A Robust Authentication Protocol for Multi-server Architecture Using Elliptic Curve Cryptography

Xueqin Zhang, Baoping Wang, Wenpeng Zhang
(Corresponding author: Baoping Wang)

Software School, Nanyang Normal University
No. 1638, Wolong Road, Wolong District, Nanyang 473000, China
(Email: baoping_wang@outlook.com)
(Received July 17, 2017; revised and accepted Nov. 5, 2017)

Abstract

The multi-server architecture authentication scheme enables users access to the multiple distributed servers with only one single registration procedure. It provides a scalable solution for repeated registration issue in multi-server environment. In this paper, we present a secure remote authentication scheme for multiple servers architecture with elliptic curves cryptosystem (ECC). The proposed scheme could resolve many grave flaws and provide message authenticity, while preserving user anonymity. In the security analysis, we prove the completeness of the proposal BAN-logic, which one of the important formal methods for evaluating information exchange protocols. Noticeable, our scheme also shows impressive efficiency and practicability comparing with other related schemes.

Keywords: Anonymity; Authentication; BAN-logic; Elliptic Curve Cryptography; Multi-server

1 Introduction

In the digital information world, users can easily obtain the information services of the distributed networks anywhere and anytime such as online shopping, online bank, and pay-TV. Authentication plays an important part to construct a secure communication channel between participants in the information systems. To ensure the security of the communication between these participants, more robust remote authentication protocols are urgent needed.

In 1981, Lamport [14] proposed a well-known authentication protocol based on password for the insecure communication, since then, ample of remote user authentication protocols have been presented to improve security and efficiency [2,5,7,8,17,32,33]. However, these protocols are designed for single-server architecture. If conventional protocols are applied to the multi-server environment, the network users not only need to log into various remote servers with repetitive registrations, but also need to remember various identities and passwords. In this paper, we propose a comparatively robust remote user authentication protocol suiting for multiple servers environment, which guarantees better efficiency and achieves various of the security properties. specifically, we analyze the validity of the proposed protocol with formal proof BAN-logic, which is widely employed to validate the beliefs of the involved participants in information exchange protocol.

In the first eight years of the 21st century, many researchers have proposed authentication protocols for multi-server architecture, respectively [3,10,18,23,29,30]. However, in these protocols, user's identity is transmitted in the form of plaintext through public communication channel. In order to resolve the privacy problems raised by static ID, Liao and Wang [22] proposed a dynamic ID based remote user authentication protocol for multi-server architecture, which could eliminate the risk of ID-theft and protect users' privacy. However, their protocol cannot withstand insider attack and masquerade attack. Besides, their scheme fails to provide mutual authentication. Later on, Hsiang and Shih [6] proposed an improved multi-server password authenticated key agreement protocol. In their scheme, only the registration center possesses master secret x and it uses it to issue the private keys for service provider and legal users. The solutions is seemingly to remedy these vulnerabilities of Liao and Wang's protocol, and the authors claim their protocol could resist masquerade attack, server spoofing, registration center spoofing attack and insider attack. Nevertheless, Sood *et al.* [27] pointed out their protocol was susceptible to replay attack, impersonation attack and stolen smart card attack, more over, the password change phase of their protocol was incorrect. Meanwhile, Sood *et al.* presented a multi-server authentication protocol with two-server paradigm, in which the service provider is exposed to users and the control server (Registration center) is not directly acces-

sible to them between verification process. This strategy protect the control server is less likely to be attack. In 2012, Li *et al.* [21] demonstrated Sood *et al.*'s protocol was vulnerable to leak-of-verifier attack and stolen smart card attack. Furthermore, the authentication and session key agreement of the scheme was wrong. In order to tackle these problems, Li *et al.* proposed a more robust authentication protocol for multi-server environment using smart cards. The authors employed the verification strategy introduced in Sood *et al.*'s proposal and also inherited its critical vulnerabilities. Subsequently, Li *et al.*'s protocol was demonstrated that it failed to tackle the replay attack, the password guessing attack and the masquerade attack [11].

In 2013, Pippal *et al.* [26] introduced multiple servers authentication scheme without verification table. Furthermore, it allows the legal users could access multiple servers with no help of registration center (in other words, users and service servers could complete mutual authentication independently). Nevertheless, its verification method has a fatal problem that too much sensitive parameters are stored in users' smart card. Li *et al.* [20] demonstrated that their scheme was susceptible to off-line password guessing attack, impersonation attack and privileged insider attack. They also present their remediation with a flexible registration, which the number of servers is no longer fixed. In 2017, Srinivas *et al.* [28] showed that Li *et al.*'s protocol was vulnerable to a range of ignored security flaws and proposed a new authentication for multiple servers environment. Recently, a pile of multi-server authentication protocols are published for providing stronger robustness and better efficiency [15, 16, 19, 25, 34].

The structure of our paper is organized as follows. In Section 2, we present a robust multiple servers authentication schemes. Then, the security analysis of our protocol and the comparisons between our proposal and related protocols are presented in Sections 3 and 4, respectively. Finally, Section 5 presents the conclusion.

2 Our Scheme

The multiple servers system consists of three involved parties, registration center RC, authorized servers S_j and users U_i. RC is the trusted party and administrates the whole system. S_j has the jurisdiction to offer network services and U_i could access these services.

In this section, we present a new authentication scheme for multi-server architecture, which can be divided into five phases: initialization phase, server registration phase, user registration phase, authenticated key agreement phase and password change phase. The abbreviations and notions used in our protocol are listed in Table 1. The briefly steps are described as follows.

Table 1: Notations

Notations	Meaning
U_i	The ith user
S_j	The jth service providing server
RC	The registration center
ID_i	The identity of the user U_i
PW_i	The password of the user U_i
SID_j	The identity of the server S_j
x	The master secret key of the RC
P	The generator of G
P_{pub}	RC's public key, where $P_{pub} = xP$
SK	The session key shared among U_i, S_j
$H(\cdot)$	A one-way hash function
$Enc_{Key}(M)$	Encryption of messages M using Key
$Dec_{Key}(C)$	Decryption of ciphertext C using Key
$\oplus$	Exclusive-OR operation
$\|$	String concatenation operation

2.1 Initialization Phase

In this phase, RC chooses two large prime numbers p and q with $p = 2q + 1$. Subsequently, RC selects a generator P of order q on the elliptic curve $E_p(a, b)$, which possesses good security properties [9, 12, 31]. Finally, RC generates x as the master secret key, which is minimum of 1024 bits for security purpose.

2.2 Server Registration Phase

When a server S_j wants to register and become an authorized server, S_j and RC should execute the following interactions.

SR.1: S_j chooses its identity SID_j and transmits it to RC for registration via a secured communication channel.

SR.2: RC computes $s_j = H(SID_j \| x)$ and assigns it to S_j via secure channels.

SR.3: On receiving s_j, S_j stores it secretly and finishes the registration.

2.3 User Registration Phase

U_i and RC should execute the following interactions to finish the registration phase:

UR.1: U_i selects his/her identity ID_i, the password PW_i and random number r, then U_i computes $RPW_i = H(PW_i \| r)$ and sends $\{ID_i, RPW_i\}$ to RC for registration.

UR.2: Upon receiving U_i's registration request, RC calculates $A_i = H(ID_i \| RPW_i)$, $K_i = H(ID_i \| x)$, $B_i = K_i \oplus A_i$, where x is the master secret key of RC and kept by RC privately. Then RC stores $\{B_i, Enc(), P, P_{pub}, H(\cdot)\}$ on U_i's smart card and issues it to U_i via a secure channel.

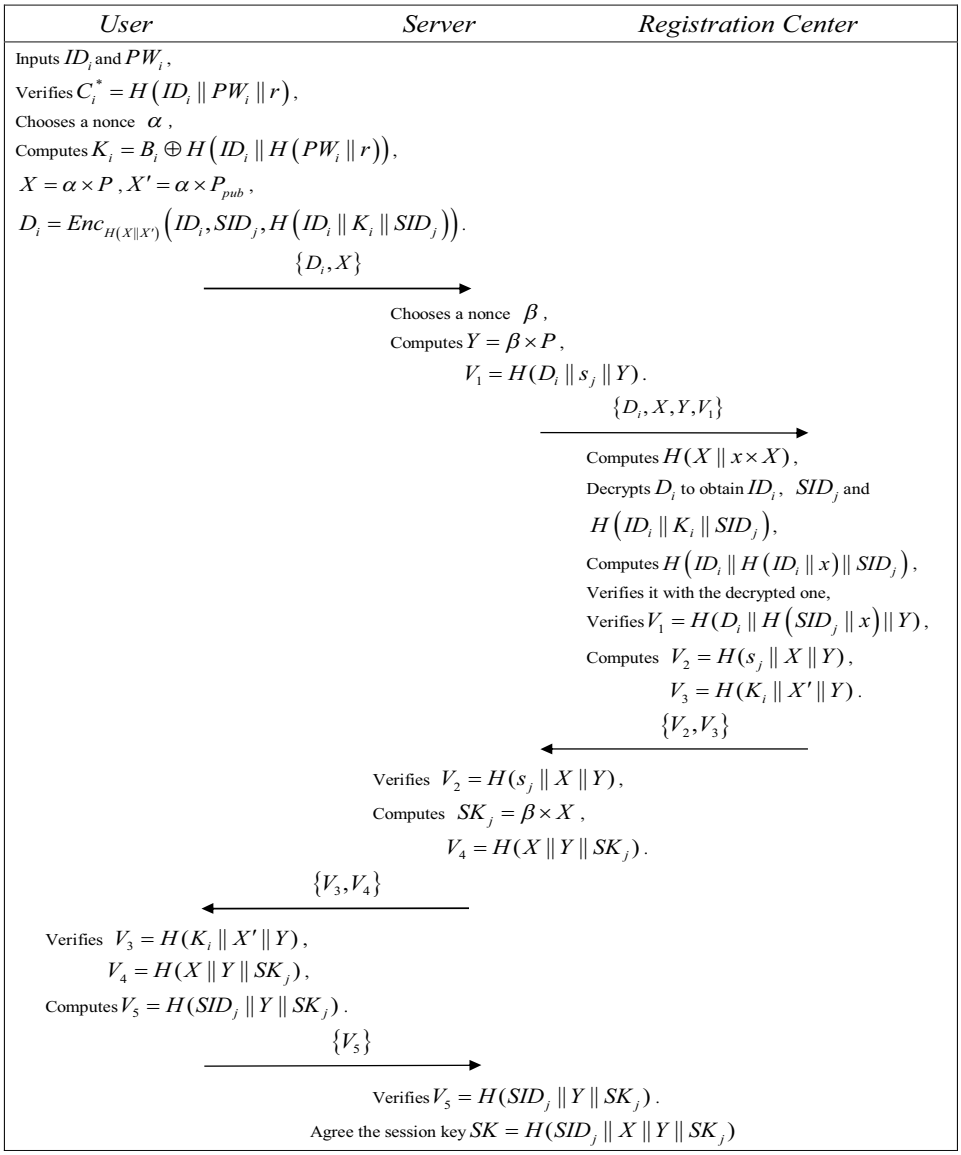

Figure 1: Authenticated key agreement phase

UR.3: U_i stores the random number r and $C_i = H(ID_i \| PW_i \| r)$ into the issued smart card.

2.4 Authenticated Key Agreement Phase

Whenever U_i wants to access the services of R_j, the following operations will be performed during the authenticated key agreement phase.

A.1: U_i inserts his/her smart card into the card reader and inputs ID_i, PW_i. Then the smart card computes $C_i^* = H(ID_i \| PW_i \| r)$ and checks whether it is equal to the stored value C_i. If so, the smart card proceeds the following steps. Otherwise, the smart card aborts this procedure. Then, the smart card computes $K_i = B_i \oplus H(ID_i \| H(PW_i \| r))$, $X = \alpha \times P$, $X' = \alpha \times P_{pub}$, $D_i = Enc_{H(X\|X')}(ID_i, SID_j, H(ID_i \| K_i \| SID_j))$ with a chosen random nonce α. After that, U_i sends the login request message $M_1 = \{D_i, X\}$ to S_j.

A.2: Upon receiving M_1, S_j also generates a random integer number β and calculates $Y = \beta \times P$, $V_1 = H(D_i \| s_j \| Y)$. Then, S_j transmits $M_2 = \{D_i, X, Y, V_1\}$ to RC.

A.3: Upon receiving M_2, RC computes $X' = x \times X$ firstly. Then, RC can get U_i's secret value $\{ID_i, SID_j, H(ID_i \| K_i \| SID_j)\}$ of login request by calculating $Dec_{H(X\|X')}(D_i)$. Subsequently, RC computes $H(ID_i \| H(ID_i \| x) \| SID_j)$ and compares it with the retrieved one in D_i to validate U_i. If the computed one does not exist in the decrypted results from D_i, RC will terminate this session. Else, RC authenticates U_i successfully and will continue to verify the legitimacy of S_j. RC uses the aforementioned decrypted value SID_j from D_i to calculate $V_1^* = H(D_i \| H(SID_j \| x) \| Y)$ and checks whether $V_1^* ? = V_1$. If the equation does not hold, RC rejects this request and terminates this session. Else, RC ac-

cepts this request and computes $V_2 = H(s_j \| X \| Y)$, $V_3 = H(K_i \| X' \| Y)$. Finally, RC sends the reply message $M_3 = \{V_2, V_3\}$ to S_j.

A.4: On receiving M_3, S_j computes $H(s_j \| X \| Y)$ and checks it with the received V_2. If they are not equal, S_j rejects these messages and terminates this session. Otherwise, S_j successfully authenticates RC, and then computes $SK_j = \beta \times X = \alpha\beta \times P$, $V_4 = H(X \| Y \| SK_j)$. After that, S_j submits $M_4 = \{V_3, V_4, Y\}$ to U_i.

A.5: Upon receiving the response M_4, the smart card checks whether the equation $V_3 = H(K_i \| X' \| Y)$ holds or not. If not, the smart card stops this session. Otherwise, the smart card calculates $SK_j = \alpha \times Y = \alpha\beta \times P$ and checks whether $H(X \| Y \| SK_j)$ is equal to received V_4. If not, the smart card stops this session. Otherwise, the smart card computes $V_5 = H(SID_j \| Y \| SK_j)$. Finally, the smart card sends the response message $M_5 = \{V_5\}$ to S_j.

A.6: S_j computes and checks $V_5? = H(SID_j \| Y \| SK_j)$ after receiving M_5. If this equation holds, S_j successfully authenticates U_i and mutual authentication is completed. Otherwise, the session will be terminated.

After finishing the mutual authentication of U_i, S_j and RC, U_i and S_j shares the common session key $SK = H(SID_j \| X \| Y \| SK_j)$.

2.5 Password Change Phase

Suppose U_i wants to select a new password PW_i^{new} to replace original password. Then the smart card should execute the following procedures.

Step 1: U_i makes a request to the smart card and enters ID_i and old password PW_i to the smart card.

Step 2: U_i's smart card checks $C_i? = H(ID_i \| PW_i \| r)$. If yes, U_i inputs a new password PW_i^{new}. Otherwise, the smart card rejects the password change request and terminates this procedure.

Step 3: The smart card computes $A_i^{new} = H(ID_i \| H(PW_i^{new} \| r))$, $B_i^{new} = B_i \oplus A_i \oplus A_i^{new}$, $C_i^{new} = H(ID_i \| PW_i^{new} \| r)$ and stores B_i^{new}, C_i^{new} into its memory to replace B_i, C_i.

3 Security Analysis and Discussion

In the following we will evaluated our scheme by BAN-logic and demonstrate it could withstand common network attacks.

3.1 Validity Proof Based on BAN-logic

In this section, the validity of our proposed scheme is evaluated by BAN-logic [1]. Specifically, BAN-logic helps each participants to trust the exchanged messages and it is a widely employed method for analyzing authentication protocol. We define ample of notations used in the following proof procedures are defined.

$\mathcal{P} \mid\equiv X$: The principal $\mathcal{P}$ believes X.

$\sharp(X)$: The formula X is fresh.

$\mathcal{P} \Rightarrow X$: The principal $\mathcal{P}$ has jurisdiction over X.

$\mathcal{P} \triangleleft X$: The principal $\mathcal{P}$ sees X.

$\mathcal{P} \mid\sim X$: The principal $\mathcal{P}$ once said the statement X.

(X, Y): The formula X or Y is the part of (X, Y).

$\langle X \rangle_Y$: The formula X is combined with Y.

$\{X\}_Y$: This represents the formula X is message and it is encrypted under the key Y.

$\mathcal{P} \overset{k}{\longleftrightarrow} \mathcal{Q}$: The principals $\mathcal{P}$ and $\mathcal{Q}$ communicate with each other with the shared key k. Note that, k will never be known to any other principals.

$\mathcal{P} \overset{k}{\rightleftharpoons} \mathcal{Q}$: $\mathcal{P}$ and $\mathcal{Q}$ shared a secret k, which is possibly known to other principals trusted by them.

SK: the formula SK represents the session key used in the current session.

In the following, we present some logical postulates which used in the demonstration of our protocol:

- The message-meaning rule: $\frac{\mathcal{P} \mid\equiv \mathcal{Q} \overset{k}{\rightleftharpoons} \mathcal{P}, \mathcal{P} \triangleleft \langle X \rangle_k}{\mathcal{P} \mid\equiv \mathcal{Q} \mid\sim X}$.
- The freshness-conjuncatenation rule: $\frac{\mathcal{P} \mid\equiv \sharp(X)}{\mathcal{P} \mid\equiv \sharp(X, Y)}$.
- The nonce-verification rule: $\frac{\mathcal{P} \mid\equiv \sharp(X), \mathcal{P} \mid\equiv \mathcal{Q} \mid\sim X}{\mathcal{P} \mid\equiv \mathcal{Q} \mid\equiv X}$.
- The jurisdiction rule: $\frac{\mathcal{P} \mid\equiv \mathcal{Q} \Rightarrow X, \mathcal{P} \mid\equiv \mathcal{Q} \mid\equiv X}{\mathcal{P} \mid\equiv X}$, $\frac{\mathcal{P} \mid\equiv (X, Y)}{\mathcal{P} \mid\equiv X}$, $\frac{\mathcal{P} \triangleleft (X, Y)}{\mathcal{P} \triangleleft X}$, $\frac{\mathcal{P} \mid\equiv \mathcal{Q} \mid\sim (X, Y)}{\mathcal{P} \mid\equiv \mathcal{Q} \mid\sim X}$.

Let present some authentication goals we should proved in the demonstration of the proposed authentication scheme.

Goal 1: $U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_j)$;

Goal 2: $S_j \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_j)$.

Next, let present the corresponding idealised protocol.

Message 1: $U_i \rightarrow S_j$: $(\{ID_i, SID_j, \langle ID_i, SID_j \rangle_{K_i}\}_{X'}, X)$;

Message 2: $S_j \rightarrow RC$: $(X, Y, \{ID_i, SID_j, \langle ID_i, SID_j \rangle_{K_i}\}_{X'}, \langle \{ID_i, SID_j, \langle ID_i, SID_j \rangle_{K_i}\}_{X'}, Y \rangle_{s_j})$;

Message 3: $RC \rightarrow S_j$: $(\langle X, Y\rangle_{s_j}, \langle X', Y, S_j \mid\sim Y\rangle_{K_i})$;

Message 4: $S_j \rightarrow U_i$: $(\langle X', Y, S_j \mid\sim Y\rangle_{K_i}, \langle X, Y\rangle_{SK_j})$;

Message 5: $U_i \rightarrow S_j$: $\langle SID_j, Y\rangle_{SK_j}$.

We make the following assumptions about the initial state of the scheme to further analyze the proposed scheme:

Let present the following assumptions for analyzing our scheme:

Assumption 1: $U_i \mid\equiv (U_i \overset{K_i}{\rightleftharpoons} RC)$
Assumption 2: $S_j \mid\equiv (S_j \overset{s_j}{\rightleftharpoons} RC)$
Assumption 3: $RC \mid\equiv (S_j \overset{s_j}{\rightleftharpoons} RC)$
Assumption 4: $U_i \mid\equiv \sharp(X')$
Assumption 5: $S_j \mid\equiv \sharp(Y)$
Assumption 6: $S_j \mid\equiv RC \Rightarrow (X, Y)$
Assumption 7: $S_j \mid\equiv \beta$
Assumption 8: $U_i \mid\equiv RC \Rightarrow (X', Y, S_j \mid\sim Y)$
Assumption 9: $U_i \mid\equiv \alpha$
Assumption 10: $U_i \mid\equiv X$
Assumption 11: $U_i \mid\equiv SID_j$
Assumption 12: $S_j \mid\equiv Y$
Assumption 13: $S_j \mid\equiv SID_j$

With the above assumptions and logical postulates, we prove the completeness of our scheme as follows:

Upon RC obtaining Message 2, we can prove that:

$$RC \triangleleft (X, Y, \{ID_i, SID_j, \langle ID_i, SID_j\rangle_{K_i}\}_{X'}, \langle \{ID_i, SID_j, \langle ID_i, SID_j\rangle_{K_i}\}_{X'}, Y\rangle_{s_j}).$$

Based on the jurisdiction rule, we can prove that:

$$RC \triangleleft \langle \{ID_i, SID_j, \langle ID_i, SID_j\rangle_{K_i}\}_{X'}, Y\rangle_{s_j}.$$

Based on the Assumption 3 and the message-meaning rule, we can prove that:

$$RC \mid\equiv S_j \mid\sim (\{ID_i, SID_j, \langle ID_i, SID_j\rangle_{K_i}\}_{X'}, Y).$$

Based on the jurisdiction rule, we can prove that:

$$RC \mid\equiv S_j \mid\sim Y.$$

Upon S_j obtaining Message 3, we can prove that:

$$S_j \triangleleft (\langle X, Y\rangle_{s_j}, \langle X', Y, S_j \mid\sim Y\rangle_{K_i}).$$

Based on the jurisdiction rule, we can prove that:

$$S_j \triangleleft \langle X, Y\rangle_{s_j}.$$

Based on Assumption 2 and the message-meaning rule, we can prove that:

$$S_j \mid\equiv RC \mid\sim (X, Y).$$

Based on Assumption 5 and the freshness-conjuncatenation rule, we can prove that:

$$S_j \mid\equiv \sharp(X, Y).$$

Based on $S_j \mid\equiv RC \mid\sim (X, Y)$ and the nonce-verification rule, we can prove that:

$$S_j \mid\equiv RC \mid\equiv (X, Y).$$

Based on Assumption 6 and the jurisdiction rule, we can prove that:

$$S_j \mid\equiv (X, Y).$$

Based on the jurisdiction rule, we can prove that:

$$S_j \mid\equiv X.$$

Based on $SK_j = \beta \times X$ and Assumption 7, we can prove that:

$$S_j \mid\equiv SK_j.$$

Based on $SK = H(SID_j \| X \| Y \| SK_j)$, $S_j \mid\equiv SK_j$ and Assumption 12, 13, we can prove that:

$$S_j \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_j) (\textbf{Goal 2}).$$

Upon U_i receiving Message 4, we can prove that:

$$U_i \triangleleft (\langle X', Y, S_j \mid\sim Y\rangle_{K_i}, \langle X, Y\rangle_{SK_j}).$$

Based on the jurisdiction rule, we can prove that:

$$U_i \triangleleft \langle X', Y, S_j \mid\sim Y\rangle_{K_i}.$$

Based on the Assumption 1 and the message-meaning rule, we can prove that:

$$U_i \mid\equiv RC \mid\sim (X', Y, S_j \mid\sim Y).$$

Based on Assumption 4 and the freshness-conjuncatenation rule, we can prove that:

$$U_i \mid\equiv \sharp(X', Y, S_j \mid\sim Y).$$

Based on $U_i \mid\equiv RC \mid\sim (X', Y, S_j \mid\sim Y)$ and the nonce-verification rule, we can prove that:

$$U_i \mid\equiv RC \mid\equiv (X', Y, S_j \mid\sim Y).$$

Based on Assumption 8 and the jurisdiction rule, we can prove that:

$$U_i \mid\equiv (X', Y, S_j \mid\sim Y).$$

Based on the jurisdiction rule, we can prove that:

$$U_i \mid\equiv S_j \mid\sim Y,$$

$$U_i \mid\equiv Y.$$

Based on $SK_j = \alpha \times Y$ and Assumption 9, we can prove that:

$$U_i \mid\equiv SK_j.$$

Based on $SK = H(SID_j \| X \| Y \| SK_j)$, $U_i \mid\equiv SK_j$ and Assumption 10, 11, we can prove that:

$$U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_j) (\textbf{Goal 1}).$$

3.2 Security Evaluation

In this section, we prove our protocol could eliminate some common security flaws and achieve several significative properties.

3.2.1 Preserve User Anonymity

Suppose that all of authentication messages $\{D_i, X, Y, V_1, V_2, V_3, V_4, V_5\}$ transmitted between U_i, S_j and RC are obtained by attackers. The chosen random numbers α and β have randomness property, and they guarantee these parameters are all session-variant. Accordingly, without knowing α and β, the adversary will have to solve the computation Diffie-Hellman problem to retrieve specific static element in the transmitted messages. Hence, our scheme could overcome the security flaw of user anonymity breach.

3.2.2 Forward secrecy

In the proposed protocol, random numbers α and β are used to compute the session key SK, which security is guaranteed by the computation Diffie-Hellman problem. Hence, the adversary need to solve the hard problem to generate the session key, in other words, our protocol provides the property of forward secrecy.

3.2.3 Off-line Password Guessing Attack

The non-tamper resistant smart cards no longer secure stored data, and the adversary can reveal the secret information $\{B_i, C_i, r, Enc(), P, P_{pub}, H(\cdot)\}$ in another legitimated user U_i's smart card [13,24]. Even after gathering these information, the attacker could not guess ID_i and PW_i from $C_i = H(ID_i \| PW_i \| r)$ at the same time. The impossibility of guessing two parameters correctly simultaneously in polynomial time demonstrated that our scheme could resist off-line password guessing attack with smart card security breach.

3.2.4 Forgery Attack

In our proposal, the adversary has to generate a valid message $\{D_i, X\}$ if he wants to forgery the legal user U_i, where $D_i = Enc_{H(X\|X')}(ID_i, SID_j, H(ID_i \| K_i \| SID_j))$. The adversary $\mathcal{A}$ could not generate D_i with the knowledge of K_i, which is secured by $A_i = H(ID_i \| RPW_i)$ and stored in the U_i's smart card. With the demonstrated identity and password confidentiality, we can obtain that our scheme could overcome forgery attack.

3.2.5 Server Impersonating Attack

In the proposal, the adversary $\mathcal{A}$ impersonates S_j to fool the remote user U_i with a forgery response message $\{V_3, V_4\}$, where $V_3 = H(K_i \| X' \| Y)$, $V_4 = H(X \| Y \| SK_j)$. Nevertheless, $SK_j = \beta \times X = \alpha\beta \times P$ is impossible for $\mathcal{A}$ to compute without the knowledge of α or β. Thus, $\mathcal{A}$ could not transmit to U_i a valid response message to fool U_i and our proposal is able to withstand server impersonating attack.

3.2.6 Replay Attacks

The replay attack is that attackers re-submit authentication messages transmitted between U_i, S_j, RC to tamper with the information. It is impossible for our proposal since the authentication messages are contributed to random nonce. Neither the replay of an old login message $\{X, D_i\}$ in the step A.1 nor the replay of the response message $\{V_3, V_4\}$ of the service providing server S_j in the step A.4 of the authenticated key agreement phase, due to the random numbers are updated for every session and $\mathcal{A}$ could not get the random numbers, as it will fail in step A.4 and step A.6 of authenticated key agreement phase. Therefore, our protocol can withstand replay attack.

3.2.7 Known Key Attack

Since neither the structure of session key SK is the same with any other authentication message, nor SK functions as part of any other authentication message, the leakage of SK does not affect other unexposed sessions. Thus, the known key attack is resisted effectively.

3.2.8 Proper Mutual Authentication

Our proposed authentication scheme for multiple servers architecture could offer proper mutual authentication. U_i transmits the login request $\{D_i, X\}$ to server S_j for service access. And then, S_j adds its computed values Y and V_1 for mutual authentication. The registration center RC employs these messages to validate U_i and S_j. If any one is unauthentic, RC rejects the login request. Otherwise, it distributes the parameters $\{V_2, V_3\}$ to S_j. S_j verifies the correction of V_2 and computes V_4 as the challenge message to U_i. Subsequently, U_i uses the received messages $\{V_3, V_4\}$ to validate both RC and S_j. Further, he/she responses V_5 for the final session key verification. Noticeable, any fabricated message in the whole process cannot pass the verification. Therefore, our scheme could offer proper mutual authentication.

4 Performance and Functionality Analysis

In this section, we will evaluate our protocol in the performance and functionality by making comparisons with some other related protocols [25,28,34]. In the following, let define some notations used to analyze the computational complexity for the aforementioned protocol: T_{sym} indicates the time complexity of symmetrical encryption and T_{asy} is the time complexity of the asymmetric encryption. Noticeable, executing exclusion-OR operation and string concatenation operation consume very few computation resources, in the evaluation of performance we usually neglect the computational complexity of them.

Table 2: Comparisons of functionality

	Srinivas et al.'s [28]	Zhu et al.'s [34]	Mishra's [25]	Ours
Preserving User anonymity	No	Yes	Yes	Yes
Prevention of forgery attack	Yes	No	No	Yes
Prevention of off-line dictionary attack	No	No	Yes	Yes
Prevention of server impersonating attack	Yes	No	No	Yes
Prevention of replay attack	Yes	Yes	Yes	Yes
Prevention of known key attack	Yes	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes	Yes
Providing correct proof of BAN-logic	No	Yes	No	Yes

Table 3: Performance comparisons

	Srinivas *et al.*'s [28]	Zhu *et al.*'s [34]	Mishra's [25]	Ours
Computational cost	$11T_{sys} + 4T_{asy}$	$22T_{sys} + 8T_{asy}$	$9T_{sys} + 8T_{asy}$	$19T_{sys} + 6T_{asy}$

Table 2 lists the functionality comparisons of our proposed protocol and other related protocols [25,28,34]. Obviously, we can conclude that our protocol is more robust, due to it not only could prevent all known attacks, but also provides several security properties. Furthermore, we also provide the formal proof validated by BAN-logic.

Table 3 shows the performance comparisons of our protocol and other related protocols [25, 28, 34]. According to Table 3, we know that the cost of the proposed protocol is slightly higher than the [25, 28] and lower than the scheme in [34]. However, our protocol can achieve all security properties as mentioned in Table 2.

5 Conclusions

In this paper, we present a robust remote user authentication scheme for multi-server architecture using elliptic curve cryptosystem. The proposal not only could overcome a range of network flaws, but also achieves ample of security properties. In addition, we employed BAN-logic to validate the proposed scheme. The performance of our scheme also indicates relative excellent performance, which is more suitable for practical applications.

References

[1] M. Burrows, M. Abadi and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18-36, 1990.

[2] C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme using user identify cryptography," *International Journal of Network Security*, vol. 15, no. 2, pp. 139-147, 2013.

[3] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, Nov. 2013.

[4] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments," *International Journal of Network Security*, vol. 16, no. 4, pp. 318–321, 2014.

[5] D. L. Guo and F. T. Wen, "A more robust authentication scheme for roaming service in global mobility networks using ECC," *International Journal of Network Security*, vol. 18, no. 2, pp. 217-233, 2016.

[6] H. C. Hsiang and W. K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interface*, vol. 31, no. 6, pp. 1118-1123, 2009.

[7] M. S. Hwang, C. C. Lee, Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack", *International Journal of Informatica*, vol. 12, no. 2, pp.297–302, Apr. 2001.

[8] M. S. Hwang, Li-Hua Li, "A New Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[9] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[10] W. S. Juang, "Efficient multi-server password authenticated key agreement using smart cards," *IEEE Trans on Consumer Electronics*, vol. 50, no. 1, pp. 251-255, 2004.

[11] M. K. Khan and D. B. He, "A new dynamic identity-based authentication protocol for multi-server environment using elliptic curve cryptography," *Security & Communication Networks*, vol. 5, no. 11, pp. 1260-1266, 2012.

[12] N. Koblitz, "Elliptic curve cryptosystem," *Mathematics of Computation*, vol. 48, no. 177, pp.203-209, 1987.

[13] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," *Proceedings of Advances in Cryptology*, pp. 388-397, 1999.

[14] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.
[15] C. C. Lee, Y. M. Lai and C. T. Li, "An improved secure dynamic ID based remote user authentication scheme for multi-server environment, *International Journal of Security and Its Applications*, vol. 6, no. 2, pp. 203-210, 2012.
[16] C. C. Lee, T. H. Lin and R. X. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards," *Expert Systems with Applications*, vol. 38, no. 11, pp. 13863-13870, 2011.
[17] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol", *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.
[18] L. H. Li, L. C. Lin and M. S. Hwang, "A remote password authentication scheme for multiserver architecture using neural networks," *IEEE Trans on Neural Network*, vol. 12, no. 6, pp. 1498-1504, 2001.
[19] X. Li, J. Ma, W. D. Wang, Y. P. Xiong and J. Z. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments," *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 85-95, 2013.
[20] X. Li, J. Niu, S. Kumari, J. Liao and W. Liang, "An enhancement of a smart card authentication scheme for multi-server architecture," *Wireless Personal Communications An International Journal*, vol. 80, no. 1, pp. 175-192, 2015.
[21] X. Li, Y. P. Xiong, J. Ma and W. D. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 763-769, 2012.
[22] Y. P. Liao and S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interface*, vol. 31, no. 1, pp. 24-29, 2009.
[23] I. C. Lin, M. S. Hwang and L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer System*, vol. 19, no. 1, pp. 13-22, 2003.
[24] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans Comput*, vol. 5, no.51, pp. 541-552, 2002.
[25] D. Mishra, "Design and analysis of a provably secure multi-server authentication scheme," *Wireless Personal Communications*, vol. 86, no. 3, pp. 1-25, 2016.
[26] R. S. Pippal, C. D. Jaidhar and S. Tapaswi, "Robust smart card authentication scheme for multi-server architecture," *Wireless Personal Communications*, vol. 72, no. 1, pp. 729-745, 2013.
[27] S. K. Sood, A. K. Sarje and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 609-618, 2011.
[28] J. Srinivas, S. Mukhopadhyay and D. Mishra, "A self-verifiable password based authentication scheme for multi-server architecture using smart card," *Wireless Personal Communications*, 2017. DOI:10.1007/s11277-017-4476-9
[29] W. J. Tsaur, C. C. Wu and W. B. Lee, "A smart card-based remote scheme for password authentication in multi-server Internet services," *Computer Standards & Interfaces*, vol. 27, no. 1, pp. 39-51, 2004.
[30] J. L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table," *Computers & Security*, vol. 27, no. 3-4, pp. 115-121, 2008.
[31] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, 2004.
[32] Y. Y. Wang, J. Y. Liu, F. X. Xiao and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Computer Communications*, vol. 4, no. 32, pp.583-585, 2009.
[33] J. H. Wei, W. F. Liu and X. X. Hu, "Secure and efficient smart card based remote user password authentication scheme," *International Journal of Network Security*, vol. 18, no. 4, pp. 782-792, 2016.
[34] H. F. Zhu, Y. F. Zhang and Y. Sun, "Provably Secure Multi-server Privacy-Protection System Based on Chebyshev Chaotic Maps without Using Symmetric Cryptography," *International Journal of Network Security*, vol. 18, no. 5, pp. 803-815, 2016.

Biography

Xueqin Zhang received the B.S. and M.S. degrees in Computer Science and Technology from Henan Polytechnic University, Jiaozuo, Henan, China in 2005 and 2008, respectively. She is a lecturer in Nanyang Normal University, Nanyang, Henan, China. Her research interests include data mining and information security.

Baoping Wang received B.S. degree in Computer Application Technology from Henan University, Kaifeng, China in 1997 and M.S. in Computer Application Technology from Guizhou University, Guiyang, China in 2006. He is an associate professor in Nanyang Normal University, Henan, China. His research interests include computer network technology and information security.

Wenpeng Zhang received B.S. degree in Computer Application Technology from Henan University, Kaifeng, China, in 1997, and M.S. in Computer Application Technology from Wuhan University of Technology, Wuhan, China, in 2007. He is an associate professor in Nanyang Normal University, Henan, China. His research interests include computer network technology and Database technology.