Robust Biometrics-Based Authentication Scheme for Multiserver Environment

Debiao He, *Member, IEEE*, and Ding Wang

***Abstract*—The authentication scheme is an important cryptographic mechanism, through which two communication parties could authenticate each other in the open network environment. To satisfy the requirement of practical applications, many authentication schemes using passwords and smart cards have been proposed. However, passwords might be divulged or forgotten, and smart cards might be shared, lost, or stolen. In contrast, biometric methods, such as fingerprints or iris scans, have no such drawbacks. Therefore, biometrics-based authentication schemes gain wide attention. In this paper, we propose a biometrics-based authentication scheme for multiserver environment using elliptic curve cryptography. To the best of our knowledge, the proposed scheme is the first truly three-factor authenticated scheme for multiserver environment. We also demonstrate the completeness of the proposed scheme using the Burrows–Abadi–Needham logic.**

***Index Terms*—Authentication scheme, biometrics, elliptical curve cryptosystem, smart card.**

I. INTRODUCTION

AS a basic pattern recognition system, the biometric system has been widely used in our life. Such system acquires a biometric key (e.g., fingerprints, faces, irises, hand geometry, palm prints, etc.) from an individual, extracts a feature set, and stores it in the database. Upon receiving a new biometric key, the system extracts a new feature set and compares it with that stored in the database. If the two feature sets are matching, the system could recognize the individual; otherwise, the system will reject the individual [1]–[3]. Compared with cryptographic keys and passwords, biometric keys have many advantages. Several advantages are described as follows [4]:

1) it is difficult to lose or forget biometric keys;
2) it is difficult to copy or share biometric keys;
3) it is difficult to forge or distribute biometrics;
4) it is difficult to guess biometric keys;
5) it is more difficult to break biometric keys.

Therefore, the biometric key is very suitable for modern cryptography. It has been used in the design of encryption schemes [5], [6], digital signature schemes [7], [8], and signcryption schemes [9], [10]. The authentication scheme is an important cryptographic mechanism, through which two communication parties could authenticate each other in the open network environment. Due to advantages of biometric keys, the biometrics-based authentication scheme is inherently more reliable than traditional password-based authentication. Therefore, it has been studied widely.

Lee *et al.* [11] proposed a fingerprint-based remote-user authentication scheme using smart cards. Unfortunately, Lin and Lai [12] and Chang and Lin [13] pointed out that Lee *et al.*'s scheme cannot withstand the masquerade attack and the conspiring attack separately. To overcome these weaknesses, Kim *et al.* [14] proposed a new fingerprint-based authentication scheme using smart cards. However, Scott [15] found that Kim *et al.*'s scheme is not secure at all. Later, Khan and Zhang have pointed out that Lin and Lai's scheme [16] is vulnerable to the server spoofing attack and proposed a security-enhanced scheme. In 2010, Li and Hwang [17] has proposed a new biometrics-based authentication using smart cards. Unfortunately, Li and Hwang's scheme cannot provide proper authentication [18]–[20] and is not secure against man-in-the-middle [18] and denial-of-service attacks [18], [19]. Three improved schemes [18]–[20] were also proposed to overcome the weaknesses in Li and Hwang's scheme.

With the widespread use of the distributed system, more and more multiserver environments are used to provide convenient and efficient network services. Therefore, the biometrics-based authentication scheme for multiserver environment is required by practical applications. However, those biometrics-based authentication schemes [11], [12], [14], [18]–[20] are designed for client–server environment and are not suitable for multiserver environment since the users have to remember many passwords. To solve the problem, Yoon and Yoo [21] proposed a biometrics-based authentication scheme for multiserver environment using elliptical curve cryptosystem (ECC) and smart cards. However, Kim *et al.* [22] found that Yoon and Yoo's scheme cannot withstand the offline password-guessing attack when the smart card is lost. Kim *et al.* [22] also proposed an improved scheme to the weaknesses. He [23] also pointed out that Yoon and Yoo's scheme is vulnerable to the privileged insider attack and the impersonation attack. It is easy to say that He's attacks are valid for Kim *et al.*'s scheme. Furthermore, neither of Yoon and Yoo's scheme and Kim *et al.*'s scheme is a truly three-factor authenticated scheme since the adversary could impersonate the user once he obtains the password and the smart card. To enhance security, we propose a new biometrics-based authentication scheme for multiserver environment using ECC and smart cards. The analysis shows

---

Manuscript received November 26, 2012; revised January 14, 2014; accepted January 15, 2014. This work was supported in part by the Open Funds of State Key Laboratory of Information Security under Grant 2013-3-3 and in part by the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant 20110141120003.

D. He is with the School of Mathematics and Statistics, Wuhan University, Wuhan 430072, China and also with State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: hedebiao@163.com).

D. Wang is with the School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China (e-mail: wangdingg@mail.nankai.edu.cn).

Digital Object Identifier 10.1109/JSYST.2014.2301517

TABLE I
NOTATIONS

n, p	two large prime numbers
F_p	A finite prime field
E	A non-super singular elliptic curve over a finite field F_p
G	The additive group consisting of points on E
P	A generator of G with order n
$h(\cdot)$	A secure hash function
$\|\|$	The concatenation operation
$\oplus$	The bit-wise exclusive-or(XOR) operation
U_i	The i th user
PW_i	The password of U_i
ID_i	The identity of U_i
S_j	The j th server
SID_j	The identity of ..
RC	The registration center
k	The secret key of RC
P_{pub}	The public key of RC , where $P_{pub}= kP$

that the proposed scheme could overcome the weaknesses in Yoon and Yoo's scheme and Kim *et al.*'s scheme, To the best of our knowledge, the proposed scheme is the first truly three-factor authentication scheme for multiserver environment.

The remainder of this paper is organized as follows. Section II gives some background of the fuzzy extractor. Section III describes our new biometrics-based authentication scheme for multiserver environment. Security analysis and performance analysis are given in Sections IV and V separately. Finally, we conclude this paper in Section VI.

II. BASIC CONCEPT OF FUZZY EXTRACTOR

Given biometric input B, a fuzzy extractor could extract a random string σ. One important property of the fuzzy extractor is that it could output the same random string when the input changes, but it remains close. To recover σ from a new biometric input B^*, a uniformly random auxiliary string ϑ will be generated and used in the following operations. The fuzzy extractor is formally defined as follows.

Definition 1 (Fuzzy Extractor) [24]: A fuzzy extractor is given by two procedures (Gen, Rep).

1) Gen is a probabilistic generation procedure. Upon receiving biometric input B, the procedure will output a random string σ and a random auxiliary string ϑ.
2) Rep is a deterministic reproduction procedure. Upon receiving a close biometric input B^* and the corresponding random auxiliary string ϑ, the procedure will recover σ.

We call a fuzzy extractor is secure if it is difficult to recover σ from a closed biometric input B^* without the auxiliary string ϑ.

III. NEW BIOMETRICS-BASED AUTHENTICATION SCHEME

Here, we give the detail of our new biometrics-based authentication scheme for multiserver environment. There are four phases in the proposed scheme, which are the server registration phase, the user registration phase, the authentication phase, and the password change phase. For convenience, notations used in this paper are summarized in Table I.

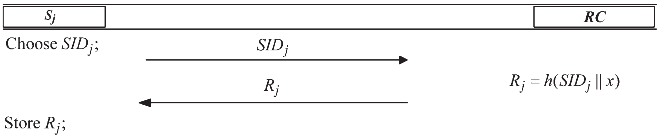


Fig. 1. Server registration phase.

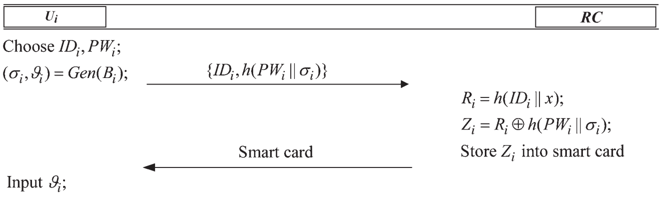


Fig. 2. User registration phase.

A. Server Registration Phase

In this phase, S_j sends the registration request to RC and obtains his secret key from RC. As shown in Fig. 1, the detail of the phase is presented as follows:

1) S_j chooses his identity SID_j and sends it to RC through a secure channel;
2) After receiving SID_j, RC computes $R_j = h(\mathrm{SID}_j \| k)$ and sends it to S_j through a secure channel;
3) After receiving R_j, S_j stores it secretly.

B. User Registration Phase

In this phase, U_i sends the registration request to RC and obtains a smart card containing his secret key from RC. As shown in Fig. 2, the detail of the phase is presented as follows:

1) U_i chooses his identity ID_i and password PW_i and imprints his personal biometric impression B_i at the sensor. U_i computes $(\sigma_i, \vartheta_i) = \mathrm{Gen}(B_i)$ and sends $\{\mathrm{ID}_i, h(\mathrm{PW}_i \| \sigma_i)\}$ to RC through a secure channel;
2) After receiving $\{\mathrm{ID}_i, h(\mathrm{PW}_i \| \sigma_i)\}$, RC computes $R_i = h(\mathrm{ID}_i \| k)$, $Z_i = R_i \oplus h(\mathrm{PW}_i \| \sigma_i)$ and stores Z_i into a smart card. Finally, RC issues the smart card to U_i face to face;
3) After receiving the smart card, U_i stores ϑ_i in it.

C. Authentication Phase

In this phase, U_i and S_j authenticate each other in the help of RC. In addition, a session key for future communication is generated between U_i and S_j. As shown in Fig. 3, the detail of the phase is presented as follows.

1) U_i inserts his smart card into a card reader, inputs PW_i and ID_i, and imprints his personal biometric impression B_i^* at the sensor. U_i generates a random number $x \in Z_n^*$ and computes $\mathrm{Rep}(B_i^*, \vartheta_i) = \sigma_i$, $R_i = Z_i \oplus h(\mathrm{PW}_i \| \sigma_i)$, $X = xP$, $X^* = xP_{\mathrm{pub}}$, $\mathrm{CID}_i = \mathrm{ID}_i \oplus h(X^*)$, and $\alpha = h(\mathrm{ID}_i \| \mathrm{SID}_j \| R_i \| X \| X^*)$. Finally, U_i sends the message $\{\mathrm{CID}_i, X, \alpha\}$ to S_j.
2) After receiving $\{\mathrm{CID}_i, X, \alpha\}$, S_j generates a random number $y \in Z_n^*$ and computes $Y = yP$, $Y^* = yP_{\mathrm{pub}}$, $\beta = h(\mathrm{CID}_i \| X \| \alpha \| \mathrm{SID}_j \| R_j \| Y \| Y^*)$, and $C\mathrm{SID}_j = \mathrm{SID}_j \oplus h(Y^*)$. Finally, S_j sends the message $\{\mathrm{CID}_i, X, \alpha, C\mathrm{SID}_j, Y, \beta\}$ to RC.

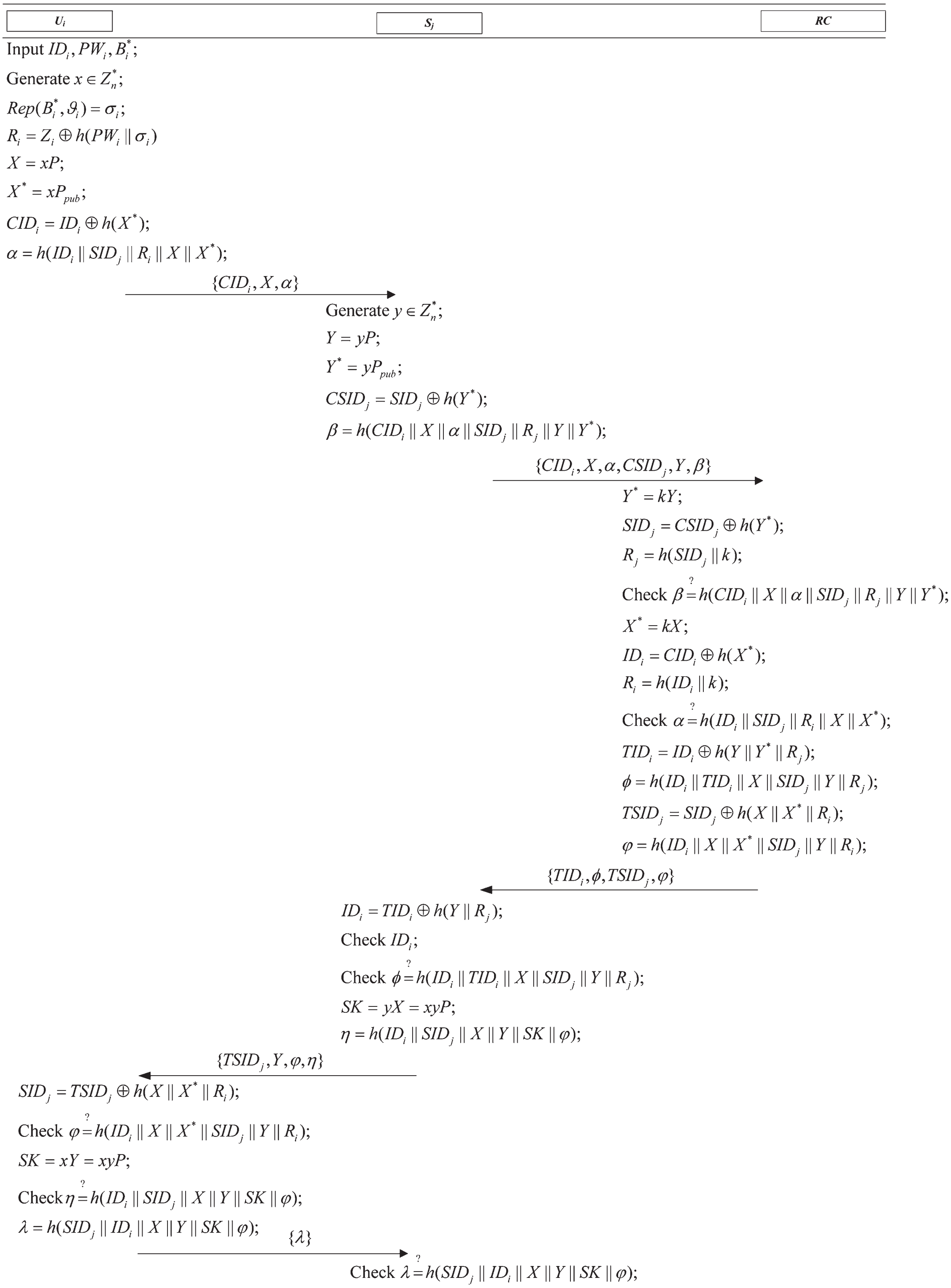


Fig. 3. Authenticated key exchange phase.

3) After receiving $\{\mathrm{CID}_i, X, \alpha, C\mathrm{SID}_j, Y, \beta\}$, RC computes $Y^* = kY$, $\mathrm{SID}_j = C\mathrm{SID}_j \oplus h(Y^*)$, and $R_j = h(\mathrm{SID}_j \| k)$. Then, RC checks whether β and $h(\mathrm{CID}_i \| X \| \alpha \| \mathrm{SID}_j \| R_j \| Y \| Y^*)$ are equal. If they are not equal, RC rejects the session; otherwise, RC computes $X^* = kX$, $\mathrm{ID}_i = \mathrm{CID}_i \oplus h(X^*)$, and $R_i = h(\mathrm{ID}_i \| k)$. RC checks whether α and $h(\mathrm{ID}_i \| \mathrm{SID}_j \| R_i \| X \| X^*)$ are equal. If they are not equal, RC reject the session; otherwise, RC computes $\mathrm{TID}_i = \mathrm{ID}_i \oplus h(Y \| Y^* \| R_j)$, $\phi = h(\mathrm{ID}_i \| \mathrm{TID}_i \| X \| \mathrm{SID}_j \| Y \| R_j)$, $\mathrm{TSID}_j = \mathrm{SID}_j \oplus h(X \| X^* \| R_i)$, and $\varphi = h(\mathrm{ID}_i \| X \| X^* \| \mathrm{SID}_j \| Y \| R_i)$. Finally, RC sends the message $\{\mathrm{TID}_i, \phi, \mathrm{TSID}_j, \varphi\}$ to S_j.

4) After receiving $\{\mathrm{TID}_i, \phi, \mathrm{TSID}_j, \varphi\}$, S_j computes $\mathrm{ID}_i = \mathrm{TID}_i \oplus h(Y \| Y^* \| R_j)$ and checks the validity of ID_i. If it is not valid, S_j stops the session; otherwise, S_j checks whether ϕ and $h(\mathrm{ID}_i \| \mathrm{TID}_i \| X \| \mathrm{SID}_j \| Y \| R_j)$

are equal; if they are not equal, S_j stops the session; otherwise, S_j computes the session key $SK = yX = xyP$ and $\eta = h(\mathrm{ID}_i\|\mathrm{SID}_j\|X\|Y\|SK\|\varphi)$. Finally, S_j sends the message $\{\mathrm{TSID}_j,\ Y,\ \varphi,\ \eta\}$ to U_i.

5) After receiving $\{\mathrm{TSID}_j,\ Y,\ \varphi,\ \eta\}$, U_i computes $\mathrm{SID}_j = \mathrm{TSID}_j \oplus h(X\|X^*\|R_i)$ and checks whether φ and $h(\mathrm{ID}_i\|X\|X^*\|\mathrm{SID}_j\|Y\|R_i)$ are equal. If they are not equal, U_i stops the session; otherwise, U_i computes the session key $SK = xY = xyP$ and checks whether $\eta = h(\mathrm{ID}_i\|\mathrm{SID}_j\|X\|Y\|SK\|\varphi)$ holds. If it does not hold, U_i stops the session; otherwise, U_i computes $\lambda = h(\mathrm{SID}_j\|\mathrm{ID}_i\|X\|Y\|SK\|\varphi)$ and sends the message $\{\lambda\}$ to S_j.
6) After receiving $\{\lambda\}$, S_j checks whether $\lambda = h(\mathrm{SID}_j\|\mathrm{ID}_i\|X\|Y\|SK\|\varphi)$ holds. If it does not hold, S_j stops the session; otherwise, S_j confirms that U_i is a legal user.

D. Password Change Phase

In this phase, U_i could change the old password PW_i to a new password $\mathrm{PW}_i^{\mathrm{new}}$. The following steps will be executed in the phase.

1) U_i inserts his smart card into a card reader, inputs PW_i, ID_i, and imprints his personal biometric impression B_i^* at the sensor. U_i also inputs the new password $\mathrm{PW}_i^{\mathrm{new}}$.
2) The smart card computes $\mathrm{Rep}(B_i^*, \vartheta_i) = \sigma_i$, $R_i = Z_i \oplus h(\mathrm{PW}_i\|\sigma_i)$, and $Z_i^{\mathrm{new}} = R_i \oplus h(\mathrm{PW}_i^{\mathrm{new}}\|\sigma_i)$.
3) The smart card replaces Z_i with Z_i^{new}.

IV. SECURITY ANALYSIS

In this section, we will analyze the security of our authentication scheme. First, we will use the famous Burrows–Abadi–Needham (BAN) logic [25] to demonstrate that the proposed scheme is valid and practical. Then, we will show the proposed scheme could withstand many known attacks and satisfy the security requirement of multiserver environment.

A. Authentication Proof Based on BAN Logic

The BAN logic [25] is a well-known formal mode for cryptographic protocols. It has been widely used in analyzing authentication protocols. Some notations and logical postulates of the BAN logic are described in Table II.

TABLE II
NOTATIONS

$P \mid\equiv X$	P believes X
$\#(X)$	X is fresh
$P \Rightarrow X$	P has jurisdiction over X
$P \lhd X$	P sees X
$P \mid\sim X$	P once said X
(X, Y)	X or Y is one part of (X, Y)
$< X >_Y$	X combined with Y
$(X)_Y$	X is hash with the key K
$P \xleftrightarrow{K} Q$	P and Q use the shared key K to communicate
SK	The session key used in the current session
$\dfrac{P \mid\equiv P \overset{K}{\leftrightarrow} Q, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$	The message-meaning rule
$\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}$	The freshness-conjuncatenation rule
$\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$	The nonce-verification rule
$\dfrac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$	The jurisdiction rule

According to the analytic procedures of BAN logic, the proposed scheme will satisfy the following goals.

1) Goal 1: $U_i| \equiv (U_i \xleftrightarrow{SK} S_j)$.
2) Goal 2: $U_i| \equiv S_j| \equiv (U_i \xleftrightarrow{SK} S_j)$.
3) Goal 3: $S_j| \equiv (U_i \xleftrightarrow{SK} S_j)$.
4) Goal 4: $S_j| \equiv U_i| \equiv (U_i \xleftrightarrow{SK} S_j)$.

First, we transform our proposed scheme to the idealized form as follows.

1) Msg 1: $U_i \rightarrow RC : (\mathrm{ID}_i, X)_{h(\mathrm{ID}_i\|k)}$.
2) Msg 2: $S_j \rightarrow RC : (\mathrm{ID}_i, X, \mathrm{SID}_j, Y)_{h(\mathrm{SID}_j\|k)}$.
3) Msg 3: $RC \rightarrow U_i : (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{Y} S_j)_{h(\mathrm{ID}_i\|k)}$.
4) Msg 4: $RC \rightarrow S_j : (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{X} S_j)_{h(\mathrm{SID}_j\|k)}$.
5) Msg 5: $S_j \rightarrow U_i : (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{SK} S_j)_{SK}$.
6) Msg 6: $U_i \rightarrow S_j : (\mathrm{SID}_j, \mathrm{ID}_i, X, Y, U_i \xleftrightarrow{SK} S_j)_{SK}$.

Second, we make the following assumptions about the initial state of the scheme to analyze the proposed scheme:

$$A_1 : U_i| \equiv \#(X)$$
$$A_2 : S_j| \equiv \#(Y)$$
$$A_3 : U_i| \equiv U_i \xleftrightarrow{h(\mathrm{ID}_i\|k)} RC$$
$$A_4 : RC| \equiv U_i \xleftrightarrow{h(\mathrm{ID}_i\|k)} RC$$
$$A_5 : S_j| \equiv S_j| \xleftrightarrow{h(\mathrm{SID}_j\|k)} RC$$
$$A_6 : RC| \equiv S_j| \xleftrightarrow{h(\mathrm{SID}_j\|k)} RC$$
$$A_7 : U_i| \equiv RC \Rightarrow (U_i \xleftrightarrow{Y} S_j)$$
$$A_8 : S_j| \equiv RC \Rightarrow (U_i \xleftrightarrow{X} S_j)$$
$$A_9 : S_j| \equiv U_i \Rightarrow (U_i \xleftrightarrow{SK} S_j)$$
$$A_{10} : U_i| \equiv S_j \Rightarrow (U_i \xleftrightarrow{SK} S_j).$$

Third, we analyze the idealized form of the proposed scheme based on the BAN logic rules and the assumptions. The main proofs are stated as follows:

According to Msg 1, we could get

$$S_1 : RC \lhd (\mathrm{ID}_i,\ X)_{h(\mathrm{ID}_i\|k)}.$$

According to assumption A_4, we apply the message-meaning rule to obtain

$$S_2 : RC| \equiv U_i| \sim (\mathrm{ID}_i,\ X).$$

According to Msg 2, we could obtain

$$S_3 : RC \ \triangleleft\ (\mathrm{ID}_i, X, \mathrm{SID}_j, Y)_{h(\mathrm{SID}_j\|k)}.$$

According to assumption A_6, we apply the message-meaning rule to obtain

$$S_4 : RC| \equiv S_j| \sim (\mathrm{ID}_i, X, \mathrm{SID}_j, Y).$$

According to Msg 3, we could obtain

$$S_5 : U_i \triangleleft (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{Y} S_j)_{h(\mathrm{ID}_i\|k)}.$$

According to assumption A_4, we apply the message-meaning rule to obtain

$$S_6 : U_i| \equiv RC| \sim (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{Y} S_j).$$

According to assumption A_3, we apply the freshness conjuncatenation rule to obtain

$$S_7 : U_i| \equiv RC| \equiv (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{Y} S_j).$$

According toS_7, we apply the BAN logic rule to break conjunctions to produce

$$S_8 : U_i| \equiv RC| \equiv U_i \xleftrightarrow{Y} S_j.$$

According to assumption A_7, we apply the jurisdiction rule to obtain

$$S_9 : U_i| \equiv U_i \xleftrightarrow{Y} S_j.$$

According to $sk = a \times Y = ab \times P$, we could obtain

$$S_{10} : U_i| \equiv U_i \xleftrightarrow{SK} S_j \qquad \text{(Goal 1)}.$$

According to Msg 4, we could obtain

$$S_{11} : S_j \ \triangleleft\ (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{X} S_j)_{h(\mathrm{SID}_j\|k)}.$$

According to assumption A_5, we apply the message-meaning rule to obtain

$$S_{12} : S_j| \equiv RC| \sim (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{X} S_j).$$

According to assumption A_2, we apply the freshness conjuncatenation rule to obtain

$$S_{13} : S_j| \equiv RC| \equiv (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{X} S_j).$$

According to S_{13}, we apply the BAN logic rule to break conjunctions to produce

$$S_{14} : S_j| \equiv RC| \equiv U_i \xleftrightarrow{X} S_j.$$

According to assumption A_8, we apply the jurisdiction rule to obtain

$$S_{15} : S_j| \equiv U_i \xleftrightarrow{X} S_j.$$

According to $sk = b \times X = ab \times P$, we could obtain

$$S_{16} : S_j| \equiv U_i \xleftrightarrow{SK} S_j. \qquad \text{(Goal 3)}$$

According to Msg 5, we could obtain

$$S_{17} : U_i \ \triangleleft\ (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{sk} S_j)_{sk}.$$

According to assumption S_{10}, we apply the message-meaning rule to obtain

$$S_{18} : U_i| \equiv S_j| \sim (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{SK} S_j).$$

According to assumption A_1, we apply the freshness conjuncatenation rule to obtain

$$S_{19} : U_i| \equiv S_j| \equiv (\mathrm{ID}_i, \mathrm{SID}_j, X, Y, U_i \xleftrightarrow{SK} S_j).$$

According to S_{19}, we apply the BAN logic rule to break conjunctions to produce

$$S_{20} : U_i| \equiv S_j| \equiv U_i \xleftrightarrow{SK} S_j. \qquad \text{(Goal 2)}.$$

According to Msg 6, we could obtain

$$S_{21} : S_j \ \triangleleft\ (\mathrm{SID}_j, \mathrm{ID}_i, X, Y, U_i \xleftrightarrow{SK} S_j)_{SK}.$$

According to assumption S_{16}, we apply the message-meaning rule to obtain

$$S_{22} : S_j| \equiv U_i| \sim (\mathrm{SID}_j, \mathrm{ID}_i, X, Y, U_i \xleftrightarrow{SK} S_j).$$

According to assumption A_2, we apply the freshness conjuncatenation rule to obtain

$$S_{23} : S_j| \equiv U_i| \equiv (\mathrm{SID}_j, \mathrm{ID}_i, X, Y, U_i \xleftrightarrow{sk} S_j).$$

According to S_{23}, we apply the BAN logic rule to break conjunctions to produce

$$S_{24} : S_j| \equiv U_i| \equiv U_i \xleftrightarrow{SK} S_j. \qquad \text{(Goal 4)}.$$

According to (Goal 1), (Goal 2), (Goal 3), and (Goal 4), we know that both of U_i and S_j believe that the session key $SK = xyP$ is shared between U_i and S_j.

B. Other Discussions

To demonstrate the proposed scheme is suitable for multiserver environment, we will show that the proposed scheme not only provide anonymity, mutual authentication, three-factor security, and perfect forward secrecy but also could withstand various attacks.

Mutual Authentication: In Step 3 of the authentication phase, RC could authenticate U_i by checking whether α and $h(\mathrm{ID}_i \| \mathrm{SID}_j \| R_i \| X \| X^*)$ are equal. If they are equal, RC will generate the authentication code $\phi = h(\mathrm{ID}_i \| \mathrm{TID}_i \| X \| \mathrm{SID}_j \| Y \| R_j)$ and send it to S_j for future authentication. With the help of RC, S_j could authenticate U_i and RC by checking the validity of ϕ in Step 4 of the authentication.

In Step 3 of the authentication phase, RC could authenticate S_j by checking whether β and $h(\mathrm{CID}_i \| X \| \alpha \| \mathrm{SID}_j \| R_j \| Y \| Y^*)$ are equal. If they are equal, RC will generate $\varphi = h(\mathrm{ID}_i \| X \| X^* \| \mathrm{SID}_j \| Y \| R_i)$ and send it to U_i for future authentication. With the help of RC, U_i could authenticate S_j and RC by checking validity of ϕ in Step 5 of the authentication.

Therefore, the proposed scheme could provide mutual authentication among U_i, S_j, and RC.

Anonymity: In the proposed scheme, U_i's identity is included in $\mathrm{CID}_i = \mathrm{ID}_i \oplus h(X^*)$ and $\mathrm{TID}_i = \mathrm{ID}_i \oplus h(Y \| Y^* \| R_j)$, where $X = xP$, $X^* = xP_{\mathrm{pub}}$, $Y = yP$, $Y^* = yP_{\mathrm{pub}}$, and $P_{\mathrm{pub}} = kP$. To obtain the real identity, the adversary has to compute X^*/Y^* from $(Y, P_{\mathrm{pub}})/(Y, P_{\mathrm{pub}})$. He has to solve the computational Diffie–Hellman problem; otherwise, he cannot obtain U_i's identity.

In the proposed scheme, S_j's identity is included in $C\mathrm{SID}_j = \mathrm{SID}_j \oplus h(Y^*)$ and $\mathrm{TSID}_j = \mathrm{SID}_j \oplus h(X \| X^* \| R_i)$, where $X = xP$, $X^* = xP_{\mathrm{pub}}$, $Y = yP$, $Y^* = yP_{\mathrm{pub}}$, and $P_{\mathrm{pub}} = kP$. To obtain the real identity, the adversary has to computes X^*/Y^* from $(Y, P_{\mathrm{pub}})/(Y, P_{\mathrm{pub}})$. He has to solve the computational Diffie–Hellman problem; otherwise, he cannot obtain S_j's identity.

Therefore, the proposed scheme could provide anonymity.

Three-Factor Security: It is easy to say the user with three factors i.e., a password, a smart card, and biometrics, could log in on the server. We will show that the adversary $\mathcal{A}$ cannot impersonate a legal user even if he has any two factors. We just need to show that $\mathcal{A}$ cannot generate a legal request message $\{\mathrm{CID}_i, X, \alpha\}$. Since $X = xP$, $X^* = aP_{\mathrm{pub}}$, and $\alpha = h(\mathrm{ID}_i \| \mathrm{SID}_j \| R_i \| X \| X^*)$, then we just need to show $\mathcal{A}$ cannot obtain correct $R_i = h(\mathrm{ID}_i \| k)$ without three factors.

Case 1: $\mathcal{A}$ has user's password and smart card.

Kocher *et al.* [26] and Messerges *et al.* [27] pointed out that all existing smart cards are vulnerable in that the confidential information stored in the device could be extracted by physically monitoring its power consumption; once a card is lost, all the secrets in it may be revealed.

Upon getting the smart card, $\mathcal{A}$ could extract the secret value $\{Z_i, \vartheta_i, h(\cdot)\}$ stored in the smart card, where $Z_i = R_i \oplus h(\mathrm{PW}_i \| \sigma_i)$, and $R_i = h(\mathrm{ID}_i \| k)$. If $\mathcal{A}$ wants to impersonate the user, he has to compute R_i from Z_i. However, $\mathcal{A}$ cannot recover σ_i from ϑ_i since he does have biometrics of the user. Then, $\mathcal{A}$ has no ability to generate correct R_i.

Case 2: $\mathcal{A}$ has user's biometrics and a smart card.

$\mathcal{A}$ could extract the secret value $\{Z_i, \vartheta_i, h(\cdot)\}$ stored in the smart card, where $Z_i = R_i \oplus h(\mathrm{PW}_i \| \sigma_i)$, and $R_i = h(\mathrm{ID}_i \| k)$. If $\mathcal{A}$ wants to impersonate the user, he has to compute R_i from Z_i. $\mathcal{A}$ could recover σ from ϑ since he has the user's biometrics. $\mathcal{A}$ could also intercept the transmitted message $\{\mathrm{CID}_i, X, \alpha\}$, where $X = xP$, $X^* = xP_{\mathrm{pub}}$, and $\alpha = h(\mathrm{ID}_i \| \mathrm{SID}_j \| R_i \| X \| X^*)$. $\mathcal{A}$ may guess password PW' and computes $R_i' = Z_i \oplus h(\mathrm{PW}' \| \sigma_i)$. However, $\mathcal{A}$ cannot verify if PW' is correct since he has to compute $X^* = xkP$ from $X = xP$ and $P_{\mathrm{pub}} = kP$. $\mathcal{A}$ cannot compute $h(\mathrm{PW}_i \| \sigma_i)$ since he does know the user's password. Then, $\mathcal{A}$ has no ability to generate correct R_i.

Case 3: $\mathcal{A}$ has user's password and biometrics.

It is easy to say that $\mathcal{A}$ cannot generate correct R_i without the master key k since $R_i = h(\mathrm{ID}_i \| k)$. Therefore, $\mathcal{A}$ cannot impersonate the user.

From the given discussion, we know that the adversary $\mathcal{A}$ cannot generate a legal message $\{\mathrm{CID}_i, X, \alpha\}$ with only two factors. Therefore, the proposed scheme could provide three-factor security.

Perfect Forward Secrecy: In the proposed scheme, U_i and S_j will generate the session key $SK = xyP$. To obtain the session key, the adversary has to compute xyP from $X = xP$ and $Y = yP$. He has to solve the computational Diffie–Hellman problem. Then, he cannot obtain the session key even if he knows U_i and S_j secret keys. Therefore, the proposed scheme could provide perfect forward secrecy.

Privileged Insider Attack: In the user registration phase of the proposed scheme, U_i sends ID_i and $h(\mathrm{PW}_i \| \sigma_i)$ instead of PW_i. Then the privileged insider of RC cannot obtain PW_i from $h(\mathrm{PW}_i \| \sigma_i)$ since he does not know σ_i and $h(\cdot)$ is a secure hash function. Therefore, the proposed scheme could withstand the privileged insider attack.

Replay Attack: Suppose the adversary intercepts the message $\{\mathrm{CID}_i, X, \alpha\}$ and tries to impersonate U_i by replaying it to S_j. S_j could obviously find the attack by checking the validity of $\lambda = h(\mathrm{SID}_j \| \mathrm{ID}_i \| X \| Y \| SK \| \varphi)$ in Step 6 of the authentication phase since S_j generates a new Y for every session. Using the similar method, we could show U_i finds the replay attack by checking the validity of $\varphi = h(\mathrm{ID}_i \| X \| X^* \| \mathrm{SID}_j \| Y \| R_i)$. Therefore, the proposed scheme could withstand the replay attack.

Stolen Verifier Attack: In the user registration phase of the proposed scheme, RC computes U_i's secret key and sends it to U_i. RC maintains no verifier table about U_i's password or secret key. Then, the adversary cannot obtain authentication information of U_i even if he could access RC's database. Therefore, the proposed scheme could withstand the stolen verifier attack.

User Impersonation Attack: From the given discussion, we know that the adversary cannot generate a legal message $\{\mathrm{CID}_i, X, \alpha\}$, although he obtains two factors for authentication. Therefore, we conclude that the proposed scheme could withstand the user impersonation attack.

Server Spoofing Attack: To impersonate S_j to U_i and RC, the adversary has to generate the valid message $\beta = h(\mathrm{CID}_i \| X \| \alpha \| \mathrm{SID}_j \| R_j \| Y \| Y^*)$ to obtain the authentication code $\varphi = h(\mathrm{ID}_i \| X \| X^* \| \mathrm{SID}_j \| Y \| R_i)$. It is easy to know if he cannot finish the task since he has no knowledge of R_j and if $h(\cdot)$ is a secure hash function. Therefore, the proposed scheme could withstand the server spoofing attack.

Modification Attack: Suppose that the adversary modifies the message $\{\mathrm{CID}_i, X, \alpha\}$ and sends it to S_j, where $X = xP$, $X^* = xP_{\mathrm{pub}}$, $\mathrm{CID}_i = \mathrm{ID}_i \oplus h(X^*)$, and $\alpha = h(\mathrm{ID}_i \| \mathrm{SID}_j \| R_i \| X \| X^*)$. RC could find the modification by

TABLE III
COMPARISONS OF THE SECURITY PROPERTY

	Yoon et al.'s scheme [21]	Kim et al.'s scheme [22]	The proposed scheme
C1	Yes	Yes	Yes
C2	No	No	Yes
C3	No	No	Yes
C4	Yes	Yes	Yes
C5	No	No	Yes
C6	Yes	Yes	Yes
C7	Yes	Yes	Yes
C8	No	No	Yes
C9	Yes	Yes	Yes
C10	Yes	Yes	Yes
C11	Yes	Yes	Yes
C12	Yes	Yes	Yes

C1: Mutual authentication
C2: Anonymity
C3: Three-factor security
C4: Perfect forward secrecy
C5: Privileged insider attack resistance
C6: Replay attack resistance
C7: Stolen-verifier attack resistance
C8: User impersonation attack resistance
C9: Server spoofing attack resistance
C10: Modification attack resistance
C11: Man-in-the-middle attack resistance
C12: Support multi-server environment

TABLE IV
COMPARISONS OF THE COMMUNICATIONAL COST

	Yoon et al.'s scheme [21]	Kim et al.'s scheme [22]	The proposed scheme
D1	192bits	192bits	192bits
D2	192bits	192bits	192bits
D3	2496bits	2496bits	3520bits
D4	-	-	-

D1: Communicational cost of the server registration phase
D2: Communicational cost of the user registration phase
D3: Communicational cost of the authentication phase
D4: Communicational cost of the password change phase

TABLE V
COMPARISONS OF THE COMPUTATIONAL COST

	Yoon et al.'s scheme [21]	Kim et al.'s scheme [22]	The proposed scheme
User	$2T_m+5T_h$	$2T_m+5T_h$	$3T_m+7T_h$
Server	$2T_m+5T_h$	$2T_m+5T_h$	$2T_m+5T_h$
Registration center	$5T_h$	$5T_h$	$2T_m+9T_h$
Total	$4T_m+15T_h$	$4T_m+15T_h$	$10T_m+21T_h$

checking the validity of α in Step 3 of the authentication phase. Using the similar method, we could show one of the three participants could find the modification of other messages. Therefore, the proposed scheme could withstand the modification attack.

Man-in-the-Middle Attack: From the above discussion, we know that the proposed scheme could provide mutual authentication among U_i, S_j, and RC. Therefore, the proposed scheme could withstand the man-in-the-middle attack.

Support Multiserver Environment: From the description of the proposed scheme, we know that U_i could access many services from different servers and only needs to registers with RC once. Then, U_i only needs to remember one password for authentication. Therefore, the proposed scheme is suitable for the multiserver environment.

V. COMPARISONS WITH OTHER RELATED SCHEMES

In this section, we will compare the proposed scheme with two latest biometrics-based authentication schemes for multiserver environment, i.e., Yoon and Yoo's scheme [21] and Kim *et al.*'s scheme [22].

The comparison of the security property among the proposed scheme and other biometrics-based schemes [21], [22] are listed in Table III. We can see that the proposed scheme could satisfy the security property of biometrics-based authentication schemes for multiserver environment. Both of Yoon and Yoo's scheme [21] and Kim *et al.*'s scheme [22] cannot provide anonymity and three-factor security. In addition, both of the two schemes [21], [22] are vulnerable to the privileged insider attack and the user impersonation attack.

Assume that the length of identity, the block size of output length of a secure hash function, and the length of an elliptic curve point are 32, 160, and 320 bits separately. In the server registration phase, the server sends his identity SID_j, and the registration center sends $R_j = h(\mathrm{SID}_j \| k)$ to the server. Then, the communicational cost of the server registration phase is $32 + 160 = 192$ bits. In the user registration phase of the proposed scheme, the user sends the message $\{\mathrm{ID}_i, h(\mathrm{PW}_i \| \sigma_i)\}$ to the registration center. Then, the communicational cost of the user registration phase is $32 + 160 = 192$ bits. In the authentication phase of our scheme, the length of the five messages $\{\mathrm{CID}_i, X, \alpha\}$, $\{\mathrm{CID}_i, X, \alpha, C\mathrm{SID}_j, Y, \beta\}$, $\{\mathrm{TID}_i, \phi, \mathrm{TSID}_j, \varphi\}$, $\{\mathrm{TSID}_j, Y, \varphi, \eta\}$, and $\{\lambda\}$ are $160 + 320 + 160 = 640$ bits, $160 + 320 + 160 + 160 + 320 + 160 = 1280$ bits, $160 + 160 + 160 + 160$ bits $= 640$ bits, $160 + 320 + 160 + 160 = 800$ bits, and 160 bits separately. Table IV demonstrates the comparisons of communicational cost among the related schemes.

Compared with the computational cost of an elliptical curve scale multiplication operation and a hash function operation, that of a bitwise EXCLUSIVE-OR operation could be ignored. Therefore, we only need to consider the computation cost of an elliptical curve scale multiplication operation and a hash function operation in computational cost. Table V compares the computational costs in authentication phase of the proposed scheme and that of two latest biometrics-based authentication schemes for multiserver environment [21], [22].

In Tables IV and V, we can see that the proposed scheme has higher communicational cost and communicational cost than Yoon and Yoo's scheme [21] and Kim *et al.*'s scheme [22]. However, both of Yoon and Yoo's scheme and Kim *et al.*'s scheme cannot withstand the privileged insider attack and the impersonation attack. Furthermore, both of their schemes cannot provide anonymity and three-factor security. For a cryptographic protocol, the security is the most important. Then, it is worth achieving such high level of security at the cost of increasing computational cost and communicational cost slightly. The proposed scheme could overcome weaknesses in Yoon and Yoo's scheme [21] and Kim *et al.*'s scheme [22]. Therefore, the proposed scheme is more suitable for multiserver environment.

VI. Conclusion

In this paper, we propose a robust biometrics-based authentication scheme for multiserver environment using elliptical curve cryptography. Security analysis shows that the proposed scheme could satisfy security requirement of multiserver environment. Performance analysis shows that the proposed scheme could overcome weaknesses in previous schemes at the cost of increasing computational cost and communicational cost slightly. Therefore, the proposed scheme is suitable for use in distributed multiserver network environments.

Acknowledgment

The authors would like to thank Prof. V. Piuri, Prof. S. Y. Shaneyfelt, and the anonymous reviewers for their valuable comments.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York, NY, USA: Springer-Verlag, 2009.

[3] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy Mag.*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[4] X. Li, J. Niu, and M. K. Khan, "Robust Biometrics Based Three-Factor Remote User Authentication Scheme with Key Agreement," in *Proc. IEEE Int. Symp. Biometr. Security Technol.*, 2013, pp. 105–110.

[5] N. D. Sarier, "Generic constructions of biometric identity based encryption systems," in *Proc. Security Privacy Mobile Devices Wireless Commun.*, 2010, pp. 90–105.

[6] N. D. Sarier, "A new biometric identity based encryption scheme secure against DoS attacks," *Security Commun. Netw.*, vol. 4, no. 1, pp. 23–32, Jan. 2011.

[7] A. Burnett, F. Byrne, T. Dowling, and A. Duffy, "A biometric identity based signature scheme," *Int. J. Netw. Security*, vol. 5, no. 3, pp. 317–326, 2007.

[8] Y. Yang, Y. Hu, and L. Zhang, "An efficient biometric identity based signature scheme," *KSII Trans. Internet Inf. Syst.*, vol. 7, no. 8, pp. 2010–2026, Aug. 2013.

[9] F. Li and M. K. Khan, "A biometric identity-based signcryption scheme," *Future Gener. Comput. Syst.*, vol. 28, no. 1, pp. 306–310, Jan. 2012.

[10] M. Wang and D. Tang, "A bovel biometric signcryption scheme that is identity-based and group-oriented," *Appl. Math. Inf. Sci.*, vol. 6, no. 3S, pp. 849–854, 2012.

[11] J.-K. Lee, S.-R. Ryu, and K.-Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electron. Lett.*, vol. 38, no. 12, pp. 554–555, 2002.

[12] C.-H. Lin and Y.-Y. Lai, "A flexible biometrics remote user authentication scheme," *Comput. Standards & Interfaces*, vol. 27, no. 1, pp. 19–23, Nov. 2004.

[13] C.-C. Chang and I.-C. Lin, "Remarks on fingerprint-based remote user authentication scheme using smart cards," *ACM SIGOPS Oper. Syst. Rev.*, vol. 38, no. 4, pp. 91–96, Oct. 2004.

[14] H.-S. Kim, S.-W. Lee, and K.-Y. Yoo, "ID-based password authentication scheme using smart cards and fingerprints," *ACM SIGOPS Oper. Syst. Rev.*, vol. 37, no. 4, pp. 32–41, Oct. 2003.

[15] M. Scott, "Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints," *ACM SIGOPS Oper. Syst. Rev.*, vol. 38, no. 2, pp. 73–75, Apr. 2004.

[16] M.-K. Khan and J.-S. Zhang, "Improving the security of 'a flexible biometrics remote user authentication scheme," *Comput. Standards Interfaces*, vol. 29, no. 1, pp. 82–85, Jan. 2007.

[17] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 33, no. 1, pp. 1–5, Jan. 2010.

[18] X. Li, J. Niu, J. Ma, W. Wang, and C. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 73–79, Jan. 2011.

[19] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Inf. Security*, vol. 5, no. 3, pp. 145–151, Sep. 2011.

[20] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. Deng, "A generic framework for three-factor authentication: preserving security and privacy in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 8, pp. 1390–1397, Aug. 2011.

[21] E. Yoon and K. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *J. Supercomput.*, vol. 63, no. 1, pp. 235–255, Jan. 2013.

[22] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme," in *Proc. Int. Conf. Comput. Sci. Appl.*, 2012, pp. 391–406.

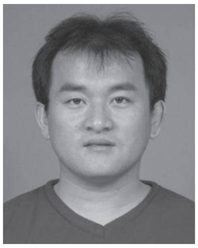
[23] D. He, Security flaws in a biometrics-based multi-server authentication with key agreement scheme, Tech. Rep. 2011/365, ePrint Archive. [Online]. Available: http://eprint.iacr.org/2011/365.pdf

[24] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptograph. Tech.*, 2004, pp. 523–540.

[25] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

[26] J. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Adv. CRYPTO*, 1999, pp. 388–397.

[27] T. Messerges, E. Dabbish, and R. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.



Debiao He (M'13) received the Ph.D. degree in applied mathematics from Wuhan University, Wuhan, China, in 2009.

He is currently a Lecturer with the School of Mathematics and Statistics, Wuhan University, and he is also with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China. His main research interests include cryptography and information security, particularly cryptographic protocols.

Ding Wang received the B.S. degree in information security from Nankai University, Tianjin, China, in 2008. He is currently working toward the Ph.D. degree with Peking University, Beijing, China.

He was with the PLA Information Engineering University, Zhengzhou, China. He is the author of a number of referred research papers at Elsevier and Wiley journals, and papers presented at conferences such as the 2012 Conference on Data and Applications Security and Privacy, the 2012 International Conference on Information and Communications Security, the 2013 Information Security Conference, and the 2014 IEEE Wireless Communications and Networking Conference. His research interests include cryptography and wireless network security.