# A New Remote Authentication Scheme for Anonymous Users Using Elliptic Curves Cryptosystem

Xueqin Zhang, Baoping Wang, and Wei Wang
*(Corresponding author: Xueqin Zhang)*

Software School, Nanyang Normal University
No. 1638, Wolong Road, Wolong District, Nanyang 473000, China
(Email: zhangxueqin01@outlook.com)

*(Received Jan. 10, 2017; revised and accepted Apr. 11, 2017)*

## Abstract

Along with the large-scale proliferation of network and information technology, users can obtain the information resources conveniently via intelligent device. Authentication mechanism is a fundamental tool for ensuring secure communications and the validity of communicating party. In this paper, we propose a new authentication scheme for anonymous users using elliptic curves cryptosystem (ECC) which achieves mutual authentication and forward security. Specifically, we certify the validity of our proposal by employing BAN-logic, which is one of the important formal methods. Further, the performance comparison shows that our scheme is more suitable for application scenarios where efficiency and security concerned.

*Keywords: Anonymity; Authentication; BAN-logic; Security*

## 1 Introduction

It is necessary for service providing servers to authenticate remote users in the insecure communication channel when users access resources through networks, remote authentication schemes can provide the convenient and secure mechanism for them to verify each other. However, due to the open nature of the Internet networks, the remote authentication schemes are vulnerable to various attacks. How to design a secure remote authentication scheme to resist these attacks is an important issue for researchers.

In 1981, Lamport [14] firstly proposed a password based remote user authentication scheme using password table. However, the proposed scheme was insecure if the password table was compromised. In password based authentication schemes based on [14], adversaries could easily obtain users' passwords by brute force attack and threat system security, due to the low information entropy of these memorable password. Further, the password table is susceptible to the collision attack.

For solving the inherent limitations of password based authentication schemes, smart card was introduced as the second factor to devise protocols due to the convenience and secure computation. In 2004, Das *et al.* [5] proposed a dynamic ID based remote user authentication scheme using smart cards which allowed users to choose and change their passwords freely without responding to servers. However, later on, some researchers revealed that their scheme was not as much secured as they claimed [2]. In 2009, Wang *et al.* [19] pointed that Das *et al.*'s scheme allowed an attacker to complete the authentication without knowing the password and could not provide the mutual authentication. Meanwhile, the authors proposed a dynamic ID-based authentication scheme and claimed that their scheme was more efficient and secure, as well as keeping the merits of Das *et al.*'s scheme. However, Wang *et al.*'s scheme also could not provide anonymity of users during the authentication and was vulnerable to insider attack, stolen smart card attack.

In the aforementioned authentication schemes, smart card is assumed to be a tamper-resistant device (the parameters stored in smart card cannot be compromised). However, many research results have introduced that sensitive data could be extracted by power analysis and fault injection [12,18]. This is the most critical problem which results in security flaws. And hence, a secure authentication scheme should guarantee security rely on sensitivity of secret parameters, rather than confidence of smart card.

In order to overcome the problems mentioned above, a number of password authentication schemes have been proposed [1, 4, 6, 8–11, 15–17, 20–22]. In 2011, Khan et al. [11] presented a remote authentication scheme using smart card which could provide user anonymity, mutual authentication, session key establishment, and resist various attacks. Later on, He *et al.* [9] showed that Khan *et al.*'s scheme failed to preserve user anonymity. Most recently, Jiang *et al.* [10] illustrated that some previous authentication protocol have a range of ignored security flaws, then they proposed an enhanced authentication scheme and claimed that their scheme could eliminate various malicious attacks. Unfortunately, Wei *et al.* [20] demonstrated that Jiang *et al.*'s scheme could not provide perfect forward secrecy and then presented an improved smart card based authentication scheme.

In this paper, we propose a new remote authentication scheme using elliptic curves cryptosystem (ECC) as well as demonstrating its validity through BAN-logic. BAN logic [3] devotes to validate the beliefs of the involved principals in the protocol and has been widely applied in analyzing the security of authentication schemes. Noticeably, the proposed scheme can achieve various of the required security properties and guarantee high efficiency.

The structure of our paper is organized as follows. In Section 2, we propose a new robust authentication scheme. Subsequently, we prove the completeness of the proposal and analyze its security in Section 3. Then, we evaluate its performance in the next section. At last, Section 5 concludes this paper.

# 2 Our Proposed Scheme

In this section, we propose a new remote authentication scheme which can preserve user anonymity. Our scheme is divided into four phases: registration phase, login phase, authentication and session key exchange phase and password updating phase. The notations used in our scheme are listed in Table 1.

Table 1: Notations

| Notations | Meaning |
|---|---|
| $U_i$ | The $ith$ user with identity $ID_i$ |
| $S$ | The remote server |
| $ID_i$ | The identity of $U_i$ |
| $PW_i$ | The password of $U_i$ |
| $x$ | The master secret key of $S$ |
| $a, b$ | The chosen random numbers |
| $T$ | The current timestamp |
| $SK$ | The session key shared among $U_i$ and $S$ |
| $H(\cdot)$ | A one-way hash function |
| $\oplus$ | Exclusive-OR operation |
| $\|$ | String concatenation operation |
| $p, q$ | Two distinct large primes such that $p = 2q + 1$ |
| $E_p(a, b)$ | The elliptic curve over a finite field $Z_p$ |
| $P$ | $P$ is a generator of order $q$ on the elliptic curve $E_p(a, b)$ |
| $Q$ | $S$'s public key, where $Q = x \cdot P$ |

## 2.1 Registration Phase

This phase is invoked whenever $U_i$ initially registers to $S$. Initially, $S$ chooses two distinct large primes $p$ and $q$ with $p = 2q + 1$. $E_p(a, b)$ is an elliptic curve in the finite field $Z_p$ [7,13]. $P$ is a generator of order $q$ on the elliptic curve $E_p(a, b)$ and $q$ must be large enough, so that the ECDLP is difficult to solve with a polynomial-time algorithm. $S$ uses its master secret key $x$ to compute $Q = x \cdot P \ mod \ p$ and public the parameters $\{P, p, Q, E_p(a, b)\}$.

**Step R1.** $U_i$ selects his/her identity and password tuple $(ID_i, PW_i)$. Then he/she chooses a random number $r$ to calculate $A_i = H(r\|PW_i)$ and sends $\{ID_i, A_i\}$ to $S$ for registration via a trusted network.

**Step R2.** After receiving the registration request $(ID_i, A_i)$, $S$ utilizes the master secret key $x$ to compute $X_i = H(ID_i \cdot x \cdot Q)$ and $B_i = X_i \oplus H(ID_i\|A_i)$.

**Step R3.** Then $S$ writes $\{B_i, p, E_p(a, b), P, Q, H(\cdot)\}$ into the smart card and issues it to $U_i$ through a secure channel.

**Step R4.** $U_i$ stores $r$ on the received card, which contains $\{r, B_i, p, E_p(a, b), P, Q, H(\cdot)\}$.

## 2.2 Login Phase

When $U_i$ wants to login $S$, he/she should insert his/her smart card to the terminal and key $ID_i$ with $PW_i$, then the smart card performs the following steps (See Figure 1):

**Step L1.** The smart card generates a random nonce $a$ and computes $A_i = H(r\|PW_i)$, $X_i = B_i \oplus H(ID_i\|A_i)$, $C_i = ID_i \cdot P + a \cdot Q$, $R_i = a \cdot P$, $V_i = X_i \oplus H(a \cdot Q\|T_i)$ where $T_i$ is the fresh current timestamp.

**Step L2.** After that, $U_i$ transmits the login request $\{C_i, R_i, V_i, T_i\}$ to $S$ by a public channel.

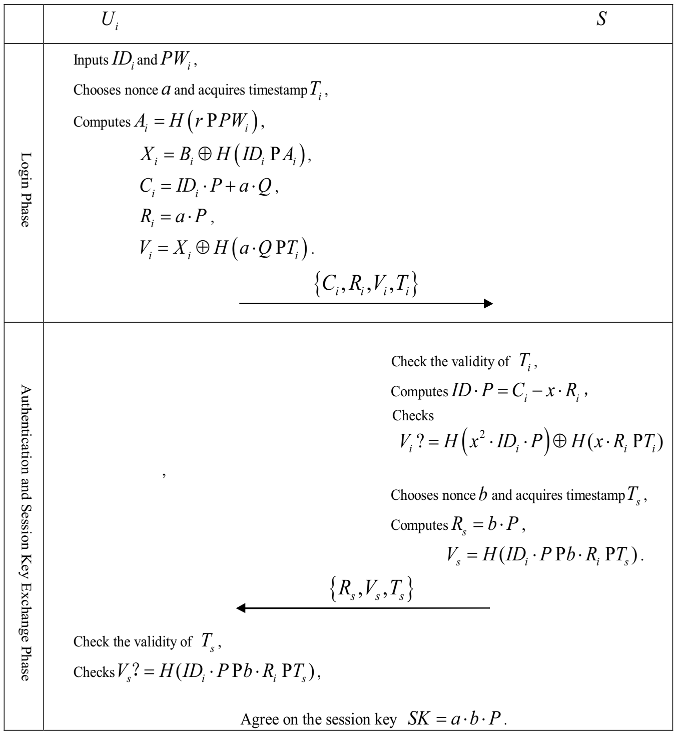
## 2.3 Authentication and Session Key Exchange Phase

Upon receiving the login request message $\{C_i, R_i, V_i, T_i\}$, $U_i$ and $S$ need to perform the following steps to finish the mutual authentication.

**Step A1.** $S$ checks the validity of the time stamp $T_i$, if $T_i' - T_i \leq \triangle T$ holds, $S$ continues to execute the next step.

**Step A2.** Then $S$ calculates $ID_i \cdot P = C_i - x \cdot R_i$ and $V_i^* = H(x^2 \cdot ID_i \cdot P) \oplus H(x \cdot R_i\|T_i)$. If the computed value $V_i^*$ is equal to the received $V_i$, $S$ will execute the following steps and if $V_i^* \neq V_i$, the login request will be rejected.

**Step A3.** After the verification of $U_i$, $S$ chooses a random number $b$ and current timestamp $T_s$ to compute $R_s = b \cdot P$ and $V_s = H(ID_i \cdot P\|b \cdot R_i\|T_s)$. Then $S$ replies the message $\{R_s, V_s, T_s\}$ to $U_i$ via public channel.



Inputs $ID_i$ and $PW_i$,

Chooses nonce $a$ and acquires timestamp $T_i$,

Computes $A_i = H\left(r \mathrm{P} PW_i\right)$,

$X_i = B_i \oplus H\left(ID_i \mathrm{P} A_i\right)$,

$C_i = ID_i \cdot P + a \cdot Q$,

$R_i = a \cdot P$,

$V_i = X_i \oplus H\left(a \cdot Q \mathrm{P} T_i\right)$.

$\{C_i, R_i, V_i, T_i\}$

Check the validity of $T_i$,

Computes $ID \cdot P = C_i - x \cdot R_i$,

Checks

$V_i ? = H\left(x^2 \cdot ID_i \cdot P\right) \oplus H(x \cdot R_i \mathrm{P} T_i)$

,

Chooses nonce $b$ and acquires timestamp $T_s$,

Computes $R_s = b \cdot P$,

$V_s = H(ID_i \cdot P \mathrm{P} b \cdot R_i \mathrm{P} T_s)$.

$\{R_s, V_s, T_s\}$

Check the validity of $T_s$,

Checks $V_s ? = H(ID_i \cdot P \mathrm{P} b \cdot R_i \mathrm{P} T_s)$,

Agree on the session key $SK = a \cdot b \cdot P$.

Figure 1: Login phase and authentication and session key exchange phase

**Step A4.** Upon receiving the replication, the smart card verifies the freshness of the time interval between $T'_s$ and $T_s$, where $T'_s$ is the current time when the mutual authentication message is received. Then the smart card computes $V'_s = H(ID_i \cdot P \| a \cdot R_s \| T_s)$ and checks whether $V_s$ is equal to the computed one. If they are equal, the legitimacy of $S$ is verified by $U_i$; otherwise, the smart card terminates this session.

After finishing the mutual authentication, $U_i$ and $S$ agree on the common session key $SK = a \cdot b \cdot P$.

### 2.4 Password Updating Phase

When $U_i$ wants to update his/her password without the help of $S$, $U_i$ should insert his/her smart card into a card reader and input $ID_i$ and $PW_i$.

**Step P1.** $U_i$ is allowed to input a new password $PW_i^{new}$.

**Step P2.** The smart card computes $A_i = H(r\|PW_i)$, $A_i^{new} = H(r\|PW_i^{new})$, $B_i^{new} = B_i \oplus H(ID_i\|A_i) \oplus H(ID_i\|A_i^{new})$, and stores $B_i^{new}$ into the smart card to replace $B_i$ and performs an password update successfully.

## 3 Security Analysis of Our Scheme

In this section, we demonstrate the security performance of our proposed authentication protocol.

### 3.1 Validity Proof Based on BAN-logic

BAN-logic [3] is a logic belief for analyzing information exchange protocols. Note that, it helps users to ensure whether exchanged messages are trustworthy and secured against eavesdropping. In this section, we demonstrate the completeness of the proposed scheme using BAN-logic.

In the following, we define some notations used in the proof:

$\mathcal{P} \mid\equiv X$: 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.

Let present several logical postulates which is essential for the demonstration as follows:

- The message-meaning rule: $\frac{\mathcal{P}\mid\equiv\mathcal{Q}\overset{k}{\longleftrightarrow}\mathcal{P},\mathcal{P}\triangleleft\{X\}_k}{\mathcal{P}\mid\equiv\mathcal{Q}\mid\sim X}$, $\frac{\mathcal{P}\mid\equiv\mathcal{Q}\overset{k}{\rightleftharpoons}\mathcal{P},\mathcal{P}\triangleleft\langle X\rangle_k}{\mathcal{P}\mid\equiv\mathcal{Q}\mid\sim X}$.
- 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: $\frac{\mathcal{P}\mid\equiv\mathcal{Q}\Rightarrow X,\mathcal{P}\mid\equiv\mathcal{Q}\mid\equiv X}{\mathcal{P}\mid\equiv X}$, $\frac{\mathcal{P}\mid\equiv(X,Y)}{\mathcal{P}\mid\equiv X}$, $\frac{\mathcal{P}\triangleleft(X,Y)}{\mathcal{P}\triangleleft X}$, $\frac{\mathcal{P}\mid\equiv\mathcal{Q}\mid\sim(X,Y)}{\mathcal{P}\mid\equiv\mathcal{Q}\mid\sim X}$.

Here are some the authentication goals which will be proved for the proper mutual authentication and the agreement of the session key of our scheme.

*Goal 1*: $U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S)$

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

Next, the corresponding idealised protocol (transmitted by the conventional description of our scheme) is then:

Message 1: $U_i \rightarrow S$: $(C_i, \{R_i, T_i\}_{\langle ID_i \rangle_x}, T_i)$

Message 2: $S \rightarrow U_i$: $(T_s, \langle R_s, T_s \rangle_{\langle ID_i \rangle_{R_i}})$.

The following assumptions are presented to further analyze our scheme:

Assumption 1: $U_i \mid\equiv (U_i \overset{\langle ID_i \rangle_{R_i}}{\rightleftharpoons} S)$

Assumption 2: $S \mid\equiv (S \overset{\langle ID_i \rangle_x}{\longleftrightarrow} U_i)$

Assumption 3: $U_i \mid\equiv \sharp(T_s)$

Assumption 4: $S \mid\equiv \sharp(T_i)$

Assumption 5: $S \mid\equiv U_i \Rightarrow (R_i, T_i)$
Assumption 6: $S \mid\equiv U_i \Rightarrow (R_s, T_s)$
Assumption 7: $U_i \mid\equiv a$
Assumption 8: $S \mid\equiv b$

Based on the aforementioned assumptions and the defined logical postulates, we present the main steps of analysis of our scheme as follows:

When $S$ receiving Message 1, we can prove that:

$$S \triangleleft (C_i, \{R_i, T_i\}_{\langle ID_i \rangle_x}, T_i).$$

Based on the jurisdiction rule, we can prove that:
$S \triangleleft \{R_i, T_i\}_{\langle ID_i \rangle_x}$.

Based on Assumption 2 and the message-meaning rule, we can prove that:
$S \mid\equiv U_i \mid\sim (R_i, T_i)$.

Based on Assumption 4 and the freshness-conjuncatenation rule, we can prove that:
$S \mid\equiv \sharp(R_i, T_i)$.

Based on the proved $S \mid\equiv U_i \mid\sim (R_i, T_i)$ and the nonce-verification rule, we can prove that:
$S \mid\equiv U_i \mid\equiv (R_i, T_i)$.

Based on Assumption 5 and the jurisdiction rule, we can prove that:
$S \mid\equiv (R_i, T_i)$.

Based on the jurisdiction rule, we can prove that:
$S \mid\equiv R_i$.

Based on $SK = H(b \cdot R_i)$ and Assumption 8, we can prove that:
$S \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S)$ (*Goal 2*).

When $U_i$ receiving Message 2, we can prove that:
$U_i \triangleleft (T_s, \langle R_s, T_s \rangle_{\langle ID_i \rangle_{R_i}})$.

Based on the jurisdiction rule, we can prove that:
$U_i \triangleleft \langle R_s, T_s \rangle_{\langle ID_i \rangle_{R_i}}$.

Based on Assumption 1 and the message-meaning rule, we can prove that:
$U_i \mid\equiv S \mid\sim (R_s, T_s)$.

Based on Assumption 3 and the freshness-conjuncatenation rule, we can prove that:
$U_i \mid\equiv \sharp(R_s, T_s)$.

Based on the proved $U_i \mid\equiv S \mid\sim (R_s, T_s)$ and the nonce-verification rule, we can prove that:
$U_i \mid\equiv S \mid\equiv (R_s, T_s)$.

Based on Assumption 6 and the jurisdiction rule, we can prove that:
$U_i \mid\equiv (R_s, T_s)$.

Based on the jurisdiction rule, we can prove that:
$U_i \mid\equiv R_s$.

Based on $SK = a \cdot R_s$ and Assumption 7, we can prove that:
$U_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S)$ (*Goal 1*).

## 3.2 Security Analysis on Possible Attacks

Here, we present that our scheme has the ability to withstand common attacks and achieves some available security properties. Firstly, we assume that the problem list as follows is difficult to solve in polynomial-time. In other words, there are no efficient polynomial-time algorithm to solve it [7]: Given three points $P, s \cdot P, t \cdot P \in E_p(a,b)$, where $s, t \in Z_p^*$, the computation Diffie-Hellman problem(CDHP) is to find the point $(s \cdot t) \cdot P$ on $E_p(a,b)$.

### 3.2.1 Preserving Anonymity and Nontraceability

The transmitted messages via the public communication channels may leak some useful information about user's identity or activities. In our scheme, the blinded parameter $C_i = ID_i \cdot P + a \cdot Q$ is the only parameter by which server can identify users, and it is session variant due to the random number $a$. Even if the adversary has obtained the login request $C_i, R_i, V_i, T_i$ of $U_i$, he/she also cannot compute the $a \cdot Q$ with $Q$ and $R_i$ due to the hardness of computation Diffie-Hellman problem. Further, he/she is unable to retrieve $ID_i \cdot P$ from $C_i$, while $ID_i \cdot P$ is the only specific static element in the transmitted messages. Hence, our scheme can withstand user anonymity and traceability breach.

### 3.2.2 Perfect Forward Secrecy

The finished conversation should be confidential even the long-term master secret key compromised. In our scheme, the session key $SK = a \cdot b \cdot P$ is computed with the contribution of $a$ and $b$. The adversary can only compute $SK$ by two element $R_i$, $R_s$ which should solve the computation Diffie-Hellman problem. Thus the attacker cannot compute the previously generated session keys and our remote authentication scheme provides the property of perfect forward secrecy.

### 3.2.3 Off-line Password Guessing Attack

Many existing works suffer from off-line password guessing attack because the low entropy password could be easily obtained by brute force attack. In our proposal, each parameters of the login request are attached with random numbers. Note that, even the attacker has eavesdropped and recorded the login request $C_i, R_i, V_i, T_i$ in the login phase, it is useless for guessing password without knowing $H(a \cdot Q \| T_i)$. Even if the adversary has gotten $U_i$'s smart card and extracted its secret parameters $\{r, B_i, p, E_p(a,b), P, Q, H(\cdot)\}$, he/she cannot construct a equation to verify the correctness of disclosed password. And hence our proposed scheme can resist off-line password guessing attack with smart card security breach.

### 3.2.4 Forgery Attack

In the scenario of forgery attack, someone masquerades as other legitimate users for illegal access. In our scheme, in order to impersonate as a legal user, the adversary needs to forge a legal login request message $C_i, R_i, V_i, T_i$. However, he/she cannot compute the $C_i$ and $V_i$ without knowing $ID_i$ and the key $X_i$ generated by $S$. In a extend scenario, even if the attacker has extracted the secret values $\{r, B_i, p, E_p(a,b), P, Q, H(\cdot)\}$ stored in $U_i$'s smart

Table 2: Comparisons of functionality

| Functionality | [15] | [22] | [10] | [20] | Ours |
|---|---|---|---|---|---|
| Resistance of forgery attack | No | Yes | Yes | No | Yes |
| Resistance of off-line password guessing attack | Yes | Yes | Yes | Yes | Yes |
| Resistance server impersonating attack | No | No | Yes | Yes | Yes |
| Resistance of replay attack | Yes | Yes | Yes | Yes | Yes |
| Provision user anonymity | No | No | No | No | Yes |
| Achieving mutual authentication | Yes | Yes | Yes | Yes | Yes |
| Provision of perfect forward secrecy | Yes | Yes | No | Yes | Yes |
| Session key establishment | Yes | Yes | Yes | Yes | Yes |

Table 3: Performance comparisons

| | Type of operation | [15] | [22] | [10] | [20] | ours |
|---|---|---|---|---|---|---|
| Computation cost | $T_H$ | 9 | 14 | 6 | 12 | 7 |
| | $T_{asy}$ | 4 | 5 | 6 | 4 | 7 |

card, he/she also cannot obtain $X_i$ without knowing $ID_i$ and $PW_i$. Hence, the adversary cannot impersonate as a legal user to login $S$ by launching the forgery attack.

### 3.2.5 Server Impersonating Attack

Suppose that the adversary intercepts the login request of $U_i$, and responds a forged reply message to impersonate servers. However, he/she cannot obtain the key information $ID_i \cdot P$ and $a \cdot b \cdot P$ without knowing the master secret key $x$ which kept only by $S$, even if the attacker has extracted the data from $U_i$'s smart card. $U_i$ can verify $V_s$ to authenticate $S$, which is contributed with theses two key information. Hence, the attacker cannot masquerade as $S$ to fool $U_i$ by launching the server impersonating attack.

### 3.2.6 Known Key Attack

Due to the session key $SK$ is computed by two random numbers which employs the principle of Diffi-Hellman key exchange protocol. Thus neither the value of session key $SK$ is the same with any other authentication message, nor $SK$ as a part of any other authentication message. The leakage of $SK$ does not affect other unexposed sessions. Thus, the known key attack is resisted effectively.

### 3.2.7 Reply Attack

The replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. If the adversary can eavesdrop any request from $U_i$ to $S$, and replays the intercepted one to $S$. Firstly, $S$ can reject mostly session by verifying the freshness of timestamp. Secondly, even if the login request passes the verification of timestamp, $S$ will return $R_s, V_s, T_s$ with contribution of random number $b$. the attacker also cannot obtain $a$ which is implied in the login request to compute the session key $SK$. Hence, our scheme can effectively resist replay attack.

## 4 Performance Analysis

In this section, we compare the security features and efficiency with some existing state-of-the-art such as: Lee *et al.*'s [15], Xue *et al.*'s [22], Jiang *et al.*'s and Wei *et al.*'s schemes to evaluating our scheme. And the comparative summary of the proposed scheme is presented in the Table 2. It is clear that only our proposed scheme can achieve all requirements list in Table2. Specifically, the innovative feature is that we prove the completeness of our scheme by employing BAN-logic.

Table 3 summarizes the comparison among our scheme and the aforementioned related works in terms of efficiency. We define the $T_H$ indicates the time complexity of hash function and $T_{asy}$ is the time complexity of the asymmetric encryption. The computations cost of Lee *et al.*'s [15], Xue *et al.*'s [22], Jiang *et al.*'s [10] and Wei *et al.*'s [20] schemes are $9T_H + 4T_{asy}$, $14T_H + 4T_{asy}$, $6T_H + 6T_{asy}$, $12T_H + 4T_{asy}$. Our schemes need $7T_H + 7T_{asy}$ which slightly needs more computational cost than other schemes in asymmetric encryption operation. However, our scheme can achieve formal proof security and more admired security properties.

## 5 Conclusions

In this paper, we propose a secure authentication scheme using elliptic curves cryptosystem which could conquer a range of potential network attacks. Furthermore, the formal proof based on BAN-logic shows that the validity of the proposed scheme. The performance analysis indicates that our proposed scheme is relatively more robust than the related schemes, while increasing little computational efficiency.

## Acknowledgments

This study was supported by the Nanyang Normal University Project under grant QN2015008. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

## References

[1] D. S. AbdElminaam, H. M. Abdul Kader, M. M. Hadhoud, S. M. El-Sayed, "Increase the Performance of Mobile Smartphones using Partition and Migration of Mobile Applications to Cloud Computing," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 34-44, 2014.

[2] A. K Awasthi, "Comment on a dynamic ID-based remote user authentication scheme," *Transactions on Cryptology*, vol. 1, no. 2, pp. 15-16, 2004.

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

[4] C. C. Chang, 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.

[5] M. L. Das, A. Saxena, V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no.2, pp. 629-631, 2004.

[6] D. L. Guo, 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.

[7] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer Science & Business Media, 2006.

[8] M. S. Hwang, C. C. Lee, S. K. Chong, J. W. Lo, "A Key Management for Wireless Communications," *International Journal of Innovative Computing, Information and Control*, Vol. 4, No. 8, pp. 2045-2056, 2008.

[9] D. B. He, J. H. Chen, R. Zhang, "Weaknesses of a dynamic ID-based remote user authentication scheme," *International Journal of Electronic Security and Digital Forensics*, vol. 3, no. 4, pp. 355-362, 2010.

[10] Q. Jiang, J. Ma, G. Li, X. Li, "Improvement of robust smart-card-based password authentication scheme," *International Journal of Communication Systems*, vol. 28, no. 2, pp. 383-393, 2015.

[11] M. K. Khan, S. K. Kim, K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'," *Computer Communications*, vol. 34, no. 3, pp. 305-309, 2011.

[12] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis," *Proceedings of Advances in Cryptology*, Santa Barbara, CA, U.S.A., pp. 388-397, 1999.

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

[14] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.

[15] C. Lee, C. Chen, C. Wu, S. Huang, "An extended chaotic maps-based key agreement protocol with user anonymity," *Nonlinear Dynamics*, vol. 69, no. 1-2, pp. 79-87, 2012.

[16] X. Li, J. W. Niu, M. K. Khan, J. G. Liao, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1365-1371, 2013.

[17] Y. Lin, "Chaotic map based mobile dynamic ID authenticaed key agreement scheme," *Wireless Personal Communications*. vol. 78, no. 2, pp. 1487-1494, 2014.

[18] T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computer*, vol. 5, no. 51, pp. 541-552, 2002.

[19] Y. Y. Wang, J. Y. Liu, F. X. Xiao, J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," *Computer Communications*, vol. 4, no. 32, pp. 583-585, 2009.

[20] J. H. Wei, W. F. Liu, 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.

[21] D. Xiao, X. Liao, S. Deng, "A novel key agreement protocol based on chaotic maps," *Information Sciences*, vol. 177, no. 4, pp. 1136-1142, 2007.

[22] K. Xue, P. Hong, "Security improvement on an anonymious key agreement protocol based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 7, pp. 2969-2977, 2012.

**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.

**Wei Wang** received the B.S. and M.S. degrees in Computer Science and Technology from Northwest agriculture and forestry university of science and technology, Yangling, Shanxi, China in 2003 and 2006, respectively. He is a lecturer in Nanyang Normal University, Nanyang, Henan, China. Her research interests include data mining and information security.