bio}(C_2||s))$, $X = h(C_1 \bmod l)$, $Y = M \oplus C_1$, $W = C_2$, and writes $\{ID_{SC}, h(\cdot), h_{Bio}(\cdot), X, Y, l, n\}$ into SC and delivers it to U_i. Finally, S stores $\{ID_i, W_0, W\}$ into the dynamic verification table where $W_0 = NULL$.

Step R3: U_i writes $Z = r_1 \oplus h_{Bio}(T_i)$ into SC after receiving SC.

B. LOGIN PHASE

If the user U_i wants to learn something from MMIS, he/she needs to execute the steps described below to forward a login request to the medical server S, as shown in Figure 3.

Step L1: U_i inserts SC into the terminal device and inputs his/her identity ID_i, password PW_i, and imprints his/her biometric information B_i.

Step L2: SC picks a random number r_2, computes $C_1^* = h(ID_i||PW_i||h_{Bio}(B_i))$ with the information in it, and checks $X^*(= h(C_1^* \bmod l))? = X$. If these two values are equal, SC computes $r_1^* = Z \oplus h_{Bio}(B_i)$, $C_3 = (ID_i||r_2||B_i \oplus r_1^*)^2 \bmod n$. Finally, SC sends $\{C_3\}$ to S through a public channel.

C. AUTHENTICATION PHASE

After getting the login request from U_i, S implements following steps to complete the mutual authentication with user U_i, as shown in Figure 3.

Step A1: S decrypts C_3 to obtain ID_i^*, r_2^* and $B_i^* \oplus r_1^*$. Then, S searches $\{W_0, W\}$ in the verification table according to the ID_i^*. After that, S first judges whether $\Delta(B_i^* \oplus r_1^*, W) \le \tau$ holds. If it holds, S sets $W_0 = W$. If it is not, S checks whether $\Delta(B_i^* \oplus r_1^*, W_0)$ is within the predefined threshold τ. If it is not, S refuses to communicate with U_i. Otherwise, S produces a random number r_3 and computes $M' = h(h_{Bio}(B_i^* \oplus r_1^*)||s)$, $C_4 = r_3 \oplus h(B_i^* \oplus r_1^*)$, $C_5 = h((B_i^* \oplus r_1^*)||r_2^*||r_3)$ and $SK = h(M'||r_2^*||r_3)$. Finally, S sends $\{C_4, C_5\}$ to U_i.

Step A2: U_i computes $r_3^* = C_5 \oplus h(B_i \oplus r_1^*)$ after receiving the message $\{C_4, C_5\}$, and checks $C_5? = h((B_i \oplus r_1^*)||r_2||r_3^*)$. If it holds, U_i computes $SK = h(M^*||r_2||r_3^*)$. Thus, U_i

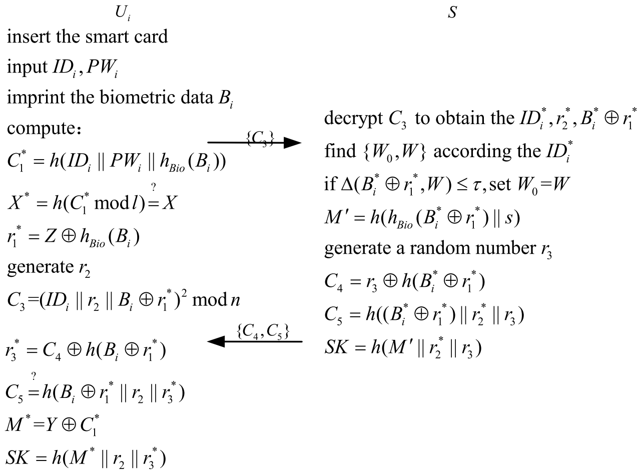

U_i
S
insert the smart card
input ID_i, PW_i
imprint the biometric data B_i
compute:
$C_1^* = h(ID_i \| PW_i \| h_{Bio}(B_i))$
$X^* = h(C_1^* \bmod l) \overset{?}{=} X$
$r_1^* = Z \oplus h_{Bio}(B_i)$
generate r_2
$C_3 = (ID_i \| r_2 \| B_i \oplus r_1^*)^2 \bmod n$
$\{C_3\}$
decrypt C_3 to obtain the $ID_i^*, r_2^*, B_i^* \oplus r_1^*$
find $\{W_0, W\}$ according the ID_i^*
if $\Delta(B_i^* \oplus r_1^*, W) \le \tau$, set $W_0 = W$
$M' = h(h_{Bio}(B_i^* \oplus r_1^*) \| s)$
generate a random number r_3
$C_4 = r_3 \oplus h(B_i^* \oplus r_1^*)$
$C_5 = h((B_i^* \oplus r_1^*) \| r_2^* \| r_3)$
$SK = h(M' \| r_2^* \| r_3)$
$\{C_4, C_5\}$
$r_3^* = C_4 \oplus h(B_i \oplus r_1^*)$
$C_5 \overset{?}{=} h(B_i \oplus r_1^* \| r_2 \| r_3^*)$
$M^* = Y \oplus C_1^*$
$SK = h(M^* \| r_2 \| r_3^*)$

FIGURE 3. Login phase and authentication phase of our protocol.

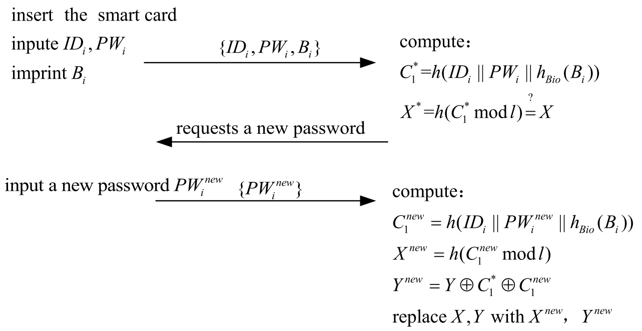

insert the smart card
inpute ID_i, PW_i
imprint B_i
$\{ID_i, PW_i, B_i\}$
compute:
$C_1^* = h(ID_i \| PW_i \| h_{Bio}(B_i))$
$X^* = h(C_1^* \bmod l) \overset{?}{=} X$
requests a new password
input a new password PW_i^{new}
$\{PW_i^{new}\}$
compute:
$C_1^{new} = h(ID_i \| PW_i^{new} \| h_{Bio}(B_i))$
$X^{new} = h(C_1^{new} \bmod l)$
$Y^{new} = Y \oplus C_1^* \oplus C_1^{new}$
replace X, Y with X^{new}, Y^{new}

FIGURE 4. Password change phase of our protocol.

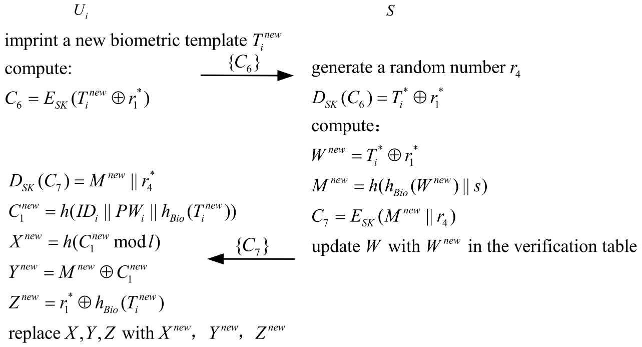
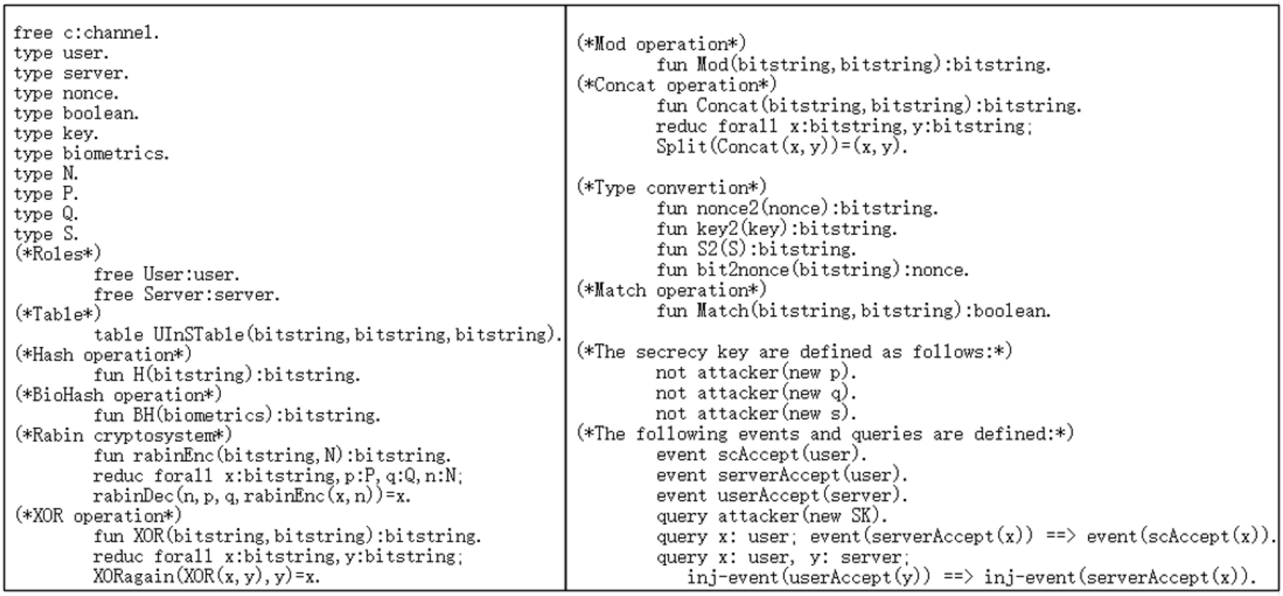

U_i
S
imprint a new biometric template T_i^{new}
compute:
$C_6 = E_{SK}(T_i^{new} \oplus r_1^*)$
$\{C_6\}$
generate a random number r_4
$D_{SK}(C_6) = T_i^* \oplus r_1^*$
compute:
$W^{new} = T_i^* \oplus r_1^*$
$M^{new} = h(h_{Bio}(W^{new}) \| s)$
$C_7 = E_{SK}(M^{new} \| r_4)$
update W with W^{new} in the verification table
$\{C_7\}$
$D_{SK}(C_7) = M^{new} \| r_4^*$
$C_1^{new} = h(ID_i \| PW_i \| h_{Bio}(T_i^{new}))$
$X^{new} = h(C_1^{new} \bmod l)$
$Y^{new} = M^{new} \oplus C_1^{new}$
$Z^{new} = r_1^* \oplus h_{Bio}(T_i^{new})$
replace X, Y, Z with X^{new}, Y^{new}, Z^{new}

FIGURE 5. Biometrics change phase of our protocol.



```
free c:channel.
type user.
type server.
type nonce.
type boolean.
type key.
type biometrics.
type N.
type P.
type Q.
type S.
(*Roles*)
        free User:user.
        free Server:server.
(*Table*)
        table UInSTable(bitstring,bitstring,bitstring).
(*Hash operation*)
        fun H(bitstring):bitstring.
(*BioHash operation*)
        fun BH(biometrics):bitstring.
(*Rabin cryptosystem*)
        fun rabinEnc(bitstring,N):bitstring.
        reduc forall x:bitstring,p:P,q:Q,n:N;
        rabinDec(n,p,q,rabinEnc(x,n))=x.
(*XOR operation*)
        fun XOR(bitstring,bitstring):bitstring.
        reduc forall x:bitstring,y:bitstring;
        XORagain(XOR(x,y),y)=x.
```

```
(*Mod operation*)
        fun Mod(bitstring,bitstring):bitstring.
(*Concat operation*)
        fun Concat(bitstring,bitstring):bitstring.
        reduc forall x:bitstring,y:bitstring;
        Split(Concat(x,y))=(x,y).

(*Type convertion*)
        fun nonce2(nonce):bitstring.
        fun key2(key):bitstring.
        fun S2(S):bitstring.
        fun bit2nonce(bitstring):nonce.
(*Match operation*)
        fun Match(bitstring,bitstring):boolean.

(*The secrecy key are defined as follows:*)
        not attacker(new p).
        not attacker(new q).
        not attacker(new s).
(*The following events and queries are defined:*)
        event scAccept(user).
        event serverAccept(user).
        event userAccept(server).
        query attacker(new SK).
        query x: user; event(serverAccept(x)) ==> event(scAccept(x)).
        query x: user, y: server;
           inj-event(userAccept(y)) ==> inj-event(serverAccept(x)).
```

FIGURE 6. Declarations.

and S have mutually authenticated and negotiated a common session key SK.

D. PASSWORD CHANGE PHASE

Zhang et al.'s protocol does not contain the password change phase, so their scheme cannot provide efficiency and user friendliness. Since in real life, if users' passwords are leaked somehow, they need to update their passwords to protect their privacy; otherwise, it will cause further loss to users. Thus, we introduce the local password change phase, see Figure 4.

Step P1: U_i inserts SC into the terminal device and inputs the ID_i, PW_i, and imprints B_i.

Step P2: SC computes $C_1^* = h(ID_i||PW_i||h_{Bio}(B_i))$, and checks whether $X^*(= h(C_1^* \bmod l))? = X$. If it holds, U_i picks a new password PW_i^{new} and sends it to SC. SC calculates $C_1^{new} = h(ID_i||PW_i^{new}||h_{Bio}(B_i))$, $X^{new} = h(C_1^{new} \bmod l)$, $Y^{new} = Y \oplus C_1^* \oplus C_1^{new}$ and replaces X, Y with X^{new}, Y^{new}.

E. BIOMETRIC CHANGE PHASE

During the change of biometrics phase, the user has to interact with MMS in the public channel. Since the server has to calculate a new value M and sends it to the user for user's subsequent calculations. Meanwhile, S has to update the dynamic verification table in its database. Therefore, in order to ensure the transmitted data's security, symmetric encryption is introduced to protect the transmitted data. The detailed biometrics change phase is shown in Figure 5.

After a successful mutual authentication between the user U_i and the medical multimedia server S. U_i and S negotiate a shared session key $SK = h(M^*||r_2||r_3^*) = h(M'||r_2^*||r_3)$. Now we can use a symmetric encryption/decryption with this key.

Step B1: U_i imprints a new biometric template T_i^{new}, and computes $C_6 = E_{SK}(T_i^{new} \oplus r_1^*)$ where r_1^* is generated in early stage. Finally, U_i transmits message $\{C_6\}$ to S.

Step B2: After obtaining $\{C_6\}$, S decrypts C_6 with SK to obtain some useful information. Next, S computes $M^{new} = h(h_{Bio}(T_i^* \oplus r_1^*)||s)$ with master key s and sets $W^{new} = T_i^* \oplus r_1^*$. Then, S selects a number r_4 and sends $C_7 = E_{SK}(M^{new}||r_4)$ to U_i. At last, S updates the verification table by setting $W = W^{new}$.

Step B3: U_i decrypts C_7 with SK, then computes $C_1^{new} = h(ID_i||PW_i||h_{Bio}(T_i^{new}))$, $X^{new} = h(C_1^{new} \bmod l)$, $Y^{new} = M^{new} \oplus C_1^{new}$ and $Z^{new} = r_1^* \oplus h_{Bio}(T_i^{new})$, replaces X, Y, Z with X^{new}, Y^{new}, Z^{new}.

VI. SECURITY ANALYSIS

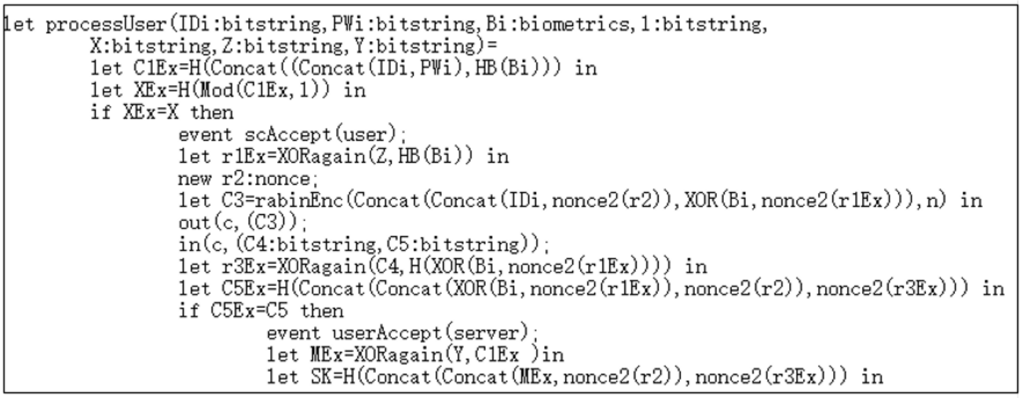
This section depicts the security of our enhanced scheme. We use an automated tool ProVerif which has a large number of built-in encryption, decryption algorithms and some functions to prove the security properties of the proposed scheme and informal analysis is presented later.

A. FORMAL VERIFICATION WITH PROVERIF

ProVerif [41] is a widely used validation tool to verify the protocol and its input language is a variant of pi calculus. A protocol's ProVerif model consists of three parts: declarations, process macros and a main process.

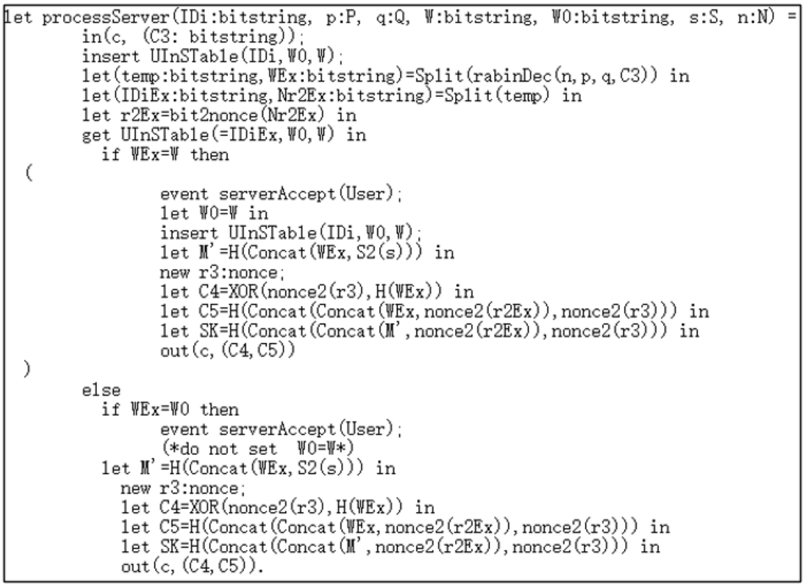
The declaration is shown in Figure 6. The channel which used for communication between user and server is modeled by c. The UInSTable indicates the server's verification table which stores the users' identities and encrypted biometrics.

Next, we model the user process processUser and the server process processServer as two parties to complete the interaction in our protocol. Specifically, the processUser is



```
let processUser(IDi:bitstring,PWi:bitstring,Bi:biometrics,l:bitstring,
        X:bitstring,Z:bitstring,Y:bitstring)=
        let C1Ex=H(Concat((Concat(IDi,PWi),HB(Bi))) in
        let XEx=H(Mod(C1Ex,l)) in
        if XEx=X then
                event scAccept(user);
                let r1Ex=XORagain(Z,HB(Bi)) in
                new r2:nonce;
                let C3=rabinEnc(Concat(Concat(IDi,nonce2(r2)),XOR(Bi,nonce2(r1Ex))),n) in
                out(c, (C3));
                in(c, (C4:bitstring,C5:bitstring));
                let r3Ex=XORagain(C4,H(XOR(Bi,nonce2(r1Ex)))) in
                let C5Ex=H(Concat(Concat(XOR(Bi,nonce2(r1Ex)),nonce2(r2)),nonce2(r3Ex))) in
                if C5Ex=C5 then
                        event userAccept(server);
                        let MEx=XORagain(Y,C1Ex )in
                        let SK=H(Concat(Concat(MEx,nonce2(r2)),nonce2(r3Ex))) in
```

FIGURE 7. The process of user.



```
let processServer(IDi:bitstring, p:P, q:Q, W:bitstring, W0:bitstring, s:S, n:N) =
        in(c, (C3: bitstring));
        insert UInSTable(IDi,W0,W);
        let(temp:bitstring,WEx:bitstring)=Split(rabinDec(n,p,q,C3)) in
        let(IDiEx:bitstring,Nr2Ex:bitstring)=Split(temp) in
        let r2Ex=bit2nonce(Nr2Ex) in
        get UInSTable(=IDiEx,W0,W) in
          if WEx=W then
  (
                event serverAccept(User);
                let W0=W in
                insert UInSTable(IDi,W0,W);
                let M'=H(Concat(WEx,S2(s))) in
                new r3:nonce;
                let C4=XOR(nonce2(r3),H(WEx)) in
                let C5=H(Concat(Concat(WEx,nonce2(r2Ex)),nonce2(r3))) in
                let SK=H(Concat(Concat(M',nonce2(r2Ex)),nonce2(r3))) in
                out(c, (C4,C5))
  )
        else
          if WEx=W0 then
                event serverAccept(User);
                (*do not set  W0=W*)
          let M'=H(Concat(WEx,S2(s))) in
            new r3:nonce;
            let C4=XOR(nonce2(r3),H(WEx)) in
            let C5=H(Concat(Concat(WEx,nonce2(r2Ex)),nonce2(r3))) in
            let SK=H(Concat(Concat(M',nonce2(r2Ex)),nonce2(r3))) in
            out(c, (C4,C5)).
```

FIGURE 8. The process of server.

modeled as shown in Figure 7. The process of processServer is modeled as shown in Figure 8. The main process is modeled as shown in Figure 9. The user's identity, password and biometrics are denoted by IDi, PWi and Bi, respectively. SK indicates the secret key negotiated between user and server and s is the master key for server.

The verification result is shown in Figure 10.

The above result indicates that our scheme can achieve the shared secret key secrecy and mutual authentication.

B. ANALYSIS OF SECURITY PROPERTIES

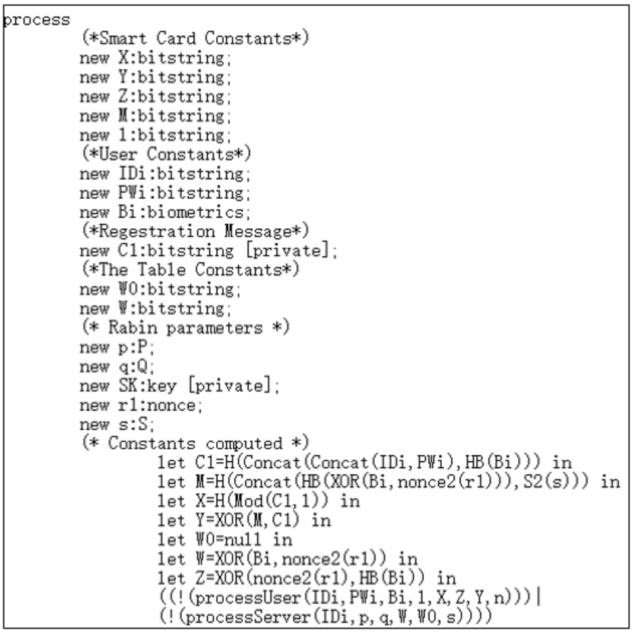
1) RESISTING OFFLINE PASSWORD GUESSING ATTACKS

Suppose an adversary A has intercepted all the messages $\{C_3, C_4, C_5\}$ in public channel and then he/she launches an offline password guessing attack. A will fail, since none of the messages intercepted from public channel contains the user's password PW_i.

Then we further allow A to hold SC and extract the secret data $\{ID_{SC}, h(\cdot), h_{Bio}(\cdot), X, Y, Z, l, n\}$ from SC by side-channel attacks or other ways, and A also owns the user's biometric data B_i. Only the message $C_1 = h(ID_i||PW_i||h_{Bio}(B_i))$ contains the password, A can only obtain C_1 by $X = h(C_1 \bmod l)$. Because of the fuzzy verifier l and the one-way hash function $h(\cdot)$, A cannot get the exact value of C_1. So, A cannot determine whether the guessed PW_i is right. Hence, A cannot perform offline password guessing attacks even he/she gets SC, the biometric data and all messages.

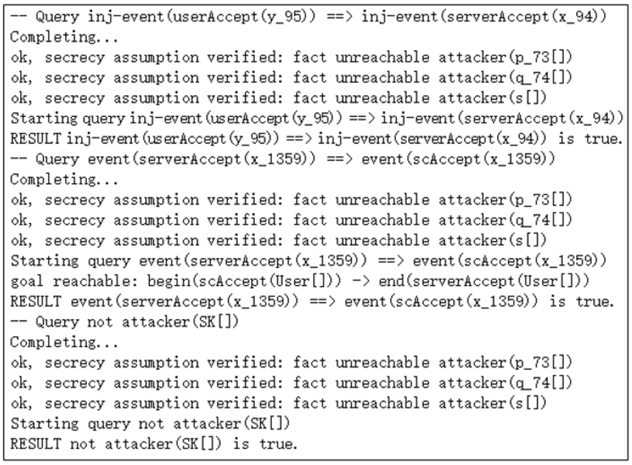
2) RESISTING DOS ATTACKS

In our protocol, the rules updating for dynamic verification table are improved as follows: if S finds the item in column W, then sets $W_0 = W$, and if it in column W_0, S doesn't change anything in the table. These rules are completely opposite to Zhang et al.'s rules. As previously analyzed, if A launches an attack with old messages, S will find the



```
process
        (*Smart Card Constants*)
        new X:bitstring;
        new Y:bitstring;
        new Z:bitstring;
        new M:bitstring;
        new l:bitstring;
        (*User Constants*)
        new IDi:bitstring;
        new PWi:bitstring;
        new Bi:biometrics;
        (*Regestration Message*)
        new C1:bitstring [private];
        (*The Table Constants*)
        new W0:bitstring;
        new W:bitstring;
        (* Rabin parameters *)
        new p:P;
        new q:Q;
        new SK:key [private];
        new r1:nonce;
        new s:S;
        (* Constants computed *)
                let C1=H(Concat(Concat(IDi,PWi),HB(Bi))) in
                let M=H(Concat(HB(XOR(Bi,nonce2(r1))),S2(s))) in
                let X=H(Mod(C1,l)) in
                let Y=XOR(M,C1) in
                let W0=null in
                let W=XOR(Bi,nonce2(r1)) in
                let Z=XOR(nonce2(r1),HB(Bi)) in
                ((!(processUser(IDi,PWi,Bi,l,X,Z,Y,n)))|
                (!(processServer(IDi,p,q,W,W0,s))))
```

FIGURE 9. The main process.



```
-- Query inj-event(userAccept(y_95)) ==> inj-event(serverAccept(x_94))
Completing...
ok, secrecy assumption verified: fact unreachable attacker(p_73[])
ok, secrecy assumption verified: fact unreachable attacker(q_74[])
ok, secrecy assumption verified: fact unreachable attacker(s[])
Starting query inj-event(userAccept(y_95)) ==> inj-event(serverAccept(x_94))
RESULT inj-event(userAccept(y_95)) ==> inj-event(serverAccept(x_94)) is true.
-- Query event(serverAccept(x_1359)) ==> event(scAccept(x_1359))
Completing...
ok, secrecy assumption verified: fact unreachable attacker(p_73[])
ok, secrecy assumption verified: fact unreachable attacker(q_74[])
ok, secrecy assumption verified: fact unreachable attacker(s[])
Starting query event(serverAccept(x_1359)) ==> event(scAccept(x_1359))
goal reachable: begin(scAccept(User[])) -> end(serverAccept(User[]))
RESULT event(serverAccept(x_1359)) ==> event(scAccept(x_1359)) is true.
-- Query not attacker(SK[])
Completing...
ok, secrecy assumption verified: fact unreachable attacker(p_73[])
ok, secrecy assumption verified: fact unreachable attacker(q_74[])
ok, secrecy assumption verified: fact unreachable attacker(s[])
Starting query not attacker(SK[])
RESULT not attacker(SK[]) is true.
```

FIGURE 10. The result of verification.

corresponding item in column W_0 with updating nothing. So, when the legal user logs in with new parameters later, S can find the item in column W without any doubt and then sets $W_0 = W$. So, whenever the legitimate user wants to log in to the system, he/she can be verified by the MMIS server successfully as long as he/she inputs the correct information. If A logs in with old messages after this stage, S cannot find the corresponding item and will refuse to communicate with this user (A). Thus, our protocol is immune to DoS attacks and implements access control.

3) RESISTING USER IMPERSONATION ATTACKS

The adversary A is unable to impersonate as a legal user to negotiate a session key with the medical server in our scheme.

To impersonate as the user U_i, A needs to calculate the right value of $\{C_3\}$. Assume A intercepts message $\{C_3\}$ sent by U_i in public channel before. If A counterfeits the user by replaying the intercepted login message, the medical server S can search an ID_i and then computes $\{C_4, C_5\}$. However, after getting the message from S, A cannot generate a valid session key SK. Since A is unable to get or guess the correct high-entropy random numbers r_2 and r_3 which are unique in each session.

Considering another situation: A counterfeits the user by modifying the intercepted login message. Then he/she cannot pass the S's verification since S cannot find W_0 or W according the forged ID_i decrypted from modified C_3. Hence, the improved protocol can counteract user impersonation attacks.

4) RESISTING SERVER IMPERSONATION ATTACKS

Assume that A impersonates the medical multimedia server S to pass the user's verification and then tries to negotiate a session key with this user. After gaining the login message from user, A needs to decrypt C_3 to obtain the user's identity ID_i. He/she will fail to get the right one without other useful information since the hard problem of large integer decomposition. Similarly, he cannot get r_2^* and $B_i^* \oplus r_1^*$, either. So, A is unable to pass the user's verification successfully.

5) RESISTING STOLEN SMART CARD ATTACKS

Assume the adversary A somehow catches SC and extracts the pivotal information in SC by side-channel attacks. If A wants to negotiate a session key $SK = h(M||r_2||r_3)$ with the user, he/she has to get M first. Then, A should obtain C_1 to compute $C_1 \oplus Y = C_1 \oplus M \oplus C_1 = M$. However, only $X = h(C_1 \bmod l)$ contains the message C_1, and C_1 is protected by fuzzy verifier in X. It's almost impossible for A to obtain C_1 with X, l. Even A gets the correct C_1, computing a right session key SK for A is also impossible, since both r_2 and r_3 are high-entropy random numbers. So, the proposed protocol can withstand stolen smart card attacks.

6) RESISTING MODIFICATION ATTACKS

In the improved protocol, no adversary A can successfully be authenticated by server after distorting any message transmitted between the user U_i and the medical server S. Suppose an adversary A intercepts all these messages of the login and authentication phase $\{C_3, C_4, C_5\}$.

In login phase, if A modifies $C_3 = (ID_i||r_2||B_i \oplus r_1^*)^2$ mod n to $C_3' = (ID_i'||r_2'||B_i' \oplus r_1')^2$ mod n and sends it to medical server S. S decrypts C_3' to obtain ID_i' and searches $\{W_0, W\}$ in the verification table. Since $ID_i' \neq ID_i$, S cannot find any item according to ID_i'. Then, S will terminate the current session. If the ID_i' which A modified is equal to ID_i coincidentally, S can find $\{W_0, W\}$. However, the comparison of $B_i' \oplus r_1'$ and W or W_0 will exceed the predefined threshold definitely. Since r_1^* is a high-entropy random number, A can hardly guess a right one. S will terminate the current session immediately.

As for authentication phase, assume A replaces C_4, C_5 with C_4', C_5' and sends them to U_i. U_i computes r_3' with C_4', then

TABLE 4. The dynamic verification table after updating.

ID	W_0	W
ID_i	$T_i \oplus r_1$	$T_i^{new} \oplus r_1$

compares C_5' to $h((B_i \oplus r_1^*)||r_2||r_3')$. It is difficult to equal because of r_2. As a result, the adversary cannot launch the modification attacks successfully.

7) RESISTING REPLAY ATTACKS

Suppose A tries to lunch replay attacks with messages he/she intercepted from previous sessions between the user U_i and the server S. He/she will fail. The reason for this resembles the analysis of impersonation attacks. Since A cannot negotiate a correct session key SK with the medical multimedia server S even he/she can pass the verification of the S. What's more, A cannot generate a key SK with U_i by replaying old message sent by S, either. So, the proposed protocol can resist replay attacks.

8) RESISTING DE-SYNCHRONIZATION ATTACKS

In the proposed protocol, the existence of the dynamic verification table mechanism can resist de-synchronization attacks. The details are as follows:

The server has updated the data in the dynamic verification table after authentication phase as shown in Table 4. However, the user does not update the relevant data in SC since the message C_7 does not be transmitted to the user successfully due to network delay or other issues. Thus, the user has to log in with the old data ($T_i \oplus r_1$). In our dynamic verification table, the old data is stored in the column W_0, so S can find item in it, and U_i can pass the verification.

9) MUTUAL AUTHENTICATION

In authentication phase, S authenticates U_i by verifying whether $\Delta(B_i^* \oplus r_1^*, W) \leq \tau$ or $\Delta(B_i^* \oplus r_1^*, W_0) \leq \tau$. Then, U_i authenticates S by verifying the correctness of $C_5 = h((B_i \oplus r_1^*)||r_2||r_3^*)$. Thus, mutual authentication is achieved in our improved protocol between S and U_i.

10) SESSION KEY AGREEMENT

At the end of authentication phase, the medical server S and the user U_i negotiate a secret session key $SK = h(M'||r_2^*||r_3) = h(M^*||r_2||r_3^*)$ for the subsequent session after the mutual authentication. It is worth noting that the randomness of numbers involved in the protocol and the secrecy of the S's master key s determinate the secrecy of the session key. Hence, session key agreement is provided in our protocol and it is secure enough.

11) USER ANONYMITY

As mentioned earlier, privacy is critical for the MMIS. Since the identity of the user is encrypted by Rabin cryptosystem, it does not reveal user's identity and the adversary is unable to guess the identity of the user. Even though the medical server S is compromised, an adversary A obtains the verification table which stores the identity of all registered users. A cannot get information about which user is communicating with him/her, since the identity is connected with the high-entropy number r_2 and encrypted by Rabin cryptosystem. Without knowledge of other vital information, A can hardly obtain user's identity from receiving messages. Thus, our protocol achieves user anonymity.

12) USER UNTRACEABILITY

The encryption of user's identity with the integer r_2 will realize user's anonymity, since r_2 is a high-entropy random number and is unique in each session. Thus, $C_3 = (ID_i||r_2||B_i \oplus r_1^*)^2 \bmod n$ is also totally different in every session. Therefore, the adversary A cannot track U_i according the message C_3. As for other messages transmitted in public channel, they do not involve the user's identity. So, A cannot trace the user successfully.

13) BIOMETRIC DATA PRIVACY

In the enhanced protocol, the biometric B_i is computed by biohash function $h_{Bio}(\cdot)$ and protected by r_1 through the login and authentication phase. Since r_1 is a high-entropy random number, it is impossible for A to guess an exact biometric data. Thus, A cannot get the user's biometric data, and biometric data privacy is provided in our protocol.

14) USER FRIENDLINESS AND EFFICIENT PASSWORD CHANGE PHASE

In the proposed protocol, SC verifies the validity of the input data during the login phase, which speeds up the response and reduces the computational overhead of the server and the communication overhead when the input data are invalid. Besides, our protocol allows users change password locally at any time.

15) PERFECT FORWARD SECRECY

If a protocol dose not reveal previous session keys even both of the medical server S and the user U_i are compromised, the protocol holds perfect forward secrecy. In the proposed protocol, the adversary A cannot gain a right session key though the password PW_i of user, the secret key s of server and the data in SC are all disclosed, since r_2 and r_3 in $SK = h(M||r_2||r_3)$ are high-entropy random numbers and are different in each session, A can hardly guess them exactly. Thus, A cannot compute previous session keys and perfect forward secrecy is achieved in our protocol.

C. COMPARISON OF SECURITY FEATURES

The Table 5 lists comparisons among the enhanced protocol and other protocols according to some security features. It is worth noting in Table 5 that Amin's scheme is fragile to replay attacks and does not achieve user anonymity. As previously analyzed, Zhang et al.'s scheme is defective in offline

TABLE 5. Comparisons of the security features.

Functionality\scheme	Amin's scheme [22]	Zhang's scheme [29]	Our scheme
User anonymity	✓	✓	✓
User untraceability	✗	✓	✓
Session key agreement	✓	✓	✓
Biometric data privacy	✓	✓	✓
User friendly	✓	✗	✓
Perfect forward secrecy	✓	✓	✓
Offline password guessing attacks resistance	✓	✗	✓
Denial-of-Service attacks resistance	✓	✗	✓
User impersonation attacks resistance	✓	✓	✓
Server impersonation attacks resistance	✓	✓	✓
Stolen smart card attacks resistance	✓	✓	✓
Modification attacks resistance	✓	✓	✓
Replay attacks resistance	✗	✓	✓
De-synchronization attacks resistance	✓	✓	✓

TABLE 6. The comparisons of computational cost.

Schemes	Amin's scheme [22]	Zhang's scheme [29]	Our scheme
Login phase	$4T_h + 1T_{bh}$	$3T_h + 4T_{bh}$	$2T_h + 2T_{bh} + 1T_m + 1T_R$
Authentication phase	$6T_h$	$14T_h + 5T_{bh}$	$4T_h + 1T_{bh} + 1T_R$
Fully computational overhead	$10T_h + 1T_{bh}$	$17T_h + 9T_{bh}$	$6T_h + 3T_{bh} + 1T_m + 2T_R$

T_h : The computational cost of one-way hash function operation

T_{bh} : The computational cost of biohash function operation

T_m : The computational cost of modular operation

T_s : The computational cost of encrypt/decrypt operation of symmetric.

TABLE 7. The comparisons of communication cost.

Schemes	Amin's scheme [22]	Zhang's scheme [29]	Our scheme
Length (bits)	1056	1312	1344

password guessing attacks and DoS attacks, and is not user friendly.

VII. EFFICIENCY ANALYSIS

This section illustrates the efficiency of our protocol by comparing it and some related schemes for MMIS [22], [29]. The comparison includes computational overhead and communication cost.

The Table 6 lists comparison results of the computational cost of our protocol and other similar protocols (Amin et al.'s scheme [22], Zhang et al.'s scheme [29]). In order to contrast the computational overhead of these schemes intuitively, we mainly count the total required calculation cost of all types of operations, such as the one-way hash function, the biometric hash function, the modular operation, and the encryption/decryption operation. Compared to other operations, the time spent on XOR and concatenation operations is negligible, so we have omitted it.

By observing the comparison in Table 6, we find that the computational cost in our scheme are much lower than the two others and is more suitable for resource-constrained devices.

In Table 7, we provide comparisons of communication cost of all three protocols. For convenience, we set the identity, password, biometrics, output of the one-way hash function, and random numbers to 160 bits each. We set the output of the biohash function and the result of the modular operation to 256 bits. As for symmetric encryption/decryption algorithm, we adopt AES which is 128 bits. In the table, we can draw the conclusion that our protocol communication overhead is a little higher than the others but acceptable. However, it is worth paying attention to that the proposed protocol includes the password change phase and the biometric change phase, so it's more complete than others.

The above three types of analyses (including the section VI.C) show that the proposed protocol can provide many security features within a reasonable computation and communication cost that provides.

VIII. CONCLUSION

In this paper, we have briefly reviewed Zhang et al.'s protocol and revealed its flaws. Their scheme is far from practical use and suffers from offline password guessing attacks and DoS attacks. Besides, no local validation is provided in their scheme. Thus, we have proposed an enhanced protocol which adopts the Rabin cryptosystem and fuzzy verifier. Moreover, we have improved the dynamic verification table to prevent illegal access and de-synchronization attacks. In addition, we introduced the password change phase and the biometric change phase to improve the usability of the proposed protocol. We conducted a comprehensive analysis of security features to state that our scheme can resist many known attacks and solve the flaws in the scheme of Zhang et al. By comparing the proposed protocol and other related schemes, we showed that our protocol has more security features, and the computational cost and communication overhead are within a reasonable range.

REFERENCES

[1] D. B. David, "Mutual authentication scheme for multimedia medical information systems," *Multimedia Tools Appl.*, vol. 76, no. 8, pp. 10741–10759, Apr. 2017.

[2] C.-C. Lee, C.-W. Hsu, Y.-M. Lai, and A. Vasilakos, "An enhanced mobil E-health care emergency system based on extended chaotic maps," *J. Med. Syst.*, vol. 37, no. 5, p. 9973, Sep. 2013.

[3] C.-C. Lee, T.-H. Lin, and C.-S. Tsai, "A new authenticated group key agreement in a mobile environment," *Ann. Telecommun. Annales Des Télécommun.*, vol. 64, no. 11, p. 735, Dec. 2009.

[4] J. Xiong, X. Chen, Q. Yang, L. Chen, and Z. Yao, "A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing," *IEEE Trans. Netw. Sci. Eng.*, to be published, doi: 10.1109/TNSE.2019.2940958.

[5] D. Wu, J. Yan, H. Wang, D. Wu, and R. Wang, "Social attribute aware incentive mechanism for device-to-device video distribution," *IEEE Trans. Multimedia*, vol. 19, no. 8, pp. 1908–1920, Aug. 2017.

[6] Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen, and D. Wu, "Optimized fuzzy commitment based key agreement protocol for wireless body area network," *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2019.2949137.

[7] S. Kumari, F. Wu, X. Li, M. S. Farash, Q. Jiang, M. K. Khan, and A. K. Das, "Single round-trip SIP authentication scheme with provable security for Voice over Internet Protocol using smart card," *Multimedia Tools Appl.*, vol. 75, no. 24, pp. 17215–17245, Dec. 2016.

[8] H. Xiong, Q. Mei, and Y. Zhao, "Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2018.2890126.

[9] S. Kumari, P. Chaudhary, C.-M. Chen, and M. K. Khan, "Questioning key compromise attack on Ostad-Sharif et al.'s authentication and session key generation scheme for healthcare applications," *IEEE Access*, vol. 7, pp. 39717–39720, 2019, doi: 10.1109/ACCESS.2019.2905731.

[10] D. Wu, Z. Feng, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in mobile social networks," *Future Gener. Comput. Syst.*, vol. 87, pp. 803–815, Oct. 2017.

[11] H. Xiong, H. Zhang, and J. Sun, "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2739–2750, Sep. 2019, doi: 10.1109/JSYST.2018.2865221.

[12] J. Xiong, J. Ren, L. Chen, Z. Yao, M. Lin, D. Wu, and B. Niu, "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1530–1540, Apr. 2019.

[13] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2958–2970, Aug. 2017.

[14] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and A. C. Shehzad, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Elect. Eng.*, vol. 63, pp. 182–195, Oct. 2017.

[15] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Gener. Comput. Syst.*, vol. 63, pp. 56–75, Oct. 2016.

[16] S. Kumari, S. A. Chaudhry, F. Wu, X. Li, M. S. Farash, and M. K. Khan, "An improved smart card based authentication scheme for session initiation protocol," *Peer-Peer Netw. Appl.*, vol. 10, no. 1, pp. 92–105, Jan. 2017.

[17] K.-W. Kim and J.-D. Lee, "On the security of two remote user authentication schemes for telecare medical information systems," *J. Med. Syst.*, vol. 38, no. 5, p. 17, Apr. 2014.

[18] S. Kumari, L. Xiong, W. Fan, A. K. Das, K.-K. R. Choo, and S. Jian, "Design of a provably secure biometrics-based multi-cloud-server authentication scheme," *Future Gener. Comput. Syst.*, vol. 68, pp. 320–330, May 2017.

[19] W. Shiuh-Jeng and C. Jin-Fu, "Smart card based secure password authentication scheme," *Comput. Secur.*, vol. 15, no. 3, pp. 231–237, 1996.

[20] C.-T. Li, C.-C. Lee, C.-Y. Weng, and S.-J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for E-health care systems," *J. Med. Syst.*, vol. 40, no. 11, p. 233, Nov. 2016.

[21] A. K. Das and A. Goswami, "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *J. Med. Syst.*, vol. 37, no. 3, p. 9948, Jun. 2013.

[22] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and X. Li, "Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for E-health care systems," *J. Med. Syst.*, vol. 39, no. 11, p. 40, Nov. 2015.

[23] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for E-health clouds," *J. Supercomput.*, vol. 72, no. 10, pp. 3826–3849, Oct. 2016.

[24] X. Li, J. Niu, M. Karuppiah, S. Kumari, and F. Wu, "Secure and efficient two-factor user authentication scheme with user anonymity for network based E-Health care applications," *J. Med. Syst.*, vol. 40, no. 12, p. 268, Dec. 2016.

[25] O. Mir and M. Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for E-health services," *Wireless Pers. Commun.*, vol. 83, no. 4, pp. 2439–2461, 2015.

[26] S. A. Chaudhry, H. Naqvi, M. K. Khan, "An enhanced lightweight anonymous biometric based authentication scheme for TMIS," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 5503–5524, 2018.

[27] A. Ruhul, S. K. H. Islam, G. P. Biswas, M. K. Khan, and K. Neeraj, "An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography," *J. Med. Syst.*, vol. 39, no. 11, p. 180, Nov. 2015.

[28] A. Irshad, M. Sher, O. Nawaz, S. A. Chaudhry, I. Khan, and S. Kumari, "A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. Scheme," *Multimedia Tools Appl.*, vol. 76, no. 15, pp. 16463–16489, Aug. 2017.

[29] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for E-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795–2805, Mar. 2018.

[30] T.-Y. Chen, C.-C. Lee, M.-S. Hwang, and J.-K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *J. Supercomputing*, vol. 66, no. 2, pp. 1008–1032, Nov. 2013.

[31] C.-C. Lee, C.-T. Chen, P.-H. Wu, and T.-Y. Chen, "Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices," *Comput. Digit. Techn., IET*, vol. 7, no. 1, pp. 48–56, Jan. 2013.

[32] Q. Jiang, Y. Qian, J. Ma, X. Ma, and F. Wei, "User centric three-factor authentication protocol for cloud-assisted wearable devices," *Int. J. Commun. Syst.*, vol. 32, no. 6, Apr. 2019, Art. no. e3900.

[33] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood, "Protection of privacy in biometric data," *IEEE Access*, vol. 4, pp. 880–892, Mar. 2016.

[34] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology*. Berlin, Germany: Springer, 2004, pp. 523–540.

[35] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes Cryptography*, vol. 38, no. 2, pp. 237–257, Feb. 2004.

[36] A. T. B. Jin, D. N. C. Ling, and A. Goh, "BioHashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, Apr. 2004.

[37] R. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognit.*, vol. 40, no. 3, pp. 1057–1065, Mar. 2007.

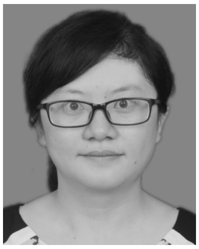
[38] M. O. Rabin, "Digitalied signatures and public key functions as intractable as factorization," MIT Lab. Comput. Sci., Cambridge, U.K., Tech. Rep. MIT/LCS/TR-212, Jan. 1979.

[39] H.-Y. Chien, "Combining rabin cryptosystem and error correction codes to facilitate anonymous authentication with un-traceability for low-end devices," *Comput. Netw.*, vol. 57, no. 14, pp. 2705–2717, Oct. 2013.

[40] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[41] B. Blanchet, "An efficient cryptographic protocol verifier based on prolog rules," in *Proc. IEEE Comput. Secur. Found. Workshop*, Jun. 2001, p. 82.

DEMING MAO is currently pursuing the Ph.D. degree with the College of Cyberspace Security, Northwestern Polytechnical University, Xi'an, Shanxi, China. He is a Senior Engineer with China Electronic Technology Cyber Security Company, Ltd., Chengdu, Sichuan, China. His research interest includes cyberspace security.



HUIHONG LIU is currently an Engineer with the Southwest Communications Institute, Chengdu, Sichuan, China. Her research interest includes cyberspace security.

WEI ZHANG received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, Sichuan, China, in 2017. He is currently an Engineer with the China Electronic Technology Cyber Security Company, Ltd., Chengdu. His research interest includes cyberspace security.