An Enhanced Anonymous Password-based Authenticated Key Agreement Scheme with Formal Proof

Min Wu, Jianhua Chen, and Ruibing Wang

(Corresponding author: Min Wu)

School of Mathematic and Statistics, Wuhan University

Wuchang, Wuhan, Hubei 430072, China

(Email: wumin9246@163.com)

(Received May 23, 2016; revised and accepted Aug. 13 & Sept. 3, 2016)

Abstract

With the development of technology, the security of password-based authentication is becoming more and more significant. Recently, Lee et al. proposed an anonymous password-based authenticated key agreement scheme with non-temper resistant smart card to reduce the computation cost of Wang et al.'s scheme. However, based on analysis, it shows that the scheme can't withstand smart card stolen or lost attack, user impersonation attack and server impersonation attack. Therefore, an enhanced scheme which can resist the attacks mentioned above is presented. By comparing the performance and security with other related schemes, our proposed scheme is more suitable for practical applications.

Keywords: Authentication Scheme; BNA Logic; Key Agreement; Network Security; Smart Card

1 Introduction

As the internet technology's development, password-based authentication with smart card is significant and widely used for remote system to access to computer network [1, 15]. To enhance the system security and management, research have been focused considerable attention on smart card based password authentication. Since Change and Wu [4] firstly proposed remote user authentication scheme using smart cards in 1993, many other password schemes were present [7, 12, 16, 18]. Traditionally, the smart card is assumed to be tamper-resistant. Namely, an adversary can't obtain the secret information about legal user stored in the smart card. However, recent research has been proved that the secret data stored in the smart card could be extracted by some means, such as monitoring the power consumption [2, 9, 14] or analyzing the leaked information [6, 13]. So such schemes based on the tamper resistance assumption of the smart card are susceptible to various attacks like impersonation attacks, off-line password guessing attacks, etc.

In 2009, Kim and Chung [8] proposed a remote user authentication scheme which claimed that their scheme is secure. However in 2011, Li et al. [11] pointed out that Kim and Chung's scheme couldn't resist various attacks and further advanced a new remote authentication based on hash function. In their scheme, they suggested that their scheme not only remedy the flaws of Kim and Chung's scheme, but also secure. But in 2012, Wang et al. [17] demonstrated that Li et al.'s scheme is insecure against denial of service attack and off-line password guessing attack under the non-tamper resistance assumption of the smart card. Moreover, their scheme failed to provide user anonymity and forward secrecy. In order to solve the problems mentioned above, Wang et al. presented a robust authentication scheme based on the secure one-way hash function and the well-known discrete logarithm problem. Later, Lee et al. [10] putted forward that Wang et al.'s scheme had high computational overhead. In order to reduce the overhead, they proposed an anonymous authentication scheme with non-tamper resistant smart cards based on password, and proved that their scheme meets all the criteria required for the authenticated key agreement scheme and eliminates security threats. Nevertheless, it indicated that their scheme is prone to smart card stolen or lost attack, user impersonation attack and server impersonation attack base on our analysis. In additional, their scheme can't provide mutual authentication. Then, an enhanced key agreement scheme with non-tamper resistant smart cards is presented. The remainder of the article is sketched as follows. In Section 2, we briefly review Lee et al.'s scheme. Section 3 presents the security analysis of Lee et al.'s scheme. In Section 4, we present an enhanced scheme. The security analysis of the proposed scheme is given in Section 5, and efficiency comparison between our scheme and other related ones is showed in Section 6. Ultimately, in Section 7, we reach the conclusion.

2 Review of Lee et al.'s Scheme

In this section, we will briefly review of Lee et al.'s scheme, which comprises four phases: registration phase, login phase, authentication phase and password change phase. The notations used in this article are described in Table 1.

Table 1: Notation

Notation	Description
U_i/U_k	user i/k
S_i	server i
E	attacker
PW_i	$U_i's$ password
ID_i	$U_i's$ identity
x	secret key generated by S_i
y	public key generated by S_i
b	a random number generated by U_i
v	a random number generated by U_i
w	a random number generated by S_i
$h(\cdot)$	a one-way hash function
$\|$	concatenation
$\oplus$	bitwise exclusive-or operation

2.1 Registration Phase

S_i generates x as the server's private key which is only kept secret by himself/herself, and computes $y = g^x \mod n$ as its corresponding public key which is stored inside each user's smart card. If a user U_i wishes to be a legal user of the system so that he/she can utilize resources provided by the server, U_i should execute the following steps.

- U_i first selects his/her identity ID_i and password PW_i. Then, U_i generates a random number b, computes $h(b\|PW_i)$ and sends $\{ID_i, h(b\|PW_i)\}$ to S_i.

- S_i checks the validity of ID_i. If it is validity, S_i calculates

$$\begin{aligned} C_1 &= h(h(ID_i) \oplus x), \\ C_2 &= C_1 \oplus h(b\|PW_i) \oplus h(ID_i), \\ C_3 &= h(C_1), \\ C_4 &= h(b\|PW_i) \oplus h(x\|y). \end{aligned}$$

  Then S_i issues a smart card including $\{C_2$, C_3, C_4, $h(\cdot)$, n, g, $y\}$ to U_i via a secure channel.

- U_i computes $B = b \oplus ID_i \oplus PW_i$, and stores B in the smart card.

2.2 Login Phase

When U_i logins the system, he/she can perform the next steps.

- U_i inserts his/her smart card into a card reader and enters the identity ID_i, password PW_i. The smart card SC computes $b' = B \oplus ID_i \oplus PW_i$, $C_1' = C_2 \oplus h(b'\|PW_i) \oplus h(ID_i)$, $C_3' = h(C_1')$, and compares C_3' with C_3 stored in the smart card. Only if the equation holds, SC performs the following steps.

- SC generates a random number v and computes $V = g^v \mod n$, $h(x\|y) = c_4 \oplus h(b\|PW_i)$, $CID_i = h(ID_i) \oplus h(V\|h(x\|y))$, $M_1 = h(CID_i\|V\|C_1)$. Then, U_i sends login request message $\{CID_i, V, M_1\}$ to S_i.

2.3 Authentication Phase

U_i and S_i achieve mutual authentication as follows.

- Upon receiving the login message $\{CID_i, V, M_1\}$, S_i computes $h(x\|y)$, $h(ID_i) = CID_i \oplus h(V\|h(x\|y))$, $C_1' = h(h(ID_i) \oplus x)$, $M_1' = h(CID_i\|V\|C_1')$, and checks whether M_1' equals to the received M_1. If they are not equal, the session is terminated. Otherwise, S_i selects a random number w and computes $W = g^w \mod n$, $SK = V^w \mod n$, $M_2 = h(SK\|W\|C_1')$. Then, S_i sends $\{M_2, W\}$ to U_i.

- SC receives the message and computes the session key $SK' = W^v \mod n$. And, SC verifies M_2 with the computed value of $h(SK'\|W\|C_1)$. If the verification holds, SC computes $M_3 = h(M_2\|C_1\|SK')$ and send $\{M_3\}$ to S_i.

- Upon receiving $\{M_3\}$, S_i computes $M_3' = h(M_2\|C_1\|SK')$ and checks whether the equation $M_3' = M_3$ holds. If it holds, S_i and U_i finish mutual authentication, and share a common session key $SK = g^{vw} \mod n$. Otherwise, the session is terminated.

2.4 Password Change Phase

Assume that SC has the ability to detect the login failure trials. If the failure times exceed a given number, SC will be soon locked to prevent from guessing password attack.

- U_i inserts the smart card into a card reader and inputs identity ID_i, password PW_i and a new password PW_i^{new}.

- SC calculates $b' = B \oplus ID_i \oplus PW_i$, $C_1' = C_2 \oplus h(b'\|PW_i \oplus h(ID_i))$, $C_3' = h(C_1')$ and verifies whether $C_3' = C_3$. If they are the same, SC accepts the change request. Otherwise, the session is terminated.

- SC computes $B^{new} = b \oplus ID_i \oplus PW_i^{new}$, $C_2^{new} = C_1' \oplus h(b'\|h(b'\|PW_i^{new})) \oplus h(ID_i)$, $C_4^{new} = C_4 \oplus h(b'\|PW_i) \oplus h(b'\|PW_i^{new})$. Finally, SC replace C_2, C_4, B with $C_2^{new}, C_4^{new}, B^{new}$ in the smart card.

3 Security Analysis of Lee et al.'s Scheme

In Lee et al.'s scheme, they claim that their scheme can resist some attacks, containing off-line password guessing attack, user impersonation attack, server masquerading attack, and so on. By analysis and study, we find that the scheme fails to resist the attacks mentioned above. The details are as follows.

3.1 Smart Card Stolen or Loss Attack

Assume that $U_i's$ smart card was stolen by a legal but malicious user U_k, and U_k had monitored the login request message $\{CID_i, V, M_1\}$ which was sent to S by U_i.

A legal but malicious user U_k acquires $\{C_2^*, C_3^*, C_4^*, h(\cdot), n, g, B^*\}$ from his/her own smart card and computes $b^* = B^* \oplus ID_k \oplus PW_k$, $h(x\|y) = C_4^* \oplus h(b^*\|PW_k)$. And the value of $h(x\|y)$ is not changed for every user. Then U_k can obtain $h(ID_i)$ and C_1 by computing $h(ID_i) = CID_i \oplus h(V\|h(x\|y))$, $C_1 = C_2 \oplus h(b\|PW_i) \oplus h(ID_i) = C_2 \oplus C_4 \oplus h(x\|y) \oplus h(ID_i)$ where C_2, C_4 is extracted from U_i's smart card. Then, U_k can continue guesses the identity as follows.

1) Guess an identity $ID_i^{'}$.

2) compute $h(ID_i^{'})$ and compare it with the values of $CID_i \oplus h(V\|h(x\|y))$. If they are not equal, go back to 1). Otherwise, $U_k^{'}$ finds the user U_i's identity ID_i.

After acquiring the user U_i's identity ID_i, U_k can go on continuing guess user's password.

1) Guess a password $PW_i^{'}$.

2) Compute $b^{'} = B \oplus ID_i \oplus PW_i^{'}$, $C_4^{'} = h(b^{'}\|PW_i^{'}) \oplus h(x\|y)$, where B is extracted from $U_i's$ smart card and $h(x\|y)$ can be obtained by Step 1. Then U_k verifies $C_4^{'} \stackrel{?}{=} C_4$. If it holds, U_k finds the correct password PW_i.

3.2 User Impersonation Attack

From Section 3.1, we know that a legal but malicious user U_k can obtain $h(x\|y)$, $h(ID_i)$, C_1. Then he/she can forge the login request message $\{CID_i, V, M_1\}$ to disguise the user U_i.

1) U_k generates a random number v^* and computes $V^* = g^{v^*} \bmod n$, $CID_i^* = h(ID_i) \oplus h(V^*\|h(x\|y))$, $M_1^* = h(CID_i^* \| V^* \| C_1)$. Then, U_k sends $\{CID_i^*, V^*, M_1^*\}$ to S_i.

2) S_i computes $h(x\|y)$, $h(ID_i) = CID_i^* \oplus h(V^*\|h(x\|y))$, $C_1^{'} = h(h(ID_i) \oplus x)$, $M_1^{'} = h(CID_i^*\|V^*\|C_1^{'})$, and checks whether $M_1^{'}$ equals to the received M_1^*. If they are equal, then S_i selects a random number w^* and computes $W^* = g^{w^*} \bmod n$, $SK^* = (V^*)^{w^*} \bmod n$, $M_2^* = h(SK^*\|W^*\|C_1^{'})$. Then, S_i sends $\{M_2^*, W^*\}$ to U_i.

3) U_k computes the session key $SK^{'} = (W^*)^{v^*} \bmod n$, $M_3^* = h(M_2^*\|C_1\|SK^*)$ and send $\{M_3^*\}$ to S_i.

4) S_i computes $M_3^{'} = h(M_2^*\|C_1^{'}\|SK^*)$ and checks whether the equation $M_3^{'} = M_3^*$ holds. As $SK^* = (V^*)^{w^*} \bmod n = (g^{v^*})^{w^*} \bmod n = (g^{w^*})^{v^*} \bmod n = (W^*)^{v^*} \bmod n = SK$, $M_3^{'} = h(M_2^*\|C_1^{'}\|SK^*) = h(M_2^*\|C_1\|SK^{'}) = M_3^*$. S_i authenticates U_k as U_i.

3.3 Server Impersonation Attack

A legal but malicious user U_k acquires $h(x\|y)$,$h(ID_i)$, C_1 by the method mentioned in Section 3.1, then U_k can impersonate server S_i to communicate with U_i.

1) When U_i sends the login request message $\{CID_i, V, M_1\}$ to S_i, U_k eavesdrops the message, selects a random number w^* and computes $W^* = g^{w^*} \bmod n$, $SK^* = V^{w^*} \bmod n$, $M_2^* = h(SK^*\|W^*\|C_1)$. Then,$S_i$ sends $\{M_2^*, W^*\}$ to U_i.

2) When U_i receives the message, the smart card computes the session key $SK^{'} = (W^*)^v \bmod n$. $SK^{'} = (W^*)^v \bmod n = (g^{w^*})^v \bmod n = (g^v)^{w^*} \bmod n = (V)^{w^*} \bmod n = SK^*$, so $M_2^* = h(SK^{'}\|W^*\|C_1)$. Then, SC computes $M_3 = h(M_2\|C_1\|SK^{'})$ and send $\{M_3\}$ to S_i.

Thus, U_k is authenticated as the legitimate server by the user U_i.

4 Our Proposed Scheme

In this section, we propose a new scheme based on Lee et al.'s scheme, which can resist the attacks mentioned in Section 3. It composes four phase: registration phase, login phase, authentication phase and password change phase. The detail description of each phase are shown below.

4.1 Registration Phase

S_i generates x as the server's private key which is only kept secret by himself/herself, and computes $y = g^x \bmod n$ as its corresponding public key which is stored inside each user's smart card. A user U_i must register to be a legal user of the system, before utilizing resources provided by the server.

- U_i first selects his/her identity ID_i and password PW_i. Then, U_i generates a random number b, computes $RPW_i = h(b\|PW_i)$ and sends $\{ID_i, RPW_i\}$ to S_i.

Table 2: The proposed scheme of registration phase

U_i		S_i
$RPW_i = h(b \Vert PW_i)$	$\xrightarrow{ID_i, RPW_i}$	
		Server's public key $y = g^x mondn$.
		checks the validity of ID_i
		generates a random number d
		$C_1 = h(ID_i \Vert x)$,$C_2 = C_1 \oplus RPW_i$
		$C_3 = h(C_1 \Vert d)$,$C_4 = h(C_1 \Vert RPW_i) \oplus d$,
$B = b \oplus ID_i \oplus PW_i$	$\xleftarrow{smart\ card}$	$D = g^d \mod n$,$C_5 = h(C_1 \oplus ID_i) \oplus h(x \Vert y \Vert D)$.
stores B in the smart card		

- S_i checks the validity of ID_i. If it is validity, S_i generates a random number d for user U_i. Then S_i performs the following computations. $C_1 = h(ID_i \Vert x)$, $C_2 = C_1 \oplus RPW_i$, $C_3 = h(C_1 \Vert d)$, $C_4 = h(C_1 \Vert RPW_i) \oplus d$, $D = g^d \mod n$, $C_5 = h(C_1 \oplus ID_i) \oplus h(x \Vert y \Vert D)$. Then S_i sends a smart card including $\{C_2, C_3, C_4, C_5, h(\cdot), n, g, y\}$ to U_i via a secure channel.

- U_i computes $B = b \oplus ID_i \oplus PW_i$, and stores B in the smart card.

4.2 Login Phase

When U_i logins the system, he/she can perform the next steps.

- U_i inserts his/her smart card into a card reader and enters the identity ID_i, password PW_i. The smart card SC computes $b = B \oplus ID_i \oplus PW_i$, $RPW_i = h(b \Vert PW_i)$, $C_1 = C_2 \oplus RPW_i$, $d = C_4 \oplus h(C_1 \Vert RPW_i)$, $C_3^{'} = h(C_1 \Vert d)$, and compares $C_3^{'}$ with C_3 stored in the smart card. Only if the equation holds, SC performs the following steps.

- SC generates a random number v and computes $V = g^v \mod n$, $D = g^d \mod n$, $h(x \Vert y \Vert D) = C_5 \oplus h(C_1 \Vert ID_i)$, $CID_i = ID_i \oplus h(V \Vert h(x \Vert y \Vert D))$, $F_1 = RPW_i \oplus h(C_1 \Vert ID_i)$, $F_2 = C_4 \oplus h(V \Vert C_1) \oplus h(x \Vert y \Vert D)$, $M_1 = h(ID_i \Vert RPW_i \Vert V \Vert C_1 \Vert d)$. Then, U_i sends login request message $\{CID_i, V, D, F_1, F_2, M_1\}$ to S_i.

4.3 Authentication Phase

U_i and S_i achieve mutual authentication as follows.

- Upon receiving the login message $\{CID_i$, V, D, F_1, F_2, $M_1\}$, S_i computes $h(x \Vert y \Vert D), ID_i = CID_i \oplus h(V \Vert h(x \Vert y \Vert D))$, $C_1 = h(ID_i \Vert x)$, $RPW_i = F_1 \oplus h(C_1 \Vert ID_i)$, $C_4 = F_2 \oplus h(V \Vert C_1) \oplus h(x \Vert y \Vert D)$, $d = C_4 \oplus h(C_1 \oplus RPW_i)$, $M_1^* = h(ID_i \Vert RPW_i \Vert V \Vert C_1 \Vert d)$, and checks whether M_1^* equals to the received M_1. If they are not equal, the session is terminated. Otherwise, S_i selects a random number w and computes $W = g^w \mod n$, $SK = V^w \mod n$, $M_2 = h(SK \Vert W \Vert C_1 \Vert RPW_i \Vert d)$. Then, S_i sends $\{M_2, W\}$ to U_i.

- SC receives the message and computes the session key $SK^{'} = W^v \mod n$. And, SC verifies M_2 with the computed value of $h(SK^{'} \Vert W \Vert C_1 \Vert RPW_i \Vert d)$. If the verification holds, SC computes $M_3 = h(M_2 \Vert C_1 \Vert SK^{'} \Vert d)$ and send $\{M_3\}$ to S_i.

- Upon receiving $\{M_3\}$, S_i computes $M_3^* = h(M_2 \Vert C_1 \Vert SK \Vert d)$ and checks whether the equation $M_3^* = M_3$ holds. If it holds, S_i and U_i finish mutual authentication, and share a common session key $SK = g^{vw} \mod n$. Otherwise, the session is terminated.

4.4 Password Change Phase

Assume that SC has the ability to detect the login failure trials. If the failure times exceed a given number, SC will be soon locked to prevent from guessing password attack.

- U_i inserts the smart card into a card reader and inputs identity ID_i, password PW_i and a new password PW_i^{new}.

- SC calculates $b = B \oplus ID_i \oplus PW_i$, $RPW_i = h(b \Vert PW_i)$, $C_1 = C_2 \oplus RPW_i$, $d = C_4 \oplus h(C_1 \Vert RPW_i)$, $C_3^{'} = h(C_1 \Vert d)$ and verifies whether $C_3^{'} = C_3$. If they are the same, SC accepts the request. Otherwise, the session is terminated.

- SC computes $B^{new} = b \oplus ID_i \oplus PW_i^{new}$, $RPW_i^{new} = h(b \Vert PW_i^{new})$, $C_2^{new} = C_1 \oplus RPW_i^{new}$, $C_4^{new} = d \oplus h(C_1 \Vert RPW_i^{new})$. Finally,$SC$ replace C_2, C_4, B with $C_2^{new}, C_4^{new}, B_{new}$ in the smart card.

5 Security Analysis

The proposed scheme advanced Lee et al.s scheme and can resist the attacks analyzed above. The details are described in the following content.

Table 3: The proposed scheme of the login and authentication phase

U_i		S_i
inputs ID_i, PW_i computes $b = B \oplus ID_i \oplus PW_i$, $RPW_i = h(b\|PW_i)$,$C_1 = C_2 \oplus RPW_i$, $d = C_4 \oplus h(C_1\|RPW_i)$, $C_3^{'} = h(C_1\|d)$,verifies $C_3^{'} \stackrel{?}{=} C_3$. selects a random number v, computes $V = g^v mondn$, $D = g^d mondn$, $h(x\|y\|D) = C_5 \oplus h(C_1 \oplus ID_i)$, $CID_i = ID_i \oplus h(V\|h(x\|y\|D))$, $F_1 = RPW_i \oplus h(C_1\|ID_i)$, $F_2 = C_4 \oplus h(V\|C_1) \oplus h(x\|y\|D)$ $M_1 = h(ID_i\|RPW_i\|V\|C_1\|d)$	$\xrightarrow{CID_i, V, D, F_1, F_2, M_1}$	computes $h(x\|y\|D)$, $ID_i = CID_i \oplus h(V\|h(x\|y\|D))$, $C_1 = h(ID_i\|x)$, $RPW_i = F_1 \oplus h(C_1\|ID_i)$, $C_4 = F_2 \oplus h(V\|C_1) \oplus h(x\|y\|D)$, $d = C_4 \oplus h(C_1 \oplus RPW_i)$, $M_1^* = h(ID_i\|RPW_i\|V\|C_1\|d)$, checks $M_1^* \stackrel{?}{=} M_1$. selects a random number w, computes $W = g^w \mod n$,
$SK^{'} = W^v \mod n$, verifies $M_2 \stackrel{?}{=} h(SK^{'}\|W\|C_1\|RPW_i\|d)$, computes $M_3 = h(M_2\|C_1\|SK^{'}\|d)$.	$\xleftarrow{M_2, W}$	$SK = V^w \mod n$, $M_2 = h(SK\|W\|C_1\|RPW_i\|d)$.
	$\xrightarrow{M_3}$	computes $M_3^* = h(M_2\|C_1\|SK\|d)$ checks $M_3^* \stackrel{?}{=} M_3$

5.1 Analysis the Proposed Scheme with BNA Logic

We analyzes out proposed scheme with BNA logic [3] in this section. The main notations of the BNA logic are shown in Table 4. Note that symbols P and Q stands for principals, X and Y range over statement, and K represent encryption keys.

Table 4: Notations of BNA logic

Notation	Meaning
$P \mid\equiv X$	P believes that X is true.
$P \lhd X$	P once received a message including X.
$P \mid\sim X$	P once said X.
$P \Rightarrow X$	P has jurisdiction over X.
$\#(X)$	X is fresh.
$(X, Y)_K$	X and Y are hashed with the key K.
$\{X, Y\}_K$	X and Y are encrypted with the key K.
$P \xleftrightarrow{K} Q$	P communicates with Q by a shared key K.

1) Idealization forms

U_i: $(ID_i, V)_{U_i \xleftrightarrow{x\|y\|D} S_i}$, V, $U_i \xleftrightarrow{d} S_i$, $(RPW_i, ID_i)_{U_i \xleftrightarrow{h(ID_i\|x)} S_i}$, $(C_4, V, U_i \xleftrightarrow{h(x\|y\|D)} S_i)_{U_i \xleftrightarrow{h(ID_i\|x)} S_i}$, $(ID_i, RPW_i, V, U_i \xleftrightarrow{d} S_i)_{U_i \xleftrightarrow{h(ID_i\|x)} S_i}$, $((U_i \xleftrightarrow{SK} S_i, W, RPW_i, U_i \xleftrightarrow{d} S_i)_{U_i \xleftrightarrow{h(ID_i\|x)} S_i}$, $U_i \xleftrightarrow{SK} S_i$, $U_i \xleftrightarrow{d} S_i)_{U_i \xleftrightarrow{h(ID_i\|x)} S_i}$

S_i: $(U_i \xleftrightarrow{SK} S_i$, W, RPW_i, $U_i \xleftrightarrow{d} S_i)_{U_i \xleftrightarrow{h(ID_i\|x)} S_i}$, W

2) Security goals

G1 $S_i \mid\equiv U_i \mid\equiv U_i \xleftrightarrow{SK} S_i$

G2 $S_i \mid\equiv U_i \xleftrightarrow{SK} S_i$

G3 $U_i \mid\equiv S_i \mid\equiv U_i \xleftrightarrow{SK} S_i$

G4 $U_i \mid\equiv U_i \xleftrightarrow{SK} S_i$

3) Initiative assumption

A1 $U_i \mid\equiv U_i \xleftrightarrow{h(ID_i\|x)} S_i$

A2 $S_i \mid\equiv U_i \xleftrightarrow{h(ID_i\|x)} S_i$

A3 $U_i \mid\equiv U_i \xleftrightarrow{d} S_i$

A4 $S_i \mid\equiv U_i \xleftrightarrow{d} S_i$

A5 $U_i \mid\equiv U_i \xleftrightarrow{h(x\|y\|D)} S_i$

A6 $S_i \mid\equiv U_i \xleftrightarrow{h(x\|y\|D)} S_i$

A7 $S_i \mid\equiv U_i \Rightarrow U_i \xleftrightarrow{SK} S_i$

A8 $U_i \mid\equiv S_i \Rightarrow U_i \xleftrightarrow{SK} S_i$

Table 5: BNA logical postulates

Rule	Formula	Meaning
Message-meaning rule	$\frac{P\mid\equiv P\overset{K}{\longleftrightarrow}Q,P\lhd\{X\}_K}{P\mid\equiv Q\mid\sim X}$	If P believes that K is the secret key shared by P with Q, and P sees X encrypted with K, then P believes that Q once said X.
Nonce-verification rule	$\frac{P\mid\equiv\#(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$	If P believes that X is fresh and Q once said X, then P believes that Q believes X.
Freshness-conjunction rule	$\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$	If P believes that X is fresh, then P believes that (X,Y) is fresh.
Jurisdiction rule	$\frac{P\mid\equiv Q\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$	If P believes that Q controls X and P believes Q believes X, then P believes X.

4) Scheme analysis
The main analysis of our proposed scheme is described as follows: Since $S_i \lhd ((U_i \overset{SK}{\longleftrightarrow} S_i, W, RPW_i, U_i \overset{d}{\leftrightarrow} S_i)_{U_i \overset{h(ID_i\|x)}{\longleftrightarrow} S_i}, U_i \overset{SK}{\longleftrightarrow} S_i, U_i \overset{d}{\leftrightarrow} S_i)_{U_i \overset{h(ID_i\|x)}{\longleftrightarrow} S_i}$ and $S_i \mid\equiv U_i \overset{h(ID_i\|x)}{\longleftrightarrow} S_i$, we can know

$$S_i \mid\equiv U_i \mid\sim ((U_i \overset{SK}{\longleftrightarrow} S_i, W, RPW_i, U_i \overset{d}{\leftrightarrow} S_i)_{U_i \overset{h(ID_i\|x)}{\longleftrightarrow} S_i}, U_i \overset{SK}{\longleftrightarrow} S_i, U_i \overset{d}{\leftrightarrow} S_i) \quad (1)$$

based on message-meaning rule.

According to freshness-conjunction rule and $S_i \mid\equiv \#(W)$, we can derive

$$S_i \mid\equiv \#((U_i \overset{SK}{\longleftrightarrow} S_i), W, RPW_i, U_i \overset{d}{\leftrightarrow} S_i)_{U_i \overset{h(ID_i\|x)}{\longleftrightarrow} S_i}, U_i \overset{SK}{\longleftrightarrow} S_i, U_i \overset{d}{\leftrightarrow} S_i). \quad (2)$$

On the basis of Equations (1), (2) and nonce-verification rule, the following can be derived

$$S_i \mid\equiv U_i \mid\equiv ((U_i \overset{SK}{\longleftrightarrow} S_i, W, RPW_i, U_i \overset{d}{\leftrightarrow} S_i)_{U_i \overset{h(ID_i\|x)}{\longleftrightarrow} S_i}, U_i \overset{SK}{\longleftrightarrow} S_i, U_i \overset{d}{\leftrightarrow} S_i). \quad (3)$$

The G1 $S_i \mid\equiv U_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} S_i$ will be deduced from Equation (3).

Based on A7, G1 and jurisdiction rule, we can derive G2 $S_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} S_i$.

Since $U_i \lhd (U_i \overset{SK}{\longleftrightarrow} S_i, W, RPW_i, U_i \overset{d}{\leftrightarrow} S_i)_{U_i \overset{h(ID_i\|x)}{\longleftrightarrow} S_i}$ and $U_i \mid\equiv U_i \overset{h(ID_i\|x)}{\longleftrightarrow} S_i$, we can know

$$U_i \mid\equiv S_i \mid\sim (U_i \overset{SK}{\longleftrightarrow} S_i, W, RPW_i, U_i \overset{d}{\leftrightarrow} S_i) \quad (4)$$

based on message-meaning rule.

If $M_3 = h(M_2\|C_1\|SK^{'}\|d), U_i \mid\equiv \#(W)$. According to freshness-conjunction rule, we can derive

$$U_i \mid\equiv \#(U_i \overset{SK}{\longleftrightarrow} S_i, W, RPW_i, U_i \overset{d}{\leftrightarrow} S_i). \quad (5)$$

On the basis of Equations (4), (5) and nonce-verification rule, the following can be derived

$$U_i \mid\equiv S_i \mid\equiv (U_i \overset{SK}{\longleftrightarrow} S_i, W, RPW_i, U_i \overset{d}{\leftrightarrow} S_i). \quad (6)$$

The G3 $U_i \mid\equiv S_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} S_i$ will be deduced from Equation (6).

Based on A8, G3 and jurisdiction rule, we can derive G4 $U_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} S_i$.

5.2 Informal Security Analysis

5.2.1 User Anonymity

1) A legal but malicious user U_k acquires $\{C_2^*, C_3^*, C_4^*, C_5^*, h(\cdot), n, g, y, B^*\}$ from his/her own smart card and computes $b^* = B^* \oplus ID_k \oplus PW_k$, $RPW_k = h(b^*\|PW_k)$, $C_1^* = C_2^* \oplus RPW_k$, $d^* = C_4^* \oplus h(C_1^*\|RPW_k)$, $D^* = g^{d^*} \bmod n$, $h(x\|y\|D^*) = C_5^* \oplus h(C_1 \oplus ID_k)$. U_k can't obtain any common values for every legal user.

2) Even If U_k obtain $\{C_2, C_3, C_4, C_5, h(\cdot), n, g, Y, B\}$ from U_i's smart card, he/she impossible to get d without knowing C_1, RPW_i, or $h(x\|y\|D)$ without the values of C_1, ID_i.

3) In unsecure channels, U_k intercepts the message $\{CID_i, V, D, F_1, F_2, M_1\}$, and tries to trace the user U_i. But the user U_i communicates with S_i by CID_i instead of his/ her own identity ID_i. It is infeasible to derive ID_i without knowing $h(x\|y\|D)$. On the other hand, it is hard to get the random number d from $D = g^d \mod n$ due to discrete logarithm problem.

Consequently, any legal but malicious user cannot obtain some useful values concerning with user U_i.

5.2.2 Offline Password Guessing Attack

1) Form the analysis of Section 5.2.1, we know that any legal but malicious user U_k cannot the common value $h(x\|y)$ for all legal users.

2) If U_k acquires $\{C_2, C_3, C_4, C_5, h(\cdot), n, g, y, B\}$ from $U_i's$ smart card, he/she has to guess the user $U_i's$ identity ID_i and password PW_i correctly at the same time to compute $b = B \oplus ID_k \oplus PW_k$. As we all known, it is difficult to guess the two parameters chosen freely by the user at the same time in polynomial time. And the proposed scheme can provide user anonymity by the above analysis.Furthermore, the adversary needs to know the server's private key x to compute $C_1 = h(ID_i\|x)$, $RPW_i = h(b\|PW_i)$. Then, he/she could get right password by comparing $C_1 \oplus RPW_i$ with C_2.

3) Assume U_k intercepts the message $\{CID_i, V, D, F_1, F_2, M_1\}$ which U_i once sent to S_i. However U_k does not have the knowledge of b, C_1 and ID_i, the verification of the computed $F_1 = RPW_i \oplus h(C_1\|ID_i)$ will fail.

5.2.3 Stolen Verifier Attack

The server S_i does not store any sensitive verification information corresponding to users in its database in our proposed scheme. Therefore even if any adversary accesses the server's database, he/she is impossible to gain any verification information related to registered users. So, the proposed scheme can withstand stolen verifier attack.

5.2.4 Insider Attack

Assume that the privileged user gets ID_i, RPW_i when a legal user U_i registers to the system S_i. However, the privileged couldn't extract PW_i from RPW_i due to one-way property of hash function. At the same time, PW_i is protected by random number b, and the privileged user is not able to guess the right password. Thus, the proposed scheme can resist insider attack.

5.2.5 Replay Attack

Suppose that an adversary E eavesdrops the login request message and tries to perform replay attack in future. Upon receiving $\{CID_i, V, D, F_1, F_2, M_1\}$ from E, the server S_i verifies $M_1^* \stackrel{?}{=} h(ID_I\|RPW_i\|V\|C_1\|d)$. The message has not been changed by E, so S_i selects a random number w^* and computes $W^* = g^{w^*} \mod n$, $SK^* = V^{w^*} \mod n$, $M_2^* = h(SK^*\|W^*\|C_1\|RPW_i\|d)$. Then, S_i sends $\{M_2^*, W^*\}$ to the adversary E. It is indispensable for the adversary E to reply $\{M_3\}$ to S_i, where $M_3 = h(M_2\|C_1\|SK\|d)$. Because E not only couldn't compute SK without random number v, but also couldn't get C_1 and d. Thus, the server cannot authenticate E. Namely, the scheme is secure against replay attack.

5.2.6 User Impersonation Attack

If an adversary E wants to pretend U_i to communicate with S_i, he/she must forge the login request message $\{CID_i, V, D, F_1, F_2, M_1\}$. Then, he/she selects a random number v^* and computes $V^* = g^{v^*} \mod n$, $U^* = Y^{v^*}$. Unfortunately, E couldn't compute CID_i^* without the user $U_i's$ identity ID_i, server's private key x. Meanwhile, U_k requires to compute $F_1^* = RPW_i \oplus h(C_1\|ID_i)$, $F_2^* = C_4 \oplus h(V^*\|C_1) \oplus h(x\|y\|D)$, which is not possible, since E does not know ID_i, RPW_i, x. That is, the proposed scheme is able to against the user spoofing attack.

5.2.7 Server Impersonation Attack

If an adversary E eavesdrops the login request message $\{CID_i, V, F_3, F_4, M_1\}$ from user U_i, he/she performs the following steps to act as the legal server S_i. E must compute $M_2 = h(SK\|W\|C_1\|RPW_i\|d)$ to respond the login request message. Even If U_k selects a random number w^* and computes $W^* = g^{w^*}$, $SK^* = V^{w^*} \mod n$, he/she cannot forge M_2 without RPW_i, C_1, d. From the above analysis, our proposed scheme could resist server impersonation attack.

5.2.8 Mutual Authentication

1) In the proposed scheme, S_i authenticates U_i by checking the validity of equation $M_3 \stackrel{?}{=} h(M_2\|C_1\|SK\|d)$. We have demonstrated that the proposed scheme can provide user anonymity and off-line password guessing attack. If an adversary replays the former login request message $\{CID_i, V, D, F_1, F_2, M_1\}$ sent to S_i by U_i, he/she would fail according to the analysis of section 5.2.5. On the other hand, suppose the adversary forge the login request message to cheat the server, we will find that it is impossible by the analysis of Section 5.2.6.

2) On the contrary, the legal user U_i authenticates S_i by comparing M_2 with the computed value $h(SK\|W\|C_1\|RPW_i\|d)$. Based on the analysis of Section 5.2.7, no one can act as legal user to deceive the server.

Therefore, the proposed scheme can provide mutual authentication.

5.2.9 Forward Secrecy

In the improved scheme, the user U_i and the server S_i establish the same session key $SK = W^v \mod n = V^w \mod n = g^{vw} \mod n$. Due to discrete logarithm problem (DLP), no one is able to compute the previously established session keys without knowing v, w. As a result, the proposed scheme provides perfect forward secrecy.

Table 6: Performance comparison

	Total of login and authentication phase	Time
[17]	$6T_e + 11T_h$	13.7303
[10]	$4T_e + 13T_h$	9.1575
[5]	$6T_e + 5T_h$	13.7261
[20]	$8T_e + 7T_h$	18.3017
[21]	$6T_e + 8T_h$	13.7282
Ours	$5T_e + 17T_h$	11.4474

6 Performance Analysis

In this section, we will show efficiency and functionality comparison among our proposed scheme and other related schemes. According to Wu et al.'s report [19], the time of executing one modular exponentiation is 2.2871ms, while the computation time of a one-way hash function is 0.0007ms. For the convenience, we define the following notations used in this section.

- T_h: time for executing a one-way hash function.
- T_e: time for executing exponential operation.
- $T_\oplus$: time for executing XOR operation.

Compared with T_e and T_h, the time of executing XOR operation can be neglected. Usually, a legal user only needs to perform once registration operation, but login and authentication phase are carried out more times in a short time. So we display the comparison of the computational cost in login and authentication phase among these schemes in Table 6. In Table 7, we show security comparison between our proposed scheme and other related ones.

From the comparison of Table 6 and Table 7, we can conclude that the performance of our scheme has better efficiency than other related schemes. Taking all into account, the proposed scheme is more suitable for practical applications.

7 Conclusions

In this paper, we review an anonymous password-based authenticated key agreement scheme with non-tamper resistant smart cards which is proposed by Lee et al. to reduce time cost under the condition of safety. However, Lee et al.s scheme is vulnerable to smart card stolen or lost attack, user impersonation attack, server impersonation attack and cannot provide mutual authentication. To overcome the weakness mentioned above, an improved scheme is proposed. Finally, we demonstrate that our scheme is more secure and applicable to practice by comparing the performance and efficiency of our scheme with other related ones.

References

[1] N. Anwar, I. Riadi, A. Luthfi, "Forensic SIM card cloning using authentication algorithm," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 71–81, 2016.

[2] A. Bogdanov, I. Kizhvatov, "Beyond the limits of dpa: Combined side-channel collision attacks," *IEEE Transactions on Computers*, vol. 61, no. 8, pp. 1153–1164, 2012.

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

[4] C. C. Chang, T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, no. 3, pp. 165–168, 1993.

[5] Y. Chen, J. S. Chou, C. H. Huang, "Improvements on two password-based authentication protocols," *Cryptology ePrint Archive*, Report 2009/561, Nov. 1990.

[6] T. Kasper, D. Oswald, C. Paar, "Side-channel analysis of cryptographic RFIDs with analog demodulation," in *7th International Workshop on RFID Security and Privacy (RFIDsec'11)*, pp. 61–77, 2011.

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

[8] S. K. Kim, M. G. Chung, "More secure remote user authentication scheme," *Computer Communications*, vol. 32, no. 6, pp. 1018–1021, 2009.

[9] T. H. Kim, C. Kim, I. Park, "Side channel analysis attacks using AM demodulation on commercial smart cards with SEED," *Journal of Systems and Software*, vol. 85, no. 12, pp. 2899–2908, 2012.

[10] Y. Lee, H. Kim, "Anonymous password-based authenticated key agreement scheme with non-temper resistant smart cards," *International Journal of Security and Its Applications*, vol. 9, no. 11, pp. 419–428, 2015.

[11] C. T. Li, C. C. Lee, C. J. Liu, C. W. Lee, "A robust remote user authentication scheme against smart card security breach," in *Proceedings of 25th Annual IFIP Conference on Data and Applications Security and Privacy (DBSec'11)*, pp. 231–238, Richmond, VA, USA, 2011.

[12] I. E. Liao, C. C. Lee, M. S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727–740, 2006.

[13] S. Mangard, E. Oswald, T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Guaz University of technology Graz, Austria, 2007.

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

Table 7: Security comparison

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
[17]	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
[10]		✓	✓	✓			✓	✓		✓		✓
[5]	✓	✓		✓			✓			✓		
[20]	✓	✓	✓				✓	✓		✓	✓	✓
[21]	✓						✓			✓		✓
Ours	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

C1 No verifier table.
C2 Password can be chosen freely.
C3 The password cannot be derived by the privileged administrator of the server.
C4 The security of the scheme is not based on the tamper resistance assumption of the smart card.
C5 Resistance to known attacks, such as offline password guessing attack, replay attack, parallel session attack, denial of service attack, stolen verifier attack, user/server impersonation attack.
C6 The password cannot be broken by guessing attack even if the smart card is lost/stolen and compromised.
C7 Establish a common session key.
C8 The scheme is not prone to the problems of clock synchronization and time-delay
C9 the user can change the password locally without any interaction with the authentication server.
C10 Mutual authentication
C11 User anonymity.
C12 Forward secrecy.

[15] E. O. Osei, J. B. Hayfron-Acquah, "Cloud computing login authentication redesign," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 1–8, 2014.

[16] S. K. Sood, "Secure dynamic identity-based authentication scheme using smart cards," *Information Security Journal: A Global Perspective*, vol. 20, no. 2, pp. 67–77, 2011.

[17] D. Wang, C. G. Ma, P. Wu, "Secure password-based remote user authentication scheme with non-tamper resistant smart cards," in *26th Annual IFIP Conference on Data and Applications Security and Privacy (DBSEC'12)*, pp. 114–121, Paris, France, July 11-13, 2012.

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

[19] F. Wu, L. Xu, S. Kumari, X. Li and A. Alelaiwi, "A new authenticated key agreement scheme based onsmart cards providing user anonymity withformal proof," *Security and Communication Networks*, vol. 8, no. 18, pp. 3847–3863, 2015.

[20] Q. Xie, "Dynamic ID-based password authentication protocol with strong security against smart card lost attacks," in *First Interanation Conference on Wireless Communications and Applications (ICWCA'11)*, pp. 412–418, Sanya, China, Aug. 1-3, 2011.

[21] J. Xu, W. Zhu, D. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards and Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

Biography

Min Wu biography. is working as an MS candidate in Applied Mathematics at Wuhan University, China. Her research interests information security and cryptographic protocol.

Jianhua Chen biography. received his BSc in Applied Mathematics from Harbin Institute of Technology, Harbin, China in1983 and received MSc and PhD degree in Applied Mathematics from Wuhan University, Wuhan, China in 1989 and 1994, respectively. Currently, he is a Professor of Wuhan University. His current research interests include number theory, information security, and network security.

Ruibing Wang biography. is working as an MS candidate in Applied Mathematics at Wuhan University, China. Herresearch interests information security and cryptographic protocol.