A Robust and Efficient Remote Authentication Scheme from Elliptic Curve Cryptosystem

Guifa Hou, Zhijie Wang
(Corresponding author: Guifa Hou)

Department of Computer Science and Information Engineering, Anyang Institute of Technology
Huanghe Avenue, Anyang 455000, China
(Email: houguifa01@outlook.com)

(Received June 18, 2016; revised and accepted Sept. 3 & Sept. 25, 2016)

Abstract

Along with the extensive prevalence of the network and the portable equipments, people can access network resources conveniently. The protection of participants' privacy and data confidentiality is significant. Authentication mechanism is essential to assure the authenticity of all participants and forbid the illegal accessing. In this paper, we propose a robust remote authentication scheme with privacy protection, which achieves the efficiency. Besides, we prove the completeness of the proposed scheme through BAN-logic. The performance comparisons show that our proposal is sufficiently robust and suitable to the practical application environment.

Keywords: Anonymity; Authentication; BAN-logic

1 Introduction

With the large-scale proliferation of Internet and network technologies, users can conveniently obtain the desire resources by kinds of portable devices such as (e.g., mobile phones, PDAs and notebook computers) at any time and any place. On the other hand, it also brings kinds of network security problems due to the open nature of the Internet. In order to solve these security problems, the password based authentication schemes using smart cards have been widely deployed to verify the legitimacy of remote users in the login process. Since the computation capacity of these potable devices is limited, these authentication schemes should be more efficient for suiting to the practical application environment.

In 1981, Lamport [20] proposed a remote authentication scheme based on static login identity (ID). Until now, ample of remote authentication schemes based on Lamport's scheme have been published in the literatures [1, 5, 8, 10, 11, 13, 26]. These schemes can be further divided into static ID and dynamic ID schemes, the main drawback of the former schemes is that users should login to the remote server with the fixed ID. However, the latter kind of schemes can eliminate the risk of ID-theft and protect users' privacy. In 2004, Das et al. [8] presented a remote user authentication scheme based on dynamic ID using smart cards, which allowed users to choose and change their passwords freely, and need not servers to maintain the verifier table. However, in 2004, Awashti [2] analyzed several weaknesses of Das et al.'s scheme and showed that their scheme was completely insecure. Later on, many dynamic-ID authentication schemes based on Das et al.'s scheme are published to achieve better security and efficiency [1, 5, 10, 11, 13, 16, 17, 19, 26].

Because of the convenience and secure computation of smart cards, a number of password authentication schemes using smart cards have been proposed [3, 6, 7, 9, 12, 14, 18, 21, 23, 24]. Most of the previous authentication schemes assume that smart cards are tamper-resistant (i.e., secret information stored in the smart card cannot be revealed). However, recent research results have shown that the sensitive data stored in the smart card could be extracted by monitoring the power consumption and analyzing the leaked information about the cardholder [15, 22]. Thus, such schemes rely on the tamper-resistance assumption are prone to types of attacks, such as impersonation attack, server spoofing attack, and offline password guessing attack, etc.. And hence, a secure authentication scheme should be able to withstand a series of attacks rely on stolen smart card attack.

Most of the schemes proposed in the literatures do not achieve the revocation of smart cards. This problem may lead to the abuse of lost smart cards to login the system successfully. Thereby, to avoid the misuse of smart cards, the remote server should allow users' revocation. In 2005, Fan et al. [9] proposed a robust authentication scheme based on the factoring problem. In their scheme, the smart cards revocation problem is solved. However, in 2009, Rhee et al. [23] pointed out Fan et al.'s scheme is vulnerable to server spoofing attack. At the same time, Wang et al. [25] presented an authentication scheme tried to solve smart cards revocation problem. Unfortunately, their scheme is susceptible to the known key attack and

Table 1: Notations

Notation	Meaning
U_i	The ith user
S	The remote server
ID_i	The identity of the user U_i
PW_i	The password of the user U_i
x	The master secret key of S
SK	The session key shared among U_i and S
$H(\cdot)$	A one-way hash function
$E_k(M)/D_k(C)$	The symmetric encryption/decryption
$\oplus$	Exclusive-OR operation
$\|$	String concatenation operation

the stolen smart card attack. In 2011, Wang et al. [24] proposed an improved scheme with key agreement based on the elliptic curve discrete logarithm problem. Nevertheless, in the same year, Chang et al. [6] pointed out Wang et al.'s scheme cannot withstand server spoofing attack and presented an improved authentication scheme.

In this paper, we propose a comparatively secure dynamic identity authentication scheme which achieves the criterion listed in Table II. Noticeably, in the security analysis, BAN-logic [4] is employed to prove the completeness of the proposal. From the performance and functionality comparisons, our scheme is superior for suiting the practical environment.

The structure of our paper is organized as follows. In Section 2, we propose an improved robust authentication scheme. Subsequently, we analyze the security of our proposal in Section 3 and compare the performance with the previous related protocols in Section 4. At last, Section 5 presents the overall conclusion.

2 Our Scheme

In this section, we propose an authentication scheme which can remedy a range of network attacks. It is composed five basic phases: registration phase, login phase, authentication and session key exchange phase, smart card revocation phase and off-line password change phase. The notations used in our scheme are summarized in Table 1.

2.1 Preliminaries

In this section, we introduce the basic knowledge about CAPTCHA in brief. More details about CAPTCHA are referenced in [27].

2.1.1 Related Concepts

Completely Automated Public Turing test to tell Computer and Humans Apart(CAPTCHA) is an automated test that humans can pass, but difficult for computers to pass. For example, CAPTCHA requires users to identify a series of letters that may be warped or obscured by distracting backgrounds and other noise in the image. Using CAPTCHA, S can distinguish legitimate users from computer bots while requiring minimal effort by human user.

2.2 Registration Phase

Initially, S stores a large number of CAPTCHA puzzles which correspond to answers in a database with the format $(puzzle, answer)$. Then the remote server S selects a large prime number p and two integer elements a, b, where $p > 2^{160}$ and $4a^3 + 27b^2 mod p \neq 0$. Then S chooses an elliptic curve equation $E_p(a,b) : y^2 = x^3 + ax + b mod p$. Let G be a base point of the elliptic curve, where n multiplies G is equal to O and $n > 2^{160}$.

Step 1: U_i selects his/her identity ID_i and password PW_i. After that, he/she registers in S with sending $\{ID_i, A_i\}$ over a secure communication channel, where $A_i = H(ID_i \| PW_i)$.

Step 2: Upon receiving the registration request, S computes $B_i = E_{A_i}(H(x\|n_i), n_i \cdot G)$, where x is the master secret key and n_i is a unique random number for U_i. Note that, the public key of S is $Pub_S = x \cdot G$.

Step 3: After that, S maintains a registration table which includes $(H(ID_i \oplus x) \cdot G, n_i)$. S can retrieve n_i from the registration table by $H(ID_i \oplus x) \cdot G$ in the revocation phase and in the authentication and key agreement phase.

Step 4: Then S writes $\{B_i, H(\cdot), G, E_k()/D_k()\}$ into the smart card and issues it to the client U_i through a secure channel.

2.3 Login Phase

When the user U_i wants to login S, he/she should insert the smart card to the terminal and key in ID_i with PW_i, then the smart card performs the following steps:

Step 1: The smart card computes $A_i = H(ID_i \| PW_i)$ to decrypt B_i and obtains $H(x\|n_i)$, $n_i \cdot G$. Afterwards, it generates a random nonce t in Z_p^* and computes

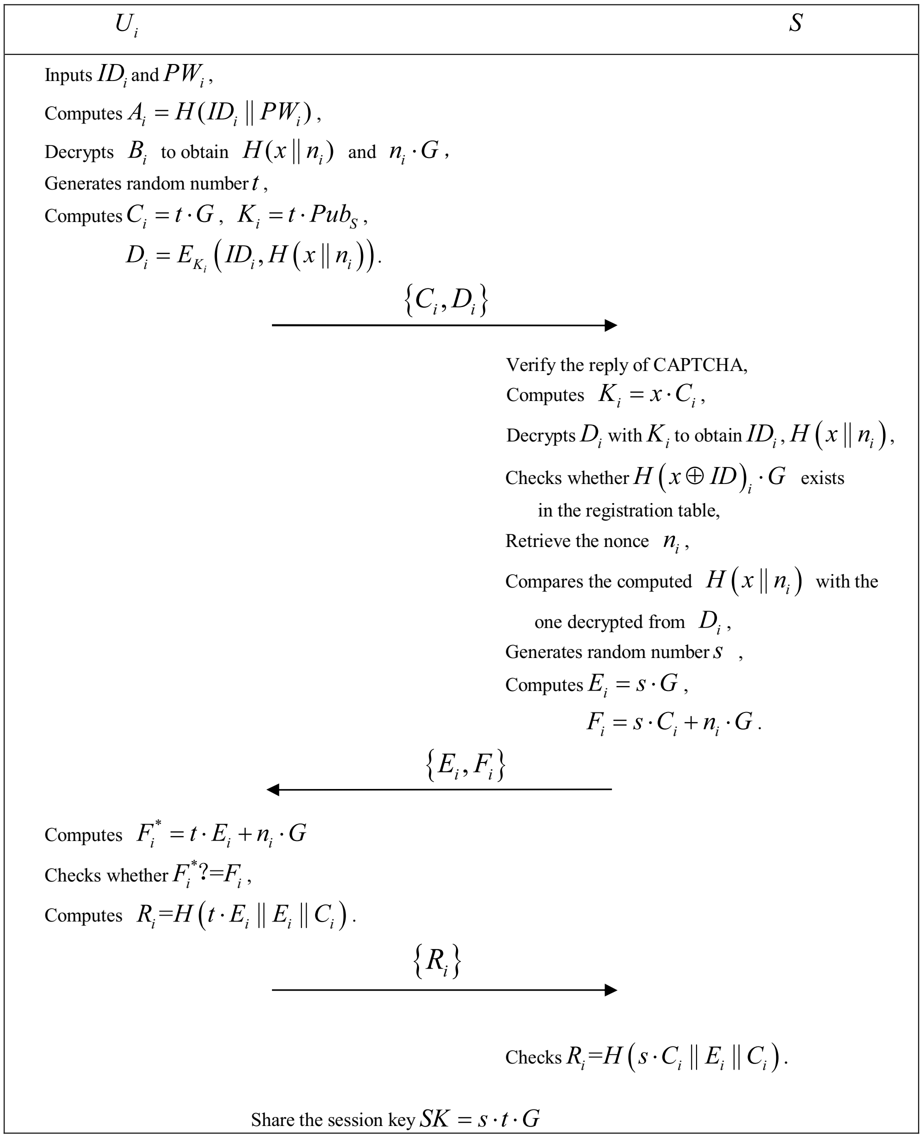
U_i
S
Inputs ID_i and PW_i,
Computes $A_i = H(ID_i \| PW_i)$,
Decrypts B_i to obtain $H(x \| n_i)$ and $n_i \cdot G$,
Generates random number t,
Computes $C_i = t \cdot G$, $K_i = t \cdot Pub_S$,
$D_i = E_{K_i}\left(ID_i, H\left(x \| n_i\right)\right)$.
$\{C_i, D_i\}$
Verify the reply of CAPTCHA,
Computes $K_i = x \cdot C_i$,
Decrypts D_i with K_i to obtain $ID_i, H\left(x \| n_i\right)$,
Checks whether $H\left(x \oplus ID\right)_i \cdot G$ exists
in the registration table,
Retrieve the nonce n_i,
Compares the computed $H\left(x \| n_i\right)$ with the
one decrypted from D_i,
Generates random number s ,
Computes $E_i = s \cdot G$,
$F_i = s \cdot C_i + n_i \cdot G$.
$\{E_i, F_i\}$
Computes $F_i^* = t \cdot E_i + n_i \cdot G$
Checks whether $F_i^*?{=}F_i$,
Computes $R_i{=}H\left(t \cdot E_i \| E_i \| C_i\right)$.
$\{R_i\}$
Checks $R_i{=}H\left(s \cdot C_i \| E_i \| C_i\right)$.
Share the session key $SK = s \cdot t \cdot G$

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

$C_i = t \cdot G$, $K_i = t \cdot Pub_S$, $D_i = E_{K_i}(ID_i, H(x\|n_i))$, then sends the login request message $\{C_i, D_i\}$ to the remote server S.

Step 2: When S receives the message $\{C_i, D_i\}$, it randomly selects a CAPTCHA puzzle in its database and sends to U_i. If S receives the incorrect reply from U_i which is not corresponding to the puzzle transmitted to U_i, the login request will be terminated.

2.4 Authentication and Session Key Exchange Phase

Step 1: After checking the reply of CAPTCHA puzzle from U_i, S computes $K_i = x \cdot C_i$. Then it decrypts D_i with K_i to obtain ID_i and $H(x\|n_i)$. Then it calculates $H(x \oplus ID_i) \cdot G$ and checks it whether exists in the registration table. If so, S can retrieve the nonce n_i; otherwise, S aborts the messages.

Step 2: S calculates $H(x\|n_i)$ with the retrieved n_i. If the computed value is equal to the decrypted $H(x\|n_i)$ from D_i, S will execute the following steps; otherwise, the login request will be rejected.

Step 3: After the verification of U_i, S generates a random number s in Z_p^* and computes $E_i = s \cdot G$ and $F_i = s \cdot C_i + n_i \cdot G$. Then S transmits the replied message $\{E_i, F_i\}$ to U_i.

Step 4: Upon receiving the replication, the smart card computes $F_i^* = t \cdot E_i + n_i \cdot G$ and checks $F_i^*? = F_i$. If the equation holds, the legitimacy of S is authentic. After that, U_i computes $R_i = H(t \cdot E_i \| E_i \| C_i)$ and transmits the session key verification message $\{R_i\}$ to S.

Step 5: Upon receiving the reply, S verifies whether R_i equals to the computed value $H(s \cdot C_i \| E_i \| C_i)$. If the equivalence holds, the mutual authentication is achieved; else, the entire authentication is failed.

After finishing the mutual authentication, U_i and S agree on the common session key $SK = s \cdot t \cdot G$.

2.5 Password Changing Phase

When U_i wants to update his/her password without the help of S. U_i inserts his/her smart card into a card reader and inputs ID_i with PW_i.

Step 1: U_i computes $A_i = H(ID_i \| PW_i)$ to decrypt B_i and obtains $H(x \| n_i)$, $n_i \cdot G$.

Step 2: U_i can be allowed to input the new password PW_i^{new}.

Step 3: The smart card computes $A_i^{new} = H(ID_i \| PW_i^{new})$, $B_i^{new} = E_{A_i^{new}}(H(x \| n_i), n_i \cdot G)$, and stores B_i^{new} into the smart card to replace B_i.

2.6 Smart Card Revocation Phase

In case of lost or stolen smart cards, U_i could request S for its revocation. In our scheme, U_i should transmit ID_i to S via a secure communication channel, then S computes $H(ID_i \oplus x) \cdot G$ and checks it whether exists in the registration table or not. If so, S removes the entry $(H(ID_i \oplus x) \cdot G, n_i)$ from the registration table.

3 Secure Analysis of Our Scheme

3.1 Completeness Proof Based on BAN-logic

In this section, we prove that the authentication goals using BAN-logic [4], which is a logic of belief focuses on the beliefs of the legitimate principals involved in the protocol. Let define the notations below:

- $\mathcal{P} \mid\equiv X$: The principal $\mathcal{P}$ believes a statement X or $\mathcal{P}$ would be entitled to believe X.
- $\sharp(X)$: The formula X is fresh.
- $\mathcal{P} \Rightarrow X$: The principal $\mathcal{P}$ has jurisdiction over the statement X.
- $\mathcal{P} \triangleleft X$: The principal $\mathcal{P}$ sees the statement X.
- $\mathcal{P} \mid\sim X$: The principal $\mathcal{P}$ once said the statement X.
- (X, Y): The formula X or Y is one part of the formula (X, Y).
- $\langle X \rangle_Y$: The formula X is combined with the formula Y.
- $\{X\}_Y$: The formula X is encrypted under the key Y.
- $\mathcal{P} \overset{k}{\longleftrightarrow} \mathcal{Q}$: The principals $\mathcal{P}$ and $\mathcal{Q}$ use the shared key k to communicate. Here, k will never be discovered by any principal except for $\mathcal{P}$ and $\mathcal{Q}$.
- $\mathcal{P} \overset{k}{\rightleftharpoons} \mathcal{Q}$: k is shared secret known to $\mathcal{P}$, $\mathcal{Q}$, and possibly to one trusted by them.
- SK: The session key used in the current session.

In the following, we introduce Some main logical postulates used in the demonstration:

- 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: $\frac{\mathcal{P} \mid\equiv \mathcal{Q} \Rightarrow X, \mathcal{P} \mid\equiv \mathcal{Q} \mid\equiv X}{\mathcal{P} \mid\equiv X}$, $\frac{\mathcal{P} \mid\equiv (X,Y)}{\mathcal{P} \mid\equiv X}$, $\frac{\mathcal{P} \triangleleft (X,Y)}{\mathcal{P} \triangleleft X}$, $\frac{\mathcal{P} \mid\equiv \mathcal{Q} \mid\sim (X,Y)}{\mathcal{P} \mid\equiv \mathcal{Q} \mid\sim X}$.

For proving the proper mutual authentication and the agreement of session key, we list the verification goals as follows:

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

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

Next, we list the idealized form transformed from the proposed scheme in the following:

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

Message 2: $S \rightarrow U_i$: $(E_i, \{S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i), C_i, E_i\}_{n_i})$.

Message 3: $U_i \rightarrow S$: $\langle C_i, E_i \rangle_{SK}$.

The following assumptions are presented to further analyze our scheme:

A.1: $U_i \mid\equiv (U_i \overset{n_i}{\longleftrightarrow} S)$;

A.2: $S \mid\equiv (S \overset{\langle n_i \rangle_x}{\longleftrightarrow} U_i)$;

A.3: $U_i \mid\equiv \sharp(C_i)$;

A.4: $S \mid\equiv \sharp(E_i)$;

A.5: $S \mid\equiv U_i \Rightarrow (ID_i, C_i)$;

A.6: $S \mid\equiv U_i \Rightarrow (C_i, E_i)$;

A.7: $U_i \mid\equiv S \Rightarrow (S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i), C_i, E_i)$;

A.8: $U_i \mid\equiv t$;

A.9: $S \mid\equiv s$.

According to the above-mentioned logical postulates and assumptions, we demonstrate the validity of our scheme in the following:

- According to Message 1, we obtain:
  $S \triangleleft (C_i, \{ID_i, C_i\}_{\langle n_i \rangle_x})$.

- According to the jurisdiction rule, we obtain:

  $S \triangleleft \{ID_i, C_i\}_{\langle n_i \rangle_x}$.

- According to Assumption A.2 and the message-meaning rule, we obtain:

  $S \mid\equiv U_i \mid\sim (ID_i, C_i)$.

- According to the jurisdiction rule, we obtain:

  $S \mid\equiv U_i \mid\sim C_i$.

- According to Message 2, we obtain:

  $U_i \triangleleft (E_i, \{S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i), C_i, E_i\}_{n_i})$.

- According to the jurisdiction rule, we obtain:

  $U_i \triangleleft \{S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i), C_i, E_i\}_{n_i}$.

- According to Assumption A.1 and the message-meaning rule, we obtain:

  $U_i \mid\equiv S \mid\sim (S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i), C_i, E_i)$.

- According to Assumption A.3 and the freshness-conjuncatenation rule, we obtain:

  $U_i \mid\equiv \sharp(S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i), C_i, E_i)$.

- According to $U_i \mid\equiv S \mid\sim (S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i), C_i, E_i)$ and the nonce-verification rule, we obtain:

  $U_i \mid\equiv S \mid\equiv (S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i), C_i, E_i)$.

- According to Assumption A.7 and the jurisdiction rule, we obtain:

  $U_i \mid\equiv (S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i), C_i, E_i)$.

- According to the jurisdiction rule, we obtain:

  $U_i \mid\equiv (S \mid\equiv (S \overset{SK}{\rightleftharpoons} U_i)),\ U_i \mid\equiv E_i$.

- According to $SK = t \cdot E_i$ and Assumption A.8, we obtain:

  $U_i \mid\equiv (U_i \xleftrightarrow{SK} S)$ (**Goal 1**).

- According to Message 3, we obtain:

  $S \triangleleft \langle C_i, E_i \rangle_{SK}$.

- According to $S \mid\equiv S \overset{SK}{\rightleftharpoons} U_i$ and message-meaning rule, we obtain:

  $S \mid\equiv U_i \mid\sim (C_i, E_i)$.

- According to Assumption A.4 and the freshness-conjuncatenation rule, we obtain:

  $S \mid\equiv \sharp(C_i, E_i)$.

- According to $S \mid\equiv U_i \mid\sim (C_i, E_i)$ and the nonce-verification rule, we obtain:

  $S \mid\equiv U_i \mid\equiv (C_i, E_i)$.

- According to Assumption A.6 and the jurisdiction rule, we obtain:

  $S \mid\equiv (C_i, E_i)$.

- According to the jurisdiction rule, we obtain:

  $S \mid\equiv C_i$.

- According to $S \mid\equiv U_i \mid\sim C_i$, $SK = s \cdot C_i$ and Assumption A.9, we obtain:

  $S \mid\equiv (U_i \xleftrightarrow{SK} S)$ (**Goal 2**).

3.2 Discussion on Possible Attacks

In the following, we demonstrate that our scheme is able to withstand DoS attack, off-line password guessing attack, replay attack, server spoofing attack, parallel session attack and impersonation attack. Moreover, our scheme achieves mutual authentication and users' anonymity.

We assume that the computation Diffie-Hellman problem (CDHP) in the elliptic curves is difficult to be solved in polynomial time.
CDHP: Given two points $s \cdot P, t \cdot P$, where $s, t \in Z_p^*$, the computation Diffie-Hellman problem (CDHP) is to find the point $(s \cdot t)P$ on $E_p(a, b)$.

3.2.1 DoS Attack

Completely Automated Public Turing test to tell Computer and Humans Apart(CAPTCHA) technique is used in our proposed scheme which makes the malicious attacker cannot launch DoS attack. When users login in the remote server S, they must reply S an answer responding to the CAPTCHA puzzle. These puzzles are difficult for computers to solve, and thus the DoS attack which launched by computers is resisted effectively.

3.2.2 Off-line Password Guessing Attack

In off-line password guessing attack, the adversary attempts to guess the identity ID_i and password PW_i from the intercepted messages transmitted between U_i and S. If an adversary eavesdrops U_i's login request message $\{C_i, D_i\}$, which $C_i = t \cdot G$, $D_i = E_{K_i}(ID_i, H(x \| n_i))$. It is impossible to obtain ID_i in real polynomial time due to the difficulty of CDHP in elliptic curve cryptosystem.

3.2.3 Mutual Authentication and Users' Anonymity

In the authentication and session key exchange phase, the remote server and users can authenticate each other such that no adversary can impersonate any participant in this system. Besides, the message transmitted between users and the server will be updated in each session, therefore, no one can trace the user by eavesdropping. Thus, our proposal provides perfect forward security, mutual authentication and users' anonymity.

Table 2: Comparisons of functionality

	Li et al.'s [21]	Chen et al.'s [7]	Jiang et al.'s [14]	Wei et al.'s [26]	Ours
Prevention of impersonation attack	No	No	Yes	No	Yes
Prevention of off-line password guessing attack	No	Yes	Yes	Yes	Yes
Prevention of server spoofing attack	Yes	Yes	Yes	Yes	Yes
Prevention of replay attack	Yes	Yes	Yes	Yes	Yes
Preserving user anonymity	No	No	No	No	Yes
Parallel session attack	Yes	Yes	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes	Yes	Yes
Perfect forward secrecy	Yes	No	No	Yes	Yes

Table 3: Performance comparisons: Computation cost

Type of operations	Li et al.'s [21]	Chen et al.'s [7]	Jiang et al.'s [14]	Wei et al.'s [26]	Ours
T_H	7	8	6	12	5
T_{sym}	0	0	0	0	2
T_{asy}	8	6	6	4	8

3.2.4 Replay Attack

The replay attack is that attackers re-submit the login message transmitted between users and the server to impersonate users. In our scheme, neither the replay of an old login message $\{C_i, D_i\}$ in the login phase nor the replay of the response message $\{E_i, F_i\}$ of the server in the authentication and session key exchange phase, it will fail in Step 2 and Step 4 of authentication and session key exchange phase, due to the random numbers are updated for every session and the adversary cannot get the real one. Therefore, our scheme can withstand replay attack.

3.2.5 Parallel Session Attack

The parallel session attack is impossible to be launched in our scheme, due to message structure transmitted between users and the server is different. Both $\{D_i, E_i, F_i\}$ and $\{M_i, N_i\}$ have different structures, so the adversary is not able to perform such an attack.

3.2.6 Perfect Forward Secrecy

Suppose the long-term secret key x is revealed by an adversary, he/she cannot derive U_i's previous session key $SK = s \cdot t \cdot G$ since they are contributed by two selected random numbers. Moreover, even the user's previous login request message $\{C_i, D_i\}$ is eavesdropped by the attacker, he/she also cannot obtain s and t. Thus, the proposed scheme is able to ensure perfect forward secrecy.

3.2.7 Impersonation Attack

An adversary can obtain $B_i = E_{A_i}(H(x\|n_i), n_i \cdot G)$, which is stored in U_i's smart card. Then, he/she needs to forge a valid login request $\{C_i, D_i\}$, in which $C_i = t \cdot G$, $D_i = E_{t \cdot Pub_S}(ID_i, H(x\|n_i))$. Nevertheless, it is impossible for the adversary to compute them without password and identity of U_i. Further, we have demonstrated that our proposed scheme could achieve the security of identity and password in the above. Thus, the attacker cannot forge the valid login request to impersonate U_i and launch such an attack.

3.2.8 Server Spoofing Attack

As illustrated above, our enhanced scheme achieves mutual authentication between users and the remote server. Moreover, the attacker cannot obtain t, s and n_i from the message $\{E_i, F_i\}$. And hence, he/she has no ability to calculate the session key $SK = s \cdot t \cdot G$. Thus, our scheme can avoid the server spoofing attack.

4 Performance Evaluation

In this section, we will evaluate the performance and functionality of the proposed scheme, and then make comparisons with Li et al.'s [21], Chen et al.'s [7], Jiang et al.'s [14] and Wei et al.'s [26] schemes. Let T_H be the time complexity for one-way hash function operations; T_{sym} indicates the time complexity of asymmetric encryption and T_{asy} is defined as the time complexity of the symmetric encryption.

Table 2 lists the functionality comparisons of the proposed scheme and other related schemes. We can see that Li et al.'s, Chen et al.'s, Jiang et al.'s and Wei et al.'s schemes satisfy only five, five, six and six requirements list in Table 2, respectively. While the proposed scheme can achieve all requirements list in Table 2. As a result, the proposed scheme is more secure and has more functionalities compared with these related schemes.

From Table 3, we can find that the total computation cost of Li et al.'s, Chen et al.'s, Jiang et al.'s, Wei et al.'s and our proposed schemes are $7T_H + 8T_{asy}$, $8T_H + 6T_{asy}$,

$6T_H + 6T_{asy}$, $12T_H + 4T_{asy}$, $5T_H + 2T_{sym} + 8T_{asy}$. Compared with other related schemes, our scheme is slightly efficient than Li et al.'s scheme and needs more computational cost than other schemes. Nevertheless, these schemes are insecure and our scheme can satisfy more admired criterion compared with them.

5 Conclusions

In this paper, we propose a secure authentication scheme using CAPTCHA technique. Then, we present its formal proof using the BAN-logic. Furthermore, the discussions on possible attacks shows that the robustness of the proposal. By comparing with several related schemes, our scheme satisfies many admired criterion to suit for practical application.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] D. S. AbdElminaam, H. M. A. Kader, M. M. Hadhoud and S. M. EI-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] G. T. Becher, *Intentional and Unintentional Sidechannels in Embedded Systems*, University of Massachusetts Amherst, 2014.

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

[5] 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.

[6] Y. F. Chang and P. Y. Chang, "An improved user authentication and key agreement scheme providing user anonymity," *Journal of Electronic Science and Technology*, vol. 4, no. 9, pp. 352–358, 2011.

[7] B. L. Chen, W. C. Kuo and L. C. Wuu, "Robust smart-card-based remote user password authentication scheme," *International Journal of Communication Systems*, vol. 27, no. 2, pp. 377–389, 2014.

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

[9] C. I. Fan, Y. C. Chan and Z. K. Zhang, "Robust remote authentication scheme with smart cards", *Computers & Secutity*, vol. 24, no. 8, pp. 619–628, 2005.

[10] 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.

[11] D. L. Guo, Q. Y. Wen, W. M. Li, H. Zhang and Z. P. Jin, "A Novel Authentication Scheme Using Self-certified Public Keys for Telecare Medical Information Systems," *Journal of Medical Systems*, vol. 39, no. 6, pp. 1–8, 2015.

[12] D. L. Guo, Q. Y. Wen, W. M. Li, H. Zhang and Z. P. Jin, "Analysis and Improvement of Chaotic Map Based Mobile Dynamic ID Authenticated Key Agreement Scheme," *Wireless Personal Communications*, vol. 83, no. 1, pp. 35–48, 2015.

[13] M. S. Hwang, C. C. Lee, S. K. Chong and 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.

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

[15] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," *Proceedings of Advances in Cryptology*, Santa Barbara, CA, USA, pp. 388–397, 1999.

[16] S. Kumari, "Design flaws of "An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography," *Multimedia Tools and Applications*, vol. 76, no. 2, pp. 1801–1815, Jan. 2017.

[17] S. Kumari, M. K. Khan and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Networks*, vol. 27, pp. 159–194, 2015.

[18] S. Kumari, M. K. Khan and X. Li, "A more secure digital rights management authentication scheme based on smart card," *Multimedia Tools and Applications*, vol. 75, no. 2, pp. 1135–1158, 2016.

[19] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Generation Computer Systems*, vol. 63, pp. 56–75, 2016.

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

[21] X. Li, J. W. Niu, M. K. Khan and 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.

[22] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat

of power analysis attacks," *IEEE Transactions on Computers*, vol. 5, no.51, pp. 541–552, 2002.

[23] H. S. Rhee, J. O. Kwon and D. H. Lee, "A remote user authentication scheme without using smart cards," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 6–13, 2009.

[24] R. C. Wang, W. S. Juang, and C. L. Lei, "Robust authentication and key agreement scheme preserving the privacy of secret key," *Computer Communications*, vol. 3, no. 34, pp. 274–280, 2011.

[25] X. M. Wang, W. F. Zhang, J. S. Zhang and M. K. Khan. "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," *Computer Standards & Interfaces*, vol. 5, no. 29, pp. 507–512, 2007.

[26] 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.

[27] L. von Ahn, M. Blum, N. Hopper and J. Langford, "CAPTCHA: Using Hard AI Problems for Security," *Advances in Cryptology (EUROCRYPT'03)*, pp. 294–311, Warsaw, Poland, 2003.

Biography

Guifa Hou received the M.S. degree in Computer software & theory from University of Science & Technology Beijing, Beijing, China, in 2007. He is now an associate professor in Anyang Institute of Technology, Henan, China. His research works focus on information integration and information security.

Zhijie Wang received the B.S. degree in Electrical Technology from Henan University, Kaifeng, Henan, China, in 1999, and the M.S. degree in Computer Applied Technology from Jiangsu University, Zhenjiang, Jiangsu, China, in 2008. His research interests include data mining and information security.