Multimedia Tools and Applications (2019) 78:27553–27568
https://doi.org/10.1007/s11042-019-07812-w

Anonymous biometrics-based authentication with key agreement scheme for multi-server environment using ECC

Mingping Qi[1] · Jianhua Chen[1]

Received: 6 February 2018 / Revised: 12 May 2019 / Accepted: 21 May 2019 /
Published online: 24 June 2019

Abstract
The rapidly evolving communication technology has now made it easy for people to enjoy kinds of online services over the insecure public internet. However, with convenience, ensuring data security as well as user privacy and authentication is particularly important and urgent. In view of this, this work presents a new biometrics-based three-factor authentication with key agreement scheme for multi-server environment using ECC. The formal authentication proof using BAN logic confirms that the new scheme can achieve mutual authentication and agree on a common session key; and the heuristic cryptanalysis shows that the new scheme provides perfect forward secrecy, preserves user anonymity and secures against various known security vulnerabilities. Furthermore, the performance evaluation demonstrates that our scheme is efficient.

Keywords Elliptic curve cryptography · Multi-server · Biometrics · Authentication · Three-factor · Smart-card

1 Introduction

The advancement of network and communication technologies has brought more and more offline services online, and people are now enjoying high-efficiency online services such as e-health, e-commerce and e-government, etc. However, these online services are provided over the insecure public internet, where adversaries can easily perform some attacks, like privacy violating, impersonation attack, replay attack, man-in-the-middle attack, etc. To deal with these security challenges, authentication with session key agreement protocol is deployed to ensure

✉ Jianhua Chen
chenjh_ecc@163.com

Mingping Qi
mpqi_math@163.com

[1] School of Mathematics and Statistics, Wuhan University, Wuhan 430072, People's Republic of China

that only certified users can enjoy services, only the legitimate service providers can be accessed, and the exchanged critical information is secured by encryption with the negotiated session key.

1.1 Related works

In recent years, numerous authentication schemes have been designed to maintain secure communications between the remote users and the servers over the internet. Many smart-card based two-factor authentication schemes [4, 8, 9, 12, 17, 20, 21, 23, 24] were proposed in which the elliptic curve cryptography (ECC) was applied to establish security since ECC can provide the same level of security with far less key size and faster computing speed. However, all these schemes are only applicable to single-server environment and many of them have been found vulnerable to various attacks. Compared with single-server environment, multi-server environment has the obvious advantage that it enables users to access various application servers with one account. To adapt to the security requirements of multi-server environment, several kinds of authentication schemes [1, 3, 5, 6, 10, 11, 13, 15, 16, 18, 19, 22, 25] with respect to multi-server environment have therefore been presented.

In 2013, Yoon and Yoo [25] presented a biometrics-based multi-server authentication scheme using ECC, while Kim et al. [15] proved that this scheme is prone to the offline password guessing attack, and an improvement for this scheme was presented. Later, Chuang et al. [6] came up with an anonymous biometrics-based authentication scheme with respect to multi-server environment, while Mishra et al. [18] soon proved that this scheme was prone to the server spoofing, smart-card stolen and impersonation attacks, and they put forward a new scheme. However, Lu et al. [16] soon proved that Mishra et al.'s new scheme was not to secure against the forgery and server masquerading attacks, and they redesigned an authentication scheme for multi-server environment using asymmetric cryptography. Nevertheless, Lu et al.'s new scheme was soon identified by Chaudhry et al. [5] to be vulnerable to the impersonation attack.

Afterwards, Odelu et al. [19] put forward a new biometrics-based multi-server authentication scheme on the basis of He and Wang's scheme [10] with the aim to eliminate its security weaknesses. Later, Shen et al. [22] came up with a multi-server authentication scheme not preserving user anonymity. Later, Amin et al. [1] proposed an anonymity preserving authentication scheme for multi-server telemedicine information system using ECC, but very recently, their scheme was found by Irshad et al. [11] to be vulnerable to the offline password guessing and impersonation attacks. Recently, Chandrakar and Om [3] presented an anonymous three-factor authentication scheme for multi-server environment using ECC; and Jangirala et al. [13] presented a dynamic identity based multi-server authentication scheme. However, like the schemes [6, 18], Jangirala et al.'s scheme doesn't employ asymmetric cryptographic primitives to ensure security either. Thus, it fails to provide the forward secrecy.

1.2 Motivation and contributions

By investigating the related existing schemes, it can be found that various weaknesses are still within many of them. To ensure that remote users can enjoy online services and exchange critical data securely, this work designs a new robust biometrics-based authentication scheme based on previous researches for multi-server environment. The proposed scheme preserves user's biometrics template privacy by employing the fuzzy extractor [7], and the formal authentication proof by Burrows-Abadi-Needham (BAN) logic [2] shows that the new scheme can effectively realize mutual authentication and agree on a common session key. Besides, the heuristic security discussion in this paper demonstrates that our scheme can preserve user anonymity, provide perfect forward secrecy and protect users from various known security loopholes such as impersonation attack, replay attack, denial of service attack, and offline password guessing attack, etc. In addition, since our scheme has the advantage in network architecture design, i.e. the registration center in our scheme will no longer participate in the subsequent user-server session key negotiation processes after completing the user authentication, thus greatly reducing computation and communication costs in the authentication with key agreement phase. Hence, besides the security attributes, our new scheme has advantages over other relevant schemes in terms of computation and communication costs.

1.3 Organizations

The rest of this article is arranged as follows. Section 2 describes the necessary preliminaries. Section 3 introduces our new biometrics-based authentication with key agreement scheme for multi-server environment. The authentication proof by BAN logic is presented in Section 4; the security analysis of the proposed scheme is presented in Section 5; and the performance evaluation is presented in Section 6. Finally, conclusions are given in Section 7.

2 Preliminaries

This section briefly lists the notations used throughout this work, and introduces the essential notion and definitions of ECC and the fuzzy extractor.

2.1 Notation guide

The meaning of the frequently used notations in this paper is shown in Table 1.

Table 1 Notations & descriptions

Notations	Descriptions
RC	the registration center
n, p	two sufficiently large prime numbers
F_p	a prime finite field
x	the master secret key of RC
$E_p(a, b)$	an non-singular elliptic curve E over F_p, defined by $y^2 = x^3 + ax + b \mod p$
G	a base point over $E_p(a, b)$ with prime order n
P_{pub}	the public key of RC
U_i	the ith user
S_j	the jth server
ID_i, pw_i, B_i	U_i's identity, password, biometrics
SID_j	S_j's identity
Z_n^*	the interval $[1, n-1]$
$H(\cdot), h(\cdot)$	two secure one-way hash functions
$\oplus$	the bitwise XOR operation
$\|$	the concatenation operation
Δt	the preset threshold
SC_i	U_i's smart card

2.2 Elliptic curve over a prime field F_p

Let the symbol $E_p(a, b)$ denote an elliptic curve E over a prime finite field F_p, defined by the non-singular elliptic curve equation: $y^2 = x^3 + ax + b \ mod \ p, \ a, \ b \in F_p$ with the *discriminant*: $\Delta = 4a^3 + 27b^2 \ mod \ p \neq 0$. That is,
$E_p(a,b) = \{(x,y): x,y \in F_p, y^2 = x^3 + ax + b \ \ mod \ \ p, \Delta = 4a^3 + 27b^2 \ \ mod \ \ p \neq 0, \ a,b \in F_p\} \cup \{\mathcal{O}\}$.

The scalar multiplication over $E_p(a, b)$ defined as $tP = P + P + \cdots + P$ (t *times*).

A point P has order n if $nP = \mathcal{O}$ for the smallest integer $n > 0$, where $\mathcal{O}$ is the extra point called infinity point.

Definition 1 Elliptic curve discrete logarithm problem (ECDLP) is defined as follows: Given $P \in E_p(a, b)$ with order n and $Q = kP \in E_p(a, b)$, it is infeasible to derive the integer $k \in [1, n-1]$.

Definition 2 Computational Diffie-Hellman problem (CDHP) is defined as follows: Given P, aP, $bP \in E_p(a, b)$, it is intractable to compute $abP \in E_p(a, b)$.

2.3 Fuzzy extractor

Fuzzy extractor [7] is used to extract a uniform random string σ_i from the inputted biometrics template B_i in an error-tolerant way, which means σ_i can be derived each time with a noisy biometrics template B_i^* and an auxiliary string θ_i if B_i^* is reasonably similar to the original B_i. A fuzzy extractor comprises two procedures, namely, the probabilistic generation procedure *Gen* and the deterministic reproduction procedure *Rep*. More concrete descriptions are as follows:

(1) $(\sigma_i, \theta_i) = Gen(B_i)$ means when receiving the inputted biometrics B_i, *Gen* outputs a uniform random string σ_i and an auxiliary string θ_i.
(2) $\sigma_i = Rep(B_i^*, \theta_i)$ means *Rep* can recover σ_i with the noisy biometrics B_i^* and the corresponding random auxiliary string θ_i when $dis(B_i^*, B_i) < \Delta t$, where *dis* represents the distance function and Δt is the error threshold.

3 Our proposed scheme

This section presents our new biometrics-based authentication with key agreement protocol for multi-server environment, which comprises the following four phases.

3.1 System initialization phase

The registration center *RC* first takes the following steps to initialize the system parameters.

(1) *RC* selects an non-singular elliptic curve $E_p(a, b)$ with a large prime order n, and a base point G with the order n over $E_p(a, b)$.
(2) *RC* selects two cryptographic hash functions: $H : \{0,1\}^* \rightarrow Z_p^*$, $h : \{0,1\}^* \rightarrow Z_p^*$.

(3) RC generates its private key $x \in Z_n^*$ which should be kept secret strictly, and then computes its public key $P_{pub} = x \cdot G$.
(4) RC publishes the system parameters $\{E_p(a, b), G, n, P_{pub}, H(\cdot), h(\cdot)\}$.

3.2 Registration phase

The registration phase of our scheme comprises the following two phases.

3.2.1 Server registration phase

To deploy a new server S_j to be a legal server, the following steps also shown in Fig. 1 need to be executed.

(1) S_j selects its identity SID_j and transmits it to RC via a secure channel.
(2) RC generates a random number r_j and computes the secret key $k_j = h(SID_j \| x \| r_j)$, then stores $\{SID_j, r_j\}$ into its security database and transmits k_j back to S_j via a secure channel, where x is the system private key.
(3) Upon receiving k_j, S_j keeps it secretly.

3.2.2 User registration phase

To be a legal user, U_i needs to take the following steps also shown in Fig. 2, to register in RC.

(1) U_i inputs his/her identity ID_i, pw_i and imprints B_i on a sensor.
(2) U_i computes $(\sigma_i, \theta_i) = Gen(B_i)$, $MP_i = h(pw_i \| \sigma_i)$ and transmits ID_i, MP_i to RC by a secure channel.
(3) Upon receiving ID_i and MP_i, RC checks the validity of ID_i and whether $h(ID_i)$ exists in RC's user database. If not, RC stores $h(ID_i)$ in its user database and computes $r_i = h(ID_i \| x)$ $k_i = r_i \oplus MP_i$, $v_i = H(ID_i \| r_i \| MP_i)$, where x is the system private key, and then RC stores $\{k_i, v_i, H(\cdot), h(\cdot)\}$ into a smart-card SC_i and returns it back to U_i; otherwise RC aborts the procedure.
(4) After receiving SC_i, U_i stores θ_i into SC_i.

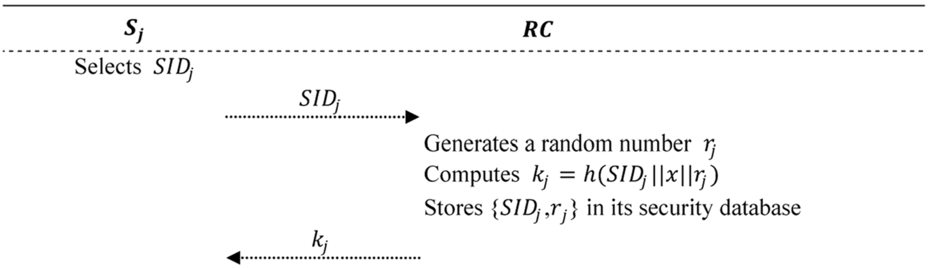

Fig. 1 Server registration phase

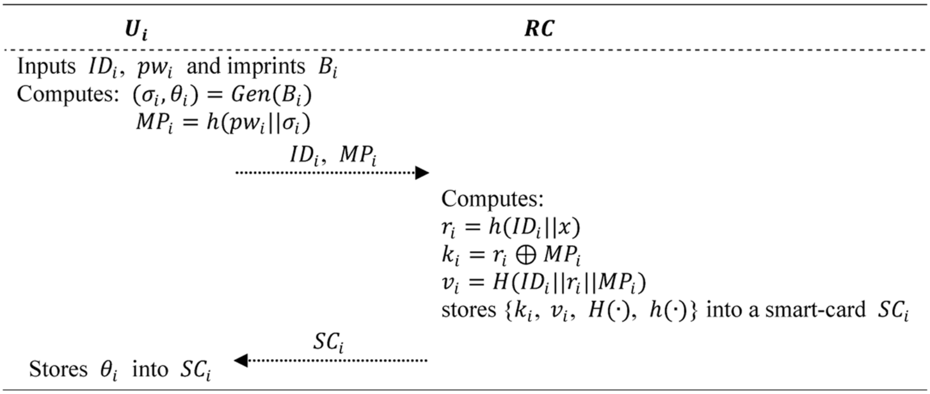

Fig. 2 User registration phase

3.3 Login and mutual authentication with key agreement phase

Assume that a remote user U_i wants to enjoy online services from S_j, then, he/she needs to perform the following steps to accomplish the mutual authentication processes and agree on a session key for encrypting the subsequent communications over the insecure public channel as shown in Fig. 3.

(1) U_i inserts his/her smart-card SC_i into a card reader, then inputs ID_i, pw_i, and imprints B_i at a sensor.

(2) SC_i computes $\sigma_i = Rep(B_i, \theta_i)$, $MP_i^{'} = h(pw_i \| \sigma_i)$, $r_i = k_i \oplus MP_i^{'}$, and checks whether $v_i = H\left(ID_i \| r_i \| MP_i^{'}\right)$ holds. If not, SC_i rejects U_i, otherwise, SC_i generates a random number α to compute $X = \alpha \cdot G$, $K = \alpha \cdot P_{pub}$, $k = h(K)$, $c_1 = E_k(SID_j \| ID_i \| H(r_i \| X \| t_1))$, where t_1 is the current timestamp of U_i, and sends $\{c_1, X, t_1\}$ to RC.

(3) Upon receiving the message $\{c_1, X, t_1\}$, RC gets its current timestamp $t_1^{'}$ and checks whether $t_1^{'} - t_1 < \Delta t$ holds. If not, RC aborts the procedure, otherwise, RC computes $K^{'} = x \cdot X$, $k^{'} = h(K^{'})$, $SID_j^{'} \| ID_i^{'} \| H^{'}(r_i \| X \| t_1) = D_{k^{'}}(c_1)$, $r_i^{'} = H\left(ID_i^{'} \| x\right)$ and checks whether $H^{'}(r_i \| X \| t_1) = H\left(r_i^{'} \| X \| t_1\right)$ holds. If not, RC aborts the procedure; otherwise, RC retrieves the random number r_j by $SID_j^{'}$ and computes $k_j = h\left(SID_j^{'} \| x \| r_j\right)$, $che = H\left(ID_i^{'} \| H\left(r_i^{'}\right) \| X\right)$, $c_2 = E_{k_j}\left(SID_j^{'} \| ID_i^{'} \| H\left(r_i^{'}\right) \| X \| che \| t_2\right)$ and sends $\{c_2, t_2\}$ to S_j.

(4) Upon receiving the message $\{c_2, t_2\}$, S_j gets its current timestamp $t_2^{'}$ and checks whether $t_2^{'} - t_2 < \Delta t$ holds. If not, S_j aborts the procedure, otherwise, computes $SID_j^{'} \| ID_i^{'} \| H\left(r_i^{'}\right) \| X \| che^{'} \| t_2^{'} = D_{k_j}(c_2)$ and checks whether $t_2^{'} = t_2$ and $che^{'} = H\left(ID_i^{'} \| H\left(r_i^{'}\right) \| X\right)$ hold. If not, S_j aborts the procedure, otherwise, generates a random number β to compute $Y = \beta \cdot G$, $Z = \beta \cdot X$, $SK_s = h\left(ID_i^{'} \| SID_j \| H\left(r_i^{'}\right) \| X \| Y \| Z\right)$, $V_j = H\left(SK_s \| H\left(r_i^{'}\right) \| X \| Y \| t_3\right)$ where t_3 is the current timestamp of S_j, and sends $\{V_j, Y, t_3\}$ to U_i.

(5) Upon receiving the message $\{V_j, Y, t_3\}$, U_i gets its current time stamp $t_3^{'}$ and checks whether $t_3^{'} - t_3 < \Delta t$ holds. If not, U_i aborts the procedure, otherwise, computes $Z = \alpha \cdot Y$, $SK_i = h(ID_i \| SID_j \| H(r_i) \| X \| Y \| Z)$ and checks $V_j ?= H(SK_i \| H(r_i) \| X \| Y \| t_3)$; if not, U_i aborts the procedure, otherwise, accepts $SK = h(ID_i \| SID_j \| H(r_i) \| X \| Y \| Z)$ as the session key, then, computes $V_i = H(SK_i \| H(r_i) \| Y)$ and sends $\{V_i\}$ to S_j.

U_i	RC	S_j
Inputs ID_i, pw_i and imprints B_i Computes $\sigma_i = Rep(B_i, \theta_i)$, $MP_i' = h(pw_i\|\|\sigma_i)$ $r_i = k_i \oplus MP_i'$ Checks $v_i \ ?= H(ID_i\|\|r_i\|\|MP_i')$ Generates a random number α $X = \alpha \cdot G$, $K = \alpha \cdot P_{pub}$ $k = h(K)$ $c_1 = E_k(SID_j\|\|ID_i\|\|H(r_i\|\|X\|\|t_1))$		
$\{c_1, X, t_1\}$ →		
	$t_1' - t_1 < \Delta t$, aborts if not true $K' = x \cdot X$ $k' = h(K')$ $SID_j'\|\|ID_i'\|\|H'(r_i\|\|X\|\|t_1) = D_{k'}(c_1)$ $r_i' = h(ID_i'\|\|x)$ Checks $H'(r_i\|\|X\|\|t_1) \ ?= H(r_i'\|\|X\|\|t_1)$ Retrieves the random number r_j by SID_j' $k_j = h(SID_j'\|\|x\|\|r_j)$ $che = H(ID_i'\|\|H(r_i')\|\|X)$ $c_2 = E_{k_j}(SID_j'\|\|ID_i'\|\|H(r_i')\|\|X\|\|che\|\|t_2)$	
	$\{c_2, t_2\}$ →	
		$t_2' - t_2 < \Delta t$, aborts if not true $SID_j'\|\|ID_i'\|\|H(r_i')\|\|X\|\|che'\|\|t_2' = D_{k_j}(c_2)$ Checks $t_2' \ ?= t_2$ $che' \ ?= H(ID_i'\|\|H(r_i')\|\|X)$ Generates a random number β $Y = \beta \cdot G$, $Z = \beta \cdot X$ $SK_s = h(ID_i'\|\|SID_j\|\|H(r_i')\|\|X\|\|Y\|\|Z)$ $V_j = H(SK_s\|\|H(r_i')\|\|X\|\|Y\|\|t_3)$
← $\{V_j, Y, t_3\}$		
$t_3' - t_3 < \Delta t$, aborts if not true $Z = \alpha \cdot Y$ $SK_i = h(ID_i\|\|SID_j\|\|H(r_i)\|\|X\|\|Y\|\|Z)$ Checks $V_j \ ?= H(SK_i\|\|H(r_i)\|\|X\|\|Y\|\|t_3)$ $V_i = H(SK_i\|\|H(r_i)\|\|Y)$		
$\{V_i\}$ →		
		Checks $V_i \ ?= H(SK_s\|\|H(r_i')\|\|Y)$

Fig. 3 Login and mutual authentication with key agreement phase

(6) Upon receiving the message $\{V_i\}$, S_j checks $V_i? = H\left(SK_s \| H\left(r_i'\right) \| Y\right)$. If not, S_j aborts the procedure, otherwise, S_j accepts $SK = h(ID_i \| SID_j \| H(r_i) \| X \| Y \| Z)$ as the session key for subsequent communications.

3.4 Password change phase

A legal user U_i may for security reasons need to change the old password pw_i, and then, he/she just needs take the following steps without connecting to RC or S_j.

(1) U_i inserts his/her smart card SC_i into a card reader, then inputs ID_i, pw_i and imprints B_i at a sensor.
(2) SC_i computes $\sigma_i = Rep(B_i, \theta_i)$, $MP_i^{'} = h(pw_i \| \sigma_i)$, $r_i = k_i \oplus MP_i^{'}$, and checks whether $v_i = H\left(ID_i \| r_i \| MP_i^{'}\right)$ holds. If not, SC_i rejects U_i; otherwise, SC_i asks U_i to input new password pw_i^*.
(3) Upon receiving pw_i^*, SC_i computes $MP_i^* = h\left(pw_i^* \| \sigma_i\right)$, $k_i^* = k_i \oplus MP_i \oplus MP_i^*$, $v_i^* = H\left(ID_i \| r_i \| MP_i^*\right)$ and replaces k_i, v_i with k_i^*, v_i^*, respectively.

4 Authentication proof by BAN logic

This section formally proves that our new scheme can achieve mutual authentication with session key agreement by BAN logic [2]. Detailed proof is as follows.

- **BAN logic notations:**

– $P \mid \equiv X$: The principal P believes X.
– $\#(X)$: The formula X is fresh.
– $P \Rightarrow X$: P has jurisdiction over X.
– $P \mid \sim X$: P once said the statement X.
– $P \mid \lhd X$: P sees the statement X.
– (X, Y): X or Y is one part of the (X, Y).
– $\{X\}_K$: X is encrypted with the key K.
– $(X)_K$: X is hashed with the key K.
– $\langle X \rangle_K$: X is combined with the key K.
– $P \overset{K}{\leftrightarrow} Q$: P and Q use the shared session key K to communicate, and K will never be discovered by any principal except P and Q.

- **BAN logic rules:**

– $Rule(1):$ Message-meaning rule: $\frac{P|\equiv P \overset{K}{\leftrightarrow} Q, \quad P \mid \lhd \{X\}_K}{P|\equiv Q|\sim X}$
– $Rule(2):$ Nonce-verification rule: $\frac{P|\equiv \#(X), \quad P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$
– $Rule(3):$ Jurisdication rule: $\frac{P|\equiv Q \Rightarrow X, \quad P|\equiv Q|\equiv X}{P|\equiv X}$
– $Rule(4):$ Freshness-conjuncatenation rule: $\frac{P|\equiv \#(X)}{P|\equiv \#(X, \quad Y)}$

- **Establishment of security goals:**

– $Goal$ 1: $S_j|\equiv U_i \overset{H(r_i)}{\longleftrightarrow} S_j$.
– $Goal$ 2: $U_i\big|\equiv S_j\big|\equiv U_i \overset{SK_s}{\longleftrightarrow} S_j$.
– $Goal$ 3: $U_i\big|\equiv U_i \overset{SK_s}{\longleftrightarrow} S_j$.
– $Goal$ 4: $S_j|\equiv U_i|\equiv U_i \overset{SK_i}{\longleftrightarrow} S_j$.
– $Goal$ 5: $S_j|\equiv U_i \overset{SK_i}{\longleftrightarrow} S_j$.

- **Idealized the proposed scheme**

$$M_1\ (U_i \rightarrow RC):\ \left\{\{SID_j, ID_i, H(r_i||X||t_1)\}_k, X, t_1\right\}$$
$$M_2\ (RC \rightarrow S_j):\ \left\{\left\{SID_j', ID_i', U_i \overset{H(r_i)}{\longleftrightarrow} S_j, X, che, t_2\right\}_{k_j}, t_2\right\}$$
$$M_3\ (S_j \rightarrow U_i):\ \left\{\left(U_i \overset{SK_s}{\longleftrightarrow} S_j, X, Y, t_3\right)_{H(r_i)}, Y, t_3\right\}$$
$$M_4\ (U_i \rightarrow S_j):\ \left\{\left(U_i \overset{SK_i}{\longleftrightarrow} S_j, Y\right)_{H(r_i)}\right\}$$

- **Hypotheses of the proposed scheme**

$$H_1 : U_i|\equiv\#(X = \alpha\cdot G)$$
$$H_2 : S_j|\equiv\#(Y = \beta\cdot G)$$
$$H_3 : S_j|\equiv\#(t_2)$$
$$H_4 : U_i|\equiv U_i \overset{H(r_i)}{\longleftrightarrow} S_j$$
$$H_5 : S_j|\equiv S_j \overset{k_j}{\longleftrightarrow} RC$$
$$H_6 : S_j|\equiv RC \Rightarrow U_i \overset{H(r_i)}{\longleftrightarrow} S_j$$
$$H_7 : U_i|\equiv S_j \Rightarrow U_i \overset{SK_s}{\longleftrightarrow} S_j$$
$$H_8 : S_j|\equiv U_i \Rightarrow U_i \overset{SK_i}{\longleftrightarrow} S_j$$

- **The proof of our proposed scheme**

– According to M_2, we have

$$S_1 : S_j \triangleleft \left\{SID_j', ID_i', U_i \overset{H(r_i)}{\longleftrightarrow} S_j, X, che, t_2\right\}_{k_j}$$

– According to S_1, H_5 and *Rule*(1), we have

$$S_2 : S_j|\equiv RC\ |\sim\left\{SID_j', ID_i', U_i \overset{H(r_i)}{\longleftrightarrow} S_j, X, che, t_2\right\}$$

– According to S_2, H_3, *Rule*(4) and *Rule*(2), we have

$$S_3 : S_j|\equiv RC|\equiv\left\{SID_j', ID_i', U_i \overset{H(r_i)}{\longleftrightarrow} S_j, X, che, t_2\right\}$$

– According to S_3, we have

$$S_4 : S_j|\equiv RC|\equiv U_i \overset{H(r_i)}{\longleftrightarrow} S_j$$

- According to S_4, H_6 and $Rule(3)$, we have

$$S_5 : S_j|\equiv U_i \overset{H(r_i)}{\longleftrightarrow} S_j \quad (\textbf{Goal 1})$$

- According to M_3, we have

$$S_6 : U_i \lhd \left(U_i \overset{SK_s}{\longleftrightarrow} S_j, X, Y, t_3\right)_{H(r_i)}$$

- According to S_6, H_4 and $Rule(1)$, we have

$$S_7 : U_i|\equiv S_j|\sim\left(U_i \overset{SK_s}{\longleftrightarrow} S_j, X, Y, t_3\right)$$

- According to H_1, $Rule(4)$, S_7 and $Rule(2)$, we have

$$S_8 : U_i|\equiv S_j|\equiv\left(U_i \overset{SK_s}{\longleftrightarrow} S_j, X, Y, t_3\right)$$

- According to S_8, we have

$$\mathrm{S}_9 : U_i|\equiv S_j|\equiv U_i \overset{SK_s}{\longleftrightarrow} S_j \quad (\textbf{Goal 2})$$

- According to H_7, S_9 and $Rule(3)$, we have

$$\mathrm{S}_{10} : U_i|\equiv U_i \overset{SK_s}{\longleftrightarrow} S_j \quad (\textbf{Goal 3})$$

- According to M_4, we have

$$S_{11} : S_j \lhd \left(U_i \overset{SK_i}{\longleftrightarrow} S_j, Y\right)_{H(r_i)}$$

- According to S_5, S_{11} and $Rule(1)$, we have

$$S_{12} : S_j|\equiv U_i|\sim\left(U_i \overset{SK_i}{\longleftrightarrow} S_j, Y\right)$$

- According to H_2, $Rule(4)$, S_{12} and $Rule(2)$, we have

$$S_{13} : S_j|\equiv U_i|\equiv\left(U_i \overset{SK_i}{\longleftrightarrow} S_j, Y\right)$$

- According to S_{13}, we have

$$S_{14} : S_j|\equiv U_i|\equiv U_i \overset{SK_i}{\longleftrightarrow} S_j \quad (\textbf{Goal 4})$$

- According to H_8, S_{14} and $Rule(3)$, we have

$$S_{15} : S_j|\equiv U_i \overset{SK_i}{\longleftrightarrow} S_j \quad (\textbf{Goal 5})$$

5 Security analysis

This section demonstrates how our scheme accomplishes perfect security requirements and resists all well known attacks in the heuristic way. Detailed analysis is as follows.

5.1 Perfect forward secrecy

The negotiated session key is $SK = h(ID_i \| SID_j \| H(r_i) \| X \| Y \| Z)$ in our scheme, where $X = \alpha \cdot G$, $Y = \beta \cdot G$, $Z = \alpha\beta \cdot G$, α and β are randomly generated in every session by U_i and S_j respectively. If an adversary A tries to derive α and β by $X = \alpha \cdot G$ and $Y = \beta \cdot G$, then A has to resolve the ECDLP, which is well-known impossible. Meanwhile, the session key SK is obviously independent of the system private key x, so even if x is leaked to A, he/she cannot get any information about the former established session keys. Thus, our scheme provides perfect forward secrecy.

5.2 User anonymity

In our scheme, U_i's original identity ID_i together with other parameters are first encrypted by k and transmitted to RC, where $k = h(K)$ and $K = \alpha \cdot P_{pub}$ are dynamic for that α is randomly generated in every session. Then, the ID_i is encrypted by RC with the shared secret key $k_j = h(SID_j \| x \| r_j)$ between RC and S_j, and the cipher text is transmitted to S_j. For an adversary A, if he/she wants to derive ID_i, then he/she has to get K or k_j, which further requires him/her to get the system private key x or solve the ECDLP ($X = \alpha \cdot G$) to obtain α. Obviously, that is impossible. So, our scheme preserves user anonymity.

5.3 Impersonation attack

In our scheme, a patient U_i must be first authenticated by RC before accessing to S_j, so if an adversary A wants to impersonate U_i, he/she has to pass the verification test performed by RC. Thus, A must try to compute $r_i = h(ID_i \| x)$, which requires A to obtain U_i's ID_i and the system private key x at the same time. Obviously, that is impossible. Another way to deceive RC is to obtain U_i's ID_i, pw_i, biometrics B_i, and smart-card SC_i simultaneously, which is also obviously impossible. Analogously, for an illegal S_j, without the secret k_j, it cannot get the parameter $H\left(r_i^{'}\right)$, and thus it cannot forge the valid message $V_j = H\left(SK_s \| H\left(r_i^{'}\right) \| X \| Y \| t_3\right)$ to deceive U_i. So, the impersonation attack is infeasible in our scheme.

5.4 Replay attack

A legal user U_i's previous login message $\{c_1, X, t_1\}$ may be intercepted by an adversary A, then A may try to replay the old message to RC, but RC will reject A for $t_1^{'} - t_1 > \Delta t$ will hold. Further, A may modify the timestamp t_1 to satisfy the condition $t_1^{'} - t_1 < \Delta t$, but RC will also reject A for the validation equation $H^{'}(r_i \| X \| t_1)? = H\left(r_i^{'} \| X \| t_1\right)$ embedded with the original timestamp t_1. If t_1 is modified, $H^{'}(r_i \| X \| t_1) \neq H\left(r_i^{'} \| X \| t_1\right)$ will hold, then RC will reject A. Analogously, A cannot replay the old messages exchanged between RC/U_i and S_j to deceive the participants. So, the replay attack is infeasible in our scheme.

5.5 Man-in-the-middle attack

For an adversary A to perform the man-in-the-middle attack, he/she needs to establish independent connections with the legal participants and replay messages between them, making them mistaken that they are talking directly to each other. Thus, A needs to successfully deceive U_i and S_j at the same time, which further requires A to obtain $H(r_i) = H(h(ID_i \| x))$ or $k_j = h(SID_j \| x \| r_j)$, and then A has to get the system private key x, which is obviously impossible. So, the man-in-the-middle attack is infeasible in our scheme.

5.6 Stolen-verifier attack

In our scheme, RC just stores $h(ID_i)$ which is useless to an adversary A, moreover, RC and S_j don't store U_i's pw_i and biometrics B_i at all. Thus, even if A breaks into RC or S_j, there are no useful authentication credentials for him/her to steal. So, the stolen-verifier attack is infeasible in our scheme.

5.7 Privileged insider attack

In our scheme, U_i's password pw_i and biometrics B_i never leave the user side, and only in the registration phase does U_i send $MP_i = h(pw_i \| \sigma_i)$ to RC, which is embedded with his/her password pw_i. It is obvious that the password pw_i is protected by one-way hash function with the random string σ_i derived by $(\sigma_i, \theta_i) = Gen(B_i)$. Thus, it is impossible for an insider to get U_i's password pw_i and biometrics B_i throughout our scheme. So, the privileged insider attack is infeasible in our scheme.

5.8 Denial of service attack

In our scheme, before launching the login message, the legality of a user U_i is first verified by the smart-card SC_i by checking whether $v_i = H\left(ID_i \| r_i \| MP_i^{'}\right)$ holds, where $r_i = k_i \oplus MP_i^{'}$, $MP_i^{'} = h(pw_i \| \sigma_i)$, $\sigma_i = Rep(B_i, \theta_i)$. If not, SC_i will directly reject U_i. In other words, only when U_i is first authenticated by SC_i locally, the login message is sent to RC. Besides, there is no information needed to be synchronized for SC_i, S_j and RC in each session. So, the denial of service attack is infeasible in our scheme.

5.9 Offline password guessing attack

Suppose that an adversary A has got U_i's smart-card SC_i by some means, and extracted the stored parameters k_i, v_i and θ_i from SC_i by side-channel attacks, then, to guess U_i's password pw_i by the equation $v_i = H(ID_i \| r_i \| MP_i)$, where $MP_i = h(pw_i \| \sigma_i)$, A has to obtain U_i's biometrics B_i to compute σ_i by $\sigma_i = Rep(B_i, \theta_i)$, which is almost impossible. So, the offline password guessing attack is infeasible in our scheme.

6 Performance evaluation

We've chosen the recent biometrics based authentication schemes [1, 10] for comparison since they have the same technology backgrounds with our scheme, i.e. all are biometrics based

Table 2 Security comparison

	Scheme		
	[10]	[1]	Our
Authentication with session key agreement	✓	✓	✓
Perfect forward secrecy	✓	✓	✓
User anonymity	✓	✓	✓
Impersonation attack resistance	✗	✗	✓
Replay attack resistance	✓	✓	✓
Man-in-the-middle attack resistance	✓	✓	✓
Stolen-verifier attack resistance	✓	✓	✓
Privileged insider attack resistance	✓	✓	✓
Denial of service attack resistance	✗	✓	✓
Offline password guessing attack resistance	✓	✗	✓

using ECC as the cryptographic foundation. Moreover both the schemes were designed for generic multi-server environments rather than a specific application environment, which are consistent with ours from the design goal. So, this section compares our proposed scheme with them in security, computation and communication costs aspects. Table 2 shows these schemes' abilities to resist the identified attacks, which signifies the robustness of our proposed scheme over the others. To conveniently evaluate our scheme with other relevant schemes in the aspects of computation and communication costs, we assume that the length of identity, timestamp, hash digest and an elliptic curve point are 64, 64, 160 and 320 bits respectively, and use the following notations to depict time complexities of different operations:

- T_m: the time for executing elliptic curve scalar point multiplication
- T_s: the time for executing symmetric encryption/decryption operation
- T_h: the time for executing hash function
- T_G: the time for executing the fuzzy extractor operation *Gen*

According to the experimental results of Kilinc and Yanik [14], T_m, T_s and T_h approximately take 2.226, 0.0046 and 0.0023 ms respectively. And we here assume that the time complexity of $Gen(\cdot)$ is the same with the elliptic curve scalar point multiplication. Then, the detailed comparison of the computation and communication costs of registration phase and

Table 3 Computation and communication costs comparison of the registration phase

scheme	User registration		Server registration	
	U_i	RC	S	RC
Computation cost:				
[10]	T_G	$2T_h$	–	T_h
[1]	–	T_m+2T_h	–	T_h
Our	T_G+T_h	$2T_h$	–	T_h
Communication cost:				
[10]	224 bits		224 bits	
[1]	288 bits		224 bits	
Our	224 bits		224 bits	

Table 4 Computation and communication costs comparison of the AKA phase

	Scheme		
	[10]	[1]	Our
Computation cost:			
U_i	$3T_m + 7T_h$	$4T_m + 1T_s + 7T_h$	$3T_m + 1T_s + 7T_h$
S_j	$3T_m + 5T_h$	$4T_m + 2T_s + 5T_h$	$2T_m + 1T_s + 3T_h$
RC	$2T_m + 9T_h$	$3T_m + 1T_s + 6T_h$	$1T_m + 2T_s + 6T_h$
Total cost	$8T_m + 21T_h$	$11T_m + 4T_s + 18T_h$	$6T_m + 4T_s + 16T_h$
Execution time	17.856 ms	24.546 ms	13.411 ms
Communication cost:	3520 bits	1792 bits	1408 bits

authentication with key agreement (AKA) phase between our scheme and the others are demonstrated in Tables 3 and 4. According to Table 3, we can see that the computation and communication costs of registration phase are almost the same in all schemes. According to Table 4, our proposed scheme consumes the lowest computation cost of 13.411 ms and communication cost of 1408 bits in the AKA phase, while the scheme [10] bears the average computation cost of 17.856 ms and communication cost of 3520 bits, and the scheme [1] bears the average computation cost of 24.546 ms and communication cost of 1792 bits. So, in the light of the fact demonstrated in Tables 2, 3 and 4, it can be concluded that our new scheme has advantages over the others, whether in terms of security and functionalities or computation and communication costs.

7 Conclusions

This work presents our biometrics-based mutual authentication with session key agreement scheme for multi-server environment. The security analysis demonstrates that our scheme has perfect security features and can resist various known attacks. The performance evaluation shows that our new scheme is more efficient in the aspects of computation cost and communication cost, for the *RC* no longer participates in the subsequent user-server session key negotiation processes after it authenticates the user, and thus reducing the computation and communication costs. Hence, it can be said that our new scheme is a more suitable authentication key exchange protocol for multi-server environment.

References

1. Amin R, Islam SH, Biswas GP, Khan MK, Kumar N (2015) An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography. J Med Syst 39(11):1–18
2. Burrows M, Abadi M, Needham R (1990) A logic of authentication. ACM Trans Comput Syst 8(1):18–36
3. Chandrakar P, Om H (2017) A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. Comput Commun 110:26–34
4. Chaudhry SA, Naqvi H, Sher M, Farash MS, Hassan MU (2015) An improved and provably secure privacy preserving authentication protocol for SIP. Peer-to-Peer Networking and Applications 10:1–15
5. Chaudhry SA, Naqvi H, Farash MS et al (2015) An improved and robust biometrics-based three factor authentication scheme for multiserver environments. J Supercomput:1–17
6. Chuang MC, Chen MC (2014) An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Syst Appl 41(4):1411–1418

7. Dodis Y, Reyzin L (2008) Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM J Comput 38(1):97–139
8. Farash MS (2016) Security analysis and enhancements of an improved authentication for session initiation protocol with provable security. Peer-to-Peer Networking and Applications 9(1):82–91
9. Farash MS, Attari MA (2014) A secure and efficient identity-based authenticated key exchange protocol for mobile client–server networks. J Supercomput 69(1):395–411
10. He D, Wang D (2015) Robust biometrics-based authentication scheme for multiserver environment. IEEE Syst J 9(3):816–823
11. Irshad A, Sher M, Nawaz O, Chaudhry SA, Khan I, Kumari S (2017) A secure and provable multi-server authenticated key agreement for tmis based on amin et al. scheme. Multimed Tools Appl 76(15):1–27
12. Islam SH, Biswas GP (2011) A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. J Syst Softw 84(11):1892–1898
13. Jangirala S, Mukhopadhyay S, Das AK (2017) A multi-server environment with secure and efficient remote user authentication scheme based on dynamic id using smart cards. Wirel Pers Commun:1–33
14. Kilinc HH, Yanik T (2014) A survey of SIP authentication and key agreement schemes. IEEE Communications Surveys & Tutorials 16(2):1005–1023
15. Kim H, Jeon W, Lee K, Lee Y, Won D (2012) Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme. In: International Conference on Computational Science and ITS Applications. Springer-Verlag, pp 391–406
16. Lu Y, Li L, Peng H et al (2015) A biometrics and smart cards-based authentication scheme for multi-server environments. Security & Communication Networks 8(17):3219–3228
17. Maitra T, Obaidat MS, Islam SH, Giri D, Amin R (2016) Security analysis and design of an efficient ECC-based two-factor password authentication scheme. Security & Communication Networks 9(17):4166–4181
18. Mishra D, Das AK, Mukhopadhyay S (2014) A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Syst Appl 41(18):8129–8143
19. Odelu V, Das AK, Goswami A (2015) A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Transactions on Information Forensics & Security 10(9):1953–1966
20. Qi M, Chen J (2017) An efficient two-party authentication key exchange protocol for mobile environment. Int J Commun Syst. https://doi.org/10.1002/dac.3341
21. Qi M, Chen J (2017) An enhanced authentication with key agreement scheme for satellite communication systems. Int J Satell Commun Netw. https://doi.org/10.1002/sat.1218
22. Shen H, Gao C, He D, Wu L (2015) New biometrics-based authentication scheme for multi-server environment in critical systems. J Ambient Intell Humaniz Comput 6(6):825–834
23. Wang RC, Juang WS, Lei CL (2011) Robust authentication and key agreement scheme preserving the privacy of secret key. Comput Commun 34(3):274–280
24. Wu F, Xu L, Kumari S et al (2015) A new authenticated key agreement scheme based on smart cards providing user anonymity with formal proof. Security & Communication Networks 8(18):3847–3863
25. Yoon EJ, Yoo KY (2013) Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. J Supercomput 63(1):235–255

Mingping Qi received his MS degree in applied mathematics from Wuhan University, China, in 2015. Now, he is working as a PhD candidate in applied mathematics in Wuhan University. His research interests include public key cryptography especially ECC, network security and cryptographic protocol.

Jianhua Chen received his BS degree in applied mathematics from Harbin Institute of Technology, Harbin, China, in 1983, and received his MS and PhD degree in applied mathematics from Wuhan University, Wuhan, China, in 1989 and 1994, respectively. Currently, he is a professor of Wuhan University. His current research interests include number theory, information security, and network security.