Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090648

A More Secure Dynamic ID-based Remote Authentication Scheme Using Smart Cards

Dianli Guo[1,2], *Fengtong Wen*[1,*] *and Chengbo Xu*[1]

[1] School of Mathematical Sciences, University of Jinan, Jinan, 250022, China
[2] Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Received: 10 Mar. 2015, Revised: 8 May 2015, Accepted: 9 May 2015
Published online: 1 Nov. 2015

Abstract: In 2013, Chang et al. proposed an untraceable dynamic-identity-based remote user authentication scheme with verifiable password update. In this paper, we analyze Chang et al.s scheme and show that their scheme suffers from off-line password guessing attack, server spoofing attack and impersonation attack. Moreover, their scheme is traceable since the attacker can obtain the identity of the user. Thereby, we propose an alternative scheme based on elliptic curve cryptosystem and completely automated public turing test to tell computer and humans apart (CAPTCHA) technique. Besides, we demonstrate the completeness of the proposed scheme through the BAN-logic. Compared with other related existing schemes, the proposed scheme is relatively more secure and well suited for the practical application environment.

Keywords: Dynamic ID, Smart card, Authentication, Password, BAN logic

1 Introduction

In communication networks, it is necessary for servers and users to verify the legitimacy of the involved communicating parties. Password and smart card authentication scheme is a convenient authentication mechanism and is widely applied to the remote login systems. Since Lamport [14] proposed a password based remote user authentication scheme in 1981, a number of remote user authentication schemes have been published in the literatures (e.g., [3,5,20]) to address the security problems. However, most of them have the following weaknesses: 1) User's identity is transmitted over the network unencrypted in all the transaction sessions, and hence, an unauthorized entity can illegally obtain the partial information corresponding to the user (e.g., login history and current location). 2) The smart card is assumed to be tamper-resistant to protect the security. Nevertheless, many researches have shown that it is hard to achieve the target of protecting the values stored in the smart card [12,15].

In 2004, Das et al. [6] presented a dynamic ID based remote user authentication scheme using smart cards. The authors claimed that their scheme could eliminate the risk of ID-theft attack, replay attack and impersonation attack. However, Awasthi [1] analyzed the security of Das et al.'s scheme and observed that their scheme fell short to a range of types attacks. Afterwards, dozens of dynamic ID authentication schemes based on Das et al.'s scheme are published [8,10,13,17,21,22,23,24]. Whereas, most of them were broken shortly after they were proposed.

In 2013, Chang et al. [3] proposed a dynamic-identity- based remote user authentication scheme with verifiable password update, which was believed to achieve low-computation requirement, user untraceability and authentication security.

Our Contributions. This contributions of this paper are twofold. Firstly, we reexamine Chang et al.'s [3] scheme and identify that their scheme cannot resist off-line password guessing attack, impersonation attack and server spoofing attack. Furthermore, their scheme is incapable to achieve the claimed untraceability.

Secondly, to rectify these security pitfalls, we propose a new dynamic ID-based remote authentication scheme that can achieve all the security requirements list in Table 3. Furthermore, we demonstrate the validity of the proposed scheme through the BAN logic.

The rest of this paper is organized as follows. Section 2 briefly reviews Chang et al.'s scheme. In next section, we show its weaknesses. Then, we present our scheme in

[*] Corresponding author e-mail: wftwq@163.com

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
s	The master secret key of S
y	A secret number of S
SID_i	The U_i's smart card identifier
SK	The session key shared among U_i and S
$H(\cdot)$	A one-way hash function
$\oplus$	Exclusive-OR operation
$\|$	String concatenation operation

Section 4, together with analyzing its security in Section 5. Section 6 provides the performance comparison of the proposed protocol with the previous schemes. Section 7 concludes the paper.

The notations used throughout this paper are summarized in Table 1.

2 Review of Chang et al.'s scheme

In this section, we review Chang et al.'s remote authentication scheme briefly. Their scheme contains four phases (i.e., registration phase, login phase, authentication phase and password change phase).

2.1 Registration phase

Step 1. U_i selects his/her identity ID_i and password PW_i, and then sends them to S.

Step 2. After receiving $\{ID_i, PW_i\}$ from U_i, S computes $N_i = H(ID_i\|s) \oplus H(PW_i)$.

Step 3. S stores $\{N_i, y, H(\cdot)\}$ in a smart card, where y is a secret value of S, and then transmits the smart card to U_i via a secure channel.

2.2 Login phase

Step 1. U_i inserts his/her smart card into a card reader and keys ID_i, PW_i. Then the smart card computes $CID_i = ID_i \oplus H(N_i\|y\|T)$, $N_i' = N_i \oplus H(y\|T)$, $B = N_i \oplus H(PW_i) = H(ID_i\|s)$, $C = H(N_i\|y\|B\|T)$, where T is the current timestamp.

Step 2. The smart card sends the login request $\{CID_i, N_i', C, T\}$ to S.

2.3 Authentication phase

Step 1. Upon receiving $\{CID_i, N_i', C, T\}$ from U_i at the time T', S checks whether $(T' - T) \leq \triangle T$. If the verification fails, S terminates this session directly; otherwise, proceeds to Step 2.

Step 2. S computes $N_i^* = N_i' \oplus H(y\|T)$, $ID_i^* = CID_i \oplus H(N_i^*\|y\|T)$, $B^* = H(ID_i^*\|s)$ and $C^* = H(N_i^*\|y\|B^*\|T)$.

Step 3. S verifies C^* with the received C. If $C^* = C$, the legitimacy of U_i is assured and S computes $a = H(B^*\|y\|T'')$, where T'' is the current timestamp. Otherwise, S aborts the login request of U_i and keeps a temporary record of ID_i^* and the cumulative times of the failed requests. If U_i's continuous request is rejected for the third time, S will neglect U_i's following login requests within a guard time interval.

Step 4. Afterwards, S sends $\{a, T''\}$ to U_i via a common channel.

Step 5. Upon receiving the reply message from S, U_i verifies the validity of T''. If the verification holds, the smart card calculates $a^* = H(B\|y\|T'')$ and examines whether a^* equals to a. If they are equal, S is authentic; otherwise, this session is terminated immediately.

2.4 Password change phase

Password change phase will be invoked whenever U_i needs to update his/her password PW_i to PW_i^{new}. In this phase, first, U_i should send the password change request $\{CID_i, N_i', C, T, password\ change\ request\}$ to S. Second, S verifies U_i as depicted in the authentication phase. Subsequently, according to the conclusion of the verification of U_i, S will sends the reply message $\{a, m, T''\}$ to U_i, where $a = H(B\|y\|m\|T'')$ and m is the reply *yes/no* to the password change request. At the last, the smart card verifies the validity of a to ensure S is authentic and the verification of the password change request. Then, the smart card asks U_i to key in the new password PW_i^{new} twice. Note that, if the entered passwords two-time are not identical, U_i needs to enter a new password two-time again. if the entered passwords two-time are identical, the smart card computes $N_i^{new} = N_i \oplus H(PW_i) \oplus H(PW_i^{new})$ and replaces N_i with N_i^{new}.

3 Cryptanalysis of Chang et al.'s scheme

In this section, we demonstrate that if any legal but malicious user of the server intercepts other legitimate users' login request messages, he/she can launch a range of types serious attacks (e.g., off-line password guessing attack, impersonation attack, server spoofing attack) to threat Chang et al.'s authentication scheme with his/her own secret number y, while does not need any secret information stored in the smart cards of legitimate users. The detailed analysis is shown as follows.

3.1 Off-line password guessing attack

Suppose attacker U_k has extracted and recorded the login request messages $\{CID_i, N_i', C, T\}$ exchanged between U_i and S in a prior transaction. Then, U_k can guess the password of U_i by performing the following malicious attack procedures:

Step 1. U_k chooses a password candidate PW_i^* from the password space $\mathcal{D}$.

Step 2. U_k gets y from his/her own smart card and computes $N_i = N_i' \oplus H(y\|T)$, $B^* = N_i \oplus H(PW_i^*)$ and $C^* = H(N_i\|y\|B^*\|T) = H(N_i\|y\|(N_i \oplus H(PW_i^*))\|T)$. Then, he/she compares C^* with C extracted from U_i's login request to ensure the correctness of PW_i^*

Step 3. Repeats Step 1 and 2 by replacing another password candidate PW_i^* until U_i's password is found.

In practice, due to the inherent limitation of human cognition, the password are often memorable shorting strings and hence the password space is very limited, e.g., $|\mathcal{D}| \le 10^6$ [25,26,7], and it follows that the above attack can be completed quite effectively.

3.2 Impersonation attack

As explained in off-line password guessing attack, if the attacker gets the password PW_i of U_i, he/she can further masquerade as U_i to login the server by performing the following procedures:

The adversary acquires the current timestamp T^* and computes $N_i = N_i' \oplus H(y\|T)$, $N_i^{*'} = N_i \oplus H(y\|T^*)$, $B^* = N_i \oplus H(PW_i)$, $C^* = H(N_i\|y\|B^*\|T^*)$, $CID_i^* = CID_i \oplus H(N_i\|y\|T) \oplus H(N_i\|y\|T^*)$, where CID_i, N_i', T are intercepted from U_i's previous login request message and y is the secret value stored in U_k's smart card. Afterwards, the attacker transmits the forged login request message $\{CID_i^*, N_i^{*'}, C^*, T^*\}$ to S.

Obviously, S can accepts the forged login request, since these forged parameters are in the correct format. Hence, Chang et al.'s scheme is susceptible to the impersonation attack.

3.3 Server spoofing attack

As explained above, with the guessed password PW_i of U_i, the adversary U_k can get the secret value $B = N_i \oplus H(PW_i)$ corresponding to U_i, and then he/she can masquerade as S to fool U_i by performing the following steps:

Step 1. Acquires the current timestamp $T^{*''}$ and computes $a^* = H(B\|y\|T^{*''})$. Then, the forged reply message $\{a^*, T^{*''}\}$ is transmitted to U_i.

Step 2. Upon receiving the reply message, U_i verifies the validity of $T^{*''}$ and a^*. It is easy to see that the response message can pass the verification due to U_k forges a^* with the correct secret information B of U_i.

3.4 Failure of preserving user untraceability

Consider that U_k has recorded U_i's previous login request message $\{CID_i, N_i', C, T\}$. Then, he/she can also compute $N_i = N_i' \oplus H(y\|T)$, $ID_i = CID_i \oplus H(N_i\|y\|T)$ using his/her own secret number y. The adversary can track the user's login history and current location with the user's identity ID_i. Hence, we can see Chang et al.'s scheme is incapable to provide user untraceability.

4 The proposed scheme

In this section, we propose a robust authentication scheme using completely automated public turing test to tell computer and humans apart (CAPTCHA) technique and elliptic curve cryptosystem (ECC). The proposed protocol consists of four phases: registration phase, login and authentication phase, password change phase and on-line secret renew phase. And the login and authentication phase is further illustrated in Fig 1.

4.1 Preliminaries

In this section, we briefly introduce the basic knowledge about CAPTCHA and elliptic curve cryptosystem. More details can be found in [19] and [9,11,16], respectively.

4.1.1 Related concepts

(1) Completely automated public turing test to tell computer and humans apart (CAPTCHA) is designed to be simple problems that can be quickly solved by humans, but difficult for computers to solve. Using CAPTCHA, S can distinguish legitimate users from computer bots easily.

(2)In elliptic curve cryptosystem, an elliptic curve equation $E_p(a,b) : y^2 \equiv x^3 + ax + b\ (mod\ p)$ is defined in a prime finite field Z_p, where p is a large prime number, $a, b \in Z_p^*, p > 3$, and $4a^3 + 27b^2 \ne 0\ (mod\ p)$. An elliptic curve consists of all the points $(x,y) \in Z_p \times Z_p$, which satisfy the equation $E_p(a,b) : y^2 \equiv x^3 + ax + b\ (mod\ p)$.

4.1.2 Cryptographic Assumptions

We assume that the two problems as follows are difficult to solve in polynomial time.

1. ECDLP: Given two points $P, Q \in E_p(a,b)$, the elliptic curve discrete logarithm problem is to find an integer $m \in Z_p^*$ such that $Q = m \cdot P$.

2.CDHP: Given three points P, $m \cdot P$, $n \cdot P \in E_p(a,b)$, where m, $n \in Z_p^*$, the computation Diffie-Hellman problem is to find the point $(m \cdot n) \cdot P$ on $E_p(a,b)$.

4.2 Registration phase

Initially, the server S selects two distinct large primes p, q with $p = 2q+1$ and choose s a generator P of order q on the elliptic curve $E_p(a,b)$. S computes the public key $Q = s \cdot P \ (mod\ p)$, where s is the master secret key of S. Subsequently, S stores a large number of CAPTCHA puzzles which correspond to answers in a database with the format $(puzzle, answer)$.

Step 1. U_i selects his/her identity ID_i, password PW_i and computes $H(r \oplus PW_i)$, where r is a random number generated by U_i. Then U_i transmits ID_i and $H(r \oplus PW_i)$ to the remote server S for registration over a secure communication channel.

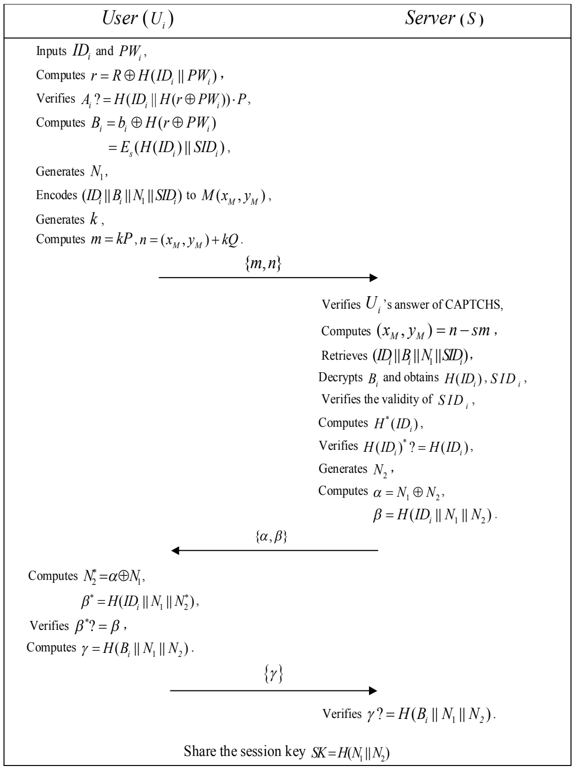
User (U_i)
Server (S)
Inputs ID_i and PW_i,
Computes $r = R \oplus H(ID_i \| PW_i)$,
Verifies $A_i ? = H(ID_i \| H(r \oplus PW_i)) \cdot P$,
Computes $B_i = b_i \oplus H(r \oplus PW_i)$
$= E_s(H(ID_i) \| SID_i)$,
Generates N_1,
Encodes $(ID_i \| B_i \| N_1 \| SID_i)$ to $M(x_M, y_M)$,
Generates k,
Computes $m = kP, n = (x_M, y_M) + kQ$.
$\{m,n\}$
Verifies U_i's answer of CAPTCHS,
Computes $(x_M, y_M) = n - sm$,
Retrieves $(ID_i \| B_i \| N_1 \| SID_i)$,
Decrypts B_i and obtains $H(ID_i)$, SID_i,
Verifies the validity of SID_i,
Computes $H^*(ID_i)$,
Verifies $H(ID_i)^* ? = H(ID_i)$,
Generates N_2,
Computes $\alpha = N_1 \oplus N_2$,
$\beta = H(ID_i \| N_1 \| N_2)$.
$\{\alpha, \beta\}$
Computes $N_2^* = \alpha \oplus N_1$,
$\beta^* = H(ID_i \| N_1 \| N_2^*)$,
Verifies $\beta^* ? = \beta$,
Computes $\gamma = H(B_i \| N_1 \| N_2)$.
$\{\gamma\}$
Verifies $\gamma ? = H(B_i \| N_1 \| N_2)$.
Share the session key $SK = H(N_1 \| N_2)$

Fig. 1: Login and authentication phase

Step 2. S calculates $b_i = E_s(H(ID_i) \| SID_i) \oplus H(r \oplus PW_i)$ and $A_i = H(ID_i \| H(r \oplus PW_i)) \cdot P$, where E_s is a secure symmetric encryption algorithm with the master secret key s kept by S. Subsequently, S personalizes the smart card with $\{b_i, A_i, SID_i, p, E_p(a,b), P, Q, H(\cdot)\}$ and issues it to U_i via a secure channel.

Step 3. After receiving the smart card, U_i computes $R = H(ID_i \| PW_i) \oplus r$ and writes the value R into his/her smart card. Finally, the smart card contains $\{b_i, A_i, SID_i, p, E_p(a,b), P, Q, R, H(\cdot)\}$.

4.3 Login and authentication phase

Step 1. U_i inserts his/her smart card into a card reader and inputs ID_i, PW_i, then smart card computes $r = R \oplus H(ID_i \| PW_i)$, $A_i^* = H(ID_i \| H(r \oplus PW_i)) \cdot P$ and checks whether $A_i^* ? = A_i$, if the equation holds, proceeds to Step 2; otherwise, this phase is terminated immediately.

Step 2. U_i computes $B_i = b_i \oplus H(r \oplus PW_i) = E_s(H(ID_i) \| SID_i)$, then chooses a random number N_1 and encodes the message $(ID_i \| B_i \| N_1 \| SID_i)$ to a point $M(x_M, y_M)$ of the elliptic curve $E_p(a,b)$ uniquely.

Step 3. U_i chooses a random number k and calculates $m = kP$, $n = (x_M, y_M) + kQ$, and then sends the message $\{m,n\}$ to S.

Step 4. S selects a random CAPTCHA puzzle in its database and sends it to U_i. If U_i's reply is right, proceeds to Step 5; otherwise, the login request is terminated.

Step 5. S computes $(x_M, y_M) = n - sm$ and decodes it to get $(ID_i \| B_i \| N_1 \| SID_i)$. Subsequently, S decrypts B_i using s to obtain $H(ID_i), SID_i$.

Step 6. After that, S checks whether the decoded SID_i equals to the decrypted SID_i. If they are not equal, S aborts the login request; else, S computes $H(ID_i)^*$ and compares it with $H(ID_i)$ decrypted from B_i. If $H(ID_i)^* = H(ID_i)$, S proceeds the next step; otherwise, S aborts the login request and terminates this session.

Step 7. S chooses a random number N_2 and computes $\alpha = N_1 \oplus N_2$, $\beta = H(ID_i \| N_1 \| N_2)$. Subsequently, S sends the response mutual message $\{\alpha, \beta\}$ to U_i.

Step 8. Upon receiving $\{\alpha, \beta\}$, U_i computes $N_2^* = \alpha \oplus N_1$, $\beta^* = H(ID_i \| N_1 \| N_2^*)$ and checks $\beta^* ? = \beta$. If the equation holds, the validity of S is verified by U_i. Afterwards, U_i calculates $\gamma = H(B_i \| N_1 \| N_2)$ and sends it to S.

Step 9. After receiving γ, S verifies $\gamma ? = H(B_i \| N_1 \| N_2)$. If the equation holds, S ensures the legitimacy of U_i; otherwise, the mutual authentication fails.

After finishing mutual authentication, U_i shares a common session key $SK = H(N_1 \| N_2)$ with S.

4.4 Password change phase

When U_i wants to update his/her password off-line, he/she proceeds the following steps:

Step 1. U_i inputs his/her identity ID_i and password PW_i. The smart card computes $r = R \oplus H(ID_i \| PW_i)$, $A_i^* = H(ID_i \| H(r \oplus PW_i)) \cdot P$ and checks $A_i^* ? = A_i$. If the equation holds, proceeds to Step 2; on the contrary, this phase is terminated.

Step 2. U_i inputs the new password PW_i^{new} and computes $b_i^{new} = b_i \oplus H(r \oplus PW_i) \oplus H(r \oplus PW_i^{new})$, $A_i^{new} = H(ID_i \| H(r \oplus PW_i^{new})) \cdot P$, $R^{new} = r \oplus H(ID_i \| PW_i^{new})$, and then stores b_i^{new}, A_i^{new}, R^{new} into the smart card to replace b_i, A_i, R, respectively.

Finally, the smart card of U_i contains $\{b_i^{new}, A_i^{new}, SID_i, p, E_p(a,b), P, Q, R^{new}, H(\cdot)\}$.

4.5 On-line secret renew phase

In order to strengthen the security of the system, the remote server should renew its master secret key aperiodically, the detail steps of this phase are as follows:

Step 1. S chooses a new s^{new} and computes $B_i^{new} = E_{s^{new}}(H(ID_i)\|SID_i)$, $Q^{new} = s^{new} \cdot P$. Then S sends $\{B_i^{new}, Q^{new}\}$ to U_i over the established private secret channel.

Step 2. Upon receiving $\{B_i^{new}, Q^{new}\}$, the smart card computes $b_i^{new} = B_i^{new} \oplus H(r \oplus PW_i)$ and replaces b_i, Q with b_i^{new}, Q^{new} in his/her smart card.

5 Secure analysis of our scheme

5.1 Authentication proof based on BAN-logic

In this section, we demonstrate that the proposed scheme is working correctly by achieving the authentication goals using BAN logic [2], which is vital to reason out the security properties, describe the beliefs of trustworthy parties involved in the protocol and on the evolution of these beliefs as a consequence of communications. The notations used in BAN logic analysis are defined as follows:

- $\mathscr{P} \mid\equiv X$: The principal $\mathscr{P}$ believes a statement X or $\mathscr{P}$ would be entitled to believe X.
- $\sharp(X)$: The formula X is fresh.
- $\mathscr{P} \Rightarrow X$: The principal $\mathscr{P}$ has jurisdiction over the statement X.
- $\mathscr{P} \lhd X$: The principal $\mathscr{P}$ sees the statement X.
- $\mathscr{P} \mid\sim X$: The principal $\mathscr{P}$ once said the statement X.
- (X,Y): The formula X or Y is one part of the formula (X,Y).
- $\{X\}_Y$: The formula X is encrypted under the key Y.
- $\langle X\rangle_Y$: The formula X combined with a secret parameter Y.
- $\xmapsto{K} \mathscr{P}$: The formula K is a public key of the principal $\mathscr{P}$. The matching secret key (K^{-1}, the inverse of K) is saved privately by $\mathscr{P}$.
- $\mathscr{P} \overset{K}{\rightleftharpoons} \mathscr{R}$: The formula K is a secret known only to the principals $\mathscr{P}$ and $\mathscr{R}$.
- $\mathscr{P} \xleftrightarrow{K} \mathscr{R}$: The principals $\mathscr{P}$ and $\mathscr{R}$ use the shared key K to communicate. Here, K will never be discovered by any principal except for $\mathscr{P}$ and $\mathscr{R}$.
- SK: The session key used in the current session.

Some main logical postulates of BAN logic are described as follows:

- The message-meaning rule: $\frac{\mathscr{P}\mid\equiv\mathscr{R}\overset{K}{\rightleftharpoons}\mathscr{P},\,\mathscr{P}\lhd\langle X\rangle_K}{\mathscr{P}\mid\equiv\mathscr{R}\mid\sim X}$.
- The freshness-conjuncatenation rule: $\frac{\mathscr{P}\mid\equiv\sharp(X)}{\mathscr{P}\mid\equiv\sharp(X,Y)}$.
- The nonce-verification rule: $\frac{\mathscr{P}\mid\equiv\sharp(X),\,\mathscr{P}\mid\equiv\mathscr{R}\mid\sim X}{\mathscr{P}\mid\equiv\mathscr{R}\mid\equiv X}$.
- The jurisdiction rule: $\frac{\mathscr{P}\mid\equiv\mathscr{R}\Rightarrow X,\,\mathscr{P}\mid\equiv\mathscr{R}\mid\equiv X}{\mathscr{P}\mid\equiv X}$, $\frac{\mathscr{P}\mid\equiv\xmapsto{K}\mathscr{P},\,\mathscr{P}\lhd\{X\}_K}{\mathscr{P}\lhd X}$, $\frac{\mathscr{P}\mid\equiv\langle X,Y\rangle}{\mathscr{P}\mid\equiv X}$, $\frac{\mathscr{P}\mid\equiv\mathscr{R}\mid\sim\langle X,Y\rangle}{\mathscr{P}\mid\equiv\mathscr{R}\mid\sim X}$.

According to the analytic procedures of BAN logic, we list the verification goals of the proposed scheme in the following:

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

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

Next, the proposed scheme is arranged from the generic type to the idealized form in the following:

Message 1: $U_i \to S$: $\{\langle ID_i, N_1, SID_i\rangle_{B_i}\}_Q$

Message 2: $S \to U_i$: $\langle N_1, N_2\rangle_{ID_i}$

Message 2: $U_i \to S$: $\langle N_1, N_2\rangle_{B_i}$

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

A.1: $U_i \mid\equiv \sharp(N_1)$

A.2: $S \mid\equiv \sharp(N_2)$

A.3: $U_i \mid\equiv (U_i \overset{ID_i}{\rightleftharpoons} S)$

A.4: $S \mid\equiv (U_i \overset{B_i}{\rightleftharpoons} S)$

A.5: $S \mid\equiv (\xmapsto{Q} S)$

A.6: $U_i \mid\equiv S \Rightarrow \langle N_1, N_2\rangle$

A.7: $S \mid\equiv U_i \Rightarrow \langle N_1, N_2\rangle$

Based on the above-mentioned assumptions and rules of BAN logic, we analyze the idealized form of the proposed scheme and the main procedures of proof as follows:

According to the message 1, we obtain:

$S \lhd \{\langle ID_i, N_1, SID_i\rangle_{B_i}\}_Q$.

According to the assumption A.5 and the message meaning rule, we obtain:

$S \lhd \langle ID_i, N_1, SID_i\rangle_{B_i}$.

According to the assumption A.4 and the message meaning rule, we obtain:

$S \mid\equiv U_i \mid\sim \langle ID_i, N_1, SID_i\rangle$.

According to the jurisdiction rule, we obtain:

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

According to the message 2, we obtain:

$U_i \lhd \langle N_1, N_2\rangle_{ID_i}$.

According to the assumption A.3 and the message-meaning rule, we obtain:

$U_i \mid\equiv S \mid\sim \langle N_1, N_2\rangle$.

According to the assumption A.1 and the freshness-conjuncatenation rule, we obtain:

$U_i \mid\equiv \sharp(\langle N_1, N_2\rangle)$.

According to $U_i \mid\equiv S \mid\sim \langle N_1, N_2\rangle$ and the nonce verification rule, we obtain:

$U_i \mid\equiv S \mid\equiv \langle N_1, N_2\rangle$.

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

$U_i \mid\equiv \langle N_1, N_2\rangle$.

According to the jurisdiction rule, we obtain:

$U_i \mid\equiv N_2$.

According to $SK = H(N_1\|N_2)$, we obtain:

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

According to the message 3, we obtain:

$S \lhd \langle N_1, N_2\rangle_{B_i}$.

According to the assumption A.4 and the message-meaning rule, we obtain:

$S \mid\equiv U_i \mid\sim \langle N_1, N_2 \rangle$.

According to the assumption A.2 and the freshness-conjuncatenation rule, we obtain:

$S \mid\equiv \sharp(\langle N_1, N_2 \rangle)$.

According to $S \mid\equiv U_i \mid\sim \langle N_1, N_2 \rangle$ and the nonce verification rule, we obtain:

$S \mid\equiv U_i \mid\equiv \langle N_1, N_2 \rangle$.

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

$S \mid\equiv \langle N_1, N_2 \rangle$.

According to the jurisdiction rule, we obtain:

$S \mid\equiv N_1$.

According to $SK = H(N_1 \| N_2)$, we obtain:

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

5.2 Discussion on the possible attacks

In the following, we analyze the security of the proposed scheme and show that it can resist different types of attacks and provides user anonymity.

5.2.1 User anonymity

Consider an adversary intercepts U_i's login request message $\{m, n\}$, he/she tries to retrieve any static parameter from these parameters. Here, it is infeasible for the adversary to retrieve $(ID_i \| B_i \| N_1 \| SID_i)$ from $\{m, n\}$ without the secret key s of S. Furthermore, $\{m, n\}$ are session-variant due to the randomness of N_1, k. Hence, our proposed scheme can achieve user anonymity.

5.2.2 Off-line password guessing attack

Off-line password guessing attack means that the adversary can employ the revealed secret values stored in the smart card to guess the password of a specific user. If the attacker reveals the information $\{b_i, A_i, SID_i, R\}$ stored in U_i's smart card, where $R = r \oplus H(ID_i \| PW_i)$, $A_i = H(ID_i \| H(r \oplus PW_i)) \cdot P$. It is hard for the adversary to retrieve ID_i, PW_i due to he/she needs to guess them simultaneously. Passwords are usually composed of digits and English letters. As pointed out in [7], the probability to guess a correct password or an identity composed of exact n characters approximates $\frac{1}{2^{6n}}$. If the length of r is m bits (in our scheme, $m = 160$), the probability to guess correct ID_i, PW_i and r at the same time is approximately $\frac{1}{2^{12n+160}}$, which is very negligible.

5.2.3 Impersonation attack

An adversary can obtain $b_i = E_s(H(ID_i) \| SID_i) \oplus H(r \oplus PW_i)$, which is stored in U_i's smart card. Then, he/she needs to forge a valid login request $\{m, n\}$, which are generated by $(ID_i \| B_i \| N_1 \| SID_i) = (ID_i \| E_s(H(ID_i) \| SID_i) \| N_1 \| SID_i)$. Nevertheless, it is impossible for the adversary to compute them without password and identity of U_i. Moreover, we have demonstrated that our scheme achieves the security of identity and password in the above. Thus, the attacker cannot forge the valid login request to impersonate U_i.

5.2.4 Server spoofing attack

In this attack, the adversary may try to reply a legal mutual authentication message to cheat users. However, it is impossible for an attacker to launch server spoofing attack to cheat users in the proposed scheme, because he/she cannot get N_1 and ID_i from the login request $\{m, n\}$ of U_i to compute a valid response message $\{\alpha, \beta\}$ without knowing the master secret key s. Moreover, the attacker cannot calculate the session key $SK = H(N_1 \| N_2)$. Therefore, the proposed scheme can resist server spoofing attack.

5.2.5 DoS attack

CAPTCHA technique is used in our proposed scheme which makes the malicious attacker cannot use the early message to launch DoS attack. When users login in the remote server S, they must reply S an answer responding to the CAPTCHA puzzle. However, these puzzles are difficult for computers to solve, so the DoS attack which launched by computers is resisted effectively.

5.2.6 Replay attack

The replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. We assume an adversary re-submits the login request message $\{m, n\}$ to S, and he/she can get the reply message $\{\alpha, \beta\}$ from S. Since the adversary does not know N_1 and the fresh random value N_2, he/she cannot compute the valid responding message $\gamma = H(B_i \| N_1 \| N_2)$. Therefore, our scheme can withstand replay attack.

5.2.7 Man-in-the-middle attack

Man-in-the-middle attack means that an active attacker intercepts the exchanged messages to masquerade the server or the user to obtain sensitive information. Nevertheless, in the proposed scheme, the attacker is unable to generate the valid m, n which results in failure to achieve server authentication without knowledge of U_i's identity ID_i and password PW_i. Also, the attacker could not generate the correct α and β due to lack of the master secret key s.

Table 2: Comparisons of related works

	Wang et al. [21]	Chang et al. [3]	Ours
F1	Yes	No	Yes
F2	Yes	No	Yes
F3	No	No	Yes
F4	No	No	Yes
F5	No	No	Yes
F6	No	No	Yes
F7	No	No	Yes

Table 3: Comparisons of related works

	Wang et al. [21]	Chang et al. [3]	Ours
P1	$3T_H$	$5T_H$	$5T_H$+$3T_{mul}$
P2	$3T_H$	$5T_H$	$3T_H$+T_{sym}
C1	$6i$	$6i$	$5i$

P1: the computation cost of the smart card;
P2: the computation cost of the server;
C1: the communication cost between U_i and S.

5.2.8 Known key security

After the mutual authentication, the user and the server agree on a temporary session key SK. The known key security means that it should make no difference on other session keys even one session key is compromised. In the proposed scheme, with the compromised session key $SK = H(N_1||N_2)$, the adversary still cannot further compromise other unexposed session keys due to the randomness of N_1 and N_2.

6 Performance analysis

(1) We compare the performance of the proposed scheme with other schemes due to Wang et al.'s [21] and Chang et al.'s [3]. We summarize the comparisons of the related works in the Table II. We consider the following functional requirements of a robust password based authentication scheme: F1: The password can be chosen and changed freely by the clients; F2: The scheme can provide the mutual authentication with the session key agreement; F3: The scheme should achieve user anonymity; F4: The scheme does not have a serious time-synchronization problem; F5: The prevention of off-line password guessing attack; F6: The prevention of impersonation attack; F7: The prevention of server spoofing attack.

As is demonstrated in Table 2, Wang et al.'s scheme cannot satisfy the criteriion F3-F7 and Chang et al.'s scheme cannot satisfy any criteria list in Table 2. While our proposed scheme can achieve all of essential criterion F1-F7. Thus, our scheme provides the higher security strength and the more security functionalities than other related schemes.

(2)Typically, We define the notation T_H as the time complexity of the hash function computation; T_{sym} is defined as the time complexity of the symmetric encryption/decryption; T_{mul} indicates the time complexity of modular multiplications. Due to the exclusion-OR operation and string concatenation operation require very few computations, we usually neglect considering their computation cost. We also define i is the length of one parameter in the transmitted messages, such as the length of $\{m\}$ is i and the length of $\{m,n\}$ is $2i$. Under the above assumptions, we summarize the solution of comparisons of computation and communication cost in Table 3.

From the comparisons, we can find that the computation cost of our proposed scheme is slightly higher than the other two schemes. Nevertheless, these two schemes are insecure and our scheme can satisfy more admired criterion.

From Table 3, it can be seen that the communication cost of our proposed scheme between U_i and S is $5i$. While Wang et al.'s and Chang et al.'s schemes require $6i$. As a result, our scheme is more efficient than Wang et al.'s and Chang et al.'s schemes in the communication cost.

7 Conclusion

In this paper, we analyzed Chang et al.'s remote authentication scheme with smart card and showed that their scheme suffered from off-line password guessing attack, impersonation attack, server spoofing attack and failed to preserve user untraceability. In order to rectify the aforementioned security flaws, we then proposed a new scheme using CAPTCHA technique. The security and performance analysis demonstrated that our presented scheme satisfied more admired criterion and thus our scheme was more secure and suitable for practical application environment.

Acknowledgement

We thank the anonymous reviewers for their invaluable comments and suggestions. This work is supported by Natural Science Foundation of Shandong Province (NO.ZR2013FM009).

References

[1] A.K.Awasthi, Comment on a dynamic ID-based remote user authentication scheme. Transactions on Cryptology; 1(2):15-16(2004).

[2] M.Burrows, M.Abadi, R. Needham, A logic of authentication. ACM Transactions on Computer Systems; 8(1):18-36(1990).

[3] Y.F.Chang,W.L. Tai, H.C.Chang, Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update. International Journal of Communication Systems, 27(11):3430-3440(2014).

[4] C.C.Chang, T.C.Wu, Remote password authentication with smart cards. IEEE Proceedings-Computers and Digital Techniques; 138(3):165-168(1991).
[5] H.Y.Chien,J.K. Jan, Y.M.Tseng, An efficient and practical solution to remote authentication: smart card. Computers and Security; 21(4):372-375(2002).
[6] M.L.Das, A.Saxena,V.P. Gulati, A dynamic ID-based remote user authentication scheme. IEEE Trans on Consumer Electronics; 50(2):665-667(2004).
[7] A.K.Das,A. Goswami, A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. Journal of Medical Systemes; 37(3):9948
[8] A.K.Das, b. Bruhadeshwar, An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system. Journal of Medical Systemes; 37:9969
[9] D.Hankerson, A. Menezes, S.Vanstone, Guide to elliptic curve cryptography. Springer-Verlag, USA(2003).
[10] C.H.Huang, J.S.Chou, Y.Chen, et al., Improved multi-server authentication protocol. Security and Communication Networks; 5(3):331-341(2012).
[11] N.Koblitz, Elliptic curve cryptosystem. Mathematics of Computation; 48: 203-209(1987).
[12] P.Kocher, J.Jaffe, B.Jun, Differential power analysis: 19th Annual international cryptology conference; pp. 388-97(1999).
[13] W.C.Ku, S.T.Chang, Impersonation attacks on a dynamic ID-based remote user authentication scheme using smart cards. IEICS Transactions on Communication; E88-B(5):2165-2167(2005).
[14] Lamport,Password authentication with insecure communication. Commun ACM; 24(11):770-772(1981).
[15] T.S.Messerges, E.A.Dabbish, R.H.Sloan, Examining smart - card security under the threat of power analysis attacks. IEEE Trans Comput; 51(5):541-552(2002).
[16] V.S.Miller, Use of elliptic curves in cryptography, Advances in cryptology. in Proc. CRYPTO; pp.417-426(1986).
[17] J.Niu, X.Li, A novel user authentication scheme with anonymity for wireless communications. Security and Communication Networks; 7(10):1467-1476(2014)
[18] H.S.Rhee, J.O.Kwon, D.H.Lee, A remote user authentication scheme without using smart cards. Computer Standards & Interfaces; 31(1):6-13(2009).
[19] L.von Ahn, M.Blum, N.Hopper, J.Langford, CAPTCHAUsing Hard AI Problems for Security. Advances in Cryptology, Eurocrypt; pp. 294-311(2003).
[20] S.J.Wang, Yet another log-in authentication using N-dimensional constrction based on circle property. IEEE Transactions on Consumer Electronics; 49(2):337-341(2003).
[21] 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; 32(4):583-585(2009).
[22] F.T.Wen, X.L.Li, An improved dynamic ID-based remote user authentication with key agreement scheme. Computers and Electrical Engineering; 38(2):381-387(2012).
[23] F.T.Wen, W.Susilo,G.M. Yang, A robust smart card?based anonymous user authentication protocol for wireless communications. Security and Communication Networks; 7:987-993, 2014 .
[24] H. J. Kim, E. J. Yoon, Cryptanalysis of Modified Dynamic ID-based User Authentication Scheme Resisting Smart-Card-Theft Attack, International Journal of Mathematical Analysis, 8:, 2413-2419, (2014).
[25] J.Bonneau, The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In proc. IEEE Security & Privacy 2012. pp.538-552(2012).
[26] M.Dell'Amico, P. Michiardi , Y.Roudier, Password strenth: an empirical analysis. In: Proc. INFOCOM 2010. pp. 1-9(2010).

Dianli Guo is Master student of school of mathematical sciences, university of jinan. He received the Bachelor degree in applied mathematics at Heze college.Now,he is a PhD candidate of Beijing university of posts and Telecommunications. His main research interests is cryptography.

Fengtong Wen is a professor of school of mathematical sciences, university of jinan, China. He received the PhD degree in Cryptography at Beijing university of posts and Telecommunications. His main research interests are in the areas of applied mathematics, information security, and cryptography. He has published more than 30 research articles in reputed international journals of mathematical and computer sciences.

Chengbo Xu received the PhD degree in computer science from Beijing University of Posts and Telecommunications, Beijing, China. He is a faculty member with the School of Mathematical Sciences at University of Jinan. His current research interests are authentication schemes in wireless sensor networks,vehicular networks and RFID systems.