An Improved Anonymous Password Authentication Scheme Using Nonce and Bilinear Pairings

Jie Ling, Guangqiang Zhao
(Corresponding author: Guangqiang Zhao)
Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China
(Email: gqzh88@126.com)
(Received Jan. 09, 2015; revised and accepted Apr. 27 & June 4, 2015)

Abstract

In 2013, Li et al. pointed out the security problems of Chen's password authentication scheme. they proposed an enhanced smart card based remote user password authentication scheme and claimed their scheme is secure against replay attacks, forgery attacks. In this paper, we state that the scheme is vulnerable to user impersonation attack. It also suffers from user anonymity violation and clock synchronization problem. Furthermore, an improved anonymity enhancement password authentication scheme using nonce and bilinear pairing is proposed. The analysis shows that the proposed scheme is more suitable for applications with high security requirements.
Keywords: Anonymity, authentication, bilinear pairing, clock synchronization nonce

1 Introduction

With the rapid development of network technologies, the client/server based service architecture has become the major service mode for Internet. It enables a single computer to serve a huge amount of clients which are dispersed over different regions around the world [6]. More and more services such as online banking, online trading and online money transfers etc. are provided by the internet. However, almost all of them are operated through the open networks, which may be intrusion by a malicious adversary or illegal users and lead to the private information leakage and properties missing of legal users [4, 20]. Hence, a considerable amount of researches have been carried out to enhance the security of communications over insecure networks. Password authentication scheme using smart card becomes one of the most widely used methods. Although quite a number of remote user authentication schemes with smart cards have been proposed, none of them can solve all possible problems and withstand all possible attacks [8]. Zhu [21] presented an authentication scheme for wireless environments which was proved to be insecure by Lee in 2006, and Lee proposed a new enhanced one [10].

In 2008, Liao put forward a dynamic ID based remote user authentication scheme which could not withstand impersonation attacks and reflection attacks [14]. It was insecure when a user could log in the remote server successfully with a random password, Xu [19] proposed a password authentication scheme based on smart card in 2009 and claimed it is secure. However, Sood [17] and Song [15] proved that the scheme was vulnerable to impersonation and internal attacks and proposed their improved schemes respectively. Nevertheless, Chen et al. [3] found that there still exist security problems, where mutual authentication is not achieved in the scheme of Sood and offline guessing attacks cannot be resisted in the scheme of Song. Then they proposed an improved password authentication and key agreement scheme. Unfortunately, Saru et al. [9] pointed out that Chen's scheme fails to resist impersonation attack and insider attack, it does not provide important features such as user anonymity and confidentiality to air messages. Later, Li et al. [12] also showed that Chen et al.'s scheme cannot ensure forward secrecy and the password change phase of the scheme is inefficient when the users update their passwords, in order to eliminate these problems, they proposed a modified smart card based user authentication scheme and claimed it is more secure. However, we find that Li et al.'s scheme is vulnerable to user impersonation attack, insider attack. Besides, it also suffers from user anonymity violation and clock synchronization problem. Furthermore, we propose an anonymous password authentication scheme based on smart card using nonce and bilinear pairings. We prove it can overcome the above security flaws and is more suitable for practical applications.

The rest of the paper is organized as follows: in Section 2, we introduce the notions used in this paper and bilinear pairings knowledge which is the security of our enhanced scheme. In Section 3, we provide a brief review of Li's scheme and demonstrate the security weakness of

the scheme. Meanwhile, our proposed scheme and corresponding scheme analysis are presented in Section 4, respectively. At last, we draw our conclusions in Section 5.

2 Preliminaries

2.1 Notations

The notations used through out this paper are summarized as follows:

- U_i: the ith user.
- SC: the smart card.
- S: the authentication server.
- ID_i: the identity of U_i.
- PW_i: the password of U_i.
- x: the master secret key hold by server S.
- $\triangle T$: the maximum transmission delay.
- p,q: two large prime numbers that satisfy $p = 2q + 1$.
- Z_q: the ring of integers modulo q.

2.2 Bilinear Pairings

Suppose G_1 is an additive cyclic group generated by P, Whose order is a prime q,and G_2 is a multiplicative cyclic group of the same order.A map e: $G_1 \times G_1 \Rightarrow G_2$ is called a bilinear mapping if it satisfies the following properties:

1) Bilinear:$e(aP,bQ) = e(P, Q)^{ab}$ for all $P,Q \in G_1$ and $a,b \in Z_q$.
2) Non-degenerate: there exist $P,Q \in G_1$ such that $e(P, Q) \neq 1$.
3) Computable: there is an efficient algorithm to compute $e(aP,bQ)$ for all $P,Q \in G_1$.

We note that G_1 is the group of points on an elliptic curve and G_2 is a multiplicative subgroup of a finite field. Typically, the mapping e will be derived from either the Weil or the Tate pairing on an elliptic curve over a finite field.

3 Review and Discussion

Li's scheme consists of Registration phase, Login phase, Authentication phase and Password change phase. The detailed steps of these phases are shown as follows and also in Figure 1.

3.1 Registration Phase

Step 1. U_i chooses his identity ID_i and password PW_i and submits them to S via a secure channel.

Step 2. S computes $A_i \doteq h(ID_i||PW_i)^{PWi} \bmod p$. $B_i = h(ID_i)^{x+PW_i} \bmod p$.

Step 3. S stores $\{A_i,B_i,h(),p,q\}$ in a SC and issues the SC to U_i via a secure channel.

3.2 Login Phase

Step 1. U_i inserts SC into a card reader and inputs his identity ID_i and password PW_i.

Step 2. SC computes ${A_i}^* \doteq h(ID_i||PW_i)^{PWi} \bmod p$, and compares ${A_i}^*$ with A_i, where A_i is stored in SC. If they are not equal, it means the user entered a wrong password and SC terminates the session. If $A_i = {A_i}^*$, SC performs the following steps.

Step 3. SC chooses a random number $\alpha \in {Z_q}^*$ and computes: $C_i = B_i \ / \ h(ID_i)^{PWi} \bmod p$, $D_i = h(ID_i)^{\alpha} \bmod p$,$M_i = h(ID_i \| C_i \| D_i \| T_i)$, where T_i is the current time.

Step 4. SC sends the login request message $\{ID_i,D_i,M_i,T_i\}$ to S.

3.3 Authentication Phase

Step 1. S checks that the ID_i is valid and that ${T_i}^*$ - $T_i \leq \triangle T$, where ${T_i}^*$ is the time the login request was received. If either or both are invalid, the login request is rejected.

Step 2. S computes ${C_i}^* = h(ID_i)^x \bmod p$, $M_i^* = h(ID_i \ \| \ C_i^* \ \| \ D_i \ \| \ T_i)$.

Step 3. S compares ${M_i}^*$ with received M_i. If equal, the login request is accepted and U_i is authenticated by server S; otherwise, the login request is rejected.

Step 4. S generates a random number $\beta \in {Z_q}^*$ and computes:$V_i = h(ID_i)^{\beta} \bmod p$, and the shared session key $sk = {D_i}^{\beta} \bmod p$.

Step 5. S gets the current time stamp T_S, and computes $M_S = h(ID_i \| {C_i}^* \| V_i \| sk \| T_S)$, and sends the mutual-authentication message $\{ID_i,V_i,M_S,T_S\}$ to U_i.

Step 6. Upon receiving the message, U_i checks ID_i and compares T_S with ${T_S}^*$, where ${T_S}^*$ is the time the mutual authentication message was received. If ID_i is valid and ${T_S}^*$ - $T_S \leq \triangle T$, U_i performs the following steps.

Step 7. U_i computes: $sk^* = V_i^{\alpha} \bmod p$, $M_S^* = h(ID_i \ \| \ C_i \ \| \ V_i \ \| \ sk^* \ \| \ T_S)$, and compares ${M_S}^*$ with the received M_S. If they are not equal, the session is terminated. On the contrary, if ${M_S}^* = M_S$, the server S is authenticated by the user U_i.

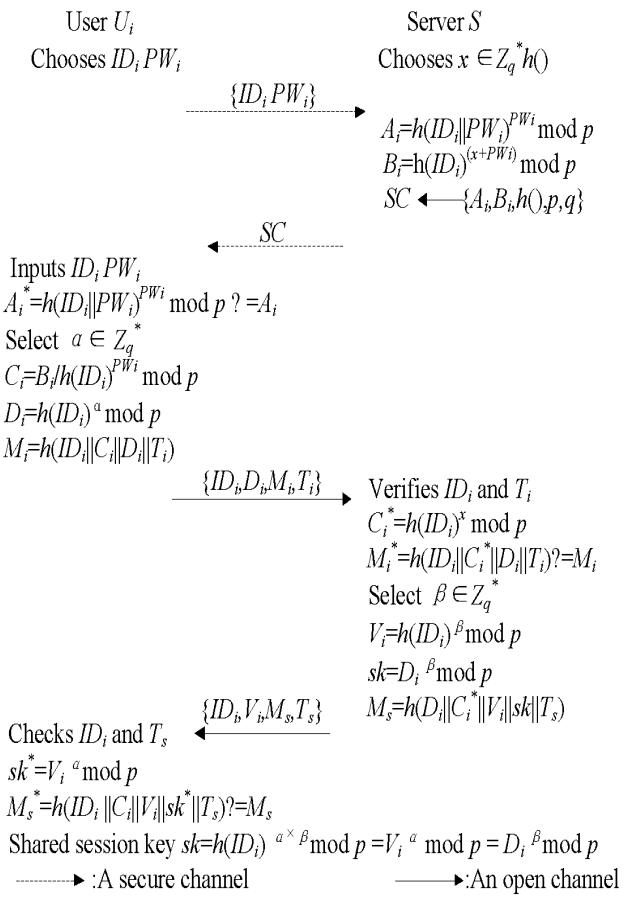

Figure 1: Li's scheme

At last, the user U_i and the server S share an agreed session key $sk = {D_i}^{\alpha\beta} \bmod p$.

3.4 Password Change Phase

This phase is invoked whenever U_i wants to change his passwordPW_i with a new password ${PW_i}^{new}$, and it can be finished without communicating with the server S.

Step 1. U_i inserts his/her smart card into a card reader and submits his/her identity ID_i, password PW_i, and requests to change the password.

Step 2. SC computes ${A_i}^* = h(ID_i||PW_i)^{PWi} \bmod p$, and compares ${A_i}^*$ with A_i, where A_i is stored in SC. If they are not equal, SC rejects the password change request. On the contrary, if ${A_i}^* = A_i$, the user is asked to key a new password ${PW_i}^{new}$.

Step 3. SC computes ${A_i}^{new} = h(ID_i||{PW_i}^{new})^{PW_i new} \bmod p, {B_i}^{new} = B_i \times h(ID_i)^{PW_i new}/h(ID_i)^{PW_i} \bmod p$.

Step 4. SC replaces A_i,B_i with ${A_i}^{new}$, ${B_i}^{new}$, respectively.

3.5 Cryptanalysis of Li et al. Scheme

3.5.1 User Impersonation Attack

During login phase, U_i sends login message $\{ID_i, D_i, M_i, T_i\}$ to S, An attacker U_a can easily obtain the ID_i of U_i by intercepting any login request between U_i and S. Then in near future, U_a can impersonate U_i to cheat S as follows:

1) U_a sends the registration request message ID_i, PW_a, where ID_i is the identity of U_i and PW_a is chosen by U_a as his password.

2) S sends the SC which contains $\{A_a,B_a,h(),p,q\}$ to U_a,where $A_a = h(ID_i||PW_a)^{PWa} \bmod p$,$B_a = h(ID_i)^{x+PWa} \bmod p$.

3) U_a extracts values $\{A_a,B_a,h(),p,q\}$from his/her smart card and computes C_i=B_a $/h(ID_i)^{PWa} \bmod p = h(ID_i)^x \bmod p$.

4) U_a chooses a random number $a^* \in Z_q^*$ and computes: $D_a = h(ID_i)^{a*}$, M_a= $h(ID_i||C_i||D_a||T_a)$, where T_a is the current time of U_a.

5) U_a sends the login request $\{ID_i,D_a,M_a,T_a\}$ to S.

It is easy to see that, S will of course accept it as a legal user because of the reasons:

1) It contains valid identity ID_i of U and the fresh timestamp T_a.

2) The equivalence ${M_a}^* = M_a$ holds since ${M_a}^* = h(ID_i||{C_i}^*||D_a||T_a)$ where ${C_i}^*= C_i = h(ID_i)^x \bmod p$.

S accept the adversary U_a and sends the response $\{ID_i,V_i,M_S,T_S\}$,upon the adversary U_a receiving the response message, just ignore it and computes the session key $sk = {V_i}^{a*}$.

3.5.2 Server Impersonation Attack

Here we move one step forward from the above user impersonation attack. Assume that the attacker possessing ID_i and $C_i = h(ID_i)^x \bmod p$ corresponding to U can impersonate S to cheat U_i as explained below:

1) Suppose U_i sends the login request $\{ID_i,D_i,M_i,T_i\}$ to S.

2) The attack intercepts and blocks $\{ID_i,D_i,M_i,T_i\}$ from reaching up to S, The attacker generates a random number $\beta \in {Z_q}^*$, and computes $V_i = h(ID_i)^\beta \bmod p$,$sk = {D_i}^\beta \bmod p$. S gets the current time stamp T_S, and computes $M_S = h(ID_i||{C_i}^*||V_i||sk||T_S)$, and sends the mutual authentication message $\{ID_i,D_i,M_S,T_S\}$ to U_i.

The message will pass the verification test at U_i because follows:

1) It contains the valid identity ID_i of U_i and fresh timestamp T_S.

2) The equivalence $M_S{}^* = M_S$ holds due to the fact that $sk^* = (V_i)^{\alpha} \bmod p = (D_i)^{\beta} \bmod p = D_i{}^{\alpha\beta} \bmod p$, $M_S{}^* = h(ID_i \| C_i \| V_i \| sk^* \| T_S) = M_S$.

3.5.3 Inside Attack

Password authentication is the most important and convenient protocol for verifying users to get the system's resources.If the password of a user can be derived by the server in the registration protocol, it is called the insider attack; it is a common practice in the real world that many users use the same passwords to access different servers for their convenience without remembering different passwords for different servers. However, the security of Li's authentication scheme relies on the secrecy of his password. Moreover, disclosure of users passwords to anyone is risky. Li skip this important aspect while building the registration phase of their scheme. Users submit the registration request message $\{ID_i, PW_i\}$ consisting their plaintext passwords to S. Therefore, malicious privileged insiders at S have direct access to users passwords PW and they can misuse them to impersonate the legal users or craft other harms.

3.5.4 Clock Synchronization Problem

Remote user authentication schemes employing timestamps to provide message freshness may still suffer from replay attacks as the transmission delay is unpredictable in existing networks. In addition, clock synchronization is difficult and expensive in existing network environments, especially in wireless and mobile networks and distributed networks [5]. Hence, these schemes employing the timestamp mechanism to resist replay attacks are not suitable for mobile applications [2, 7]. In He's scheme, this principle is violated.

3.5.5 Failure of Preserving User Anonymity

Most of the password authentication protocols are based on static identity, which can be used by the attacker to trace and identify the different requests belonging to the same user. On the other hand, the dynamic identity based authentication protocols are more suitable to e-commerce applications [16, 13], for they provide multi-factor authentication based on the identity, password, and smart card. In many cases such as secret online-order placement electronic auditing and electronic voting etc. it is very important to preserve user privacy. In Li's scheme, the user identity ID_i is transmitted in plaintext, which may leak the identity of the logging user once the login messages were eavesdropped. That is to say, without employing any effort an adversary can distinguish and recognize the particular transactions performed by the specific user U. Moreover, the user identity ID_i is static in all the login phases, which may facilitate the attacker to trace out the different login request messages belonging to the same user and to derive some information related to the user U_i. In summary, neither initiator anonymity nor initiator un-traceability can be preserved in their scheme [18].

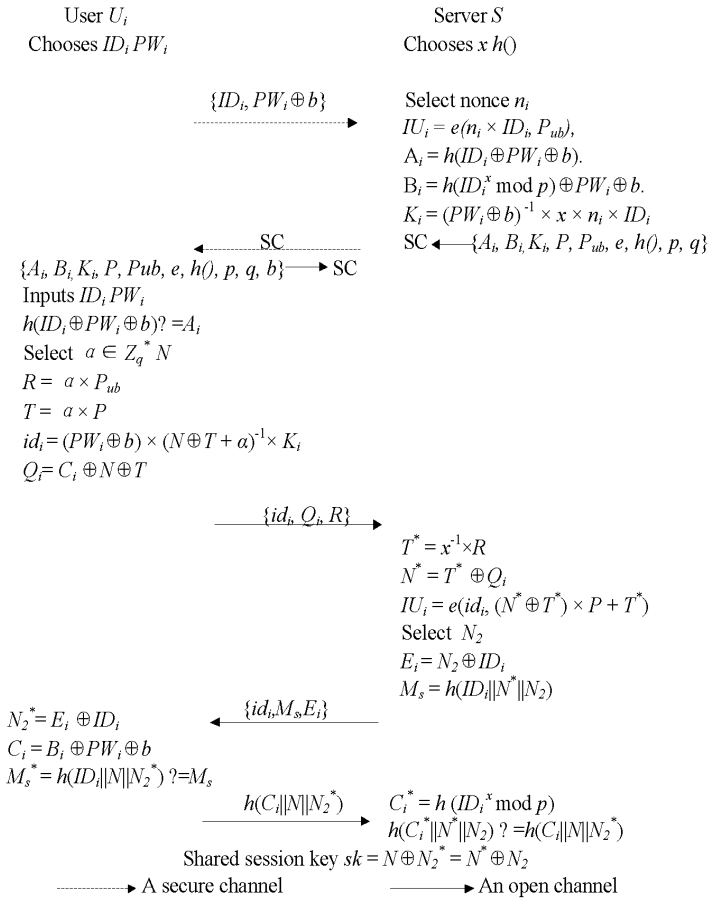

Figure 2: The proposed scheme

4 Our Proposed Scheme

In this section, we use bilinear pairings and nonce to propose an enhancement on Li's scheme that can withstand the security flaws described in previous sections. The proposed scheme performs as follows, and it is also shown in Figure 2.

4.1 The Setup Phase

Let G_1 be an additive cyclic group of a prime order q, and G_2 be a multiplicative cyclic group of the same order. Let P be a generator of G_1,e: $G_1 \times G_1 \Rightarrow G_2$ be a bilinear mapping and h:$\{0,1\} \Rightarrow G_1$ be a cryptographic one-way hash function which maps a string to a point of the additive cyclic group G_1, The server choose a secret key x and computes the corresponding public key $P_{ub} = x \times P$. The server publishes the system parameters $\{ G_1, G_2, e, q, P, P_u b, h()\}$and keeps x secret.

4.2 The Registration Phase

Step 1. U_i chooses ID_i, PW_i, and a random number b, then computes $PW_i \oplus b$ and submits $\{ID_i, PW_i \oplus b\}$ to S via a secure channel.

Step 2. Upon receiving the register message $\{ID_i, PW_i \oplus b\}$, S checks the uniqueness of ID_i in Table 1, if ID_i is in Table 1, it means the identity has been registered before. then U_i will be informed an illegal ID_i and asked to choose a new one, if not, S chooses a random nonce n_i, computes $K_i = 1/(PW_i \oplus b) \times x \times n_i \times ID_i$, $IU_i = e(n_i \times ID_i, P_{ub})$, $A_i = h(ID_i \oplus PW_i \oplus b)$, $B_i = h(ID_i^x \bmod p) \oplus PW_i \oplus b$.

Step 3. S stores $\{A_i, B_i, K_i, P, P_{ub}, e, h(), p, q\}$ in a SC and issues the SC to U_i via a secure channel and S stores $\{IU_i, ID_i\}$ in Table 1 which in a secure database.

Step 4. U_i inserts b into SC, that is, SC contains $\{A_i, B_i, K_i, P, P_u b, e, h(), p, q, b\}$.

Table 1: Index of U and its related identity

Index of the users identity	User identity
IU_1	ID_1
IU_2	ID_2
IU_3	ID_3
$\cdots$	$\cdots$

4.3 The Login Phase

Step 1. U_i inserts his smart card into a card reader and inputs ID_i and PW_i.

Step 2. SC computes and compares $h(ID_i \oplus PW_i \oplus b)$ with A_i. If not equal, it means enter a wrong password or an illegal identity, the smart card terminates the session. If $h(ID_i \oplus PW_i \oplus b) = A_i$, SC performs the following steps.

Step 3. SC chooses a random number $\alpha \in {Z_q}^*$ and computes $R = \alpha \times P_{ub}$, $T = \alpha \times P$, besides, chooses a nonce N, computes the temporary identity of U_i, $id_i = PW_i \oplus b \times 1/(N \oplus T + \alpha) \times K_i$, $Q_i = N \oplus T$, then SC sends the message $\{id_i, Q_i, R\}$ to the server.

4.4 The Authentication Phase

Step 1. Upon receiving the message, S computes $T^* = 1/x \times R$, $N^* = Q_i \oplus T^*$, $IU_i = e(id_i, (N^* \oplus T^*) \times P + T^*)$,Then S search for ID_i related to IU_i in Table 1, if fails, S terminated the session, otherwise, S gets ID_i and performs steps below:

Step 2. S computes $E_i = ID_i \oplus N_2$, where N_2 is a random nonce in sequence. $M_S = h(ID_i \| N^* \| N_2)$ and sends the message $\{id_i, M_S, E_i\}$ to U_i.

Step 3. After received the message, U_i checks id_i and computes ${N_2}^* = ID_i \oplus E_i$, ${M_S}^* = h(ID_i \| N \| {N_2}^*)$ and compares ${M_S}^*$ with M_S, if they are equal, S is authenticated by U_i. U_i computes $C_i = B_i \oplus PW_i \oplus b$ and sends S the message $h(C_i \| N \| {N_2}^*)$.

Step 4. S computes ${C_i}^* = h({ID_i}^x \bmod p)$ and verifies $h({C_i}^* \| N^* \| N) = h(C_i \| N \| {N_2}^*)$. If equal, S believes U_i is authenticated.

Step 5. SC and S compute the shared session key $sk = N \oplus {N_2}^* = N^* \oplus N_2$.

4.5 The Password Change Phase

Step 1. U_i inserts SC into a terminal and submits ID_i, PW_i, SC computes and compares $h(ID_i \oplus PW_i \oplus b)$ with A_i, if equal, the users is asked for a new password ${PW_i}^{new}$.

Step 2. SC computes ${A_i}^{new} = h(ID_i \oplus {PW_i}^{new} \oplus b)$, ${K_i}^{new} = K_i \times (PW_i \oplus b) \times 1/({PW_i}^{new} \oplus b)$, ${B_i}^{new} = B_i \oplus PW_i \oplus {PW_i}^{new} \bmod p$.

Step 3. SC replaces A_i, K_i, B_i with ${A_i}^{new}$, ${K_i}^{new}$, ${B_i}^{new}$ respectively.

4.6 Correctness, Security and Performance

4.6.1 Correctness

If S received the message $\{id_i, Q_i, R\}$, S computes the index of the identity of U_i based the equation $IU_i = e(id_i, (N^* \oplus T^*) \times P + T^*)$ of Step1 of the authentication phase holds, which is verified as below:

$$
\begin{aligned}
& e(id_i, (N^* \oplus T^*) \times P + T^*) \\
= \; & e((PW_i \oplus b) \times 1/(N \oplus T + \alpha) \times K_i, \\
& \quad (N^* \oplus T^*) \times P + T^*) \\
= \; & e((PW_i \oplus b) \times 1/(N \oplus T + \alpha) \times K_i, \\
& \quad (N^* \oplus T^*) \times P + 1/x \times \alpha \times x \times P) \\
= \; & e((PW_i \oplus b) \times 1/(N \oplus T + \alpha) \times K_i, \\
& \quad ((N^* \oplus T^*) + \alpha) \times P) \\
= \; & e((PW_i \oplus b) \times 1/(N \oplus (\alpha \times P) + \alpha) \times K_i \times N^* \\
& \quad \oplus (1/x \times \alpha \times x \times P) + \alpha), P) \\
= \; & e((PW_i \oplus b) \times 1/(PW_i \oplus b) \times x \times n_i \times ID_i, P) \\
= \; & e(x \times n_i \times ID_i, P) \\
= \; & e(n_i \times ID_i, x \times P) \\
= \; & e(n_i \times ID_i, P_{ub}) \\
= \; & U_i.
\end{aligned}
$$

4.6.2 Security

We analyze the security of our enhanced scheme and compare it with other related schemes. The functionality comparison of our proposed scheme and other related works

Table 2: Functionality comparisons

schemes	S1	S2	S3	S4	S5	S6	S7	S8
Xu et al. [19]	Y	Y	N	N	Y	N	N	N
Sood et al. [17]	N	N	N	N	Y	N	N	N
Song [15]	Y	Y	N	N	Y	N	N	N
Chen et al. [3]	N	N	N	N	Y	N	N	N
Li et a [12]	N	N	N	N	Y	Y	Y	N
Ours	Y	Y	Y	Y	Y	Y	Y	Y

is summarized in Table 2, from which we can see that the proposed scheme is more secure than other related schemes. We demonstrate this as below:

S1: Preventing User Impersonation Attack.
This attack means that an adversary may try to intercepted the login messages $\{id_i,Q_i,R\}$ or forge a message to masquerade a legal user to cheat S. Unfortunately, it is impossible for the adversary to compute valid value $h(C_i\|N\|{N_2}^*)$ of Step3 in the authentication phase. Because the plaintexts of C_i,N and ${N_2}^*$ are not transmitted on the channel. Moreover, the adversary cannot compute C_i and ${N_2}^*$ based on $\{id_i,M_i,,E_i\}$ without knowing the secret key x of S and ID_i of U_i. Hence, our scheme can resist user impersonation attack.

S2: Preventing Server Spoofing Attack.
The adversary may attempt to cheat the requesting user U_i.However, it has to forge a valid response message $\{id_i,M_S,E_i\}$ after receiving message $\{id_i,Q_i,R\}$,due to $E_i = ID_i \oplus N_2$, and ID_i can only get through IU_i,IU_i=$e(id_i,(N^* \oplus T^*)\times P + T^*)$and T^*=$1/x \times R$, the adversary cannot computer IU_i without knowing the secret key x of S. Therefore, our proposed scheme can resist server spoofing attack.

S3: Preventing the Insider Attack.
The insider attack occurs when the user password is obtained by the server in the registration phase. Therefore, the users must conceal their passwords from the server to prevent this kind attack. In our enhanced scheme, the user sends the register message $\{ID,PW_i \oplus b\}$ to S, S cannot know the PW of U since the entropy of b is very large. Hence, the malicious adversary in the server cannot carry out this attack.

S4: User Anonymity and Intractability.
User anonymity requires that only the server knows the identity of the user with whom he is interacting, while any third party is unable to do this. User intractability requires that any adversary should be prevented from linking one unknown user interacting with the server to another transcript, that is to say, the adversary is not capable of telling whether he has seen the same user twice [11]. Our proposed scheme use bilinear pairings to protect user true identity. A secure login message is used for protect the user identity form disclosure. In the login phase of the scheme, the user U_i submits the masked identity id_i=$(PW_i \oplus b)\times 1/(N \oplus T + \alpha)\times K_i$, The attacker cannot compute the true identity of U_i based on id_i and IU_i =$e(id_i,(N^* \oplus T^*)\times P + T^*)$, because he cannot computes T^* without knowing the secret key x of S. Meanwhile, the temporary identity of U_i changes every time. Therefore, the true identity of U_i is protected. From the above analysis, we can see that our proposed protocol can provide the user anonymity and intractability.

S5: Preventing Replay Attacks.
The replay attack is when an attacker tries to imitate a legal user to log in to the server by resending the messages transmitted between U_i and S. In our proposed scheme, U_i first chooses a nonce N, computes id_i and send it to S. The second nonce N_2 is chosen by S and embedded in sk and E_i. The attacker may replay the previously used login request message and mutual authentication message to cheat the server or the user, However, he cannot replay an old login message $\{id_i,Q_i,R\}$ in login phase because he cannot compute the valid $h(C_i\|N\|{N_2}^*)$ without knowing ID_i and x.

S6: Perfect Forward Secrecy.
Perfect forward secrecy is an important property for session key distribution; which means that if a long term secret is compromised, the session key of previous sessions still cannot be derived. In our proposed scheme, the session key sk=$N \oplus {N_2}^*$, where N and N_2 are random nonce chosen by U and S, respectively. Also, N and N_2 change each time. Even if the attacker get the previous session key, he cannot computes the next session key between U and S. because N and N_2 are use only once by U and S.

S7: Prompt Detection of the Wrong Password.
Our proposed scheme uses the smart card password detection mechanism in the login phase. When U_i enters ID_i and PW_i, SC computes and compares $h(ID_i \oplus {PW_i}^{new} \oplus b)$ with A_i. If equals, SC performs the remaining steps of the login phase. If not. It

Table 3: Running time of different operations

Notations	Descriptions
T_e	pairing-based exponentiation, $1T_e \approx 11.20$ ms
T_h	hash operations, $1T_h \approx 432$ ms
T_m	elliptic curve scalar point multiplication, $1T_m \approx 6.38$ ms
T_s	encryption operations, $1T_s \approx 2826$ ms
T_d	decryption operations, $1T_d \approx 4357$ ms
T_b	bilinear pairing operation $1T_b \approx 20.01$ ms

Table 4: Performance comparisons

time	Computing	time	Running	time(ms)
schemes	Client	Server	Client	Server
Xu et al. [19]	$2T_e+4T_h$	$2T_e+4T_h$	1750.4	1750.4
Song [15]	$1T_s+4T_h$	$1T_e+1T_d+4T_h$	4554	6096.2
Sood et al. [17]	$3T_e+2T_m+3T_h$	$2T_e+1T_m+3T_h$	1342.36	1324.78
Chen et al. [3]	$2T_e+2T_m+4T_h$	$1T_e+1T_m+4T_h$	1763.16	1745.58
Li et al. [12]	$4T_e+1T_m+4T_h$	$3T_e+3T_h$	1779.18	1329.6
Ours	$4T_m+3T_h$	$1T_e+2T_m+3T_h+1T_b$	1321.52	1339.97

means the user entered an incorrect password SC terminates the session. Therefore, the wrong password will be detected timely at the beginning of the login phase by SC. It will not waste unnecessary extra communication and computation of S.

S8: Prevention of Clock Synchronization Problem. The timestamp is used to prevent replay attack in remote password authentication schemes. Meanwhile, it brings the clock synchronization problem. In our scheme, we discard the timestamp to avoid this problem. The enhanced scheme uses nonce not only prevents the clock synchronization problem but also can resist replay attack efficiently.

4.6.3 Performance

We evaluate the performance of our enhanced scheme and make comparisons with other related schemes. Since the login phase and the authentication phase are two principal parts of each password authentication scheme and should be performed in each session. We only consider the computation costs of these two phases. Let T_m, T_h, T_s, T_d, T_e, T_b be the time of multiplication/division operation, hashing operation, symmetric key encryption operation, symmetric key decryption operation, exponentiation and bilinear pairing operation respectively. The article [1] addressing the implementation of elliptic curve cryptosystems and bilinear on elliptic and estimated the running time of different cryptographic operations in Table 3. We estimate the executing time hash operation and encryption/decryption operation using Microsoft Visual C++ 6.0 software and C language in the environment of Windows XP operating system. The test data is less than 1024 bits. It shows the average time of hash operation is roughly 432 ms. The average executing time of encryption/decryption operation is 2826ms/4357 ms respectively. Table 4 shows the performance comparisons of our scheme and other related schemes. However, the proposed scheme is more secure and practical.

5 Conclusion

In this paper, we firstly showed that Li's scheme cannot resist user impersonation attack, server spoofing attack and insider attack, besides; it also suffers from user anonymity violation and clock synchronization problem. Then we proposed an anonymous password authentication scheme based on smart card using nonce and bilinear pairings, the enhanced scheme overcomes security weaknesses of the previous one. Compared with Li'scheme and other related scheme. Our improved scheme is as efficient as other related schemes and overcomes their weaknesses, which makes it is more secure and suitable for the practical applications.

Acknowledgments

This work is supported by the Project of Guangzhou Science and Technology(No.2014J4100201), and the Project of Guangdong Province Science and Technology(No.2013B040401017,2014A010103029), and the Key Program of the Natural Science Foundation of Guangdong Province(No.S2012020011071).

References

[1] X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Sciences*, vol. 180, no. 15, pp. 2895–2903, 2010.

[2] C. Chang and C. Lee, "A secure single sign-on mechanism for distributed computer networks," *IEEE Transactions on Industrial Electronics*, vol. 14, no. 6, pp. 629–637, 2012.

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

[4] L. Y. Gong, J. X. Pan, and B. B. Liu, "A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords," *Journal of Computer and System Sciences*, vol. 79, no. 2, pp. 122–130, 2013.

[5] J. Han and D. Jeong, "A practical implementation of transparent clock for distributed measurement and control systems," *IEEE Transactions on Instrumentation and Measurement*, vol. 32, no. 5, pp. 433–439, 2010.

[6] M. S. Hwang, S. K. Chong, and T. Yu Chen, "DoS-resistant ID-based password authentication scheme using smart cards," *Journal of Systems and Software*, vol. 83, no. 2, pp. 163–172, 2010.

[7] S. Islam and Biswas G, "A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Journal of Systems and Software*, vol. 31, no. 2, pp. 1892–1898, 2011.

[8] M. Kumar, "A new secure remote user authentication scheme with smart cards," *International Journal of Network Security*, vol. 11, no. 2, pp. 88–93, 2010.

[9] S. Kumari and M. K. Khan, "Cryptanalysis and improvement of a robust smart-card-based remote user password authentication scheme," *International Journal of Communications Systems*, vol. 27, no. 2, pp. 377–389, 2014.

[10] C. C. Lee, M. S. Hwang, and I-En Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, 2006.

[11] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[12] X. Li and J. W. Niu, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1365–1371, 2013.

[13] Y. Lu, X. Yang, and X. Wu, "A secure anonymous authentication scheme for wireless communications using smart cards," *International Journal of Network Security*, vol. 17, no. 3, pp. 237–245, 2015.

[14] Bin du CS M.M, "Cryptanalysis of Lia-Lee-Hwang's dynamic ID scheme," *International Journal of Network Security*, vol. 6, no. 2, pp. 211–213, 2008.

[15] R. Song, "Advanced smart card based password authentication protocol," *Computer Standards and Interfaces*, vol. 32, no. 5, pp. 321–325, 2010.

[16] S. K. Sood, "An improved and secure smart card based dynamic identity authentication protocol," *International Journal of Network Security*, vol. 14, no. 6, pp. 39–46, 2012.

[17] S. K. Sood, A. K. Sarje, and K. Singh, "An improvement of Xu et al.'s authentication scheme using smart cards," *Proceedings of the Third Annual ACM Bangalore Conference*, vol. 11, no. 4, pp. 5–7, 2010.

[18] D. Wang, C. G. Ma, and M. S. Hwang, "Cryptanalysis of a remote user authentication scheme for mobile client-server environment based on ECC," *Information Fusion*, vol. 14, no. 2, pp. 498–503, 2013.

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

[20] M. Zarepoor, P. Shamsolmoali, and M. A. Alam, "Establishing safe cloud: Ensure data security and performance evaluation," *International Journal of Electronics and Information Engineering*, vol. 2, no. 1, pp. 88–99, 2014.

[21] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 13, no. 2, pp. 84–91, 2010.

Jie Ling received Ph.D degree in computation mathematics from Sun Yat-sen University (China) in June 1988. He is a professor in computer science in Guangdong University of Technology.His current research interest fields include information security and Intelligent video processing technology.

Guang-qiang Zhao received his M.S degree in computer science from North China University of Water Resources and Electric Power (China) in June 2012, He is currently a Master degree candidate in Guangdong University of Technology (China). His current research interest fields include information security and cloud computing.