A Novel Biometrics-based One-Time Commitment Authenticated Key Agreement Scheme with Privacy Protection for Mobile Network

Hongfeng Zhu, Yan Zhang, Haiyang Li, and Lin Lin
(Corresponding author: Hongfeng Zhu)

Software College & Shenyang Normal University of China
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C. 110034 - China
(Email:zhuhongfeng1978@163.com)
(Received Oct. 30, 2014; revised and accepted Jan. 16 & June 21, 2015)

Abstract

In recent years, due to the wide applications of social network and electronic business, privacy protection in the cyber world has attracted much attention. And in general, in order to solve the problems to set up a secure channel over public Internet, authenticated key agreement protocols can be adopted because it can achieve authentication of the corresponding participants and confidentiality of data transmission at the same time. Next, many authenticated key agreement protocols use various functional algorithms, such as dynamic identity and chaotic maps to achieve privacy protection. In this paper, we firstly put forward a new method to solve privacy protection problem, called One-Time Commitment, which is more efficient than One-Time Password. Then a new robust biometrics-based authenticated key agreement protocol with privacy protection using interactive hashing is given for mobile network. Our protocol has the feature of high-efficient and user friendly at the same time. Security of the protocol is based on the biometric authentication, a secure one way hash function and a pair of secure interactive hashing. Moreover the proposed protocol can not only refrain from many consuming algorithms, such as modular exponential computing, scalar multiplication on an elliptic curve, and even symmetric encryption, but is also robust to many kinds of attacks, such as replay attack, perfect forward secrecy and so on. Finally, we provide the secure proof and the efficiency analysis about our proposed scheme.

Keywords: Authentication, biometrics, interactive hashing, mobile network

1 Introduction

With the rapid development of the mobile internet related to many service providers such as stock exchanging, commodity trading, and banking, many key agreement protocols have been studied widely. However, many authentication key agreement protocols used in M-commerce are designed for cable network and consume many communication rounds and computation costs, making them unfit for mobile internet surroundings. Furthermore, M-commerce is designed to satisfy user experience, especially for security and efficiency. So the paper purposes to design an authenticated key agreement scheme for E-coupon system which can achieve high-level security, high-efficiency and user friendly at the same time.

One time password (OTP) means that the password can be used only once. Nowadays, OTP has been widely used in the financial sectors, telecommunications, online game fields and so on. As a general rule, traditional static password, for its security, can be easily stolen because of Trojan horse and keylogger program. It may also be cracked by brute force if an adversary spends enough time on it. Attackers can impersonate the legal user to communicate with the service server, and even modify the password of the legal user so that legal user cannot login the server. To address these conditions, OTP was developed as a solution. It is an approach to effectively protect the safety of the users.

Lamport [8] firstly put forward a method of user password authentication using a one way function to encode the password in 1981. Obviously, due to the higher safety request of the users, many schemes based on this

method [1, 5, 10, 12, 13, 14, 16] have been proposed. In 2000, Tang [14] proposed a strong directed OTP authentication protocol with discrete logarithm assumption. In 2010, based on the use of OTP in the context of password-authentication key exchange (PAKE), which can offer mutual authentication, session key exchange, and resistance to phishing attacks, Paterson et al. [13] proposed a general technique which allows for the secure use of pseudo randomly generated and time-dependent passwords. In 2011, Fuglerud et al. [1] proposed an accessible and secure authentication way to log in to a banking server, which used a talking mobile OTP client rather than dedicated OTP generators. Later, Li et al. [10] proposed a two-layer authentication protocol with anonymous routing on small Ad-hoc devices. In 2012, Mohan et al. [12] proposed a new method using OTP to ensure that authenticating to services, such as online shopping, was done in a very secure manner. In 2013, Huang et al. [5] proposed an effective simple OTP method that generates a unique passcode for each user. In Huang's method, OTP calculation used time stamps and sequence numbers. In addition, a two-factor authentication prototype for mobile phones using Huang's method has been used in practice for a year. In 2014, Xu et al. [16] proposed a self-updating OTP mutual authentication scheme based upon a hash chain for Ad hoc network. The updating process can be unlimited used without building a new hash chain.

However, these literatures [1, 5, 8, 10, 12, 13, 14, 16] only care about covering the password with one-time password. In fact, the identity information is equally important. Because an adversary can retrieve much useful information from the static identity by connecting with other information. From another point of view, one-time password need a hash chain can update by itself smoothly and securely through capturing the secure bit of the tip, will consume a large amount of hash computation and a lot of storage space. We can use one-time commitment (OTC) to replace the OTP for achieving the same level security, and saving much hash computation and storage space. Based on these motivations, the article presents a new simple biometrics-based one-time commitment authenticated with key agreement protocol for mobile device using interactive hashing [3] between user and server to mobile internet communication setting. Compared with previous related protocols, the proposed scheme has the following more practical advantages: (1) it firstly presents the concept of OTC. (2) it provides a kind of biometric authentication function securely [9], (3) it provides simple and robust session key agreement by adopting OTC, (4) it provides secure OTC and biometrics and password update function by using update protocol, and (5) it can decrease the total calculated amount and storage space due to the interactive hashing and XORed operation, (6) it is secure against most of well-known attacks and a high-efficiency scheme.

The organization of the article is described as follows: some preliminaries are given in Section 2. Next, a biometrics-based one-time commitment with key agreement scheme is described in Section 3. Then, the security analysis efficiency is given in Section 4 and Section 5. This paper is finally concluded in Section 6.

2 Preliminaries

2.1 One-way Hash Function

A secure cryptographic one-way hash function h: $a \rightarrow b$ has four main properties:

1) The function h takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output;

2) The function h is one-way in the sense that given a, it is easy to compute $h(a) = b$. However, given b, it is hard to compute $h^{-1}(b) = a$;

3) Given a, it is computationally infeasible to find a' such that $a' \neq a$, but $h(a') = h(a)$;

4) It is computationally infeasible to find any pair a, a' such that $a' \neq a$, but $h(a') = h(a)$.

2.2 Biometric Authentication

Each user has their unique biometric characteristics, such as voice, fingerprints, iris recognition and so on. These biometric characteristics have irreplaceable advantages: reliability, availability, non-repudiation and less cost. Therefore, biometric authentication has widely used. Figure 1 is the flow diagram of biometric characteristics collection and authentication. During the biometric collection phase, a biometric sample is collected, processed by a smart device, and stored that prepared for subsequent comparison (Figure 1). During the biometric authentication phase, the biometric system compares the stored sample with a newly captured sample (Figure 1). Obviously, smart device has powerful information confidentiality and flexible portability. When performing a biometric authentication process, a user inputs a smart device, and utilizes a simple finger touch or a glance at a camera to authenticate himself/herself [9].

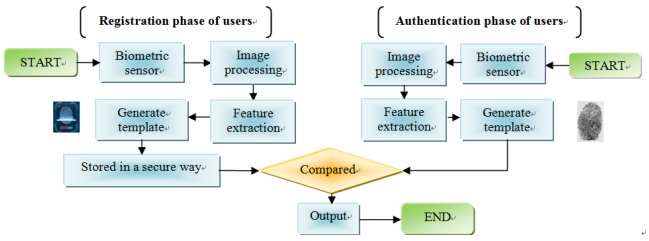

Figure 1: The flow diagram of biometric characteristics collection and authentication

2.3 Interactive Hashing

A secure cryptographic interactive hashing [3] is a major component in all known constructions of statistically hiding commitment schemes and of statistical zero-knowledge arguments based on general one-way permutations/functions.

Interactive hashing is a two-tuple $< f(), g() >$, which with respect to a one-way function f is a two-party protocol that enables a sender who knows $y = f(x)$ to transfer a random hash $z = g(y)$ to a receiver such that the sender is committed to y: the sender cannot come up with x and x' such that $f(x) \neq f(x')$, but $g(f(x)) = g(f(x')) = z$.

2.4 Protocol $NOVY\langle\overline{H}\rangle$ [2]

Definition 1. *Given a sequence of functions* $\overline{h} = (h_1, \cdots, h_s)$ *defined over* $\{0,1\}^n$, *let* $\overline{h}(x) = h_1(x) \circ \cdots \circ h_s(x)$, *where* $\circ$ *denotes string concatenation. A family of length s function sequences is called* $s-$*piece function family.*

The NOVY paradigm instantiated with an s-piece family $\overline{H}$ over strings of length n, denoted $NOVY\langle\overline{H}\rangle$. Protocol $NOVY\langle\overline{H}\rangle$ can generate the interactive hashing which can be described as follows (S: sender; R: receiver).

Common input: 1^n;

S's input: $y \in \{0,1\}^n$;

Steps:

1) R choose uniformly at random $\overline{h} = (h_1, \cdots, h_s) \in \overline{H}$.
2) Do for $i = 1$ to s:
   a. R sends h_i to S.
   b. S aborts if $(h_1, \cdots, h_s)$ is not a prefix of some element in $\overline{H}$. Otherwise, S sends $z_i = h_i(y)$ back to R.
3) R outputs $(\overline{h}, \overline{z} = (z_1, \cdots, z_s))$.

3 The Proposed Protocol

In this section, biometrics-based one-time commitment authenticated key agreement scheme is proposed which consists of three phases: the user registration phase, authenticated key agreement phase and the biometric and password update phase (because the temporary identity and the commitment are updated in every authenticated key agreement phase). But firstly some notations are given which used in the proposed scheme.

3.1 Notations

The concrete notation used hereafter is shown in Table 1.

Table 1: Notations

Symbol	Definition
Alice	A typical user
ID_A ID_S	The identity of a Alice and the server, respectively
TID_t	The temporary identity of Alice
R_A, R_S	Nonces
B	The biometric sample of Alice
τ	Predetermined threshold for biometric verification
$d()$	Symmetric parametric function
$< f(), g() >$	Interactive hashing
$E_K() / D_K()$	a pair of secure symmetric encryption/decryption functions with the key K
h	A secure one-way hash function that output length is the same length with TID_A
$\oplus$	XORed operation

3.2 User Registration Phase

Concerning the fact that the proposed scheme mainly relies on the design of one-time commitment, it is assumed that the user can register at his appointed server in some secure ways or by secure channels. Figure 2 illustrates the user registration phase.

Step 1. When Alice wants to be a new legal user, she chooses her identity ID_A at liberty, a password PW_A, and inputs her personal biometric image sample B at the mobile device. The mobile device selects a random R_{A_0} and sends $\{R_{A_0}, ID_A, h(PW_A||B)\}$ to the appointed server.

Step 2. Upon receiving the request from Alice, the server selects a random number R_{S_0} and carries out the protocol NOVY to generate the interactive hashing $< f(), g() >$. Then the server initialize the temporary identity TID_0 and computes $y_0 = f(R_{A_0}||R_{S_0})$, $Z_0 = g(y_0)$, $C_0 = h(ID_A||x) \oplus y_0 \oplus h(PW_A||B)$, $C_0' = h(y_0) \oplus h(PW_A||B)$ and sends $\{TID_{A_0}, C_0, C_0'\}$ to Alice via a secure channel. Finally, the server stores $\{TID_0, ID_A, Z_0, \langle f(), g()\rangle\}$ securely.

Step 3. Upon receiving the message $\{TID_{A_0}, C_0, C_0'\}$, the mobile device computes $E_{h(ID_A||PW_A)}(B)$ and stores $Store\{TID_0, E_{h(ID_A||PW_A)}(B), h, E_K/D_K, d(), \tau, C_0, C_0'\}$ securely, where $d()$ is a symmetric parametric function and τ is predetermined threshold for biometric authentication.

Remark: The role of the information C_0, C_0' is to protect the one-time commitment y_0, which can be recovered by the server using the long secret x.

3.3 Authenticated Key Agreement Phase

This concrete process is presented in Figure 3.

Step 1. Alice inputs ID_A, PW_A, B^* and the smart card computes $h(ID_A||PW_A)$ to decrypt $E_{h(ID_A||PW_A)}(B)$. Then verify $d(B^*, B) < \tau$. If holds, the smart card selects a random number R_{A_t} (the same length with the output of $h()$) and computes $\overline{C_t} = C_{t-1} \oplus h(PW_A||B) = H(ID_A||x) \oplus y_{t-1}$, $\overline{C_t'} = C_{t-1}' \oplus h(PW_A||B) \oplus R_{A_t} = H(y_{t-1}) \oplus R_{A_t}$,

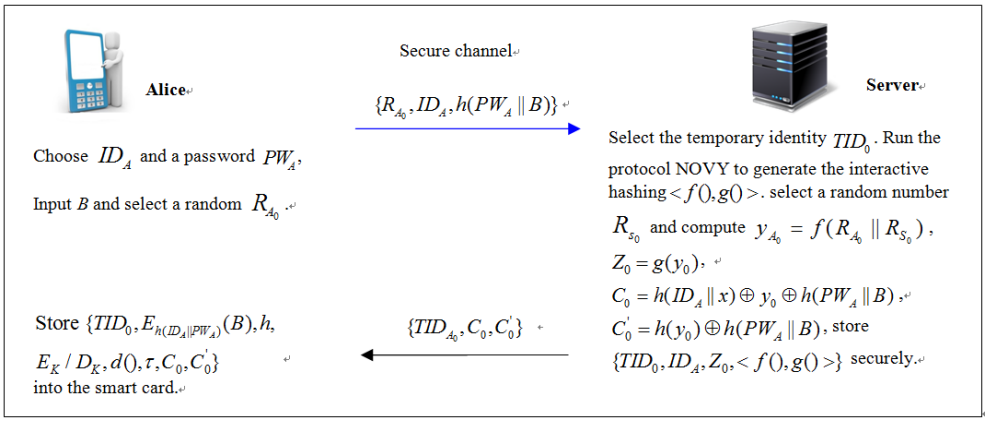

Figure 2: User registration phase

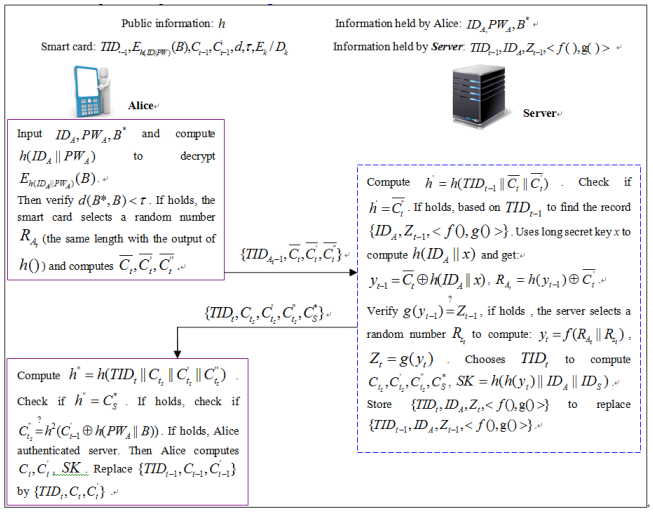

Figure 3: Authenticated key agreement phase

$\overline{C''_t} = h(TID_{t-1} || \overline{C_t} || \overline{C'_t})$ using $h(ID_A || PW_A)$. After that, the mobile device sends $\{TID_{A_t-1}, \overline{C_t}, \overline{C'_t}, \overline{C''_t}\}$ to the server.

Step 2. After receiving the message $\{TID_{A_t-1}, \overline{C_t}, \overline{C'_t}, \overline{C''_t}\}$ from Alice, the server will do the following tasks:

1) Compute $h' = h(TID_{t-1} || \overline{C_t} || \overline{C'_t})$. The server verifies whether $h' = \overline{C''_t}$ or not. If it does not hold, the server terminates it. Otherwise, the server continues to 2).
2) Using TID_{t-1} to find the record $\{ID_A, Z_{t-1}, < f(), g() >\}$. Using long secret key x to compute $h(ID_A||x)$ and get $y_{t-1} = \overline{C_t} \oplus h(ID_A||x)$, $R_{A_t} = h(y_{t-1}) \oplus \overline{C'_t}$.
3) The server verifies $g(y_{t-1}) \stackrel{?}{=} Z_{t-1}$. If it does not hold, the server terminates it. Otherwise, the server Authenticates Alice by one-time commitment and continues to 4).
4) The server selects a random number R_{S_t} to compute $y_t = f(R_{A_t}||R_{S_t})$, $Z_t = g(y_t)$. Chooses TID_t to compute $C_{t_s} = h(ID_A||x) \oplus y_t$, $C'_{t_s} = h(y_t) \oplus h^2(y_{t-1})$, $C''_{t_s} = h^3(y_{t-1})$, $C^*_S = h(TID_t||C_{t_s}||C'_{t_s}||C''_{t_s})$ and $SK = h(h(y_t)||ID_A||ID_S)$. The server stores $\{TID_t, ID_A, Z_t, < f(), g() >\}$ to replace $\{TID_{t-1}, ID_A, Z_{t-1}, < f(), g() >\}$ securely. Finally the server sends the message $\{TID_t, C_{t_s}, C'_{t_s}, C''_{t_s}, C^*_S\}$ to Alice.

Step 3. After receiving the message $C'_{t_s}, C''_{t_s}, C^*_S\}$, Alice's smart card will compute, $h'' = h(TID_t||C_{t_s}||C'_{t_s}||C''_{t_s})$ and check if $h'' = C^*_S$. If holds, check if $C''_{t_s} \stackrel{?}{=} h^2(C'_{t-1} \oplus h(PW_A|B|))$. If any one of the two equation does not hold, Alice terminates it simply. Otherwise that means Alice authenticates the server in this instance. Then Alice computes $C_t = C_{t_s} \oplus h(PW_A||B)$, $C'_t = C'_{t_s} \oplus h^2(y_{t-1}) \oplus h(PW_A||B)$ and $SK = h(h(y_t)||ID_A||ID_S)$.Replace $\{TID_{t-1}, C_{t-1}, C'_{t-1}\}$ by $\{TID_t, C_t, C'_t\}$.

3.4 The Biometric and Password Update Phase

When updating biometric or password or both of them, a significant advantage of our proposed protocol is that users achieve authentication and updating information with smart card locally without exchanging any message with the server, which can save much calculated amount and communication traffic. Because the server only stores the user's one-time commitment with some identities. Moreover, any adversary cannot carry out off-line dictionary/guessing attacks with stolen mobile device attacks, because all the authenticated information has been encrypted in the smart card. Figure 4 illustrates biometrics and password update phase.

Step 1. Alice inputs her smart card into a smart card reader, opens the password and biometrics changing

software, starts the biosensor, imprints his/her new biometric. And then Alice inputs ID_A, PW_A, then the smart card computes $h(ID_A||PW_A)$ to decrypt $E_{h(ID_A||PW_A)}(B)$. Then verify $d(B^*, B) < \tau$. If it holds, an accept response is given to Alice. Next, we describe the changing phase in the following three cases.

Step 2. (Case 1): Only changing the password.
Alice inputs her new password PW_A^{new}. The smart card computes $T_{emp} = h(PW_A||B) \oplus h(PW_A^{new}||B)$, $C_t^{new} = C_t \oplus T_{emp}$, $C_t'^{new} = C_t' \oplus T_{emp}$. Replaces $\{C_t, C_t'\}$ by $\{C_t^{new}, C_t'^{new}\}$ and $E_{h(ID_A||PW_A)}(B)$ by $E_{h(ID_A||PW_A^{new})}(B)$ into it.

Step 2. (Case 2): Only changing the biometrics.
Alice inputs her new biometrics B^{new}. The smart card computes $T_{emp} = h(PW_A||B) \oplus h(PW_A||B^{new})$, $C_t^{new} = C_t \oplus T_{emp}$, $C_t'^{new} = C_t' \oplus T_{emp}$. Replaces $\{C_t, C_t'\}$ by $\{C_t^{new}, C_t'^{new}\}$ and $E_{h(ID_A||PW_A)}(B)$ by $E_{h(ID_A||PW_A)}(B^{new})$ into it.

Step 2. (Case 3): Changing the password and biometrics.
Alice inputs her new biometrics B^{new} and new password PW_A^{new}.The smart card automatically computes $T_{emp} = h(PW_A||B) \oplus h(PW_A^{new}||B^{new})$, $C_t^{new} = C_t \oplus T_{emp}$, $C_t'^{new} = C_t' \oplus T_{emp}$.Replaces $\{C_t, C_t'\}$ by $\{C_t^{new}, C_t'^{new}\}$ and $E_{h(ID_A||PW_A)}(B)$ by $E_{h(ID_A||PW_A^{new})}(B^{new})$ into it.

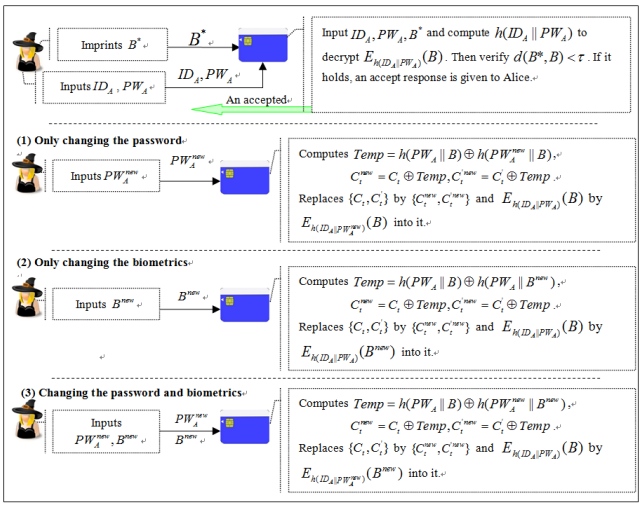

Figure 4: The biometric and password update phase

4 Security Consideration

The section analyzes the security of our proposed protocol. The structure of analysis security just sees the

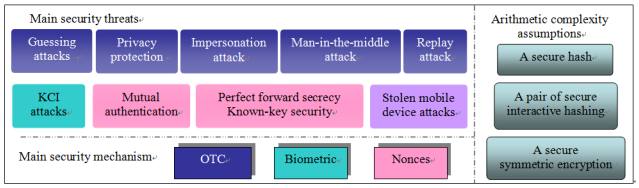

Figure 5: The biometric and password update phase

Figure 5. Let us assume that there are three secure components, including a secure one-way hash function, a secure symmetric encryption and a pair of secure interactive hashing. Assume that the adversary has fully control over the insecure channel including eavesdropping, recording, intercepting, modifying the transmitted messages. The definitions and analysis of the security requirements [15] will be illustrated as follows:

- Security threats can be wiped out owing to shift static identity to dynamic identity with OTC.

  1) Off-line dictionary/guessing attacks.
  In an off-line dictionary/guessing attack, an attacker random chooses a word from a dictionary or guesses a password and verifies his choose or guess, but he does not need to participate in any communication phase because he has already downloaded the necessary information.
  In our proposed scheme of the authenticated key exchange phase, the off-line dictionary/guessing attack will not affect, because there are multiple variables involved in the transmission messages, which are all encrypted, such as $\overline{C_t}, \overline{C_t'}, \overline{C_t''}$ and $C_{t_s}, C_{t_s}', C_{t_s}'', C_S^*$. The adversary cannot get a function that views the password as the unique input during the transmission. Therefore, the proposed scheme can resist guessing attacks.

  2) Privacy protection.
  Our proposed protocol can protect user's privacy because we firstly adopt the dynamic identity. For example, the messages $\{TID_{A_{t-1}}\overline{C_t}, \overline{C_t'}, \overline{C_t''}\}$, there are two kinds of information: one is a temporary identity used only once, the other are some cipher texts. So an adversary cannot get any useful information about users or the server during the transmitting procedure. And for other transmitted messages, there are also no useful information about users or the server. Therefore, the proposed scheme can provide privacy protection.

  3) Impersonation attack.
  impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.
  An adversary cannot impersonate anyone of the user or the server. First of all, owing to

adopt dynamic identity idea, an adversary cannot launch an impersonation attack because he doesn't know the identity of the user at all. Even if the adversary eavesdropping on the line year by year, he gets the temporary identities which are nothing but some random numbers.

Even if the adversary gets the real identity of a user in a certain way (such as social engineering), he also cannot launch an impersonation attack. Because the users and the server all choose the random numbers (RS_t, R_{A_t}) to protect sensitive information and keep messages fresh, there is no way for an adversary to have a chance to carry out impersonation attack.

4) Man-in-the-middle attack.
The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

First of all, an adversary cannot launch a man-in-the-middle attack because he doesn't know the identity of the user. The adversary doesn't know how to become the middle man between the two hiding men.

Even if the adversary get the real identity of a user in a certain way (such as social engineering), and he also cannot launch a man-in-the-middle attack. Because $\overline{C_t}, \overline{C'_t}, \overline{C''_t}$ and $C_{t_s}, C'_{t_s}, C''_{t_s}, C^*_S$ contain the secret one-time commitment and the nonce, a man-in-the-middle attack cannot succeed.

5) Replay attack.
A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. Any replay attack cannot be carried out, because the temporary identity can be used only once.

- Immune to the security threats owing to adopt biometrics authentication.

6) Key Compromise Impersonation Attacks (KCI attacks).
An adversary is said to impersonate a party B to another party A if B is honest and the protocol instance at A accepts the session with B as one of the session peers but there exists no such partnered instance at B [6]. In a successful KCI attack, an adversary with the knowledge of the long-term private key of a party A can impersonate B to A.

Our protocol adopts two factors to authenticate legal user, even if the close friend gets the Alice's password, he/she cannot pass the authentication because the mobile device authenticated user also by user's personal biometric image sample B, the key compromise impersonation attacks will fail.

- Resist the security threat owing by nonce.

7) Mutual authentication.
Mutual authentication refers to two parties authenticating each other suitably and simultaneously.

If $g(y_{t-1})$ equals Z_{t-1}, which means that Alice was already authenticated by the server. Because only the server can retrieve the user's random number and one-time commitment by long secret x. If C''_{t_s} equals $h^2(C'_{t-1} \oplus h(PW_A||B))$, which means that the server was already authenticated by Alice. Because only the user can retrieve the $h(y_{t-1})$ by the $h(ID_A||PW_A)$.

8) Perfect forward secrecy.
An authenticated multiple key establishment protocol provides perfect forward secrecy if the compromise of both the node's secret keys cannot results in the compromise of previously established session keys.

Because there are only two kinds of information during the transmitting procedure: one is a temporary identity used only once, the other are some cipher texts. The above information is useless for adversary. Next, the session key $SK = h(h(y_t)||ID_A||ID_S)$ including $\{R_{A_t}, R_{S_t}\}$ which are random chosen by Alice and the server. So the adversary cannot previously obtain the next established session key.

9) Known-key security.
A protocol can protect the subsequent session keys from disclosing even if the previous session keys are intercepted by the adversaries, what will not affect other session keys is called known-key security. As $\{R_{A_t}, R_{S_t}\}$ are independent and different in all sessions, if an adversary knows a session key $SK = h(h(y_t)||ID_A||ID_S)$ and a pair random $\{R_{A_t}, R_{S_t}\}$, she cannot compute the previous and the future session keys without knowing the previous and the future $\{R_{A_t}, R_{S_t}\}$. Therefore, our proposed protocol can realize known-key secrecy and session key secrecy.

- Other security analysis.

10) Stolen mobile device attacks.
Anyone gets the mobile device in some way to execute some kinds of attacks.

It is very clear that the proposed scheme provides biometrics authentication. Any adversary cannot carry out stolen mobile device attacks, because the information of biometric verification is encrypted by $h(ID_A||PW_A)$ in the smart

Table 2: Security comparisons between our scheme and related scheme

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11
Zhu et al. [19]	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Yoon et al. [18]	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Xu et al. [17]	Yes	Yes	Yes	Yes	Yes	Null	Yes	Yes	Yes	Yes	--
Our scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

S1: Perfect forward secrecy; S2: known-key secrecy; S3: Mutual authentication ; S4: Key agreement; S5: Secure password/biometrics update; S6: KCI attack; S7: Resist Password guessing attack; S8: Resist replay attack; S9: Resist impersonation attack; S10: Man-in-the-middle attack; S11: Stolen mobile device attack
--:Not mentioned Yes/No: Support/Not support the security Null: Not involve

Table 3: Comparisons between the related protocols and our proposed protocol

	[19](2015)	[18] (2013)	[17] (2014)	Our scheme
Efficiency	CM-based	ECC-based	Hash Chain-based	Interactive Hashing-based
	√ √	√	√ √ √	√ √ √ √
Total computation				
Reg	$3h$	$2h$	$(N+1)h$	$2h+1S+2Ih$
Auth	$5CM+12h+8S$	$17h+4ECC$	$8h$	$15h+1S+3Ih$
Update	$2h$	$2h$	$(N+1)h$	$2h+2S$
Communication-rounds				
Reg	2	2	3	2
Auth	5	5	4	2
Update	3	3	3	3
Privacy protection	×	×	√	√ √ √ √
No need exchanging with server during updating phase	√ √	√ √	*N/A*	√ √ √ √

×: Weak; √: Ordinary; √ √: Good; √ √ √: Very Good; √ √ √ √: Excellent. *N/A* not applicable
S: Symmetric encryption, *ECC*: multiplications, *CM*: chaotic maps, *h*: hash, *Ih*: Interactive Hashing, *Reg*: registration phase, *Auth*: authentication phase, *Update*: update phase

card. Therefore, the proposed scheme can resist stolen mobile device attacks.

According to all of above, we can prove that the proposed scheme is secure. Table 2 shows the security comparisons between our scheme and related scheme.

5 Efficiency Analysis

In this section, we analyze the efficiency of our proposed scheme. According to the required operations for different entities, Table 3 summarizes the communication costs of our proposed scheme and related schemes in different phases.

To be more precise, on an Intel Pentium4 2600 MHz processor with 1024 MB RAM, where N and P are 1024 bits long, the computational time of a one-way hashing operation, a symmetric encryption/decryption operation, an elliptic curve point multiplication operation and Chebyshev polynomial operation is 0.0005s, 0.0087s, 0.063075s and 0.02102s separately [4, 7, 11]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations. The computational time of a Interactive Hashing is close to a one-way hashing operation [3].

Table 3 compares the functionalities and system efficiency of our proposed protocol and the others, related schemes [17, 18, 19]. The results of the comparisons show that our proposed scheme provides more functionalities, and is more suit for user-friendliness system.

As for storage space, our proposed scheme will save much storage space contrasting with one-time password by hash chain. For example, a hash chain needs 62.5K (assume $p_t = 128bits$, and $N = 500$) to store. And our proposed scheme only needs some random identity, encrypted data and some algorithms which can be ignored contrasting with one-time password.

6 Conclusion

The paper proposed a novel and complete biometrics-based and one-time commitment authentication scheme for mobile network. There are many advantages about our protocol which described as follows: Firstly, from the standpoint of a security analysis, our scheme uses biometrics method, dynamic ID, dynamic commitment or called one-time commitment to achieve high-level security. Then, along with OTC, we insert the dynamic ID which can consume the almost negligible computations, communications and size of memory. Compared with one-time password method, our OTC method eliminates hash chain algorithm, which can drastically reduce the computation of hash chain and the storage space of hash values. Next, the core ideas of the proposed scheme are the features of security and efficiency in the mobile device and servers side, and the feature of user friendly for the users side. Finally, through comparing with recent related work, our

proposed scheme has satisfactory security, efficiency and functionality. Therefore, our protocol is more suitable for practical applications.

References

[1] K. Fuglerud and O. Dale, "Secure and inclusive authentication with a talking mobile one-time-password client," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 27-34, 2011.

[2] I. Haitner, O. Horvitz, J. Katz, C. Koo, R. Morselli, R. Shaltiel, "Reducing complexity assumptions for statistically hiding commitment," *Journal of Cryptology*, vol. 22, no. 3, pp. 283–310, 2009.

[3] I. Haitner, O. Reingold, "A new interactive hashing theorem," *Journal of Cryptology*, vol. 27, no. 1, pp. 109–38, 2013.

[4] W. Hsieh W, J. Leu, "Anonymous authentication protocol based on elliptic curve Diffie-Hellman for wireless access networks," *Wireless Communications and Mobile Computing*, vol. 14, no. 10, pp. 995–1006, 2014.

[5] Y. Huang, Z. Huang, H. R. Zhao and X. J. Lai, "A new one-time password method," in *Informational Conference on Electronic Engineering and Computer Science*, pp. 32–37, 2013.

[6] J. Katz, J. S. Shin, "Modeling insider attacks on group key-exchange protocols," in *Proceedings of the 12th ACM Conference on Computer and Communications Security (CS'05)*, pp. 180–189, 2005.

[7] L. Kocarev, S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications*, pp.53–54, Springer, 2011.

[8] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[9] C. T. Li, M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.

[10] C. T. Li and M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless Ad Hoc networks," *Information Sciences*, vol. 181, no. 23, pp. 5333–5347, 2011.

[11] C. T. Li, M. S. Hwang, and Y. Chung, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular adhoc networks," *Computer Communication*, vol. 31, pp. 2803–2814, 2008.

[12] R. Mohan and N. Partheeban, "Secure multimodal mobile authentication using one time password," *International Journal of Recent Technology and Engineering*, vol. 1, no. 1, pp. 131–136, 2012.

[13] K. G. Paterson, G. Kenneth and D. Stebila, "One-time password authenticated key exchange," in *Proceedings of 15th Australasian Conference on Information Security and Privacy*, pp. 264–281, 2010.

[14] S. H. Tang, "Directed one-time password authentication scheme based upon discrete logarithm," *Journal of Circuits, Systems and Computes*, vol. 10, no. 3, pp. 173–180, 2000.

[15] B. Wang, M. Ma, "A smart card based efficient and secured multi-server authentication scheme," *Wireless Personal Communications*, vol. 68, no. 2, pp. 361–378, 2013.

[16] F. Xu, X. Lv, Q. Zhou and X. Liu, "Self-updating one-time password authentication protocol for adhoc network," *Transactions on Internet and Information Systems*, vol. 8, no. 5, pp. 1817–1827, 2014.

[17] F. Xu, X. Lv, Qi Zhou and X. Liu, "Self-updating one-time password mutual authentication protocol for ad hoc network," *Transactions on Internet and Information Systems*, vol. 8, no. 5, pp. 1817–1827, 2014.

[18] E. J. Yoon, K. Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *The Journal of Supercomputing*, vol. 63, no. 1, pp. 235–255, 2013.

[19] H. Zhu, X. Hao, Y. Zhang and M. Jiang, "A Biometrics-based Multi-server Key Agreement Scheme on Chaotic Maps Cryptosystem," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 2, pp. 211–224, 2015.

Hongfeng Zhu obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hongfeng Zhu is a full associate professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Dr. Zhu had published more than 50 international journal and international conference papers on the above research fields.

Yan Zhang 23 years old, an undergraduate from Shenyang Normal University, major in information security management. In the four years of college, after completing her studies, she enjoys reading the book related to this major. Under the guidance of the teacher, she has published two articles in EI journals.

Haiyang Lee graduate, graduated from Liaoning University Population Research Institute, Master demographic now at Shenyang Normal University Dean's Office Examination Management Division, lecturers title. He researches on labor and social security, wireless computer networks, network security.

Lin Lin graduate, graduated from School of Educational Technology, Shenyang Normal University, Research Associate. She concerns social security, wireless computer networks and network security.