International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.215-226
http://dx.doi.org/10.14257/ijsia.2016.10.10.20

A Secure and Efficient Multi-Factor Mutual Certificateless Authentication with Key Agreement Protocol for Mobile Client-Server Environment on ECC without the third-party

Liling Cao[1*] and Wancheng Ge[2]

Department of Electronic and Information Engineering, Tongji University, Shanghai 201306, China
[1]llcao@shou.edu.cn, [2]gwc828@tongji.edu.cn

Abstract

Authentication with key agreement (AKA) protocols are implemented to provide identity authentication and session keys for communication entities. In order to reduce the heavy trust reliance on key generator center (KGC) in identity based AKA protocols, a certificateless based AKA (CLAKA) protocol for client-server environment without the third-party (i.e., KGC) is introduced in this paper. The proposed protocol is constructed based on elliptic curve cryptosystem (ECC) and multi-factor protections (such as password, biometrics, and smart card). Moreover, security proof based on BAN-logic is carried out and shows that our protocol can provide mutual authentication, user anonymity, dynamic identity and perfect forward security, and resist to user impersonation attack, server spoofing attack and privileged insider attack. Meanwhile, security and efficiency analysis shows that our proposed protocol outperforms the previous related ones.

Keywords*: Mutual Authentication; ECC; multi-factor; CLPKC-AKA, without KGC*

1. Introduction

As a fundamental primitive, authentication with key agreement (AKA) protocols have attracted much attention. AKA protocols can provide identity authentication and shared session keys for communication entities under mobile client-server environment, such as pay-TV, online banking, internet shopping and Telecare Medicine Information Systems (TMIS). Due to the pioneering contribution by Shannon, Diffie and Hellman, AKA protocols can be constructed based on symmetric cryptosystem and public key cryptosystem.

With the increasing number of clients, the server cannot withstand the pressure to keep all long-term secret keys shared by clients and the server during the execution of symmetric cryptosystem based AKA protocols. Meanwhile, symmetric cryptosystem based AKA protocols are vulnerable to attacks such as denial of service attack, off-line guessing attack, *etc*.

Unfortunately, traditional public key infrastructure (TPKI) based AKA protocols, which suffer from complicated public key certificate management, are also impractical for mobile devices with limited computation ability and battery capacity.

An effective alternative solution to avoiding the operation of certificate is identity based (ID-based) cryptosystem initially proposed by Shamir, in which the public key of the user is easily computed from the identity of the user such as IP address or email address, while the private key is generated from the identity of the user and the master secret key of the key generator center (KGC) known as a trusted authority.

* Corresponding Author

ISSN: 1738-9976 IJSIA

To reduce the heavy trust reliance on KGC, Al-Riyami and Paterson[1] presented a novel concept called certificateless public key cryptography (CLPKC), in which long-term private key of the user is calculated from a secret key of the user, while partial private key of the user is issued by KGC. In this way, CLPKC based AKA (CLAKA) protocols can eliminate the complex certificate management burden and the insecure key escrow problem, which respectively consists in TPKI based and ID-based AKA protocols.

Previously, researchers used the following intractable computational problems to construct AKA protocols: (i) Large Number Factorization (LNF) problem is applied to RSA based authentication protocols. (ii) Quadratic Residue (QR) problem based protocols [2, 3] are equivalent in complexity to the LNF-based ones in polynomial time. (iii) Discrete Logarithm (DL) problem: the famous ElGamal cryptosystem based protocols[4, 5] fall into this category. (iv) Diffie Hellman (DH) problem is adopted in protocol [6]. However, traditional protocols in these types require expensive computation cost for modular exponentiation operations.

To solve such problem, various elliptic curve cryptosystem (ECC) based AKA protocols are proposed, which offer better performances in mobile devices. Compared with the aforementioned traditional protocols, ECC based ones can provide greater security with a smaller key size. However, previous research works used bilinear pairing[7] [8], which was also an expensive operation, to construct ECC based protocols. Therefore, many pairing free ECC based AKA protocols [9, 10] have been put forward to improve the efficiency under the following problems: (v) Elliptic Curve Computational Diffie Hellman (ECCDH) problem and (vi) Elliptic Curve Decision Diffie Hellman (ECDDH) problem.

Besides, (vii) Hash Function (HF) with collision free and indirection performance, which shows the low complexity in computation, has been extensive used, as well.

Accordingly, numerous protocols based on the combination problems of above (i)~(vii) are then proposed to improve the security[11].

For the above, CLAKA protocols without pairings on ECC gradually become a research hotspot. Most researchers have been investigating secure and efficient CLAKA protocols under different environments such as online contracts and online meetings for two-part or three parties[12-14]. However, all these CLAKA protocols suppose that a KGC is needed in the authentication system. But in many practical applications under client-server environment, the third-party authority (*i.e.*, KGC) can be replaced by the server. To the best of the authors' knowledge, the CLAKA protocol under client-server environment without the third-party (*i.e.*, KGC) is seldom discussed.

In another way, remote AKA protocols under mobile client-server environment can be implemented on the following three categories (i) knowledge based, (ii) object based, and (iii) biometrics based. However, protocols in type (i), such as password based ones, are simple, convenient, but vulnerable to leaking attacks. Object based protocols, which base on physical possession such as smart card, may be insecure when the smart card is lost. Though protocols in type (iii) are superior to others, because biometric keys such as fingerprints cannot be forgotten or lost, they are also insecure because biometric samples can be captured in a system database[15]. Absolutely, multi-factor authentication protocols, which base on passwords, smart cards and fingerprints, outperform those in type (i)~(iii) [16]. Although plenty of multi-factor AKA protocols[17-20] have been proposed, few of them adopts the certificateless public key cryptography. Moreover, most of them cannot resist the smart privileged insider attack introduced by us. Section 5 describes the attacks on some of the existing multi-factor AKA protocols.

According to the above descriptions, in order to satisfy the requirement of practical applications and reduce the heavy trust reliance on KGC, we propose a multi-factor mutual CLAKA protocol for mobile client-server environment on ECC without the

third-party, which bases on password, biometrics, and smart card protections. Compared with related multi-factor AKA protocols, our protocol is secure with efficiency.

The remainder of our paper is organized as follows. Section 2 presents the basic concept of ECC and fuzzy extractor. Section 3 presents our multi-factor mutual CLAKA protocol. Section 4 gives security proof based on BAN-logic. Section 5 and section 6 provide security and efficiency analysis. Finally, Section 7 concludes the paper.

2. Technical Backgrounds

2.1. ECC

Let F_q be a finite prime field with a large prime number q. An elliptic curve E over the finite field F_q is the set of all pairs satisfying the equation $y^2(mod\ q) = x^3 + ax + b\ (mod\ q), a, b \in Fq, \Delta = 4a^3 + 27b^2(mod\ \ q) \neq 0$, along with an imaginary point representing the infinity. An additive group G_q of all points on elliptic curve E includes an addition operation.

Let P be a generator of G_q. Let the order of G_q be an integer n. Let $Z_n^* = [1, \mathrm{n} - 1]$. Following computational problems over the elliptic curve E are frequently used in AKA protocols construction. The probability to solve these problems is negligible with any polynomial time algorithm.

Discrete Logarithm (DL) problem: for unknown $a \in Z_n^*$, by giving $P, aP, P \in E/\ Fq$, compute a.

Computational Diffie Hellman (CDH) problem: for unknown $a, b \in Z_n^*$, by giving $P, aP, bP, P \in E/\ Fq$, compute abP.

Decision Diffie Hellman (DDH) problem: for unknown $a, b, c \in Z_n^*$, by giving $P, aP, bP, cP, P \in E/\ Fq$, decide whether $abP = cP$.

Gap Diffie Hellman (GDH) problem: for unknown $a, b \in Z_n^*$, by giving $P, aP, bP, P \in E/\ Fq$ and an oracle DDH(aP, bP, cP), that outputs 1 if $abP = cP$, otherwise 0, compute abP.

2.2. Fuzzy Extractor[21]

A fuzzy extractor consists of a pair of procedures (GEN, REP).

$GEN(b_{ci}) = (\alpha_{ci}, \beta_{ci})$: b_{ci} is the biometric input of the client i. α_{ci} is the extracted secret string. β_{ci} is a random helper string.

$REP(b_{ci}^{\ *}, \beta_{ci}) = \alpha_{ci}$: $b_{ci}^{\ *}$ is a close biometric input of the client i. Procedure REP will recover α_{ci}.

A secure fuzzy extractor cannot recover α_{ci} without the helper string β_{ci}.

3. Our Protocol

In this section, we propose an efficient multi-factor pairing free mutual CLAKA protocol for mobile client-server environment on ECC. The proposed protocol is composed of four phases. Notations used in this paper are described in Table 1.

Table 1. Notations

Notation	Description	Notation	Description
C_i	Client i	(x,P_s)	Private/public key pair of S, where $P_s=xP$
S	Server	b_{ci}	Biometric input of the client i
A	Attacker	x_{ci}	Long-term private key of C_i
ID_{ci}	Identity of the client i	P_{ci1}, P_{ci2}	Public key of C_i

ID_s	Identity of the server	$\|$	concatenation operation
pw_{ci}	Login password of C_i	D_{ci}	Partial private key of C_i
$C_i \rightarrow S(T)$	C_i transmits T to S by secure channel	$C_i \sim S$	C_i transmits T to S by insecure channel

3.1. System Initializing Phase

(I1) S chooses an elliptic curve equation E;
(I2) S selects a point P with order n on E;
(I3) S selects master key $x \in Z_n^*$ and computes public key $P_s=xP$;
(I4) S chooses $H_1(\cdot)$, $H_2(\cdot)$, $H_3(\cdot)$, $H_4(\cdot)$. Then, x is kept in private and $\{F_q, E, n, P, P_s, H_1, H_2, H_3, H_4\}$in public.

3.2. Client Registration Phase

(R1) The client C_i chooses ID_{ci}, pw_{ci}, provides biometric input b_{ci} via a specific device, selects a random number r_{ci}, computes $GEN(b_{ci}) = (\alpha_{ci}, \beta_{ci})$, $h_{ci} = H_1(ID_{ci}, r_{ci})$, $B_{ci} = H_1(\alpha_{ci}, h_{ci})$, $PW_{ci} = H_1(pw_{ci}, h_{ci})$, $BPW = B_{ci} \cdot PW_{ci}$, $P_{ci1} = (BPW \bmod n) \cdot P$, submits the registration message to remote server: $C_i \rightarrow S$ (ID_{ci}, BPW). Then, P_{ci1} is kept in public and considered as the public key of C_i.
(R2)The client C_i chooses $x_{ci} \in Z_n^*$ as his long-term private key, computes $P_{ci2} = x_{ci} \cdot P$. Then, P_{ci2} is kept in public and considered as the public key of C_i.
(R3)On receiving (ID_{ci}, BPW), S checks the validity of ID_{ci}, selects a random number r_s, computes, $h_s = H_1(ID_s, r_s)$, $W = h_s + x \cdot BPW$, $M = (h_s \bmod n) \cdot P$, $D_{ci} = H_2(ID_{Ci} || x) \oplus BPW$, sends to the client a smart card containing (D_{ci}, W, M), in which D_{ci} is the partial private key of the client C_i.
(R4)The client checks if $(W \bmod n) \cdot P = M + (BPW \bmod n) \cdot P_s$ holds. If the equation holds, C_i stores (r_{ci}, β_{ci}) into the smart card.

3.3. Login and Mutual Authentication with Key Agreement Phase

(A1) The client C_i inserts a smart card into a mobile device and offers his ID_{ci}, pw_{ci}, and b_{ci}^*. Then, the mobile device extracts the information $(r_{ci}, D_{ci}, \beta_{ci})$ in the card, computes $h_{ci} = H_1(ID_{ci}, r_{ci})$, $REP(b_{ci}^*, \beta_{ci}) = \alpha_{ci}$, $B_{ci} = H_1(\alpha_{ci}, h_{ci})$, $PW_{ci} = H_1(pw_{ci}, h_{ci})$, $BPW = B_{ci} \cdot PW_{ci}$, $C_1 = D_{ci} \oplus BPW$.
(A2) The client C_i chooses random numbers $t_{ci} \in Z_n^*$, computes $T_{ci} = t_{ci} \cdot P$, $C_2 = ID_{Ci} \oplus t_{ci} \cdot P_s$
(A3) $C_i \sim S$ (T_{ci}, C_2).
(A4) On receiving the message in A3, S computes $S_1 = C_2 \oplus T_{ci} \cdot x$, then randomly chooses a number $t_s \in Z_n^*$, computes $T_s = t_s \cdot P$.
(A5) $S \sim C_i (T_s)$.
(A6) On receiving the message in A5, C_i computes K_{cis} and the session key sk.

$$K_{cis} = (T_s + (C_1 \bmod n) \cdot P)(t_{ci} + BPW \bmod n + x_{ci}) \quad (1)$$

$$sk_{cis} = H_3(ID_{Ci} || t_{ci} T_s || K_{cis}) \quad (2)$$

(A7) On receiving the message in A3, S computes K_{sci} and the session key sk.

$$K_{sci} = (t_s + H_2(S_1 || x) \bmod n)(T_{ci} + P_{ci1} + P_{ci2}) \quad (3)$$

$$sk_{sci} = H_3(S_1 || t_s T_{ci} || K_{sci}) \quad (4)$$

(A8) C_i computes $E_{c1} = H_4(sk_{cis}, t_{ci}T_s)$, C_i ~ S (E_{c1}).

(A9) S computes $E_{s1} = H_4(sk_{sci}, t_sT_{ci})$, checks if $E_{s1} = E_{c1}$, S authenticates C_i as legal user, then S computes $E_{s2} = H_4(sk_{sci}, S_1 \oplus t_sT_{ci})$, then S ~ C_i (E_{s2}). If three failing authentication appears in a defined short time, ID_{Ci} will be frozen.

(A10) C_i computes $E_{c2} = H_4(sk_{cis}, ID_{Ci} \oplus t_{ci}T_s)$, checks if $E_{c2} = E_{s2}$, C_i authenticates S as legal user.

Actually, after step A8, C_i and S has constructed a session key. The same session key $sk_{cis} = sk_{sci}$ used to communicate with each other in the subsequent session will achieve the successful authentication between C_i and S. Step A9 and A10 are designed for security proof in Section 4.

According to the step A6 and A7, C_i and S share the same session key.

Since $T_s = t_s \cdot P$, $T_{ci} = t_{ci} \cdot P$, $P_s = x \cdot P$, $C_1 = D_{ci} \oplus BPW = H_2(ID_{Ci} ||x)$, $S_1 = C_2 \oplus T_{ci} \cdot x = ID_{Ci} \oplus t_{ci} \cdot P_s \oplus T_{ci} \cdot x = ID_{Ci}$, $P_{ci1} = (BPW \ mod \ n) \cdot P$, $P_{ci2}=x_{ci} \cdot P$, then $sk_{cis} = sk_{sci}$.

$$K_{cis} = (T_s + (C_1 \ mod \ n) \cdot P)(t_{ci} + BPW \ mod \ n + x_{ci})$$
$$=(t_s + H_2(ID_{Ci} ||x) \ mod \ n) \ (t_{ci} + BPW \ mod \ n + x_{ci}) \cdot P \quad (5)$$

$$K_{sci} = (t_s + H_2(S_1 ||x) mod \ n)(T_{ci} + P_{ci1} + P_{ci2})$$
$$= (t_s + H_2(ID_{Ci} ||x) \ mod \ n) \ (t_{ci} + BPW \ mod \ n + x_{ci}) \cdot P \quad (6)$$

3.4. Password/Private Key Updating Phase

When C_i successfully logins to the remote server and exchanges the session key sk with S, C_i may send a request message encrypted by sk for password/partial private key updating.

(P1) The client C_i chooses a new pw_{cinew}, provides biometric template b_{ci} via a specific device, selects a random number r_{cinew}, computes $GEN(b_{ci}) = (\alpha_{ci}, \beta_{ci})$, $h_{cinew} = H_1(ID_{ci}, r_{cinew})$, $B_{cinew} = H_1(\alpha_{ci}, h_{cinew})$, $PW_{cinew} = H_1(pw_{cinew}, h_{cinew})$, $BPW_{new} = B_{cinew} \cdot PW_{cinew}$, $P_{ci1new} = (BPW_{new} \bmod n) \cdot P$, submits the password/ partial private key updating message encrypted by sk to remote server: $C_i \sim S$ $(ID_{ci}, BPW_{new})_{sk}$. Then, P_{ci1new} is kept in public and considered as the new public key of C_i.

(P2) S decrypts the receiving message $(ID_{ci}, BPW_{new})_{sk}$, selects a random number r_{snew}, computes $h_{snew} = H_1(ID_s, r_{snew})$, $W_{new} = h_{snew} + x \cdot BPW_{new}$, $M_{new} = (h_{snew} \bmod n) \cdot P$, $D_{cinew} = H_2(ID_{Ci} ||x) \oplus BPW_{new}$, sends to the client a smart card containing $(D_{cinew}, W_{new}, M_{new})$.

(P3)The client checks if $(W_{new} mod \ n) \cdot P = M_{new} + (BPW_{new} \ mod \ n) \cdot P_s$ holds. If the equation holds, C_i stores (r_{cinew}, β_{ci}) into the smart card.

4. Security proof based on BAN-logic

BAN-logic, introduced by Burrows M, has constantly attracted researchers' attention as a well-known formal model to analyze authentication protocols. This section analyzes our protocol using BAN-logic[22]. According to BAN-logic, symbols *P* and *Q* stand for principals, while *X* and *Y* represent statements. The main notations and inference rules are listed in Table 2 and Table 3.

Table 2. Main Notations of BAN-logic

Notation	Meaning	Notation	Meaning
$P\|\equiv X$	P believes X	$P\Rightarrow X$	X is under the jurisdiction of P
$P \lhd X$	P sees X	$P \overset{K}{\leftrightarrow} Q$	P communicates with Q by using shared key K
$P\|\sim X$	P once said X	$(X)_K$	X is hash with the key K
$\#(X)$	X is fresh	(X,Y)	X or Y is one part of the formula (X,Y)

Table 3. Main Inference Rules of BAN- logic

Rule	Notation	Meaning
message-meaning rule	$\frac{P\| \equiv P \overset{K}{\leftrightarrow} Q, P \lhd (X)_K}{P\| \equiv Q\sim X}$	P believes that Q once said X if P believes that K is the secret shared key with Q, and P sees X encrypted by K
freshness-conjunction rule	$\frac{P\| \equiv \#(X)}{P\| \equiv \#(X,Y)}$	P believes that (X,Y) is fresh if P believes that X is fresh
nonce-verification rule	$\frac{P\| \equiv \#(X), P\| \equiv Q\sim X}{P\| \equiv Q\| \equiv X}$	P believes that Q believes X if P believes that X is fresh and Q has said X
jurisdiction rule	$\frac{P\|\equiv Q\| \Rightarrow X, P\| \equiv Q\| \equiv X}{P\| \equiv X}$	P believes Q on the validity of X if P believes that Q has jurisdiction over X

There are four steps [22] to analyze authentication protocols using BAN-logic. The following security proof result shows that our protocol provides mutual authentication for the server and the user.

According to the result of the judgment in step A9 and A10, if $E_{s1} = E_{c1}$ and $E_{s2} = E_{c2}$, we can derive

$$sk = sk_{cis} = sk_{sci}\,,\ ID_{Ci} = S_1\,,\ \ t_{ci}T_s{=}t_sT_{ci}\,,\ K_{cis} = K_{sci}$$

Step1, the idealization forms of our protocol are shown as follows. And the idealization forms of the message in step A3 and A5 is not useful in the proof.

$$C_i \sim S\ (E_{c1}):\ (C_i \overset{sk}{\leftrightarrow} S\,, t_{ci}T_s)_{sk} \tag{7}$$

$$S \sim C_i\,(E_{s2}):\ (C_i \overset{sk}{\leftrightarrow} S\,, S_1 \oplus t_sT_{ci})_{sk} \tag{8}$$

Step2, the goals of mutual authentication in the modified scheme are shown as follows:

$$\text{G1: } C_i\| \equiv C_i \overset{sk}{\leftrightarrow} S \tag{9}$$

$$\text{G2: } S\| \equiv C_i \overset{sk}{\leftrightarrow} S \tag{10}$$

$$\text{G3: } C_i\| \equiv S\| \equiv C_i \overset{sk}{\leftrightarrow} S \tag{11}$$

$$\text{G4: } S\| \equiv C_i\| \equiv C_i \overset{sk}{\leftrightarrow} S \tag{12}$$

Step3, since $t_{ci}T_s{=}t_sT_{ci}$, the initial state can be assumed as follows:

$$\text{A1}:\ C_i\| \equiv \#(t_s) \tag{13}$$

$$\text{A2}:\ S\| \equiv \#(t_{ci}) \tag{14}$$

Step4, according to the initial state assumptions and BAN-logic inference rules, the main analysis of our protocol are stated as follows:

According to $E_{s1} = E_{c1}$, we get

$$S| \equiv C_i \overset{sk}{\leftrightarrow} S \quad \text{(Goal2)}$$

According to $E_{s2} = E_{c2}$, we get

$$C_i| \equiv C_i \overset{sk}{\leftrightarrow} S \quad \text{(Goal1)}$$

According to idealization forms of messages in (7) (8), we get

$$S \lhd (C_i \overset{sk}{\leftrightarrow} S, t_{ci} T_s)_{sk} \quad (15)$$

$$C_i \lhd (C_i \overset{sk}{\leftrightarrow} S, S_1 \oplus t_s T_{ci})_{sk} \quad (16)$$

According to (15) (16), we get

$$S \lhd (C_i \overset{sk}{\leftrightarrow} S)_{sk} \quad (17)$$

$$C_i \lhd (C_i \overset{sk}{\leftrightarrow} S)_{sk} \quad (18)$$

According to (17), (Goal2) and the message-meaning rule, we get

$$S| \equiv C_i \sim C_i \overset{sk}{\leftrightarrow} S \quad (19)$$

According to (18), (Goal1) and the message-meaning rule, we get

$$C_i| \equiv S \sim C_i \overset{sk}{\leftrightarrow} S \quad (20)$$

According to assumption A1, A2, freshness- conjunction rule and sk, we get

$$\mathrm{S}| \equiv \#(\mathrm{C_i} \overset{\mathrm{sk}}{\leftrightarrow} \mathrm{S}) \quad (21)$$

$$\mathrm{C_i}| \equiv \#(\mathrm{C_i} \overset{\mathrm{sk}}{\leftrightarrow} \mathrm{S}) \quad (22)$$

According to (19), (21) and nonce-verification rule, we deriver

$$S| \equiv C_i| \equiv C_i \overset{sk}{\leftrightarrow} S \quad \text{(Goal4)}$$

According to (20), (22) and nonce-verification rule, we deriver

$$C_i| \equiv S| \equiv C_i \overset{sk}{\leftrightarrow} S \quad \text{(Goal3)}$$

According to (Goal1), (Goal2), (Goal3) and (Goal4), our protocol provides mutual authentication for the server and the user.

5. Security Analysis

5.1. Adversary Model

Capabilities of Attacker *A* are listed as follows:

(1) *A* completely control the communication channel. That is, they can insert, delete, modify or intercept any information over the insecure communication channel.

(2) *A* can extract the information in the smart card.

(3) *A* knows the public keys of all the users and the server but cannot replace them.

5.2. User Anonymity and Dynamic Identity

In our proposed protocol, the identity of C_i transmitted in step A3 is included in C_2, where $C_2 = ID_{Ci} \oplus t_{ci} \cdot P_s = ID_{Ci} \oplus T_{ci} \cdot x = t_{ci} \cdot x \cdot P$. The attacker A has to solve the CDH problem to get $t_{ci} \cdot x \cdot P$ with known P_s and T_{ci}. Since the probability to solve CDH problem is negligible with any polynomial time algorithm, ID_{Ci} keeps anonymous. Besides, with the random numbers t_{ci} chosen by C_i in step A2, the user gets a dynamic identity in every login phase.

5.3. Resistance to the User Impersonation Attack/Server Spoofing Attack

From the discussion in Section 5.3, with the information of any two compromised factor, our proposed protocol provides resistance to the user impersonation attack.

Our proposed protocol resists the server spoofing attack, because the attacker can pass the authentication only if he knows the master key, which is kept secret.

5.4. Mutual Authentication

The server checks whether $sk_{sci} = sk_{cis}$ or not. If they are equal, the server authenticates the user successfully. Referred to formula (1) (2) in Section 3.3, without the exact x_{ci}, BPW and D_{ci} stored in the smart card, the attacker cannot authenticated by the server successfully.

The server checks whether $sk_{cis} = sk_{sci}$ or not. If they are equal, the user authenticates the server successfully. Referred to formula (3) (4), without the exact x, the attacker cannot authenticated by the user successfully.

5.5. Multi-factor Security

Our proposed protocol is based on password, biometrics, and smart card protections. The protocol is secure even if any two factors are compromised.

Case1: password, biometrics are compromised

Referred to formula (1), even if password, biometrics are compromised, the attacker cannot compute BPW without r_{ci} which is kept in the smart card, because $BPW = B_{ci} \cdot PW_{ci} = H_1\big(\alpha_{ci}, H_1(ID_{ci}, r_{ci})\big) \cdot H_1\big(pw_{ci}, H_1(ID_{ci}, r_{ci})\big)$. Besides, C_1 is calculated from D_{ci}, which is also kept in the smart card.

Case2: password, smart card are compromised

The attacker has no ability to generate correct $BPW = B_{ci} \cdot PW_{ci}$, because $B_{ci} = H_1\big(\alpha_{ci}, H_1(ID_{ci}, r_{ci})\big)$, where α_{ci} is the extracted string of GEN function with the biometric input of the user b_{ci}.

Case3: biometrics, smart card are compromised

The attacker has no ability to generate correct $BPW = B_{ci} \cdot PW_{ci}$, because $PW_{ci} = H_1\big(pw_{ci}, H_1(ID_{ci}, r_{ci})\big)$, where pw_{ci} is kept secret.

Moreover, the attacker may guess the password, biometric input, or information in the smart card, ID_{Ci} will be frozen after three times of incorrect guessing in step A9.

Therefore, our proposed protocol provides security with three factors.

5.6. Resistance to the Smart Privileged Insider Attack

In our paper, smart privileged insider attacker is defined as the one who has the ability to capture but not to modify the information transmitted from the user to the server and the secret values (such as partial private key) generated by the server for the user in the registration phase.

In our proposed protocol, the smart privileged insider attacker who knows BPW transmitted to the server in the registration phase and the partial private key D_{ci} generated by the server cannot impersonate a legal user to compute the session key.

According to the following formula, K_{cis} is calculated from BPW, D_{ci}, t_{ci} and x_{ci}. The first three parameters are known to such attacker, but x_{ci} is unknown to him.

$$K_{cis} = (T_s + (C_1 \bmod n) \cdot P)(t_{ci} + BPW \bmod n + x_{ci})$$
$$=(T_s + (D_{ci} \oplus BPW) \bmod n) \cdot P) (t_{ci} + BPW \bmod n + x_{ci}) \quad (23)$$

However, most of the existing multi-factor AKA protocols, which do not adopt the certificateless public key cryptography, cannot withstand the smart privileged insider attack.

In [20], the smart privileged insider attacker who knows $MP_i = pw_{ci} \oplus H(b_{ci})$ and $W_i = MP_i \oplus h_2(ID_{Ci}||x)$ in registration phase can impersonate a legal user.

Similarly, in protocol [17], the smart privileged insider attacker who knows H_i, B_1^*, B_2^* and e_i in registration phase can impersonate a legal user.

Similarly, in protocol [16], the smart privileged insider attacker of the registration center who knows $pw_{ci} \oplus K$, $b_{ci} \oplus K$, e_i and n_i can impersonate a legal user.

Wu et al. [17] have illustrated many weaknesses of protocol [19]. Attackers can make user impersonation attack and server spoofing attack against protocol [19] with forged messages. Obviously, protocol [19] cannot withstand smart privileged insider attack.

5.7. Perfect Forward Security

Referred to formula (3)(4), the attacker A has to solve the CDH problem to get $t_{ci} \cdot t_s \cdot P$ with known T_s and T_{ci}. Since the probability to solve CDH problem is negligible with any polynomial time algorithm, the attacker A cannot obtain previous session keys, even if the attacker gets all the secret values of the server and user, including password, biometrics, smart card, master key of S, long-term private key of C_i .

5.8. Resistance to Replay Attack

Suppose the attacker retransmits (T_{ci}, C_2) intercepted in previous session, he cannot get the exact session key to pass the authentication without the secret values, such as password, biometrics, smart card, master key of S, long-term private key of C_i.

5.9. Comparison

Security comparison of our proposed protocol with other related ones is presented in Table 4. We use $*$ to denote that the protocol has no relation to the corresponding character. Our proposed protocol satisfies all the security properties.

In [20], the client transmits messages containing M_1, which is defined as $M_1 = d_u \cdot xP$, then the server will compute $d_u \cdot P = \frac{1}{x} \cdot M_1$, which is not a valid scalar multiplication operation over elliptic curve. Besides, protocol [20] adopts time stamp to prevent replay attack, which may cause the clock synchronization problem that is hard to overcome due to the unpredictable transmission delay in the network.

Table 4. Comparison in Security

characters	[20]	[19]	[17]	[16]	ours
User anonymity and dynamic identity	Yes	*	Yes	No	Yes
Resistance to the user impersonation attack	Yes	No	Yes	Yes	Yes
Resistance to server spoofing attack	Yes	No	Yes	Yes	Yes
Mutual authentication	Yes	No	Yes	Yes	Yes
Resistance to the privileged insider attack	No	No	No	No	Yes
Constructing a session key	Yes	No	Yes	No	Yes
Perfect forward security	Yes	*	Yes	*	Yes

Secure with formal proof	Yes	No	Yes	Yes	Yes
Not using time stamp	No	Yes	Yes	Yes	Yes

6. Efficiency Analysis

The time cost and the lengths of parameters for referred cryptographic operations are listed in Table 5. Then, the computation cost is measured with the same platform in [17, 23]. Table 6 shows the efficiency of our protocol compared with related ones in login and authentication phase.

Table 5. Notations

Notation	Description	Time cost (ms)/ Lengths of parameters(bits)
T_{mul}	One scalar multiplication operation over elliptic curve	7.3529
T_{add}	One point addition operation over elliptic curve	0.0613
T_h	a hash operation	0.0004
T_s	Symmetric encryption/decryption	0.1303
T_p	One pairing operation in group	26.7612
T_e	a modular exponentiation in a cyclic group	1.8269
	Hash Value, random number, identity of the user, time stamp	160
	The point in ECC group	320

Table 6. Comparison in Efficiency

Protocol	Time cost	Communication cost (bits)	Transmission times
[20]	C_i : $3T_{mul}+4T_h$ (22.0603ms) S: $3T_{mul}+3T_h$ (22.0599ms)	1440	2
[19]	C_i :$2T_{mul}+6T_{add}+2T_h$ (15.0744ms) S: $2T_{mul}+6T_{add}$ (15.0736ms)	2240	3
[17]	C_i :$2T_{mul}+2T_s+5T_h$ (14.9684ms) S: $2T_{mul}+2T_s+6T_h$(14.9688ms)	1856	2
[16]	C_i :$7T_h$ (0.0028ms) S: $4T_h$ (0.0016 ms)	1600	4
ours	C_i :$4T_{mul}+1T_{add}+4T_h$ (29.4745ms) S: $3T_{mul}+2T_{add}+T_h$(22.1817ms)	960	2

7. Conclusion

In this paper, a CLAKA protocol based on elliptic curve cryptosystem (ECC) and multi-factor protections (such as password, biometrics, and smart card) for client-server environment without the third-party is introduced, which reduces the heavy trust reliance on KGC. According to the security proof based on BAN-logic, the proposed protocol can meet various security requirements, including mutual authentication, user anonymity, dynamic identity, perfect forward security and resistance to user impersonation attack, server spoofing attack, privileged insider attack. Compared with related multi-factor AKA protocols, the security and efficiency analysis show that our protocol satisfies more security characters with slight higher time cost and the lowest communication cost.

References

[1] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography", Lecture Notes in Computer Science, vol. 2894, **(2003)**, pp. 452-473.
[2] C. C. Chang and Y. F. Chang, "Yet another attack on a qr-based password authentication system", Proceedings of the 18th International Conference On Advanced Information Networking And Applications, Fukuoka, Japan, **(2004)** March 29-31.
[3] T. S. Wu, H. Y. Lin, M. L. Lee and W. Y. Chen, "Fast remote user authentication scheme with smart card based on quadratic residue", Journal of Digital Information Management, vol. 9, no. 2, (2011), pp. 51-54.
[4] W. B. Lee, C. C. Wu and W. J. Tsaur, "A novel deniable authentication protocol using generalized elgamal signature scheme", Information Sciences, vol. 177, no. 6, **(2007)**, pp. 1376-1381.
[5] Y. H. Lee, YC; Lee, PJ and You, PS, "Improvement of the elgamal based remote authentication scheme using smart cards", Journal of Applied Research & Technology, vol. 12, **(2014)**, pp. 1063 - 1072.
[6] D. Fiore and R. Gennaro, "Making the diffie-hellman protocol identity-based", Lecture Notes in Computer Science, vol. 5985, **(2010)**, pp. 165-178.
[7] L. Chen, Z. Cheng and N. P. Smart, "Identity-based key agreement protocols from pairings", International Journal of Information Security, vol. 6, no. 4, **(2007)**, pp. 213-241.
[8] M. B. Hou and Q. L. Xu, "Secure certificateless-based authenticated key agreement protocol in the client-server setting", Proceedings of the IEEE International Symposium on It in Medicine & Education, Jinan, China, **(2009)** August 14-16.
[9] S. K. H. Islam and G. P. Biswas, "An improved pairing-free identity-based authenticated key agreement protocol based on ecc", Proceedings of the International Conference on Communication Technology and System Design, Coimbatore, INDIA, **(2011)** December 07-09.
[10] H. Y. Sun, Q. Y. Wen, H. Zhang and Z. P. Jin, "A strongly secure identity-based authenticated key agreement protocol without pairings under the gdh assumption", Security and Communication Networks, vol. 8, no. 17, **(2015)**, pp. 3167-3179.
[11] J. Ren, "An identity-based single-sign-on scheme for computer networks", Security and Communication Networks, vol. 2, **(2009)**, pp. 255-258.
[12] H. Xiong, Z. Chen and Z. G. Qin, "Efficient three-party authenticated key agreement protocol in certificateless cryptography", International Journal of Computer Mathematics, vol. 88, no. 13, **(2011)**, pp. 2707-2716.
[13] H. Y. Sun, Q. Y. Wen, H. Zhang and Z. P. Jin, "A novel pairing-free certificateless authenticated key agreement protocol with provable security", Frontiers of Computer Science, vol. 7, no. 4, **(2013)**, pp. 544-557.
[14] D. B. He, S. Padhye and J. H. Chen, "An efficient certificateless two-party authenticated key agreement protocol", Computers & Mathematics with Applications, vol. 64, no. 6, **(2012)**, pp. 1914-1926.
[15] S. K. Hafizul Islam and G. P. Biswas, "Comments on id-based client authentication with key agreement protocol on ecc for mobile client-server environment", Communications in Computer and Information Science, vol. 191, **(2011)**, pp. 628-635.
[16] L. L. Cao and W. C. Ge, "Analysis and improvement of a multi-factor biometric authentication scheme", Security and Communication Networks, vol. 8, no. 4, **(2015)**, pp. 617-625.
[17] F. Wu, L. L. Xu, S. Kumari and X. Li, "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client-server networks", Computers & Electrical Engineering, vol. 45, **(2015)**, pp. 274-285.
[18] M. K. Khan, S. Kumari and M. K. Gupta, "More efficient key-hash based fingerprint remote authentication scheme using mobile device", Computing, vol. 96, no. 9, **(2014)**, pp. 793-816.
[19] H. L. Yeh, T. H. Chen, K. J. Hu and W. K. Shih, "Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data", Iet Information Security, vol. 7, no. 3, **(2013)**, pp. 247-252.
[20] S. A. Chaudhry, K. Mahmood, H. Naqvi and M. K. Khan, "An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography", Journal of Medical Systems, vol. 39, no. 11, **(2015)**.
[21] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", Siam Journal on Computing, vol. 38, no. 1, **(2008)**, pp. 97-139.
[22] J. L. Tsai, T. C. Wu and K. Y. Tsai, "New dynamic id authentication scheme using smart cards", International Journal of Communication Systems, vol. 23, no. 12, **(2010)**, pp. 1449-1462.
[23] L. L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care", Journal of Medical Systems, vol. 39, no. 2, **(2015)**.

Authors

LiLing Cao, she received her B.S. and M.S. degree in Science and Technology of Electronic Information from Central South University in Changsha, Hunan, China in 2004 and 2007, respectively. She currently is a Ph.D. candidate in the Department of Electronic Information Engineering at Tong Ji University in Shanghai, China. And she is a teacher in Shanghai Ocean University simultaneously. Her research interests include security protocol and wireless communication.

WangCheng Ge, he received his Ph.D. degree in the department of Electrical engineering and computer science from University of Siegen in German in 1998. Then, he did post-doctoral research work in Technical University of Munich. He had worked in Sino-German College in Tong Ji University for 8 years as the chair of Rhodes and Schwartz communication network project fund department.