

A secure authentication scheme based on fuzzy extractor

Lihua Zhang^{1*}, Yaoping Nie²

¹*School of Electrical and electronic engineering, East China Jiaotong University, Nanchang, China*

²*School of Electronic Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai, China*

Received 1 October 2014, www.cmmt.lv

Abstract

The biometrics-based authentication schemes are more security and reliable than the traditional authentication schemes, and it is the inevitable trend of future development. However, between the existing schemes, the security of user's biometric template usually be ignored, the user's information security suffering from a great threat because of that. Recently, Yan et al. proposed a secure biometrics-based authentication scheme for telecare medicine information systems (TMIS), however, we found that Yan et al.'s scheme could not ensure the security of the user's biometric template and forward security. To overcome the above weaknesses, in this paper, a security enhanced scheme combine with the characteristics of the Fuzzy Extractor is proposed. Security and performance analyses show that the proposed scheme not only could overcome the weaknesses in Yan et al.'s scheme but also has a better practicability. We also propose the scheme with a formal security proof under the random oracle mode.

Keywords: Fuzzy Extractor, biometric, authentication, template security

1 Introduction

After Lamport [1] proposed the first authentication scheme to provide mutual authentication between the user and the server, many kinds of authentication schemes were proposed to improve security and performance of the authentication, such as password-based or smartcard-based schemes. However, as we all know, the biometrics-based authentication schemes are more security and convenient than the traditional authentication schemes. Besides, the biometrics-based authentication schemes are the inevitable trend of future development and will occupy an important position in the future. Unlike password, biometric template is not easy to be stolen or forgot and it does not need to be remembered by user. Compared with the smart card, biometric template does not need to be carried deliberately and can avoid the risk of losing smart card. However, there are still some problems in biometrics-based schemes. Firstly, each extraction of user's biometrics may be different because of the impact of environment. But some proposed schemes [2-5] have ignored the above problem. Due to the user's biometrics involve personal privacy and are uniqueness, losing any of those messages will cause a serious consequence. Thus the biometrics-based schemes must avoid that situation occurs. Secondly, when the biometrics transmits on the network, it may be faced with the danger of being stolen or manipulated [6]. Thirdly, the biometric template which stored in the database template or smart card may be attacked and stolen, i.e. scheme [7] proposed a method that can reconstruct the original biological image from the database template. In a remote biometrics-based authentication system, the security of the biometric template is a key issue but vulnerable. However, it was usually ignored in some proposed schemes [8-10]. If

the smart card which stored biometric template is lost or stolen and be compromised by some technology, the security of biometrics of user will be in danger and the lost unique biometrics cannot continue to be used.

In 2009 Yang et al. [11] suggested that the usages of biometrics in previous schemes are limited and superficial. And they also proposed a password authentication scheme using Fuzzy Extractor with smart card. They claimed that it is the first scheme which tightly combined with password authentication and biometrics. However, Duan et al. [12] found that Yang et al.'s scheme unable to withstand the masquerade attack. But their scheme could not withstand the insider attack.

In 2013 Tan et al. [4] proposed an efficient biometrics-based authentication scheme for telecare medicine information systems and claimed their scheme could withstand all kinds of attacks. Later, Yan et al. [8] demonstrated that Tan et al.'s scheme was vulnerable to the Denial-of-Service attack. To solve that problem, Yan et al. proposed a secure biometrics-based authentication scheme and claimed their scheme not only could overcome weakness in Tan et al.'s scheme but also has a better performance.

Unfortunately, although Yan et al.'s scheme could withstand the Denial-of-Service attack, their scheme could not ensure the security of user's biometric template which is very important. Besides, Yan et al.'s scheme could not ensure forward security when the session key is missing. The biometrics technique that used in Tan et al.'s scheme and Yang et al.'s scheme is Fuzzy Extractor [13-16]. The authentication schemes that using Fuzzy Extractor has some advantages such as lower complexity, lower cost computation, lower communication complexity and quantity. Thus it is the most promising technique in bio-

*Corresponding author's e-mail:lhzhangbuaa@163.com

metrics-based authentication [12]. Based on the above theories, a secure biometrics-based authentication scheme using Fuzzy Extractor is proposed to overcome the weakness in Yan et al.'s scheme. In this paper, the characteristic of the Fuzzy Extractor which could hide user's biometrics is used to avoid Yan et al.'s risk of losing biometric template, and protect the privacy and security of the user's biometrics information. In other words, the proposed scheme could overcome the above problems of previous biometrics-based authentication schemes radically and be applied to many kinds of fields such as TMIS, wireless sensor networks (WSN) or mobile payment. Besides, the scheme can also allow the lost unique biometrics continue to be used. The formal security proof and performance analyses show that the proposed scheme is security and has a better practicability.

Generally speaking, an ideal password authentication scheme should and must withstand all kinds of attacks. However, it should also achieve the following security goals [17]:

- G0. Biometric template is security.
- G1. Feasible biometrics verification.
- G2. Hide biometrics.
- G3. Reusable biometrics.
- G4. No verification table.
- G5. Password dependent.
- G6. Freely chosen password by the users.
- G7. No password reveal.
- G8. Mutual authentication.
- G9. Session key agreement.
- G10. Smart card revocation.
- G11. Forward security.

The rest of this paper is organized as follows. Yan's scheme is introduced and analyzed in Section 2. Our new proposed scheme is described in Section 3. A formal security proof under the random oracle mode is given in Section 4. Security analyses and performance analyses are

discussed in Section 5 and Section 6, respectively. Finally, a conclusion is given in Section 7.

2 Review of Yan's scheme

In this section, we review Yan's scheme in brief. For convenience, the notations that will be used are summarized in Table 1.

TABLE 1 Notations

Notation	Description	Notation	Description
S	Remote serve	$h(g)$	One-way hash function
U_i	i -th user	PW_i	U_i 's Password
ID_i	U_i 's identity	PW_i'	New password
B_i	Registered biometrics	p, q	Two large coprime numbers
B_i^*	Imprinted biometrics	Z_q^*, Z_p^*	p -order or q -order group
B_i'	Updated biometrics	\oplus	Bitwise XOR computation
x	Secret value of S	P	Concatenation operation

Yan's scheme composed of four phases, and a detailed description is given below.

2.1 THE REGISTRATION PHASE

The Registration Phase and others of Yan et al.'s scheme is shown in Figure 1.

- 1) U_i chooses his identity ID_i , PW_i and a random number N_i , imprints his biometrics B_i . Then, U_i computes $\overline{PW}_i = h(ID_i || PW_i || B_i || N_i)$ and sends ID_i and \overline{PW}_i to S through a secure channel;
- 2) S computes $X_i = h(ID_i || x)$, $Y_i = X_i \oplus h(\overline{PW}_i)$ and stores Y_i and $h(\bullet)$ into a smart card;
- 3) U_i inputs $\{N_i, B_i\}$ into the smart card.

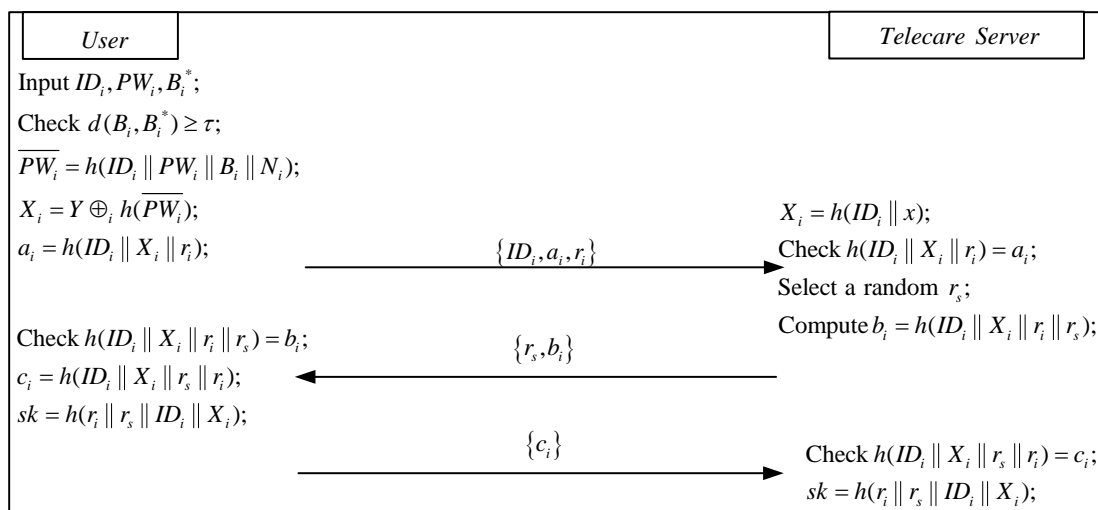


FIGURE 1 Yan et al.'s scheme

2.2 THE LOGIN PHASE

- 1) U_i inputs ID_i , PW_i and imprints B_i^* at the sensor;
- 2) The smart card compares B_i^* with B_i . If the inequality $d(B_i, B_i^*) \geq \tau$ is correct, the smart card stops the session;
- 3) The smart card generates a random number r_i and computes $\overline{PW}_i = h(ID_i \| PW_i \| B_i \| N_i)$, $X_i = Y_i \oplus h(\overline{PW}_i)$ and $a_i = h(ID_i \| X_i \| r_i)$. Then, U_i sends $\{ID_i, a_i, r_i\}$ to S .

2.3 THE AUTHENTICATION AND KEY AGREEMENT PHASE

- 1) S computes $X_i = h(ID_i \| x)$, computes and checks whether $h(ID_i \| X_i \| r_i) = a_i$ is correct. Then, S generates a random number r_s and computes $b_i = h(ID_i \| X_i \| r_i \| r_s)$ and sends $\{r_s, b_i\}$ to U_i ;
- 2) U_i 's smart card computes and checks the function $h(ID_i \| X_i \| r_i \| r_s) = b_i$, and computes $c_i = h(ID_i \| X_i \| r_s \| r_i)$ and $sk = h(r_i \| r_s \| ID_i \| X_i)$. Then, U_i sends $\{c_i\}$ to S ;
- 3) S computes and checks $h(ID_i \| X_i \| r_s \| r_i) = c_i$. Then, S computes $sk = h(r_i \| r_s \| ID_i \| X_i)$.

2.4 THE PASSWORD AND BIOMETRICS UPDATE PHASE

- 1) U_i inserts his smart card into a card reader, inputs his ID_i , old PW_i and B_i^* . U_i compares B_i^* with B_i ;
 - 2) U_i generates a new random number N_i' , a new password PW_i' and imprints a new biometrics B_i' ;
 - 3) U_i computes $\overline{PW}_i = h(ID_i \| PW_i \| B_i \| N_i)$ and $\overline{PW}_i' = h(ID_i \| PW_i' \| B_i' \| N_i')$, $Y_i' = Y_i \oplus h(\overline{PW}_i) \oplus h(\overline{PW}_i')$.
- Finally, the smart card replaces N_i , B_i and Y_i with N_i' , B_i' and Y_i' separately.

2.5 WEAKNESS OF YAN ET AL.'S SCHEME

In the registration phase of Yan et al.'s scheme, U_i compares the imprinted biometrics B_i^* with the stored biometric template B_i by checking the in equation

$d(B_i, B_i^*) \geq \tau$. It is to be noted that the biometric template B_i , which stored in smart card without any protection, measures is easy to be attacked. Though Yan et al.'s scheme overcame Tan et al.'s weakness, their scheme could not ensure the security of biometric template B_i . If an adversary illegally obtained user's smart card and analyzed it by some technology, he could get the stored biometric template B_i without difficulty. Once the stored biometric template B_i is revealed, the security of the scheme only depends on the strength of password. However, as we all know, getting the password by offline guessing is not difficult. After that, the adversary could impersonate the legitimate user to communicate with the Server S . Besides, due to the uniqueness of the biometrics, the losing biometrics could not be used anymore, and the loss is considerable for the user. In addition, a secure scheme should be capable to provide the forward security even if the smart card or system's secret key was lost or stolen. In cryptography, the forward security is a property of key-agreement protocols ensuring that previously generated session key cannot be compromised even if system's secret key has been compromised [18]. But, Tan et al.'s scheme cannot ensure the security of session key in the case of system's secret key has been compromised. Put another way, Tan et al.'s scheme cannot provide the forward security. For instance, if an adversary steals the server's secret key x he can work out $X_i = h(ID_i \| x)$. Due to the session key $sk = h(r_i \| r_s \| ID_i \| X_i)$, the adversary can get the random numbers r_s and r_i by eavesdropping the communication parties involved in the authentication process, then he could compute any previous session key sk . Therefore, we say that Yan's scheme could not ensure the security of the user's biometric template and forward security.

3 The proposed scheme

In order to overcome the weaknesses in Yan et al.'s scheme, we propose an improved scheme based on the characteristics of the Fuzzy Extractor. The proposed scheme composed of four phases, that is the registration phase, the login phase, the authentication and key agreement phase and the password and biometrics update phase. The mutual authentication between U_i and S is shown in Figure 2, and a detailed description is given below.

3.1 FUZZY EXTRACTOR

According the descriptions in schemes [11,12], a brief description of Fuzzy Extractor is given as follows.

Fuzzy Extractor consists of a pair of randomized procedures, namely procedure "generate" (*Gen*) and proce-

procedure “reproduce” (*Rep*). In this scheme, the generation procedure *Gen* on input biometrics *B* outputs an extracted random and uniform string $R \in \{0,1\}^l$ as a biometrics key and a help string $P \in \{0,1\}^m$ as a public information, $Gen(B) \rightarrow (R, P)$. The reproduce procedure *Rep* takes the biometrics B^* and public information *P* as inputs. If the

inequality $d(B^*, B) < \tau$ is correct, the reproduce procedure *Rep* will generate the biometrics key *R*, $Rep(B^*, P) \rightarrow R$. As it is known, the biometrics cannot always be completely equal because of the change of the environment. Nevertheless, this problem can be overcome by using the Fuzzy Extractor.

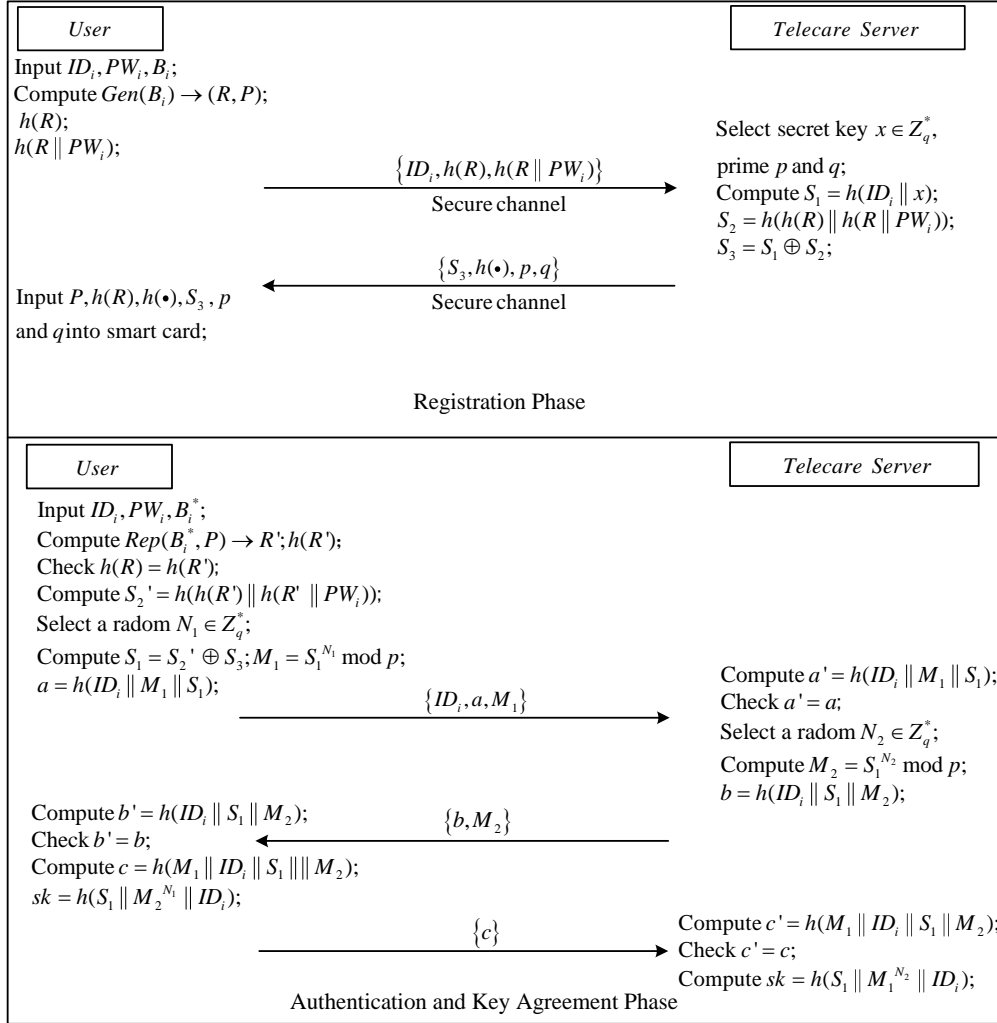


FIGURE 2 The proposed scheme

3.2 THE REGISTRATION PHASE

The Registration Phase of the proposed scheme is consists of three steps.

- 1) U_i choose his identity ID_i , password PW_i and imprints his biometrics information B_i . Then, the generation procedure *Gen* computes $Gen(B_i) \rightarrow (R, P)$, smart card computes $h(R)$ and $h(R \parallel PW_i)$. U_i send message $M_1 = \{ID_i, h(R), h(R \parallel PW_i)\}$ to *S* through a secure channel.

- 2) Upon receiving the message M_1 , *S* chooses a random number x as the secret key and two prime number p and q . Then *S* computes $S_1 = h(ID_i \parallel x)$, $S_2 = h(h(R) \parallel h(R \parallel PW_i))$, $S_3 = S_1 \oplus S_2$ and stores message $M_2 = \{S_3, h(\bullet), p, q\}$ into a smart card. Then, *S* issues it to U_i through a secure channel.
- 3) Upon receiving the smart card, U_i inputs $\{S_3, h(\bullet), h(R), P, p, q\}$ into it. The Registration Phase and others of the proposed scheme is shown in Figure 2.

3.3 THE LOGIN PHASE

- 1) U_i insert his smart card into a card reader and inputs his ID_i , PW_i and imprints biometrics B_i^* at the sensor.
- 2) The reproduce procedure Rep will generate the biometrics key R' , $Rep(B^*, P) \rightarrow R'$. If the function $h(R) = h(R')$ is incorrect, the smart card stops the session, otherwise computes $S_2' = h(h(R') || h(R' || PW_i))$ and $S_1 = S_2' \oplus S_3$.
- 3) The smart card generates a random number $N_1 \in Z_q^*$ and computes $M_1 = S_1^{N_1} \bmod p$, $a = h(ID_i || M_1 || S_1)$. Then, U_i send message $M_3 = \{ID_i, a, M_1\}$ to S through a public channel.

3.4 THE AUTHENTICATION AND KEY AGREEMENT PHASE

A session key for future communications is also generated in this phase.

- 1) Upon receiving the message M_3 , S computes $a' = h(ID_i || M_1 || S_1)$ and checks whether $a' = a$ is correct. Then, S generates a random number $N_2 \in Z_q^*$ and computes $M_2 = S_1^{N_2} \bmod p$ and sends message $M_4 = \{b, M_2\}$ to U_i through a public channel.
- 2) Upon receiving the message M_4 , U_i 's smart card computes $b' = h(ID_i || S_1 || M_2)$ and checks whether $b' = b$ is correct. Then, the smart card computes $c = h(M_1 || ID_i || S_1 || M_2)$ and the session key $sk = h(S_1 || M_2^{N_1} || ID_i)$. Finally, U_i sends message $M_5 = \{c\}$ to S through a public channel.
- 3) **Upon receiving the message M_5 , S computes $c' = h(M_1 || ID_i || S_1 || M_2)$ and checks whether $c' = c$ is correct. Then, S computes the session key $sk = h(S_1 || M_1^{N_2} || ID_i)$.**

3.5 THE PASSWORD AND BIOMETRICS UPDATE PHASE

It is noteworthy that the string R that generated by the generation procedure Gen is random and uniform, $Gen(B) \rightarrow (R, P)$. Thus, the results of string R which generated from same biometrics in different calculation times are different. In that case, the biometrics can be reused by updating, but without reducing the user's security, even if the string R is revealed or the smart card is lost. Therefore, the proposed scheme can solve an important but tough problem that the lost unique bio-

metrics cannot continue to be used. User U_i could update his own password and biometrics by following steps.

- 1) U_i inserts his smart card into a card reader and inputs his ID_i , old PW_i and B_i^* . And the reproduce procedure Rep will generate the biometrics key R' , $Rep(B^*, P) \rightarrow R'$, smart card computes and checks the function $h(R) = h(R')$ is correct or not, then computes $S_2' = h(h(R') || h(R' || PW_i))$, $S_1 = S_2' \oplus S_3$.
- 2) U_i inputs new PW_i' and B_i' , Gen computes $Gen(B_i') \rightarrow (R_N, P_N)$, and smart card computes $h(R_N)$, $h(R_N || PW_i')$, $S_2'' = h(h(R_N) || h(R_N || PW_i'))$ and $S_3' = S_2'' \oplus S_1$.
- 3) The smart card replace S_3 , $h(R)$ and P with S_3' , $h(R_N)$ and P_N , separately.

4 Security proof

In this section, we introduce a formal security proof for the improved scheme under the random oracle mode which is mainly adopted from scheme [19].

4.1 SECURITY MODEL

We first formally define the special security requirements of the proposed scheme before the proof.

In this scheme each participant is an user $U \in \text{User}$ or a server $S \in \text{Server}$. The server S holds a private key x and each user U holds a password PW , P and $h(R)$ etc. The interaction between the adversary \mathcal{A} and the protocol participants occurs only via oracle queries. In the random oracle mode, the adversary owns capabilities in a real attack. Let P^i denote the instance of a participant P , where P is a user or a server. Protocol's security is defined as a two-stage game which performs between the participant P^i and the adversary \mathcal{A} . In the first stage, all possible oracle queries are listed in the following:

$Send(P^i, m)$: This query model simulates an active attack. The adversary sends message m to P^i , then P^i outputs the corresponding message and sends it back to \mathcal{A} .

$Reveal(P^i)$: This query model simulates the misuse of session keys. Upon receiving a query from adversary \mathcal{A} , P^i returns the session key back to \mathcal{A} .

$Corrupt(U^i, a)$: This query model simulates corruption capabilities of the adversary. The outputs of P^i depends on the value of a . If $a = 0$, P^i outputs the password of U_i . If $a = 1$, P^i outputs the messages that stored in the smart card.

After querying above query models several times, the adversary \mathcal{A} could stop the first stage and choose a fresh oracle P^i and start the second stage. The fresh oracle is defined as follows.

Definition 1: An instance P^i is fresh if it meets the following conditions:

- 1) P^i has accepted;
- 2) No *Reveal* queries have been made to P^i or its partner;
- 3) If P^i is a user U^i , strictly less than two *Corrupt* queries have been made to P^i . Else if P^i is a server S^j , strictly less than two *Corrupt* queries have been made to its partner U^i .

In second stage, the adversary \mathcal{A} queries the *Test* model of the fresh Oracle P^i .

Test(P^i): This query model is used to define session key's semantic security. The adversary \mathcal{A} can query the *Corrupt* model of an oracle P^i at any time, which oracle had been accepted but never been queried the *Corrupt* model or *Reveal* model. After querying the oracle, P^i will select a random bit b . If $b=1$, P^i will send its session key back to adversary \mathcal{A} ; otherwise P^i sends back a random number with the same length of session key. However, this query can be queried only once.

Upon receiving the message sent from P^i , adversary \mathcal{A} guesses its value and uses b' instead of it. If $b'=b$, we say the adversary \mathcal{A} wins this game. And the advantage of \mathcal{A} in violating the semantic security of the protocol L is defined to be $Adv_L(\mathcal{A}) = 2Pr[Succ(\mathcal{A})] - 1$. $Succ(\mathcal{A})$ represents the event that adversary \mathcal{A} wins the second stage of the game.

The security of the proposed scheme is defined as follows.

Definition 2: An authentication protocol is security if it meets the following conditions:

- 1) When U^i and S^j are accepted, they getting the same session key;
- 2) In the end of the game, the advantage $Adv_L(\mathcal{A})$ of adversary \mathcal{A} win is negligible.

4.2 PROOF

Computational Diffie-Hellman (CDH) Assumption: Let G be a finite cyclic group of prime order p generated by an element g . If there are two given numbers g^x and g^y , there is no polynomial time algorithm can compute g^{xy} from (g^x, g^y) within time t with non-negligible probability $Adv_G^{CDH}(\mathcal{A})$.

The function $Adv_G^{CDH}(t) = \max_{\mathcal{A}} [Adv_G^{CDH}(\mathcal{A})]$ is used to represent the maximum probability of all adversaries made.

Theorem 1: Let G be a group and let D be a uniformly distributed dictionary of size $|D|$. Let \mathcal{A} be an adversary against the semantic security within a time bound t with *Send* queries, *Execute* queries, *Test* queries and P^i random oracle queries, the numbers q_{send} , q_{exe} and q_p are corresponding query times. Then the advantage of adversary \mathcal{A} wins the game is:

$$Adv_L(\mathcal{A}) \leq \frac{q_p^2 + (q_{send} + q_{exe})^2}{p} + \frac{2q_{send}}{p} + 2Adv_G^{CDH}(t) + \frac{2q_{send}}{|D|} \quad (1)$$

In the processes of the game which occur between adversary \mathcal{A} and random Oracle P^i , P^i should maintain a list with the form of (ID_i, p, r) . If the list does not exist, P^i will select a random r as a reply and add (ID_i, p, r) to the list. Due to each query of \mathcal{A} must contain the above processes, we will no longer repeat the processes in the following phases of the game. In this scheme, all possible query models occur between adversary \mathcal{A} and oracle P^i are summarized as follows.

1) *Send(U^i, \mathcal{A})*

Upon receiving the query from \mathcal{A} , U^i selects a random $N_1 \in Z_q^*$ and computes

$$S_2' = h(h(R) \| h(R \| PW)), S_1 = S_2' \oplus S_3,$$

$$M_1 = S_1^{N_1} \bmod p \text{ and } a = h(ID_i \| M_1 \| S_1), \text{ then sends}$$

$\{ID_i, a, M_1\}$ to \mathcal{A} . Later, \mathcal{A} sends $\{ID_i, a, M_1\}$ to S^j for querying.

2) *Send($S^j, \{ID_i, a, M_1\}$)*

Upon receiving the messages $\{ID_i, a, M_1\}$, S^j computes $a' = h(ID_i \| M_1 \| S_1)$ and checks $a' = a$. Then S^j selects a random $N_2 \in Z_q^*$ and computes

$$M_2 = S_1^{N_2} \bmod p, b = h(ID_i \| S_1 \| M_2) \text{ and sends}$$

$\{b, M_2\}$ to \mathcal{A} . Later, \mathcal{A} sends $\{b, M_2\}$ to U^i for querying.

3) *Send($U^i, \{b, M_2\}$)*

Upon receiving the messages $\{b, M_2\}$, U^i computes $b' = h(ID_i \| S_1 \| M_2)$ and checks $b' = b$. Then U^i computes $c = h(M_1 \| ID_i \| S_1 \| M_2)$ and session key

$sk = h(S_1 \| M_2^{N_1} \| ID_i)$, and sends $\{c\}$ to \mathcal{A} . Later, \mathcal{A} sends $\{c\}$ to S^j for querying.

4) $Send(S^j, \{c\})$.

Upon receiving the messages $\{c\}$, S^j computes $c' = h(M_1 \| ID_i \| S_1 \| M_2)$ and checks $c' = c$. Then S^j computes session key $sk = h(S_1 \| M_2^{N_1} \| ID_i)$. Finally, S^j and U^i accepts and terminates

5) $Corrupt(U^i, a)$.

Upon receiving the query, oracle P^i selects the value of a randomly. If $a = 0$, P^i outputs the password of U^i . And if $a = 1$, P^i outputs messages that stored in the smart card.

6) $Reveal(P^i)$.

If the oracle P^i accepts, and when receiving the query which comes from \mathcal{A} , P^i will send session key back to \mathcal{A} .

7) $Execute(U^i, S^j)$

This query model simulates eavesdropping attack of \mathcal{A} . \mathcal{A} could acquire all messages that were transmitted during the honest execution of the protocol.

8) $Test(P^i)$

After getting the session key by querying $Test$ model, \mathcal{A} guesses the value of b' and checks $b' = b$. If it is correct, we say the adversary \mathcal{A} wins the game.

Next, the game will begin with a full random oracle which could simulate the real attack, then separating the way of adversary wins game step by step, and ending up with a hard problem that the adversary must solve. The game is described as follows.

Game₁: We simulate this game under the random oracle model, and the $Send$, $Execute$, $Reveal$ and $Test$ oracles are also simulated as in the real attack. So this game cannot be distinguished with real attack, the deviation of probability between $Game_1$ and real attack $\Delta_1 = 0$.

Game₂: In this game, we query all possible models which occur between adversary \mathcal{A} and oracle P^i . In the query processes, \mathcal{A} may win the game because of a collision occurs in the output or transcript. According to the birthday paradox, the probability of collisions in the output of the P^i oracle and transcript is at most $[q_p^2 + (q_{send} + q_{exe})^2] / 2p$. But this game allows adversary wins without the above collisions, thus the probability of adversary wins $Game_2$ is less than the probability of ad-

versary wins $Game_1$. We have the deviation of probability between $Game_2$ and $Game_1$ that

$$\Delta_2 \leq [q_p^2 + (q_{send} + q_{exe})^2] / 2p.$$

Game₃: If adversary wins the game without making the corresponding oracle queries, the possibility of above collisions does not exist. The probability of this situation is q_{send} / p , thus $\Delta_3 \leq q_{send} / p$.

Game₄: In addition to guessing or collision, adversary \mathcal{A} also can win the game by stealing the information of $Execute$ model. The information that adversary could steal are $\{ID_i, a, M_1\}$, $\{b, M_2\}$ and $\{c\}$. It is to be noticed that the session key $sk = h(S_1 \| M_1^{N_2} \| ID_i)$ or $sk = h(S_1 \| M_2^{N_1} \| ID_i)$, if the adversary wants to compute sk from M_1 and M_2 he will face a hard problem $CDH(M_1, M_2)$. We have the probability of solving this hard problem is $Adv_G^{CDH}(\mathcal{A})$ based on the **CDH Assumption**. And if the adversary queried the $Corrupt(U^i, a)$ model, the probability of adversary knows the password is $q_{send} / |D|$. Besides, the adversary can know the password by querying $Test$ model, and the probability of it is $1/2$. Finally, we have $\Delta_3 \leq Adv_G^{CDH}(t) + q_{send} / |D|$.

In conclusion, we have the advantage of adversary \mathcal{A} wins the game is

$$Adv_L(\mathcal{A}) \leq \frac{q_p^2 + (q_{send} + q_{exe})^2}{p} + \frac{2q_{send}}{p} + 2Adv_G^{CDH}(t) + \frac{2q_{send}}{|D|}. \quad (2)$$

5 Security analyses

In this section, we will analyze the security of the proposed scheme. In the registration phase the proposed scheme extracts two random numbers R and P from the biometrics with the characteristics of Fuzzy Extractor. And the parameters that stored in the smart card are $S_3, h(\bullet), h(R)$ and P rather than user's biometric template, thus the proposed scheme could protect the user's biometric template from attacking. Besides, we use Diffie-Hellman key exchange method to ensure forward security. In the following, we analyze the security of the proposed scheme in detail.

Theorem 1: The proposed scheme could withstand the smart card loss attack.

Unlike Yan et al.'s scheme stored user's biometric template in smart card without any handle, the proposed scheme stores R 's hash value $h(R)$. If the user lost his smart card and the adversary obtained it, the adversary can only get $h(R)$ rather than user's biometric template or R . Thus, the adversary almost cannot pass the bio-

metrics authentication process and cannot get any messages of user. Thought the adversary pass the biometrics authentication process by all kinds of technological means, he cannot compute R from $h(R)$ and then cannot compute $S_2 = h(h(R) \| h(R \| PW_i))$. Therefore, the proposed scheme could withstand the smart card loss attack.

Theorem 2: The proposed scheme could withstand the Denial-of-Service attack.

Although the biometrics belonging to the same user differs slightly from time to time, the distance of two biometrics is within some predetermined threshold. The smart card checks whether $h(R) = h(R')$ is correct and determines whether the inputted biometrics B_i^* and the pre-stored biometric template B_i belonging to the same use. Therefore, the proposed scheme could withstand the Denial-of-Service attack.

Theorem 3: The proposed scheme could withstand the privilege-insider attack.

In the registration phase of the proposed scheme, the user sends $h(R)$ and $h(R \| PW_i)$ instead of the password PW_i to the server, where R is a random number generated by the generation procedure $Gen\ Gen(B_i) \rightarrow (R, P)$. The privileged insider of server cannot get PW_i and R from $h(R \| PW_i)$. Therefore, the proposed scheme could withstand the privileged insider attack.

Theorem 4: The proposed scheme could withstand the replay attack.

The adversary may intercept the messages $\{ID_i, a, M_1\}$, $\{b, M_2\}$ and $\{c\}$ that transmit between server and user, and sends it to the server, where $a = h(ID_i \| M_1 \| S_1)$, $S_1 = h(ID_i \| x)$, $M_1 = S_1^{N_1} \bmod p$, $b = h(ID_i \| S_1 \| M_2)$, $M_2 = S_1^{N_2} \bmod p$ and $c = h(M_1 \| ID_i \| S_1 \| M_2)$.

The adversary cannot compute the checking information a, b and c without server's secret key x and random numbers N_1 and N_2 . Besides, the adversary may intercept the message M_1 and M_2 and sends it to user or server. However, the user or server could find the attack by checking the validity of M_1 and M_2 . Therefore, the proposed scheme could withstand the replay attack.

Theorem 5: The proposed scheme could withstand the parallel session attack.

If the adversary intercepts the messages $\{b, M_2\}$ and impersonates a legitimate user sends $\{ID_i, b, M_2\}$ to server, where $b = h(ID_i \| S_1 \| M_2)$. Upon receiving b , server compute $a' = h(ID_i \| M_2 \| S_1)$ and checks whether $a' = b$ is correct. Obviously, $a' = h(ID_i \| M_2 \| S_1) \neq b$

server stops the session. Therefore, the proposed scheme could withstand the parallel session attack.

Theorem 6: The proposed scheme could withstand the reflection attack.

If the adversary intercepts the messages $\{ID_i, a, M_1\}$, he may modify and send it to user. Upon receiving the message, user computes $b' = h(ID_i \| S_1 \| M_1)$ and checks whether $b' = a$ is correct. However, $a = h(ID_i \| M_1 \| S_1)$ and $b' = h(ID_i \| S_1 \| M_1)$, $b' \neq a$ and user stops the session. Therefore, the proposed scheme could withstand the reflection attack.

Theorem 7: The proposed scheme could withstand the impersonation attack.

If the adversary wants to impersonate a legitimate user or server, he must compute messages $\{ID_i, a, M_1\}$, $\{b, M_2\}$ and $\{c\}$, where $a = h(ID_i \| M_1 \| S_1)$, $b = h(ID_i \| S_1 \| M_2)$, $c = h(M_1 \| ID_i \| S_1 \| M_2)$ and $S_1 = h(ID_i \| x)$. However, the adversary cannot do that without server's secret key x . Therefore, the proposed scheme could withstand the impersonation attack.

Theorem 8: The proposed scheme could withstand the Man-in-the-Middle attack.

When the adversary intercepts the messages $\{ID_i, a, M_1\}$, $\{b, M_2\}$ or $\{c\}$ and gets user's smart card, he could modify and compute some new messages $\{ID_i, a', M_1'\}$, $\{b', M_2'\}$ or $\{c'\}$.

But the user or server could find the attack by checking the validity of the new message since the adversary cannot compute a legal message without secret messages $S_1 = h(ID_i \| x)$. Therefore, the proposed scheme could withstand the Man-in-the-Middle attack.

6 Performance analyses

In this section, we will compare the performance (efficiency and accomplished goals) of our authentication scheme with Yan et al.'s scheme and other relevant schemes.

6.1 EFFICIENCY ANALYSES

First of all, some used notations are defined as follows.

T_h : the running time of a hash function operation;

T_s : the running time of a symmetric encryption (decryption) or Fuzzy Extractor or modulo operation;

T_x : the running time of a XOR operation.

We assume that the output size of hash function is 160 bits, the output size of symmetric encryption/decryption algorithm is 160 bits, the output size of modulo function is 160 bits, the size of random numbers is 160 bits and the size of client's identity is 32 bits.

The comparisons of related schemes [4,5,8,11] in term of communicational cost and computational cost are

listed in Table 2. As can be seen from Table 2, the communicational cost of the proposed scheme is the lowest and the computational cost is almost similar to the others. Although the computational cost of the proposed scheme is a little more than Yan et al.'s scheme, the proposed scheme overcomes their cannot ensure the security of the user's biometric template and forward security. Besides,

the proposed scheme also can overcome Tan's vulnerable to the Denial-of-Service attack, Li's vulnerable to the Denial-of-Service attack and privileged insider attack and Yang's vulnerable to the impersonation attack. Therefore, the proposed scheme is more security in the case of approximate efficiency.

TABLE 2 Efficiency comparison

Item	The proposed scheme	Tan	Li	Yan	Yang
Communicational cost	832bit	864bit	1312bit	832bit	1792bit
Computational cost of the user	$6T_h + 2T_s + 1T_x$	$5T_h + 1T_s + 1T_x$	$4T_h + 3T_x$	$6T_h + 1T_x$	$6T_h + 1T_s + 3T_x$
Computational cost of the server	$4T_h + 1T_s$	$5T_h + 1T_s$	$3T_h + 2T_x$	$4T_h$	$2T_h + 3T_x$

6.2 COMPLETED GOALS ANALYSES

The comparisons of related schemes [4,5,8,11] in term of accomplished goals are listed in Table 3. In the table, notations Y and N are on behalf of Yes and No, respectively. As described in the table, the proposed scheme can

achieve many kinds of security goals that an ideal biometrics-based authentication schemes required and has a more better performance. The most important is that the proposed scheme solves an important security goal G0 that usually ignored in previous schemes.

TABLE 3 Accomplished goals comparison

Goal	Our scheme	Tan	Li	Yan	Yang
G0	Y	N	N	N	N
G1	Y	N	N	Y	Y
G2	Y	N	N	N	Y
G3	Y	N	N	N	Y
G4	Y	Y	Y	Y	Y
G5	Y	Y	Y	Y	Y
G6	Y	Y	Y	Y	Y
G7	Y	Y	N	Y	N
G8	Y	Y	Y	Y	Y
G9	Y	Y	N	Y	N
G10	Y	Y	Y	Y	Y
G11	Y	N	N	N	N

7 Conclusions

In this paper, we analyzed the security problem of biometrics-based authentication schemes and mainly analyzed the weakness of Yan et al.'s scheme, we found that the security of biometric template in above schemes was usually ignored. To enhance the security of biometric template, we proposed a security and efficient biometrics-based authentication scheme combine with the characteristics of Fuzzy Extractor. The Fuzzy Extractor could extract the biometrics into two random strings, therefore, the new proposed scheme could hide and protect the biometric temp-

late. A formal security proof under the random oracle mode demonstrated the proposed scheme is security.



Acknowledgments

The author would like to thanks for the financial support by scientific research project fund of Jiangxi province (GJJ14371) and the aids from East China JiaoTong University. The authors would like to thanks the anonymous reviewers for their valuable comments and suggestions.

References

[1] Lamport L 1981 Password authentication with insecure communication *Commun ACM* 24:28-30
 [2] Lee J K, Ryu S R, Yoo KY 2002 *IEEE Electronics Letters* 38(12) 554-5
 [3] Yoon E J, Yoo K Y 2007 A secure chaotic hash-based biometric remote user authentication scheme using mobile devices *APWeb/WAIM Ws Lecture Notes in Computers Science Springer-Verlag Berlin Heidelberg* 4537 612-23

- [4] Tan Z W 2013 An efficient biometrics-based authentication scheme for telecare medicine information systems *Przeglad Elektrotechniczny* **89**(5) 200-4
- [5] Li C T, Hwang M S 2010 An efficient biometrics-based remote user authentication scheme using smart cards *Journal of Network and Computer Applications* **33** 1-5
- [6] Chan T E, Feldman D, Hopper N 2009 The frog-boiling attack: Limitations of anomaly detection for secure network coordinate systems *Security and Privacy in Communication Networks Springer* 448-58
- [7] Feng H, Wah C C 2002 Private key generation from on-line handwritten signatures *Information Management & Computers Security* **10**(4) 159-64
- [8] Yan X, Li W, Li P, Wang J, Hao X, Gong P 2013 A secure biometrics-based authentication scheme for telecare medicine information systems *Journal of medical systems* doi:10.1007/s10916-013-9972-1
- [9] Yoon E J, Yoo K Y 2013 Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem *Journal of supercomputing* **63** 235-55 doi:10.1007/s11227-010-0512-1
- [10] Khan M K, Zhang J H 2006 An efficient and practical fingerprint-based remote user authentication scheme with smart cards *ISPEC 2006 Lecture notes in Computers Science* **3903** 260-8
- [11] Yang D, Yang B 2009 A new password authentication scheme using fuzzy extractor with smart card *International Conference on Computational Intelligence and Security* doi:10.1109/CIS.2009.44
- [12] Duan X, Li X Y 2011 Security of a new password authentication scheme using fuzzy extractor with smart card *ICCSN IEEE 3rd International Conference on* 282-4
- [13] Dodis Y, Reyzin L, Smith A 2004 Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data *Advances in Cryptology-Eurocrypt Lecture Notes in Computers Science* **3027** 523-40
- [14] Boyen X 2006 Reusable cryptographic fuzzy extractors *11th ACM Conference on Computers and Communication Security*
- [15] Boyen X, Dodis Y, Katz J, Smith A 2006 Robust fuzzy extractors and authenticated key agreement from close secrets *Advances in Cryptology-Crypto'06 Lecture Notes in Computers Science* 4007
- [16] Dodis Y, Reyzin L, Smith A 2005 Fuzzy extractors: How to generate strong keys from biometrics and other noisy data *Advances in Cryptology-EUROCRYPT Lecture Notes in Computers Science* **3027** 523-40
- [17] Madhusudhan R, Mittal R C 2012 Dynamic ID-based remote user password authentication schemes using smart cards: A review *Journal of Network and Computer Applications* doi:10.1016/j.jnca.2012.01.007
- [18] Awasthi K, Lal S 2003 A remote user authentication scheme using smart cards with forward secrecy *IEEE Transactions on Consumer Electronics* **49**(4) 1246-8
- [19] Xu J, Zhu W T, Feng D G 2009 An improved smart card based password authentication scheme with provable security *Computers Standards & Interfaces* doi:10.1016/j.csi.200-8.09.006

Authors	
	<p>Lihua Zhang, Dec. 25th, 1972, Hubei Province, China.</p> <p>Current position, grades: associate professor in the School of Software at East China Jiaotong University. University studies: PhD in Electronic Engineering school, Beihang University in 2011. Scientific interest: information security. Publications: 35 papers.</p>
	<p>Yaoping Nie, Sept. 8th, 1989, Jiangxi Province, China.</p> <p>Current position, grades: Master degree candidate in the School of Electrical and Electronic Engineering at East China Jiaotong University. University studies: BSc in Equipment Engineering, Shenyang Ligong University in 2013. Scientific interest: information security. Publications: 1 paper.</p>