A Lightweight Privacy Preserving Authenticated Key Agreement Protocol for SIP-based VoIP

Liping Zhang[1,2], Shanyu Tang[1,*], *Senior Member*, *IEEE*, Shaohui Zhu[1]

[1] Secure Communication Institute, China University of Geosciences, Wuhan, 430074, China

[2] Computer& Information Science & Engineering, University of Florida, Gainesville, FL, USA

*Corresponding author: shanyu.tang@gmail.com, carolyn321@163.com,Tel/Fax:+862767848563

Abstract—Session Initiation Protocol (SIP) is an essential part of most Voice over Internet Protocol (VoIP) architecture. Although SIP provides attractive features, it is exposed to various security threats, and so an efficient and secure authentication scheme is sought to enhance the security of SIP. Several attempts have been made to address the tradeoff problem between security and efficiency, but designing a successful authenticated key agreement protocol for SIP is still a challenging task from the viewpoint of both performance and security, because performance and security as two critical factors affecting SIP applications always seem contradictory.

In this study, we employ biometrics to design a lightweight privacy preserving authentication protocol for SIP based on symmetric encryption, achieving a delicate balance between performance and security. In addition, the proposed authentication protocol can fully protect the privacy of biometric characteristics and data identity, which has not been considered in previous work. The completeness of the proposed protocol is demonstrated by Gong, Needham, and Yahalom (GNY) logic. Performance analysis shows that our proposed protocol increases efficiency significantly in comparison with other related protocols.

Key words—Session initiation protocol; Lightweight; Privacy protection; Key agreement.

I. INTRODUCTION

Voice over Internet Protocol (VoIP) systems have already spread to the markets since they can provide low cost and more flexibility implementation compared with traditional Public Switched Telephone Networks (PSTNs). In recent years, many efficient, flexible and secure signaling protocols have been proposed to boost the application versatility and rapid growth of VoIP. Among these signaling protocols, the Session Initial Protocol (SIP) is the widely used one due to its flexible, lightweight and scalable design.

SIP is a text based application layer control protocol for creating, modifying, and terminating multimedia sessions among participants [1]. Although SIP possesses many attractive merits, it is exposed to several security threats [2] such as impersonation, eavesdropping, and message modification etc, because the authentication of SIP is inherited directly from HTTP Digest authentication [3]. There is a trend towards reinforcing the security of SIP with an efficient and secure authentication protocol. But developing such an efficient and secure authentication protocol for SIP is a challenging task. On one hand, the authentication protocol should secure against various types of attacks and provide several security features to satisfy the security requirements of IP based networks. On the other hand, the authentication mechanism should not involve intensive computation in users and SIP server because VoIP communications are more sensitive to transmission latency.

Since security measures are usually inversely proportional to performance, several authenticated key agreement protocols were proposed to balance security and efficiency. The existing authentication protocols for SIP can be divided into four groups [4]: Password Authenticated Key Exchange (PAKE) based, Public Key Cryptography (PKC) based, ID based and Hash and Symmetric Encryption based. PAKE based protocols always suffer from stolen verifier attacks and require the communication parties sharing a password beforehand. PKC based protocols can resist almost all attacks, but these protocols need to implement computational cost operations. Although ID based protocols provide better security compared with other types of protocols, the Public Key Generator used in these protocols needs to be trusted; moreover, the use of expansive bilinear pairings leads to computational overhead and communication delay. In comparison, Hash-based protocols provide better performance, but these protocols have obvious security weakness. Therefore, how to design a successful authentication protocol for SIP to achieve a delicate tradeoff remains a challenge work.

In this study, our main objective is to design a lightweight authenticated key agreement protocol for SIP that meets the security requirements especially privacy protection, which has not been considered in most of previous work. The main contributions of our work are summarized as follows:

(1) Strong authentication: in the proposed protocol, biometric characteristics are employed with smart cards and passwords to provide strong authentication. The biometrics demonstrate what you are, the smart cards show what you have, and the passwords verify what you know, and those three complement one another to achieve strong authentication.

(2) Privacy protection: instead of storing the biometric template, the protected biometric data in our protocol is written into a smartcard and the smartcard can perform the correctness checking by using the protected biometric value. So that the adversary cannot obtain the user’s biometric information, even if the user’s smartcard had been lost or stolen and the data in the card was leaked. Moreover, the real identity of the user is protected by a symmetric encryption algorithm. Thus, the adversary cannot figure out the real identity of the user in the authentication process.

(3) Efficiency: symmetric encryption is adopted in our protocol to achieve lightweight authentication since the symmetric encryption and decryption operations perform almost as fast as calculating the hash value of the same size data. In addition, the SIP server does not need to maintain any password or verification table.

The rest of this paper is organized as follows. Section II introduces the related work. Section III describes the background associated with this study. In Section IV, the proposed protocol is described in detail. The security of the proposed protocol is discussed in Section V. In Section VI, the performance of the proposed protocol is evaluated and analyzed. And the paper is concluded in Section VII.

II. Relate Work

A secure and efficient authenticated key agreement protocol plays an essential role in protecting private and valuable information over audio communications in SIP-based services. However, the original authentication protocol of SIP only offers one-way authentication and cannot support integrity and confidentiality protection at an acceptable level in practice. On the other hand, since the original authentication protocol of SIP is based on hyper text transport protocol (HTTP) digest authentication, the computational cost is very high on widely used SIP proxy servers [5]. Thus, the original authentication protocol should be improved to satisfy the security and efficiency requirements of SIP. Over recent years, several authenticated key agreement protocols of SIP have been proposed to address different balance between security and efficiency. As the provision of the security features is usually inversely proportional to performance, designing an efficient and secure authenticated key agreement protocol for SIP is a challenging task.

To date, many authentication protocols for SIP have been proposed based on either hash and symmetric encryption or public key cryptography. These authentication protocols for SIP can be categorized into four groups: Password Authenticated Key Exchange based, Public Key Cryptography based, ID based and Hash and Symmetric Encryption based.

PAKE based protocols inherit from Encrypted Key Exchange protocols which rely on the Discrete Logarithm Problem (DLP). The main merit of these authentication protocols is simple. Based on Diffie-Hellman key exchange, Yang *et al.* [6] constructed a secure SIP authentication protocol by using the pre-shared hashed password. However, Jo *et al.* [7] demonstrated that Yang *et al.*'s protocol was vulnerable to the off-line password guessing attack. Furthermore, their protocol required the SIP server storing a pre-configured password table. Based on Elliptic Curve Diffie-Hellman (ECDH), Durlanik *et al.* [8] presented a new authentication protocol for SIP. Compared with other PAKE based protocols, Durlanik *et al.*'s protocol reduced the execution time since Elliptic Curve Cryptography (ECC) could achieve the same level security with faster computation and smaller key size. However, Yoon *et al.* [9] claimed that this protocol could not resist the Denning-Sacco attack due to no usage of random integer in generating the session key. Wu *et al.* [10] also suggested a SIP authentication protocol based on ECC and proved its security by using Canetti-Krawczyk (CK) security model. Unfortunately, Wu *et al.*'s protocol was suffered from off-line password guessing attacks, Denning-Sacco attacks and stolen-verifier attacks [11]. To eliminate the security flaws, Yoon *et al.* [11] proposed an improved authentication protocol based on Wu *et al.*'s protocol. Unfortunately, the improved protocol still suffered from off-line password guessing attacks and replay attacks.

The PAKE based protocols need communication parties to pre-share a password secretly in general, which limits these protocols' scalability and applicability. In addition, the passwords stored at the SIP server lead to a risk of suffering from stolen verifier attacks.

Based on PKC, Srinivasan *et al.* [12] proposed a three party SIP authentication protocol. However, in their protocol, the user could not choose their password freely, and the computational cost of creating user's certifications, signatures, and computing multiple functions on the proxy server and registrar server decreased the performance of the protocol. To address these obstacles, Nodooshan *et al.* [13] proposed an authentication protocol to move the heavy public key cryptography operation from the SIP server to the user to lighten the computational load on the proxy server and register server. Arshad *et al.* [14] also proposed an authentication protocol based on elliptic curve discrete logarithm problem for SIP. Unfortunately, He *et al.* [15] indicated that Arshad *et al.*'s protocol cannot resist off-line password-guessing attacks. Recently, Pu *et al.* [16] gave an example to show the offline password guessing in Arshad *et al.*'s protocol and proposed a new authentication protocol based on ECC. Although Pu *et al.*'s protocol overcame the security flaw of Arshad *et al.*' protocol, the expansive use of bilinear pairings decreases its practicability. Based on ECC, Yoon *et al.* [17] employed the biometric, password and smartcard three-factor to design a strong authentication for SIP. However, their protocol failed to address the privacy protection of the user's biometric. In order to protect the user's privacy, Hsiu [18] adopted the smartcard to construct an authentication protocol based on ECC for SIP, but the computational cost of the protocol was very high due to 12 times of ECC computation operations were involved.

PKC-based protocols are secure against the offline password guessing attacks, Denning Sacco attack and spoofing. But the heavy computational load could not be avoided since the implement of the PKI, the certificate revocation management and calculation of public key cryptography are all computational costing operations.

To avoid the use of a large PKI, some ID based authentication protocols of SIP were proposed. Ring *et al.* [19] proposed an authentication key agreement (AKA) for SIP by using identity-based cryptography. In order to reduce the delay of session key generation, a one-way key agreement protocol was proposed by Han *et al.* [20] to improve the performance of Ring *et al.*'s protocol. However, this protocol did not meet the requirements of the media security management protocol since it was a one-way key agreement protocol. Wang *et al.* [21] presented an authentication key agreement based on certificateless cryptography which eliminates the key escrow and supports peer-to-peer connections. Li *et al.* [22] also proposed a certificateless authenticated key agreement protocol with different Key Generation Centers. But the computational costs of both protocols were very high due to the use of expansive bilinear pairings.

ID based protocols provide better security, and they could resist most of the attacks except the collusion attack, because the Public Key Generator (PKG) used in these protocols knows all entities' secret keys. In addition, the PKG needs to be trustable, which is a limitation of the protocols. Furthermore, the use of expansive bilinear pairings, the signature generation, and the verification lead to the computational overhead and communication delay.

As VoIP communications are very sensitive to transmission latency, security measures should avoid time-consuming operations. Tao *et al.* [23] proposed a lightweight authentication protocol for SIP by using symmetric key encryption and Diffie-Hellman key exchange. But the generation and management of the shared key were complicated, which reduced its practical application. Tsai *et al.* [24] presented an authentication protocol based on nonce and hash computations. Tsai's protocol achieved low computational cost, since only one-way hash function and exclusive-or operations were used in their protocol. However, Yoon *et al.* [25] demonstrated that Tsai's protocol suffered from off-line password guessing attacks, Denning-Sacco attacks, and stolen-verifier attacks, and could not provide perfect forward secrecy. Yoon *et al.* also proposed a new protocol to overcome the above security weaknesses. But Xie *et al.* [26] demonstrated that Yoon *et al.*'s protocol was vulnerable to stolen-verifier attacks and off-line password guessing attacks.

The hash and symmetric encryption based protocol could meet low computational requirements since hash and symmetric encryption/decryption operations are faster than public key cryptography. But some of the hash based protocols suffered from offline password guessing attacks, Denning Sacco attacks, and stolen verifier attacks. And these protocols are very hard to design to provide strong security.

In general, security is inversely proportional to performance. Investigating into designing a secure and efficient authenticated key agreement protocol is an intractable task. In this paper, we present a mitigation authentication mechanism for achieving a delicate balance between performance and security for SIP. To reduce the computational cost, expansive operations should be avoided. Hash operations seem to be the best choice of designing lightweight authentication protocols, but hashed based protocols have some security weakness. Since encryption and decryption operations can perform almost as fast as calculating the hash value of the same size data [4], the symmetric encryption based protocols would achieve good performance as hash based protocols. Therefore, we adopt symmetric encryption to construct our lightweight authentication protocol. Furthermore, to satisfy the security requirements of SIP, biometric, password and smartcard are employed to enhance the security of our proposed protocol.

III. Background

In this section we first review the original SIP authentication procedure and then summarize the goals that an authenticated key agreement for SIP should achieve. Finally, we discuss the problems existing in previous related protocols.

The security of the original SIP authentication is mainly dependent on the challenge-response mechanism. The procedure of the original SIP authentication is described as follows:

Step 1: The user sends a REQUEST to the SIP server.

Step 2: The SIP server submits CHALLENGE (*nonce*, *realm*) as a response message to the user where the *nonce* is generated by the server and the *realm* is the digest algorithm.

Step 3: The user computes a RESPONSE= h(*nonce*, *realm*, *username*, *response*) by using the *nonce* value, *realm*, *username* and the computed *response* value, where $h(\cdot)$ is a one-way hash function. Then the user relays the RESPONSE to the SIP server.

Step 4: After obtaining the RESPONSE message, the SIP server extracts the user's password according to the *username* and verifies whether the *nonce* is correct. If it is correct, the SIP server calculates a hash value h(*nonce*, *realm*, *username*, *response*) to check whether it is equal to the received value of RESPONSE. If they match, the SIP server authenticates the identity of the user.

Since the original SIP authentication scheme doesn't provide mutual authentication and cannot support integrity and confidentiality protection, it suffers from several attacks. Furthermore, the computational cost of the original authentication scheme is very high on the SIP proxy servers. Therefore, the original authentication scheme should be improved to satisfy the security and efficiency requirements of SIP.

Next, we summarize the goals that an authenticated key agreement for SIP should achieve as follows:

(1) Secure against various attacks: An authenticated key agreement for SIP should be secure against replay attacks, man-in-middle attacks, modification attacks, Denning-Sacco attacks, stolen-verifier attacks, insider attacks, password disclosure attacks, server-spoofing attacks, and offline dictionary attacks with/without smartcards.

(2) Provide security features: An authenticated key agreement for SIP should provide mutual authentication, session key agreement, freely choosing and updating passwords, session key security, no verifier table, perfect forward secrecy, and known-key security features.

(3) Privacy protection: An authenticated key agreement for SIP should provide biometric protection and user identity anonymity.

(4) Light-weight: An authenticated key agreement for SIP should not involve intensive computation on both users and SIP server side.

To achieve above goals, several authenticated key agreement protocols of SIP have been proposed to balance security and efficiency. ID based and PKC based protocols are better than other protocols from the security viewpoint, but they cannot avoid computational cost operations which do not meet the lightweight requirements. The performance of hash based protocols is considerably the best one among all the protocols. However, these protocols always suffer security flaws which do not satisfy the security requirements. Since the symmetric encryption and decryption operations perform almost as fast as calculating the hash value, the symmetric encryption based protocols could be used to replace the hash based protocols to achieve lightweight and security requirements. In addition, since everyone's biometric characteristic is unique, and the characteristic could be combined with password and smartcard to enhance the security of the symmetric encryption based protocol to achieve the balance of security and efficiency.

The traditional biometric authentication process [27-29] is described in Figure 1. When a user wants to login, she/he inserts a smartcard and performs a biometric scan. The user's biometric characteristic is then extracted through an image processing on the raw data. Next, the smartcard compares the biometric template stored in it beforehand with the biometric characteristic extracted from the user's input. If the matching score is beyond a predefined threshold value, the smartcard terminates the authentication process. However, this traditional biometric authentication process has some security weakness. If the smartcard was lost or stolen, the user's biometric template stored in the smartcard could be compromised easily. And the leakage of the biometric information could damage the user's benefit because the biometric information is unique and does not change in a long time. Therefore, the biometric information stored in the smartcard should be protected.

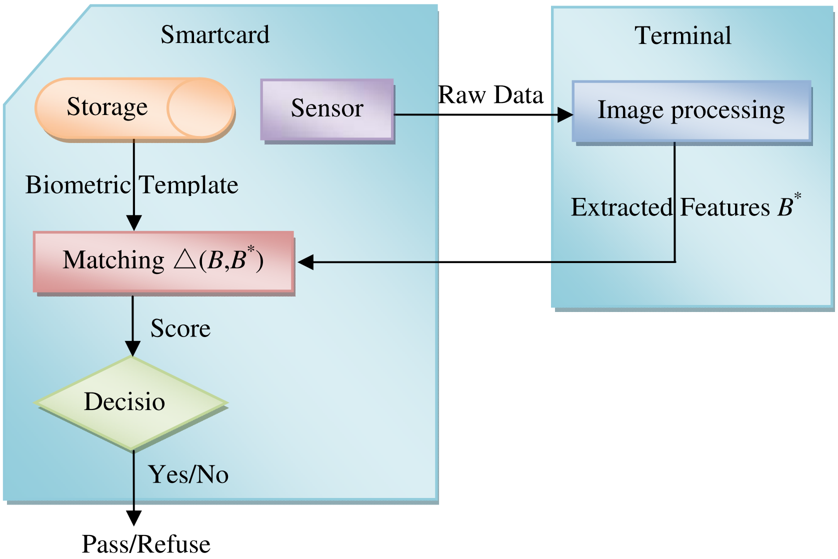

Fig.1. Verification procedure using biometric characteristics

The above problem was arisen by some researchers, and an alternative verification procedure [30-32] has been proposed as shown in Figure 2. Instead of the biometric template, the hashed biometric template is stored in the smartcard, so that even the smartcard was lost or stolen, the user's biometric template could not be compromised, because the hash function is a one way function and it is computationally infeasible to find a message that can map to the same hash value.

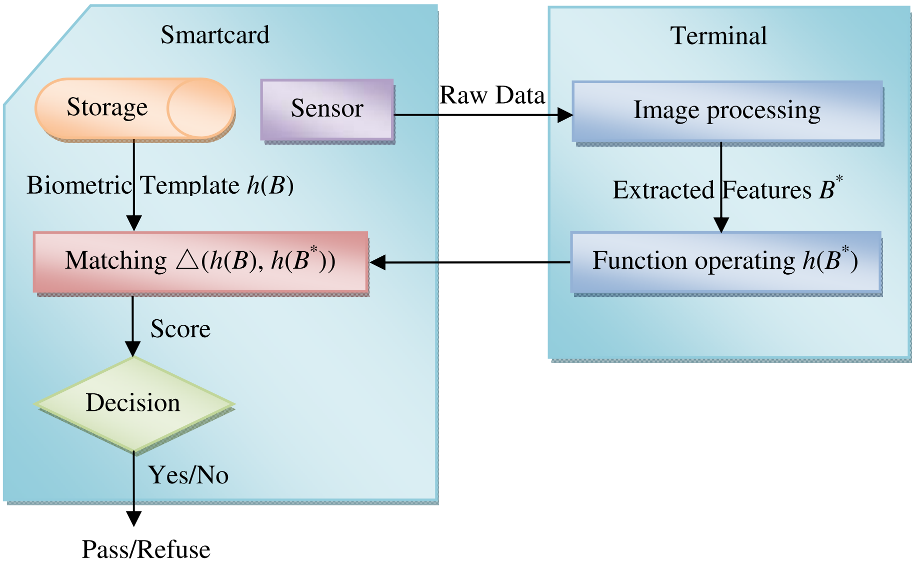

Fig.2. Checking procedure using protected biometric data

The method shown in Fig. 2 seemed to be a good solution to provide protection for the biometric template stored in the smartcard. However, our research investigation revealed that the hashed biometric template stored in the smartcard could not be used to match the hashed biometric inputs. Under this case, even the valid biometric input could not pass the biometric checking process, because the output of the hash function is sensitive to small noise of the inputs. This means that a small difference in the inputs will lead to a large different output. So the hash functions cannot apply straightforwardly to the input data with noisy such as biometrics [33, 34]. Although the above solution provides the protection of the biometric template, it also prevents the legal user from passing biometric authentication, since a small difference between the input biometric data and the biometric template will cause a larger difference between the two hashed biometric values.

IV. Lightweight Privacy Preserving Authentication key Agreement Protocol

In this section, we present our basic idea aimed to solve the problems and realize the goals. Then our lightweight authenticated key agreement protocol with privacy protection is described in detail.

In order to protect the user's biometric template, the smartcard should have the ability of checking the correctness of the user's biometric characteristics without knowing the original values. How to realize the correctness checking of the protected biometric characteristics stored in the smartcard? If the problem was solved, we could then store the protected biometric data in the smartcard and achieve the correctness checking by using the protected biometric value. So that even the smartcard was lost or stolen, the user's biometric information could not be compromised. Next we describe our solution. First, we define some notations, B and B^* represent the biometric template and input biometric data respectively. And the notation Δ denotes as the matching algorithm. If the function $F(\square)$ with secret key k satisfies the following requirements, the use of this function will not affect the matching result, and then it can be used to solve the problem.

(1) $\Delta(B,B^*)=\Delta(F_k(B),F_k(B^*))$

(2) Known $F_k(B)$, it is computationally infeasible to get B without the secret key k.

If we can find a function satisfying above requirements, the smartcard can perform the matching algorithm successfully by using the protected biometric values $F_k(B)$ and $F_k(B^*)$. In this study, we use exclusive OR operation as function $F(\square)$ and a high entropy random integer as the secret key. Since Hamming distance can be used to compare the two biometric strings [35], the exclusive OR operation will not affect the matching result which satisfies the above function requirements. So even the smartcard is lost or stolen, the user's biometric template cannot be compromised.

Based on above idea, we design a lightweight privacy preserving authenticated key agreement protocol of SIP. There are three phases in the proposed protocol, registration phase, authentication phase, and password change phase, as shown in Figures 3 and 4. Next, we describe our protocol in detail as follows:

A. *Registration phase*

When a new user *U* wants to register with the SIP server *S*, it performs the following process with the SIP server in the registration phase.

$Step\ R1: U \rightarrow S: (ID, R, h(\cdot))$

The user *U* freely chooses its identity *ID*, its password *PW* and performs an iris scan to generate a biometric template *B*. Next, it selects a one-way hash function $h(\cdot):\{0,1\}^* \rightarrow \{0,1\}^k$ and a high entropy random integer *r*, and then computes $EB = r \oplus B$, $R = PW \oplus EB \oplus ID$ and $SR = h(PW \oplus ID) \oplus r$. Finally, the user *U* submits {*ID*, *R*, $h(\cdot)$ } to the SIP server over a secure channel.

$Step\ R2$: $S \rightarrow U: Smartcard(I, T, W)$

The SIP server *S* chooses a random integer *s* as a secret key for symmetric encryption/decryption. Then it computes $I = E_s(ID)$, $V = E_s(ID \oplus s)$, $T = V \oplus R$ and *W*=*E*$_V$(*R*) through encrypting *R* via the key *V*. Next, the SIP server *S* records (*ID*, $h(\cdot)$) in an identity table and writes the secure information (*I*, *T*, *W*) to the memory of the user *U*'s smart card. Then it issues this smart card to the user *U* through a secure channel.

*Step R*3: After receiving the smart card, the user *U* stores (*SR*, $EB, h(\cdot)$) in the smart card secretly. Finally, the memory of the smart card contains (*I*, *T*, *W*, *SR*, $EB, h(\cdot)$).

B. *Authentication phase*

In the authentication phase, the user *U* and the SIP server *S* perform the following steps:

$Step\ A1$: $U \rightarrow S: REQUEST(I, C_2)$

The user *U* inserts its smartcard into the smartcard reader, and inputs its identity *ID*, its password *PW*, and takes iris scan to generate the biometric template B^*. Then the smartcard retrieves the high entropy random integer $r = SR \oplus h(PW \oplus ID)$ by using the password *PW*, identity *ID* and the secret information *SR* stored in the smartcard. After that, the smartcard uses *r* and the captured biometric data B^* to compute $EB^{'} = r \oplus B^*$. Next, it compares $EB^{'}$ with the secret information *EB* stored in it. If the matching score $\Delta(EB^{'}, EB)$ is beyond a predefined threshold value, the smartcard terminates the authentication session.

On the contrary, if the matching score $\Delta(EB^{'}, EB)$ is within the predefined threshold value, the smartcard computes $V^{'} = T \oplus PW \oplus EB \oplus ID$ by using the information (*T*, *EB*) stored in the smartcard and the user *U*'s input information (*PW*, *ID*). It then verifies whether the following equation holds $E_{V^{'}}(PW \oplus EB \oplus ID) \overset{?}{=} W$. If the equation holds, the SIP server *S* selects a random integer *a* and computes $C_1 = ((PW \oplus EB \oplus ID) \| a)$ and $C_2 = E_{V^{'}}(T \| ID \| C_1)$. Next, the user *U* submits a request message *REQUEST* (*I*, C_2) to the SIP server *S* over a public channel.

$Step\ A2{:}\ S \rightarrow U : CHALLENGE(realm, Auth_s, r_1)$

After receiving the request message, the SIP server *S* decrypts *I* with its secret key *s* to retrieve the user's identity *ID*. And then it checks whether the *ID* is valid according to the identity table. If not, it terminates the authentication session. Otherwise, the SIP server *S* uses this *ID* and its secret key *s* to compute the key $V = E_s(ID \oplus s)$. Then it decrypts the received information C_2 via the computed *V* to obtain the information *T*, C_1 and *ID*. Next, the SIP server *S* compares the value of the *ID* in *I* with that of the *ID* in C_2. If they are not equivalent, the process stops; otherwise, it computes $R = T \oplus V$ by using the decrypted message *T* and the computed message *V* and checks whether the following equation holds $PW \oplus EB \oplus ID \overset{?}{=} R$, where $PW \oplus EB \oplus ID$ is in C_1. If they are not equivalent, the process stops; otherwise, the SIP server *S* chooses two random integers (*b*, r_1) and uses the corresponding hash function $h(\cdot)$ according to the identity table to compute the session key $SK = h(a \oplus b)$ and generates an authentication message $Auth_s = E_V(C_3 \| C_4)$, where $C_3 = PW \oplus EB \oplus ID \oplus b$ and $C_4 = (h(a \oplus C_3) \| a)$. Finally, the SIP server *S* sends a challenge message *CHALLENGE* (*realm*, $Auth_s$, r_1) to the user *U*.

$Step\ A3{:}\ U \rightarrow S : RESPONSE(realm, Auth_u)$

Upon receiving the challenge message, the user *U* uses $V^{'}$ to decrypt $Auth_s$ to get C_3 and C_4. Then the smartcard extracts $b = C_3 \oplus PW \oplus EB \oplus ID$ by using the decrypted message C_3, the input information (*PW*, *ID*) and the biometric message *EB* stored in the smartcard. Next, the smart card computes $(h(a \oplus C_3) \| a)$ and checks whether it is equal to the decrypted message C_4. If not, it rejects the challenge message and terminates the authentication session. Otherwise, it sets the session key $SK^{'} = h(a \oplus b)$ and computes the authentication information $Auth_u = h(a \oplus b \| (r_1 + 1))$. After that, the user *U* sends a response message *RESPONSE* (realm, *Auth*$_u$) to the SIP server *S*.

*Step A*4: After receiving the response message, the SIP server *S* verifies whether the following equation holds $Auth_u \overset{?}{=} h(a \oplus b \| (r_1 + 1))$. If the equation holds, the SIP serve*r S* sets $SK = h(a \oplus b)$ as the shared session key with the user *U*; otherwise, it rejects the response message and stops the process.

User U | Server S

Registration Phase:

Select $ID, PW, r, h(g)$

Generate biometric template B

Compute $EB = r \oplus B$, $R = PW \oplus EB \oplus ID$, $SR = h(PW \oplus ID) \oplus r$

$$\xrightarrow{\{ID,\ R,\ h(g)\ \}}$$

Choose a secret key s

Compute $I = E_s(ID)$, $V = E_s(ID \oplus s)$, $T = V \oplus R, W = E_V(R)$

$$\xleftarrow{\text{Smartcard } (I,\ W,\ T)}$$

Store (EB, SR, $h(g)$) into Smartcard

Authentication Phase:

Input ID, PW and choose a

Scan iris to obtain B^*

Extract r from SR

Compute $EB' = r \oplus B^*$ and Compare

Compute $V' = T \oplus PW \oplus EB \oplus ID$

Verify $E_{V'}(PW \oplus EB \oplus ID) \overset{?}{=} W$

Compute $C_1 = ((PW \oplus EB \oplus ID) \| a)$ and $C_2 = E_{V'}(T \| ID \| C_1)$

$$\xrightarrow{REQUEST\ (I,\ C_2)}$$

Decrypt I to obtain ID and Check ID in the identity table

Compute $V = E_s(ID \oplus s)$

Decrypt C_2 by using V

Compare two IDs and Compute $R = T \oplus V$

Verify $R \overset{?}{=} PW \oplus EB \oplus ID$

Select r_1, b

Compute $SK = h(a \oplus b)$, $C_3 = PW \oplus EB \oplus ID \oplus b$

$C_4 = (h(a \oplus C_3) \| a)$, $Auth_s = E_V(C_3 \| C_4)$

$$\xleftarrow{CHALLENGE\ (realm,\ Auth_s,\ r_1)}$$

Decrypt $Auth_s$ by using V'

Compute $C_3 \oplus PW \oplus EB \oplus ID$ to obtain b

Verify $C_4 \overset{?}{=} (h(a \oplus C_3) \| a)$ and set $SK' = h(a \oplus b)$

Compute $Auth_u = h(a \oplus b \| (r_1 + 1))$

$$\xrightarrow{RESPONSE\ (realm,\ Auth_u)}$$

$Auth_u \overset{?}{=} h(a \oplus b \| (r_1 + 1))$

Fig. 3. Authenticated key agreement phase

C. *Password changing phase*

In the password changing phase, the user *U* can change its password *PW* freely and securely. And this process does not require an interaction with the SIP server *S*. As shown in Figure 4, all steps of the password changing phase are executed as follows:

*Step P*1: $U \rightarrow U$'*s Smartcard* (B^*, *PW*, *ID*)

When the user *U* wants to update its password, it needs to insert its smartcard and take iris scan to generate the biometric template B^*. The user *U* also needs to input its identity *ID*, previous password *PW* and then sends all the messages (B^*, *PW*, *ID*) to its smartcard.

*Step P*2: *U*'*s Smartcard* $\rightarrow U$:(*Request new password*)

After receiving the message, the smartcard computes $h(PW \oplus ID)$ by using the password *PW* and identity *ID* and then extracts the high entropy random integer $r = SR \oplus h(PW \oplus ID)$. After that it computes $EB' = r \oplus B^*$ using *r* and the captured biometric data B^*, and then compares EB' with the *EB* stored in the smartcard. If the matching score $\Delta(EB', EB)$ is beyond a predefined threshold value, the smartcard refuses the password updating request. Otherwise, it returns the message (*Request new password*) to the user *U*.

*Step P*3: $U \rightarrow U$'*s Smartcard* (PW^*)

Upon receiving the message, the user *U* inputs the new password PW^* and sends it to the smartcard.

*Step P*4: After receiving the new password PW^*, smartcard computes new $SR^* = h(PW^* \oplus ID) \oplus r$, $T^* = T \oplus PW \oplus PW^*$, and $W^* = E_{T \oplus PW \oplus EB \oplus ID}(PW^* \oplus EB \oplus ID)$, respectively. Finally the smartcard replaces the old values (*SR*, *T*, *W*) with (SR^*, T^*, W^*).

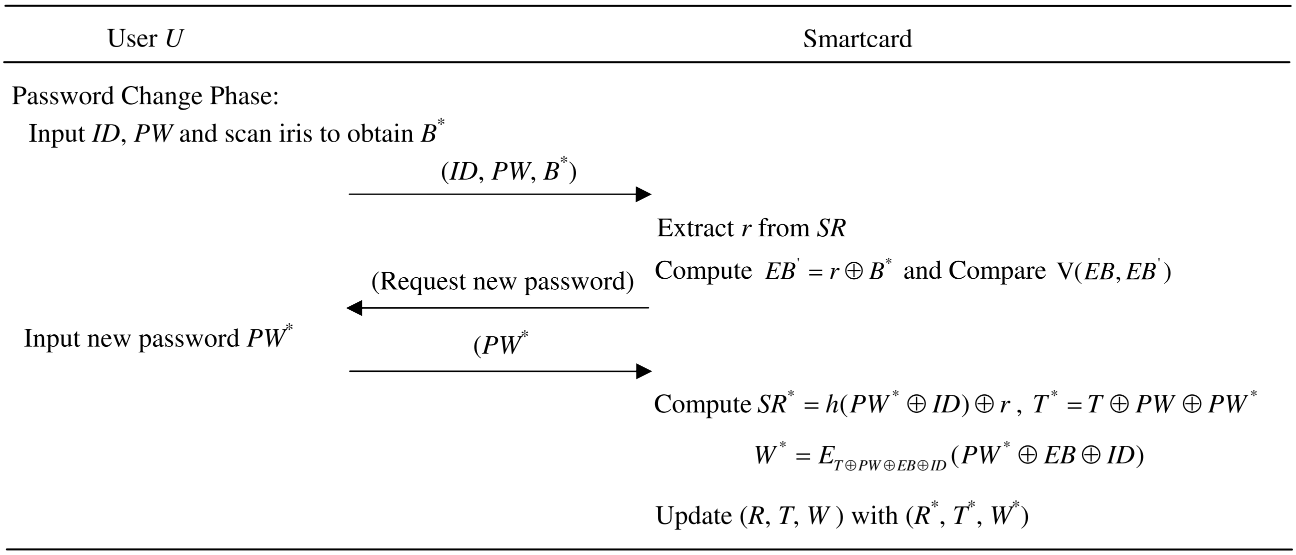
User U
Smartcard
Password Change Phase:
Input ID, PW and scan iris to obtain B^*
(ID, PW, B^*)
Extract r from SR
(Request new password)
Compute $EB^{'} = r \oplus B^*$ and Compare $\mathrm{V}(EB, EB^{'})$
Input new password PW^*
$(PW^*$
Compute $SR^* = h(PW^* \oplus ID) \oplus r$, $T^* = T \oplus PW \oplus PW^*$
$W^* = E_{T \oplus PW \oplus EB \oplus ID}(PW^* \oplus EB \oplus ID)$
Update (R, T, W) with (R^*, T^*, W^*)

Fig. 4. Password updating phase

V. Security Analysis

A. Model of Computation

Gong-Needham-Yahalom (GNY) logic [36] is one of the extensions of Burrows-Abadi-Needham Logic [37] which has been widely used to formally analyze the completeness of protocols. Since GNY has successfully disclosed redundancies or found defects in several protocols, the GNY logic is used to evaluate the security of our proposed protocol in this study. First, we describe the model of computation used in our work.

The model of computation used in our work is based on GNY's model of computation which is similar to that used in BAN work. The main aspects of the model are given as follows. For the details, please refer to [36].

A distributed environment includes principals and state-machines, which are connected by communication links. The messages running on the links are only means of communication between principals. Any principal has ability to run a message on any link. Any message being transformed on any link can also be seen and changed by the principal.

A protocol is a distributed algorithm which determines what messages will be sent. A protocol run as a session is an execution of the protocol.

A belief set and a possession set are two sets which are maintained by each principal in each session. A belief set possesses all the current beliefs of the principal and a possession set consists of all the formulae available to the principal including the principal received, and the principal has generated itself.

Principals start a session with certain initial beliefs and possessions. After that, a principal can get new beliefs, and increase its belief set. Inference rules are used to derive new beliefs based on current beliefs and incoming messages.

Beliefs and possessions are monotonic within a given session.

B. Completeness of the proposed protocol

In this subsection, we first introduce some formulae and statements used in the GNY logic; then set the goals and the assumptions of our protocol; finally we detail how to adopt the GNY logic to prove the security of the proposed protocol.

1) Formulae and statements

A formula is a name used to refer to a bit string with a particular value in a run in the GNY logic [36]. Let symbols X and Y range over formulae. We introduce the formulae used in our authentication proof as follows and the complete list of all logical postulates can be found in [36].

(1) (X, Y): conjunction of two formulae X and Y.

(2) $\{X\}_K$ and $\{X\}_K^{-1}$: symmetrically encrypt and decrypt X with the key K.

(3) $H(X)$: a one-way function of X.

(4) $*X$: X is not originated here.

A basic statement reflects some property of a formula in the GNY logic [36]. Let symbols P and Q be principals. We introduce the statements used in our authentication proof as follows:

(1) $P \triangleleft X$: P is told formula X.

(2) $P \ni X$: P possesses formula X.

(3) $P|\!\sim X$: P once conveyed formula X.

(4) $P|\!\equiv \#(X)$: P believes that X is fresh.

(5) $P|\!\equiv \phi(X)$: P believes that X is recognizable.

(6) $P|\equiv P\xleftrightarrow{S}Q$: *P* believes that *S* is a suitable secret for *P* and *Q*.

(7) $P|\Rightarrow X$: *P* has jurisdiction over *X*.

(8) $P\lhd *X$: *P* is told that formula *X* which did not convey previously in the current run.

2) Protocol descriptions and goals

To fit the GNY logic, we transform the proposed protocol into the form of $P\rightarrow Q$:(*X*) and make several changes to some notations as follows:

(1) $U\rightarrow S:(\{ID\}_s,\{T\|ID\|C_1\}_V)$

(2) $S\rightarrow U:(\{PW\oplus EB\oplus ID\oplus b\|(H(b\oplus a)\|a)\}_V,r_1)$

(3) $U\rightarrow S:(H(a\oplus b\|(r_1+1)))$

Next, we describe our goals with three aspects in detail as follows:

(1) Message content authentication

Goal 1: *S* believes the message in the first run is recognizable.

$S|\equiv\phi(\{ID\}_s,\{T\|ID\|(PW\oplus EB\oplus ID)\|a)\}_V)$

Goal 2: *U* believes the message $Auth_s$ in the second run is recognizable.

$U|\equiv\phi(\{PW\oplus EB\oplus ID\oplus b\|(H(a\oplus b\oplus PW\oplus EB\oplus ID)\|a)\}_V)$

Goal 3: *S* believes the message in the third run is recognizable.

$S|\equiv\phi(H(a\oplus b\|(r_1+1)))$

(2) Message origin authentication

Goal 4: *U* believes *S* conveys the message in the second run.

$U|\equiv S|\sim(\{PW\oplus EB\oplus ID\oplus b\|(H(a\oplus b\oplus PW\oplus EB\oplus ID)\|a)\}_V)$

Goal 5: *S* believes *U* conveys the message in the third run.

$S|\equiv U|\sim(H(a\oplus b\|(r_1+1)))$

(3) Session key material establishment

Goal 6: *U* believes that *S* believes that $a\oplus b$ is a secret shared between *U* and *S*.

$$U \mid\equiv S \mid\equiv U \xleftrightarrow{a\oplus b} S$$

Goal 7: *U* believes that $a\oplus b$ is a secret shared between *U* and *S*.

$$U \mid\equiv U \xleftrightarrow{a\oplus b} S$$

Goal 8: *S* believes that *U* possesses $a\oplus b$.

$$S \mid\equiv U \ni a\oplus b$$

Goal 9: *S* believes that *U* believes that $a\oplus b$ is a secret shared between *U* and *S*.

$$S \mid\equiv U \mid\equiv U \xleftrightarrow{a\oplus b} S$$

3) Assumption list

In this subsection, some assumptions are made as follows:

(1) Since the secret key *s* and the random integers r_1 and *b* are generated by *S*, so *S* possesses *s*, r_1 and *b*. In addition *S* believes that r_1 and *b* are fresh.

$$S \ni s , S \ni r_1,\ S \mid\equiv \#(r_1) , S \ni b, S \mid\equiv \#(b)$$

(2) The random integer *a* is generated by *U* in the protocol, so *U* possesses *a* and believes that *a* is fresh. Since *EB* and *T* are stored in the smartcard, and the user *U* holds the smartcard and know the password *PW* and the identity *ID*, then the user *U* possesses *EB*, *T*, *PW* and *ID*.

$$U \ni a, U \mid\equiv \#(a) , U \ni EB, U \ni PW, U \ni T, U \ni ID$$

(3) Since $a\oplus b$ is constructed by two high entropy random integers chosen from *U* and *S* freely and independently, we assume that *S* believes that $a\oplus b$ is a suitable secret between itself and *U*.

$$S \mid\equiv S \xleftrightarrow{a\oplus b} U$$

(4) Since *V* is a secret generated by *S*, and stored in the smartcard protected by *R*, we assume that *U* believes *V* is a suitable secret for himself and *S*.

$$U \mid\equiv U \xleftrightarrow{V} S$$

(5) *U* believes that the server *S* is an authority on generating a suitable session key material $a\oplus b$ shared between *U* and *S*.

$$U \mid\equiv S \mid\Rightarrow U \xleftrightarrow{a\oplus b} S$$

4) Authentication proof using GNY logic

In this subsection, GNY logic is adopted to analyze the proposed protocol. The complete list of the logical postulates and the index are shown in literature [31]. The notation ($T1$, $P1$) represents the index of the logical postulate in the complete list which used to explain the derivation. We show how to achieve the goals defined before by using *GNY* logic.

(1)The first run:

$$\frac{S \lhd \{ID\}_s, S \lhd \{T \| ID \| C_1\}_V}{S \ni \{ID\}_s, S \ni \{T \| ID \| C_1\}_V} \tag{A1}$$

According to $P1$, S is capable of possessing $\{ID\}_s$ and $\{T \| ID \| C_1\}_V$.

$$\frac{S \ni \{ID\}_s, S \ni s}{S \ni ID, S \ni ID \oplus s} \tag{A2}$$

According to $P6$ and $P2$, if S possesses $\{ID\}_s$ (A1) and the key s (Assumption 1), then it is capable of possessing the decryption value ID and the computed value $ID \oplus s$.

$$\frac{S \ni ID \oplus s, S \ni s}{S \ni \{ID \oplus s\}_s} \tag{A3}$$

According to $P6$, if S possesses $ID \oplus s$ (A2) and the key s (Assumption 1), it is capable of possessing the encryption value $\{ID \oplus s\}_s$ that is V.

$$\frac{S \ni \{T \| ID \| C_1\}_V, S \ni V}{S \ni (T \| ID \| C_1), S \ni H(T \| ID \| C_1)} \tag{A4}$$

According to $P6$ and $P4$, if S possesses $\{T \| ID \| C_1\}_V$ (A1) and the key V (A3), then it possesses the decryption value $(T \| ID \| C_1)$ and the one-way computationally feasible function value $H(T \| ID \| C_1)$.

$$\frac{S \ni H(T \| ID \| C_1)}{S \mid\equiv \phi(T \| ID \| C_1)} \tag{A5}$$

According to $R6$, if S possesses $H(T \| ID \| C_1)$ (A4), then it believes that $(T \| ID \| C_1)$ is recognizable.

$$\frac{S|\equiv\phi(T\|ID\|C_1), S\ni V}{S|\equiv\phi(\{T\|ID\|C_1\}_V), S|\equiv\phi(\{ID\}_s,\{T\|ID\|C_1\}_V)} \tag{A6}$$

According to $R1$ and $R2$, if S believes that $(T\|ID\|C_1)$ is recognizable (A5) and S possesses the key V(A3), then S is entitled to believe that the encryption of $(T\|ID\|C_1)$ with V is recognizable and $(\{ID\}_s,\{T\|ID\|C_1\}_V)$ of which $\{T\|ID\|C_1\}_V$ is a component is recognizable. Therefore, according to A6, S can recognize the message $(\{ID\}_s,\{T\|ID\|C_1\}_V)$ in the first run. (Goal 1)

(2) The second run:

$$\frac{U\ni a}{U\ni H(a), U|\equiv\phi(a)} \tag{A7}$$

According to $P4$ and $R6$, if U possesses a (Assumption 2), then it is capable of possessing $H(a)$ and then it is entitled to believe a is recognizable

$$\frac{U|\equiv\phi(a)}{U|\equiv\phi(PW\oplus EB\oplus ID\oplus b\|(H(a\oplus b\oplus PW\oplus EB\oplus ID)\|a))} \tag{A8}$$

According to $R1$, if U believes a is recognizable (A7), then it is entitled to believe that of $(PW\oplus EB\oplus ID\oplus b\|(H(a\oplus b\oplus PW\oplus EB\oplus ID)\|a))$ which a is a component is recognizable. That is, U believes that the formula $(C_3\|C_4)$ is recognizable.

$$\frac{U\ni PW, U\ni EB, U\ni ID, U\ni T}{U\ni PW\oplus EB\oplus ID\oplus T} \tag{A9}$$

According to $P2$, if U possesses PW, EB, ID and T (Assumption 2), then it is capable of possessing $U\ni PW\oplus EB\oplus ID\oplus T$ that is V.

$$\frac{U|\equiv\phi(PW\oplus EB\oplus ID\oplus b\|(H(a\oplus b\oplus PW\oplus EB\oplus ID)\|a)), U\ni V}{U|\equiv\phi(\{PW\oplus EB\oplus ID\oplus b\|(H(a\oplus b\oplus PW\oplus EB\oplus ID)\|a)\}_V), U|\equiv\phi(\{C_3\|C_4\}_V)} \tag{A10}$$

According to $R2$, if U believes that $PW\oplus EB\oplus ID\oplus b\|(H(a\oplus b\oplus PW\oplus EB\oplus ID)\|a)$ is recognizable (A8) and U possesses the key V (A9), and then U is entitled to believe that the encryption value $\{PW\oplus EB\oplus ID\oplus b\|(H(a\oplus b\oplus PW\oplus EB\oplus ID)\|a)\}_V$ is recognizable. Therefore, according to

A10, U can recognize the message $\{C_3 \| C_4\}_V$ that is $Auth_s$ in the second run. (Goal 2)

$$\frac{U \mid\equiv \#(a), U \ni V}{U \mid\equiv \#(PW \oplus EB \oplus ID \oplus b \| (H(a \oplus b \oplus PW \oplus EB \oplus ID) \| a)), U \mid\equiv \#(\{C_3 \| C_4\}_V)} \tag{A11}$$

According to $F1$ and $F2$, if U believes a is fresh (Assumption 2), then it is entitled to believe that $(PW \oplus EB \oplus ID \oplus b \| (H(a \oplus b \oplus PW \oplus EB \oplus ID) \| a))$ of which a is a component is fresh. That is U believes that $(C_3 \| C_4)$ is fresh. Since U possesses the key V (A9), it also believes that $\{C_3 \| C_4\}_V$ is fresh.

$$\frac{U < *\{C_3 \| C_4\}_V, U \ni V, U \mid\equiv U \overset{V}{\leftrightarrow} S, U \mid\equiv \phi(C_3 \| C_4), U \mid\equiv \#(C_3 \| C_4)}{U \mid\equiv S \mid\sim \{C_3 \| C_4\}_V, U \mid\equiv S \ni V} \tag{A12}$$

According to $I1$, if all of the following conditions hold: 1) U receives the formula $(C_3 \| C_4)$ encrypted with the key V and marked with a not-originated-here mark; 2) U possesses V (A9); 3) U believes that V is a suitable secret for itself and S (Assumption 4); 4) U believes that the formula $(C_3 \| C_4)$ is recognizable (A8); and 5) U believes that $(C_3 \| C_4)$ is fresh (A11). Then U is entitled to believe that 1) S once conveyed $\{C_3 \| C_4\}_V$ and 2) U believes that the S possesses V. (Goal 4)

According to the GNY logic, we assume that $U \mid\equiv S \mid\Rightarrow S \mid\equiv *$, that is, U believes that S is honest and competent, and then we can deduce the following statement:

$$\frac{U \mid\equiv S \mid\Rightarrow S \mid\equiv *, U \mid\equiv S \mid\sim (\{C_3 \| C_4\}_V \sim> S \mid\equiv U \xleftrightarrow{a \oplus b} S), U \mid\equiv \#(\{C_3 \| C_4\}_V)}{U \mid\equiv S \mid\equiv U \xleftrightarrow{a \oplus b} S} \tag{A13}$$

According to $J2$, if U believes that S is honest and competent; and U receives a message $(\{C_3 \| C_4\}_V \sim> S \mid\equiv U \xleftrightarrow{a \oplus b} S)$, which it believes S conveyed (A12), then U ought to believe that S really believes $U \xleftrightarrow{a \oplus b} S$. According to A13, U believes that S believes that $a \oplus b$ is a suitable secret between U and S. (Goal 6)

$$\frac{U \mid\equiv S \mid\Rightarrow U \xleftrightarrow{a \oplus b} S, U \mid\equiv S \mid\equiv U \xleftrightarrow{a \oplus b} S}{U \mid\equiv U \xleftrightarrow{a \oplus b} S} \tag{A14}$$

According to $J1$, if U believes that S is an authority on the statement $U \overset{a\oplus b}{\longleftrightarrow} S$ (Assumption 5) and S believe in $U \overset{a\oplus b}{\longleftrightarrow} S$ (A13), then U ought to believe in $U \overset{a\oplus b}{\longleftrightarrow} S$ as well. According to A14, U believes that $a \oplus b$ is a suitable secret between U and S. (Goal 7)

(3) The third run:

$$\frac{S \ni r_1}{S \ni H(r_1), S|\equiv \phi(r_1), S|\equiv \phi(a \oplus b \| (r_1+1))} \tag{A15}$$

According to $P4$, $R6$ and $R1$, if S possesses r_1 (Assumption 1), it is capable of possessing $H(r_1)$, and then it is entitled to believe that r_1 and (r_1+1) is recognizable. Therefore S believes that $a \oplus b \| (r_1+1)$ of which (r_1+1) is a component is recognizable.

$$\frac{S \ni (T \| ID \| C_1), S \ni b, S \ni r_1}{S \ni C_1, S \ni a, S \ni a \oplus b, S \ni r_1+1, S \ni (a \oplus b \| (r_1+1))} \tag{A16}$$

According to $P3$, if S possesses $(T \| ID \| C_1)$ (A4), then it is capable of possessing C_1 and a that is a concatenated component of C_1. According to $P2$, if S possesses a, b and r_1 (Assumption 1), then it is capable of possessing $a \oplus b$, r_1+1 and $(a \oplus b \| (r_1+1))$.

$$\frac{S|\equiv \phi(a \oplus b \| (r_1+1)), S \ni (a \oplus b \| (r_1+1))}{S|\equiv \phi(H(a \oplus b \| (r_1+1)))} \tag{A17}$$

According to $R5$, if S believe $a \oplus b \| (r_1+1)$ is recognizable (A15) and S also possesses $a \oplus b \| (r_1+1)$ (A16), then it is entitled to believe that the formula $H(a \oplus b \| (r_1+1))$ is recognizable. According to A17, we can say that S believes that the message $H(a \oplus b \| (r+1))$ in the third run is recognizable. (Goal3)

$$\frac{S|\equiv \#(r_1)}{S \ni |\equiv \#(r_1+1)} \tag{A18}$$

According to $F1$, if S believes r_1 is fresh (Assumption 1), then it is entitled to believe that $(r_1$+1) is fresh.

$$\frac{S < *H((r_1+1), < a \oplus b >), S \ni ((r_1+1), < a \oplus b >)), S|\equiv S \overset{a\oplus b}{\longleftrightarrow} U, S|\equiv \#(r_1+1)}{S|\equiv U|\sim ((r_1+1), < a \oplus b >), S|\equiv U|\sim H((r_1+1), < a \oplus b >)} \tag{A19}$$

According to *I*3, if all of the following conditions hold: 1) *S* receives a formula consisting of a one way function of (r_1+1) and $a \oplus b$ marked with a not-originated-here mark; 2) *S* possesses (r_1+1) and $a \oplus b$ (A16); 3) *S* believes $a \oplus b$ is a suitable secret for itself and *U* (Assumption 3); 4) *S* believes that (r_1+1) is fresh (A18). Then *S* is entitled to believe that *U* once conveyed $((r_1+1), <a \oplus b>)$ and $H((r_1+1), <a \oplus b>)$. According to A19, we can say that *S* believes that the message $Auth_s$ in the third run of the proposed protocol is conveyed from the *U*. (Goal 5)

$$\frac{S \mid\equiv U \mid\sim ((r_1+1), <a \oplus b>)}{S \mid\equiv U \mid\sim (a \oplus b)} \qquad \text{(A20)}$$

According to *I*7, if *S* believes that *U* once conveyed the formula $((r_1+1), <a \oplus b>)$ (A19), then it is entitled to believe that *U* once conveyed $a \oplus b$.

$$\frac{S \mid\equiv \#(b)}{S \mid\equiv \#(a \oplus b)} \qquad \text{(A21)}$$

According to *F*1, if *S* believes *b* is fresh (Assumption 1), then it believes that $a \oplus b$ is fresh.

$$\frac{S \mid\equiv U \mid\sim a \oplus b, S \mid\equiv \#(a \oplus b)}{S \mid\equiv U \ni a \oplus b} \qquad \text{(A22)}$$

According to *I*6, if *S* believes that *U* once conveyed formula $a \oplus b$ (A20) and $a \oplus b$ is fresh (A21), then *S* is entitled to believe that *U* possesses $a \oplus b$. According to A22, *S* believes that $a \oplus b$ is possessed by *U*. (Goal 8)

According to the GNY logic, we assume that $U \mid\equiv S \mid\Rightarrow S \mid\equiv *$, that is, *S* believes that *U* is honest and competent, and then we can deduce the following statement:

$$\frac{S \mid\equiv U \mid\Rightarrow U \mid\equiv *, S \mid\equiv U \mid\sim (H(a \oplus b \| (r_1+1))) \sim> U \mid\equiv U \xleftrightarrow{a \oplus b} S), S \mid\equiv \#(H(a \oplus b \| (r_1+1)))}{S \mid\equiv U \mid\equiv U \xleftrightarrow{a \oplus b} S} \qquad \text{(A23)}$$

According to *J*2, if *S* believes that *U* is honest and competent, and *S* receives a message $H(a \oplus b \| (r_1+1)) \sim> U \mid\equiv U \xleftrightarrow{a \oplus b} S$ which it believes is conveyed by *U* (A19), then *S* ought to believe that *U* really believes $U \xleftrightarrow{a \oplus b} S$. According to A23, we can conclude that *S* believes that $a \oplus b$ is a suitable secret between *U* and *S*. (Goal9)

C. Discussion on possible attacks

Next, we discuss the security of our proposed protocol by analyzing some possible attacks.

1) Replay attacks

Suppose, in *Step A*1, the user *U's* previous request message *REQUEST* (I, C_2) is intercepted by an adversary Bob and he replays it to the SIP server S intending to impersonate the user U. However, this replay attack will be found in *Step A*3 when the SIP server S checks the authentication information $Auth_u$. To construct a valid $Auth_u$, Bob needs to correctly guess the high entropy random integers a and b from the intercepted information C_2 and *Auths* which is protected by a secure symmetric encryption algorithm. Without the knowledge of T and the user U's privacy information *PW*, *EB* and *ID* or the SIP server's secret key s, Bob cannot compute the valid symmetric key V to decrypt C_2 and *Auths* to obtain a and b.

On the other hand, suppose Bob intercepts the previous message *CHALLENGE* (*realm*, $Auth_s$, r_1) from the SIP server S in *Step A*2 and replays it to the user U. The user U can detect this attack by checking whether the equation $C_4 \overset{?}{=} (h(a \oplus C_3) \| a)$ holds, where a and b are high entropy random integers generated by the user U and the SIP server S independently and are different in each session. So Bob cannot pass the verification process of the user U in *Step A*3. In this case, no *RESPONSE* message is sent back to Bob. Thus, Bob cannot impersonate or deceive either the user U or SIP server S through reuse of information obtained from the proposed protocol. Therefore, our proposed protocol can resist the replay attack successfully.

2) Man-in-the-middle attacks

In our protocol, the user U and the SIP server share a session key *SK* only after mutual authentication. The adversary Bob cannot impersonate the user U to make an independent connection and share a session key with the SIP server S unless he can pass the verification process of the SIP server S. However, without the knowledge of the user U's password *PW*, the user U's identity *ID* and the secret T or the SIP server's secret key s, Bob cannot pass the SIP server's verification. On the other hand, Bob cannot impersonate the SIP server S to share a session key and make an independent connection with the user U, since he cannot correctly guess the high entropy random integer *a* and the secret information (*V*, *R*) to construct a valid verification information *Auths*.

Thus, the adversary Bob cannot construct independent connections with either the *SIP* server *S* or the user *U* making them believe that they are talking directly to each other over a private connection, in fact the entire conversation is controlled by the Bob. The above analysis shows that the proposed protocol can resist the man-in-middle attack.

3) Modification attacks

In order to impersonate the user *U*, the adversary Bob needs to modify the *REQUEST* message with fraud $(I^{'}, C_2^{'})$ and delivers it to the SIP server *S*. However, without the knowledge of the SIP server's secret key *s*, Bob cannot generate a valid $I^{'}$. Then the SIP server can easily find this attack by checking the *ID* in the identity table. Even if Bob passes this *ID* verification, the SIP server can also find this attack by comparing the value of the *ID* in $I^{'}$ with that of the *ID* in $C_2^{'}$. In addition, without the knowledge of the secret key *s* or the user's private information (*PW*, *EB, ID*, *T*), Bob cannot generate a proper $C_2^{'}$ to pass the equation verification of $PW \oplus EB \oplus ID \overset{?}{=} R$. Therefore, Bob cannot impersonate the user *U* through fabricating the *REQUEST* message.

Suppose the adversary Bob sends a forgery *CHALLENGE* $(realm, Athu_s^{'}, r_1^{'})$ to the user *U* to impersonate the SIP server *S*. However, without the knowledge of the secret key *s* or the user's private information (*PW*, *EB*, *ID*, *T*) Bob cannot construct a valid symmetric key *V* and the verification information C_3 and C_4 to generate a proper $Athu_s^{'}$ to pass the verification process of the user *U*. The user *U* will find this attack by checking whether the equation $C_4 \overset{?}{=} (h(a \oplus C_3) \| a)$ holds. Therefore, Bob cannot impersonate the SIP server *S* by fabricating the *CHALLENGE* message.

Suppose Bob impersonates the user *U* and modifies the message *RESPONSE* $(realm, Athu_u^{'})$ relay to the SIP server *S*. Since Bob cannot guess the high entropy random integers *a* and *b* correctly, the SIP server *S* can find out this impersonating attack by checking the $Auth_u^{'}$ value with its computed value

$h(a \oplus b \| (r_1 + 1))$. Therefore, the adversary Bob cannot launch the modification attack successfully in the proposed protocol.

4) Denning-Sacco attacks

Assuming an adversary Bob obtains the previous session key *SK*. Bob cannot obtain the *U*'s password from the old session key *SK*, since the session key is constructed by two random integers chosen by the user *U* and the SIP server *S* independently and are not connected with the password or the SIP server's private key *s*. So even Bob compromises an old session key, he cannot find the user *U*'s password *PW* or the SIP server's private key *s*. In addition, in each session a fresh session key is generated depending on the integer *a* chosen by the user *U* and the integer *b* selected by the SIP server *S* randomly. Therefore, even Bob compromises an old session key, he cannot obtain other session keys as the session key $SK = h(a \oplus b)$ is not connected with each other in any manner. Therefore, the proposed protocol can resist Denning-Sacco attacks.

5) Stolen-verifier attacks

In the proposed protocol, there are no password or verification tables stored in the SIP server database. Therefore, the adversary Bob cannot obtain the valuable information through stealing the verification table stored on the SIP server, to masquerade as the user *U* to cheat the SIP server *S* in the authentication process. So the proposed protocol can resist the stolen-verifier attack.

6) Offline dictionary attacks without the smart card

Suppose the adversary Bob intercepts all the messages transmitting between the user *U* and the SIP server *S* through eavesdropping, and he intends to use the information to perform offline dictionary attacks. However, the user *U*'s password is protected by a secure symmetric encryption algorithm, the user *U*'s identity *ID*, biometric template *B*, and secret random integer *r*. Therefore, without the knowledge of the symmetric encryption key *V* and the user *U*'s private information (*ID*, *B*, *r*), the adversary Bob cannot determine whether each of his guessed passwords is correct or not. Additionally, when Bob tries to retrieve the user's password *PW* from the information $Auth_s$, he needs to decrypt the information $Auth_s$ and correctly guess the random integer *b*, the user *U*'s identity *ID*, biometric template *B*, and the secret random integer *r*. Therefore, the offline dictionary attack without the smart card is invalid in the proposed protocol.

7) Offline dictionary attacks with the smart card

Assuming an adversary Bob compromises the secret information (*EB*, *SR*, *T, I, W*) stored in the smart card of the user *U* and intercepts all the messages transmitted between the user *U* and the SIP server *S*. Then he carries out the offline dictionary attack to determine whether each of his guessed passwords is correct or not. Compared with the offline dictionary attack without the smart card, the addition information known by Bob in this attack is the information (*EB*, *SR*, *T, I, W*) stored in the smartcard. However, the extra information cannot help Bob to guess the user *U*'s password correctly without the knowledge of user *U*'s biometric template *B*, identity *ID*, secret integer *r* or the SIP server's secret key *s*. Therefore, the offline dictionary attack with the smart card is invalid in the proposed protocol.

8) Insider attacks

In the proposed protocol, the biometric authentication process can resist insider attacks successfully. Furthermore, in our protocol, no password or verification tables are stored on the SIP server *S*, so a privileged-insider of the SIP server *S* cannot access other servers by stealing the identity and password-verifier from the SIP server *S*'s verification table. Therefore, the insider adversary cannot launch the insider attack successfully.

9) Password disclosure attacks

In our protocol, in the registration phase, the user *U* sends $R = PW \oplus EB \oplus ID$ instead of its password *PW* to the SIP server *S*. As the password *PW* is protected by the user *U*'s biometric template *B*, the identity *ID*, and the high entropy random integer *r*, the SIP server *S* cannot find an opportunity to obtain the user *U*'s password *PW* in the register phase. Therefore, the proposed protocol can resist the password disclosure attack.

10) Session key security

In the proposed protocol, the session key $SK = h(a \oplus b)$ is not known by anyone but only the user *U* and the SIP server *S*, because the random integers *a* and *b* are protected by a secure symmetric encryption algorithm throughout the authentication process. And the random integer b is also protected by the user U's password PW, identity ID, biometric template B, and secret random integer r. In addition, in *Step A*2, the hashed $(a \oplus b \oplus PW \oplus EB \oplus ID)$ connected with a and C_3 is protected by a secure symmetric encryption algorithm when it relays from the SIP server to the user U. And in *Step A*3, the session key material $(a \oplus b)$ connected with (r_1+1) is protected by the hash function when it transmits from the user U to the SIP server S. Therefore, none of this session key $SK = h(a \oplus b)$ is known to anybody but the user U and the SIP server S. Therefore, the proposed protocol provides session key security.

11) Known-key security

In the proposed protocol, the session key $SK = h(a \oplus b)$ is generated depending on the random integer a chosen by the user U randomly and the integer b selected by the SIP server S randomly in each session. Since the user U and the SIP server S generate the random integer a and b randomly and independently, the session key SK in each run of the authentication protocol is unique. Therefore, the proposed protocol provides known-key security.

12) Perfect forward secrecy

In the proposed protocol, the long-term private key of the user U is its password PW. Suppose that the user U's password PW is compromised by the adversary Bob, in order to get the previous session key, he needs to extract the integer a from C_2 and b from $Auth_s$ or extract $(a \oplus b)$ directly from $Auth_s$ or $Auth_u$. However, Bob cannot retrieve the random integer a from the intercepted information C_2 without the knowledge of symmetric key V. And he cannot obtain the integer b from $Auth_s$ without the knowledge of symmetric key V and the user U's private information (EB, ID). In addition, for the same reason Bob cannot get $(a \oplus b)$ directly from $Auth_s$, and cannot obtain $(a \oplus b)$ from $Auth_u$ since it is protected by hash function. Furthermore, even if the adversary Bob obtains the previous session key material $(a \oplus b)$, he cannot compute the previous session key SK without the knowledge of the hash function $h(\square)$. Therefore, even the password PW is compromised by the adversary; the secrecy of previous session keys established is not affected. On the other hand, assume that the adversary Bob also compromises the long-term private key s of the SIP server. Under this case, without the knowledge of hash function $h(\square)$, the adversary cannot figure out the previous session keys. Therefore, the proposed protocol satisfies the property of perfect forward secrecy.

13) Mutual authentication

In the proposed protocol, the SIP server *S* and the user *U* can authenticate each other by checking *Authu* and *Auths*, respectively. Therefore, the proposed protocol can provide mutual authentication.

14) Security chosen and update password

In the proposed protocol, the legitimate user can freely choose her or his favorite password in the registration phase which makes users easy to remember their own passwords. The proposed protocol also provides an update password phase for users to change their password freely. And this process does not require interaction with the SIP server *S*. In addition, if the smart card was stolen or lost, other person could not change or update the password without knowing the user's privacy information (B^*, *PW*, *ID*).

15) User anonymity

The proposed protocol can provide user anonymity, which is demonstrated by the following proof. In the authentication phase, the user's real identity is protected by a secure symmetric encryption algorithm. Therefore, even if an adversary compromised the secret information stored in the smartcard and recorded the used messages transmitted between the user *U* and the SIP server *S*, he or she could not derive the real identity of the user *U* without the knowledge of the SIP server's secret key *s* or the user *U*'s password *PW*, biometric template *B*, the secret random integer *r*, and the secret *T*. Therefore, the user's real identity *ID* is fully preserved throughout the authentication process in the proposed protocol.

16) Biometric privacy

In our protocol, the user's biometric templates are protected by a high entropy random integer *r*, and *r* is protected by the user's password *PW* and identity *ID*. So, even the adversary obtains the smartcard, she or he cannot retrieve the user's biometric template without the knowledge of the user's real identity and password information. Furthermore, the value $SR = h(PW \oplus ID) \oplus r$ can be replaced with $SR = \varepsilon_B(r)$, where $\varepsilon(\square)$ is an encryption function with the biometric template *B* as the encryption key to enhance the security of the random integer *r*. In this case, even the adversary obtains the user's password *PW*, the identity *ID* and the smartcard, she or he cannot retrieve the user's biometric template without the knowledge of the user's biometric information.

VI. Performance comparison

In this section, we evaluate the performance and security aspects of the proposed protocol and other related protocols. In the proposed protocol, no password or verifier table is stored on the SIP server, so it can resist stolen-verifier attacks and insider attacks successfully. And the biometric template stored in the smartcard is protected by a high entropy random integer while the smartcard can also perform the matching algorithm to verify the user's biometric template. Therefore, even the user's smartcard is lost or stolen, the adversary cannot obtain the user's biometric data. In addition, the identity of the user is transmitted in ciphertext, which means that the adversary cannot obtain the real identity of the user, even if she or he intercepts all the messages transmitted between the user and the SIP server. As shown in Table 1, other protocols [24, 14, 15] cannot provide some security features such as no verifier table, user anonymity, and efficient password change which are very important security features in implementing a practical and universal authenticated key agreement for SIP. Yoon's protocol [17] provides an efficient password change function without involving the SIP server, but failed to provide privacy protection. Although Hsiu's protocol [18] satisfies most of the security requirements, it involves the time synchronization problem. In addition, Table 1 shows that Tsai's protocol [18] is weaker than other related protocols since it cannot resist offline password guessing attacks, stolen verifier attacks, Denning Sacco attacks. Compared with the related work [24,17,14,15,18], the proposed protocol is secure against several attacks meanwhile it provides a number of attractive features such as no password or verifier table needed, user anonymity, biometric protection, and efficient password updating, which have not been considered or provided by other related protocols, as shown in Table 1.

We also compare the computational cost of the proposed protocol with other related protocols. In the previous work, the total computational cost of the authentication protocol was calculated by adding up the execution times of all cryptographic operations directly involved in the protocol. Obviously, the final execution time of an authentication process computed by this approach is not a real time of the authentication process needed. In addition, the execution times of some cryptographic operations are associated with the size of input data such as hash operation. For example, in our experiment, the time spent in one-way hash with 512 bytes input is around 0.003ms and only 0.001ms with 128 bytes input. Therefore, the above approach used in related work is not appropriate for evaluating the execution time of an authentication protocol for SIP. In our experiments, the SIP server and the client are installed on two PCs over the local area network to simulate a practical environment. The hardware platform for SIP server is Intel Core (TM) i5 which offers maximum clock speeds of 2.53 GHz and 4GB memory. The client is Intel Pentium G630 processor with 4GB memory which offers maximum clock speeds of 2.7 GHz. Furthermore, a NIST/SECG-standard elliptic curve over a 521 bits prime field and SHA-1as a one-way hash function are used in the experiments. And a 256-bit AES (Advance Encryption Standard) (NIST 2001) encryption mechanism is adopted as the symmetric key encryption/decryption operations in the proposed protocol, since AES combines the merits of speed and security.

Table 1. The functionality comparisons between our protocol and others

Security Attacks and Features	Tsai [24]	Yoon [17]	Arshad [14]	He [15]	Hsiu [18]	Our protocol
Replay attack resist	Yes	Yes	Yes	Yes	Yes	Yes
Offline password guessing attack resist	No	Yes	No	Yes	Yes	Yes
Stolen verifier attack resist	No	Yes	Yes	Yes	Yes	Yes
Denning Sacco attack resist	No	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	Yes	Yes	Yes	Yes	Yes	Yes
Efficient password change	No	Yes	No	No	Yes	Yes
No verifier table	No	Yes	No	No	Yes	Yes
Biometric protection	A/N	No	A/N	A/N	A/N	Yes
User anonymity	No	No	No	No	No	Yes
No time synchronization	Yes	Yes	Yes	Yes	No	Yes

Now, we define some notations as follows:

(1) T_E: the time for executing a symmetric key encryption operation;

(2) T_D: the time for executing a symmetric key decryption operation;

(3) T_H: the time for executing a one-way hash function;

(4) T_M: the time for executing a scalar multiplication operation of elliptic curve;

(5) T_A: the time for executing a point addition operation of elliptic curve;

(6) T_{INV}: the time for executing a modular inversion operation.

Table 2 shows computational comparisons between the proposed protocol and other related protocols. In the registration phase, the proposed protocol requires one hash operation to compute *SR* on the user side, and needs three symmetric encryption operations to obtain *V*, *I* and *W* on the SIP server side. Then the total execution time of the registration is estimated to be 3.422ms.

In the authentication phase, the user side needs two symmetric encryption operations to obtain C_2 and verify the value of *W*; one symmetric decryption operation to decrypt message $Auth_s$; three hash operations to compute $h(a \oplus C_3)$ $Auth_u$ and *SK*. The SIP server side requires two symmetric decryption operations to decrypt message *I* and C_2 and two symmetric encryption operations to compute *V* and $Auth_s$; and three hash operations to obtain $h(a \oplus C_3)$, $h(a \oplus b \| (r_1 + 1))$ and *SK*. The experimental results show that only 8.73ms is needed to realize authentication in our protocol.

Table 2. Computational comparisons between our protocol and others

Performance Properties		Tsai [24]	Yoon [17]	Arshad [14]	He [15]	Hsiu [18]	Our protocol
Registration	User side		T_H			T_H	T_H
	Server side		T_H	$2T_H$	$2T_H$	T_H+T_M	$3T_E$
	Execute time		0.016ms	0.013ms	0.014ms	10.875ms	3.422ms
Authentication	User side	$4T_H$	$4T_H+2T_M$	$3T_H+2T_M$	$3T_H+3T_M$	$6T_H+4T_M+2T_A$	$T_D+2T_E+3T_H$
	Server side	$3T_H$	$4T_H+2T_M$	$3T_H+3T_M+T_{INV}$	$3T_H+3T_M$	$5T_H+3T_M+2T_A$	$2T_D+2T_E+3T_H$
	Execute time	0.744ms	54.432ms	66.077ms	72.505ms	103.124ms	8.73ms

As shown in Fig. 5, the protocol proposed by Tsai achieves the best performance, because the computational cost of computing a hash value is very low. However, Tsai’s protocol is vulnerable to offline password guessing attacks, stolen verifier attacks, Denning Sacco attacks, and does not provide efficient password updating, privacy protections etc, as summarized in Table 1. The experimental results demonstrate that our protocol is as efficient as Tsai's protocol [24] and is more efficient than other four protocols [17, 14, 15, 18], since no elliptic curve operations are involved in our proposed protocol.

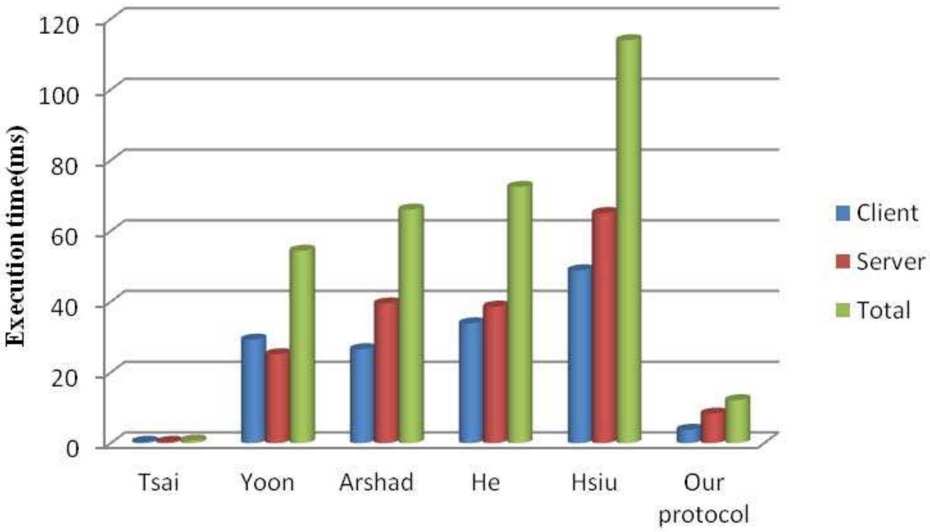

Fig. 5 Execution time comparisons between our protocol and others

Next, we discuss the communication and storage overhead by comparing our proposed protocol with other protocols. In the proposed protocol, the secret s is required to store at the server side, and the smartcard needs to store the secure information (I, T, W, SR, EB, $h(\cdot)$), where I, T, and W are 128bits, SR is 160bits, and EB is 64bits. Tsai's protocol [24] requires the SIP server to store a password table which includes the username and the corresponding password of every user. Assume that n represents the number of the registration users and the username is 32bits, and the corresponding password is 64bits. Then the storage requirement of the password table in Tsai's protocol is $n \times 96$. Arshad's protocol [14] also requires the SIP server to store a high-entropy secret key and a verifier table containing each user's name and the corresponding hashed password. Similar to Tsai's protocol, the storage requirement of the verification table in Arshad's protocol is $n \times 192$, where the username is 32bits and the corresponding verification information VPW is 160 bits for every user. Since the above protocols [14, 24] need to store the password or verifier table, the required storage increases with the growth of the registration users. Compared with these protocols, our proposed protocol reduces the storage overhead at the SIP server side significantly, because there were no password or verification tables stored in the SIP server database. He's protocol [15] only requires the SIP server to store the secret key. In the Yoon's protocol [17], the SIP server needs to store a secret key, and the smartcard requires to store the secure information including a symmetric parametric function, a predetermined threshold, a secure one way hash function, a biometric template, and a hash value. And in Hsiu's protocol [18], the smartcard requires to store the secure information containing four different hash functions, a random number, a hash value, and a point of elliptic curve. And on the SIP server side, the secret key needs to be stored. Compared with the protocols based on the smartcard [17, 18], the storage requirement of the smartcard in our protocol is lower. In addition, there is no information needed to store at the user side, and only a secret key needs to store at the SIP side in the proposed protocol.

We hereby present the communication overhead of the proposed protocol. In our experiments, the user's *ID* and the timestamp were 32 bits, the random number was 64 bits, a point of elliptic curve was 512 bits, and the output of the hash was 160 bits. In addition, the output of a 256-bit AES was based on the input of the plaintext. The communication cost comparisons between our protocol and others are shown in Table 3. In our proposed protocol, the average communication cost was 1120 bits. Compared with the protocols in [14, 15, 17, 18], the proposed protocol reduced the communication cost. Compared with Tsai's protocol, the communication overhead of our protocol was slightly higher; this was because our protocol provides more unique features.

Table 3. Communication cost comparisons between our protocol and others

	Tsai [24]	Yoon [17]	Arshad [14]	He [15]	Hsiu [18]	Our protocol
Communication cost	608 bits	1536 bits	1408 bits	1408 bits	2336 bits	1120 bits

In addition, the proposed protocol can resist various attacks and provide more attractive security features, so the proposed protocol is a successful authenticated key agreement protocol for SIP from the viewpoint of both performance and security.

VII. Conclusion

In this paper, we describe how to design a lightweight authenticated key agreement protocol with privacy protection for SIP. To achieve both the efficiency and security requirements of SIP, we employed biometric characteristics combined with password and smartcard to construct symmetric encryption-based authentication protocol with privacy protection. Security analysis demonstrates that the proposed protocol is secure against various attacks and provides several security features especially biometric protection. Furthermore, the experimental results show that the proposed protocol reduces the computational cost significantly. Therefore, the proposed protocol is a successful authenticated key agreement protocol for SIP from the viewpoint of both security and performance.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China [grant numbers 61303237, 61272469]; the Wuhan Scientific Research Program [grant number 2013010501010144]; China Postdoctoral Fund [grant number 2012194091]; and the Fundamental Research Funds for the Central Universities [Grant number 2013199037].

REFERENCES

[1] Rosenberg J., Schulzrinne H., et al. (2002) SIP: Session Initiation Protocol. RFC 3261, June.

[2] D. Geneiatakis, C. Lambrinoudakis, and G. Kambourakis (2008) An ontology based-policy for deploying secure sip-based voip services. Computer and Security, 27(7-8): 285–297.

[3] J. Franks, P. Hallam-Baker, J. Hostetler, et al. (1999) HTTP Authentication: Basic and Digest Access Authentication. Internet Engineering Task Force, RFC 2617.

[4] H.Hakan, Kilinc, Tugrul Yanik (2013). A Survey of SIP Authentication and Key Agreement Schemes. IEEE communications surveys & tutorials, DOI: 10.1109/SURV.2013.091513.00050.

[5] T. Yanik, H. H. Kilinc, M. Sarioz, and S. S.Erdem(2008) Evaluating SIP Proxy Servers Based on Real Performance Data. SPECTS2008.

[6] Yang C, Wang R, Liu W. (2005). Secure authentication scheme for session initiation protocol. Computers & Security, 24:381-386.

[7] Jo H, Lee Y, et al. (2009). Off-line Password-Guessing Attack to Yang's and Huang's Authentication Schemes for Session Initiation Protocol. In proceedings of INC, IMS and IDC, pp. 618-621.

[8] A. Durlanik and I. Sogukpinar (2005) SIP Authentication Scheme using ECDH. Enformatika, 8:350–353.

[9] E.-J. Yoon and K.-Y. (2009) Cryptanalysis of DS-SIP Authentication Scheme Using Ecdh. In Proceedings of the 2009 International Conference on New Trends in Information and Service Science, Washington, DC, USA, pp. 642–647.

[10]L. Wu, Y. Zhang, F. Wang (2009). A new provably secure authentication and key agreement protocol for SIP using ECC. Computer Standards & Interfaces, 31(2009):286-291.

[11]EJ Yoon, KY Yoo, et al. (2010). A secure and efficient SIP authentication scheme for converged VoIP networks. Computer Communications, 33(2010): 1674-1681.

[12]R. Srinivasan, V. Vaidehi, K. Harish, K. LakshmiNarasimhan, S. LokeshwerBabu, and V. Srikanth (2005) Authentication of Signaling in VoIP Applications. In APCC, Perth, Australia, October.

[13]A. M. Nodooshan, Y. Darmani, et al. (2009) A Robust and Efficient SIP Authentication Scheme. Communications in Computer and Information Science, 6:551–558.

[14]Arshad R, Ikram N. (2013). Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. Multimedia Tools and Applications, 66(2013):165-178.

[15]Debiao He, Jianhua Chen and Yitao Chen (2012). A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography. Security and Communication Networks, 5(12):1423-1429.

[16]Qiong Pu, Jian Wang, Shuhua Wu(2013). Secure SIP authentication scheme supporting lawful interception. Security and Communication Networks. 6:340-350.

[17]E. Yoon, K. Yoo (2010). A three-factor authenticated key agreement scheme for SIP on elliptic curves. 2010 Fourth International Conference on Network and System Security, pp 334-339.

[18]Hsiu-Lien Yeh, Tien-Ho Chen, Wei-Kuan Shih (2013) Robust smart card secured authentication scheme on SIP using Elliptic Curve Cryptography. Computer Standards & Interfaces 36(2): 397-402.

[19]J. Ring, K.-K. R. Choo, E. Foo, and M. Looi, “A Ne (2006) Authentication Mechanism and Key Agreement Protocol for SIP Using Identitybased Cryptography. In AusCERT Asia Pacific Information Technology Security Conference, Gold Coast, Australia, 23 May, pp 61-72.

[20]K. Han, C. Yeun, and K. Kim (2008) Design of Secure VoIP using ID-Based Cryptosystem. In The Symposium on Cryptography and Information Security (SCIS2008), Miyazaki,Japan, Jan.22-25.

[21]F. Wang and Y. Zhang (2008). A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography. Computer Communications, 31(10):2142-2149.

[22]Xiaowei Li, Yuqing Zhang, Geifei Zhang(2012). A new certificateless authenticated key agreement protocol for SIP with different KGCs. Security and communication networks, DOI:10.1002/SEC.595

[23]C. Tao, G. Qiang, and H. Baohong (2008) A lightweight authentication scheme for session initiation protocol. In Proc. ICCCAS, pp 502-505.

[24]Jia Lun Tsai. (2009). Efficient Nonce-based authentication scheme for session initiation protocol. International Journal of Network Security, 9(1):12-16.

[25]Yoon E, Shin Y, Jeon I, Yoo K. (2010). Robust mutual authentication with a key agreement scheme for the session initiation protocol. IETE Technical Review 27(2010):203-213.

[26]Qi Xie (2012). A new authenticated key agreement for session initiation protocol. International Journal of Communication Systems, 25(1): 47-54.

[27]Muhammad Khurram Khan, Jiashu Zhang(2007). Improving the security of ‘a flexible biometrics remote user authentication scheme’, Computer Standards & Interfaces, 29(2007):82-85.

[28]Eun-Jun Yoon, Kee-Young Yoo(2013). Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. J Supercomput, 63:235-255.

[29]Xiaopeng Yan, Weiheng Li, Ping Li, Jiantao Wang, Xinhong Hao, Peng Gong(2013). A Secure Biometrics-based Authentication Scheme for Telecare Medicine Information Systems. J Med Syst, 37:9972. DOI 10.1007/s10916-013-9972-1.

[30]Chun-Ta Li, Min-Shiang Hwang (2010). An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications. 33(2010):1-5.

[31]Chin-Ling Chen, Cheng-Chi Lee, Chao-Yung Hsu(2012). Mobile device integration of a fingerprint biometric remote authentication scheme. International Journal of Communication Systems. 25:585-597.

[32]M. Chuang, M. Chen (2014). An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Systems with Applications, 41(2014):1411-1418.

[33]X. Li, J. Niu, et al. (2011). Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications. 34(2011):73-79.

[34]F. Hao, R. Anderson, and J. Daugman (2006). Combining cryptography with biometrics effectively. IEEE Transactions on Computers, 55(9):1081–1088.

[35]L. Gong, R. Needham, and R. Yahalom (1990). Reasoning about belief in cryptographic protocols. Proceedings of IEEE Computer Society Symp. Research in Security and Privacy, Oakland, CA, 7-9 May, pp 234-248.

[36]M. Burrows, M. Abadi, and R. Needham (1990). A logic of authentication. ACM Transaction on Computer Systems, 8:18-36.