A New Remote User Authentication Scheme based on Bilinear Pairings for Multi-server Environment

利用雙線性配對特性對多伺服器環境所提出新的遠端使用者驗證方案

廖一評[+]*
*大同大學通訊工程研究所
[+]聖約翰科技大學資訊工程系
Email: newsun87@mail.sju.edu.tw

汪順祥
大同大學通訊工程研究所
Email: sswang@ttu.edu.tw

Abstract

With some properties of bilinear pairings, there have been active researches in cryptography. Recently, Das et al. proposed a novel remote user authentication scheme using bilinear pairings over elliptic curve. However, it does not agree with multi-server environment. In this paper, we propose a password authentication scheme based on bilinear pairings for multi-serve environment. Not only does our scheme achieve the efficient computation requirement for smart cards, but also it can construct a complete authentication scheme, including mutual authentication and session key agreement. Our scheme uses nonce instead of timestamp to withstand relay attacks. In addition, the remote server requires nothing about the secret key of the key distribution center *(KDC)* to authenticate the users. Our scheme also analyzes the security and compares the functionality with other schemes.

Key words: multi-server, bilinear pairing, elliptic curve, key distribution center

摘要

雙線性配對在密碼學上的特性已經做了許多學術研究。最近Das等人利用橢圓曲線的雙線性配對提出了一篇新的遠端身分驗證方案，但是該方案並不適用在多伺服器的環境中。在本篇文章我們提出利用雙線性配對特性對多伺服器環境提出一個使用者密碼驗證方案。此方案不但滿足智慧卡有效率運算的需求，而且也提供一個完整的驗證程序，其中包括相互驗證及會議鑰匙的協議。我們利用亂數來取代時間戳記進而抵擋重送攻擊。另外遠端伺服器也不需要知道鑰匙分配中心的密鑰就可驗證使用者的身分。此方案也對其安全性作了分析並與其它的方案做功能性的比較

關鍵字: 多伺服器，雙線性配對， 橢圓曲線， 鑰匙分配中心

一. Introduction

Password authentication is the most acceptable and widely used mechanism to protect resources of networks from unauthorized users. Due to the portability and security of the smart cards, password authentication using the smart card can be simplified, flexible, and efficient in a single server environment. In 1981, Lamport first proposed a remote user authentication schemes using password table to verify the legitimacy of the login user [1]. Since the scheme accompanies the flaw of maintaining the password table, many password-based authentication schemes without any verification table have been proposed subsequently [2-9]. However, with the rapid development of network technology, the system providing resources to be accessed over the network often consists of many different servers around the world. The multi-server environment makes the user access the network's resources more efficiently and conveniently. If conventional password authentication methods are applied to multi-servers environment, each user does not only need to log into various remote servers repetitively but also needs to remember many sets of identities and passwords. It is infeasible and easily leads to identities and passwords leaked.

Thus, Lee and Chang (2000) first proposed a user identification and key distribution scheme that is based on the difficulty of factorization and hashing functions [10]. It agreed with the multi-server environment. Next, Tsaur (2001) proposed a password based remote user authentication scheme based on RSA cryptosystem and Lagrange interpolating polynomial for multi-server environment [11]. In the same time, Li et al. proposed a remote password authentication scheme by using neural networks [12]. However, it is impractical to spend too much time and cost on training and maintaining neural networks. Later, Lin et al. (2003) proposed a new efficient remote user authentication scheme based on the simple geometric properties of the Euclidean [17]. Many schemes pointed out the weakness of the above schemes and proposed the improvement schemes intensively [13-15].

Another interactive password authentication based on hashing functions also has been proposed. Juang (2004) pointed out that Lin et al.'s scheme is not enough efficient for the authentication process, and then proposed an efficient multi-server user authentication and key agreement based on hashing function and symmetric cryptosystem [16]. He introduces the shared key inquire phase to obtain the shared secret key between the network user and the service provider, and then mitigate the load of each registered server for maintaining the encrypted keys table. However, Juang's scheme can not update user's password without the help of the third trusty party. Juang's scheme also lacks for the mechanism of checking the user's identity and password in the login phase. It will easily suffer online guessing attack after losing the smart card. Besides, if the secret parameters of the smart card are extracted with some ways [28], Juang's scheme cannot withstand offline dictionary attack. To reduce the computation cost of the shared key inquire phase, Chang-Lee (2004) proposed an efficient scheme, which assume that the secret key of the third trust party is distributed to each registered server via secure channel [18]. However, the proposed scheme can not prevent the secret key from leaking, namely the insider attack.

Recently, the pairings operations on elliptic curve have received considerable attentions. Especially after the work of the first identity-based encryption scheme used in Boneh and Franklin (2001) [19], various pairing based cryptosystem have been proposed, including identity-based encryption (IBE) and identity-based signature (IBS) [20]. Later, Das et al. (2005) first proposed a novel remote user authentication scheme based bilinear pairings using smart cards [21]. When the user registers at the system, the system distribute a secret key associated with his identity and issue a smart card to him. After the user sends an authentication message to the system, the system can computer the bilinear parings associated with user's identity and published public key to authenticate the users. Although the pairing operation takes high computation in verification phase, it remains the same secure level as public key cryptosystem but reduces the computation complexity for smart card. However, their scheme neither agrees with the multi-server environment nor withstands forgery attack. Besides, the password change phase is not faultless. Thus, many modified scheme had been addressed intensively [22-25]. At the same time, Wu et al. proposed ID-based remote authentication scheme with smart cards using elliptic curve cryptography [26]. The scheme is flexible in which any distributed remote hosts can authenticate users without knowing any secret information from the key information center. Later, Vo and Kim showed that Wu et al.'s scheme can not withstand the impersonation attack which is based on the leaking some secret information stored by remote servers [27]. In addition, Both Das et al. and Wu et al.'s scheme can not apply to business transaction since it can not provide the mutual authentication and session key agreement. As such, we will propose a bilinear pairings based remote user authentication scheme to improve the weakness aforementioned while maintaining the merits of bilinear pairings.

Before that, we summarize the following essential requirements agreed with password based remote user authentication scheme using smart card for multi-server environment [16].

(1) The users only register once at the registration center.

(2) The smart card need efficient computation cost due to the limited computing power.
(3) It needs no password tables or verification tables stored in a server.
(4) It allows a legal user to change his password as favorite strings without the help of third trusty party.
(5) It allows the user and the remote server to authenticate each other.
(6) A session key is agreed by the user and the remote server in every session.
(7) It can resist all kinds of attacks such that it can be applied in the real world.

In this paper, we propose a new remote user authentication based on bilinear pairings for multi-server environment. Our scheme can only allow both each user and each remote server to maintain one secret. Besides, our scheme achieves efficient computation compared to traditional public-key cryptosystem while marinating the same security level. The proposed scheme can be fast to detect a wrong password. That is, if the user inputs a wrong password, it will be detect by the smart card instead of the remote server. Moreover, we use nonce to remedy the weakness of time synchronization. The remainder of the paper is organized as follows. In section 2, we show the preliminaries, including bilinear pairings and computation problem. In section 3, we describe a complete scheme of remote user authentication based on bilinear pairings. After that, we analyze the security and compare the functionality of our scheme with the others in section 4 and 5. Finally, the conclusion is given in section 6.

二. Preliminaries

(一) Bilinear Pairings

The Bilinear pairings namely the Weil pairings or Tate pairings may be used in important applications of cryptography and allow us to construct the remote user authentication schemes. Suppose $< G_1, + >$ be an additive cyclic group of prime order q generated by P, where q is a prime and $< G_2, \times >$ a multiplicative cyclic group of the same order as in G_1. A bilinear pairing is a map $\hat{e}: G_1 \times G_1 \to G_2$ on the elliptic curve and satisfies the following three properties:

P1 Bilinear:

For $\forall P, Q, R \in G_1$, $\hat{e}(P+Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$ and $\hat{e}(P, Q+R) = \hat{e}(P, Q)\hat{e}(P, R)$, for all $P, Q \in G_1$ and $a, b \in Z_q^*$. Moreover, for any $a, b \in Z_q^*$, $\hat{e}(a*P, b*Q) = \hat{e}(a*b*P, Q) = \hat{e}(P, a*b*Q) = \hat{e}(P, Q)^{ab}$

P2 Non-degenerate:

$\forall P$ where P is not a generator, there exists $Q \in G_1$ such that $\hat{e}(P, Q) \neq 1$.

P3 Computable:

There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in G_1$.

(二) Computation problem

C1 Elliptic Curve Discrete Logarithm Problem *(ECDLP):* Consider the equation $Q = k*P$, where P, Q$\in G_1$. It is relatively ease to calculate Q given k and P, but it is relatively hard to determine k given Q and P.

C2 Elliptic Curve Diffie-Hellman Key Exchange Scheme (ECDHKES): Let $P(x, y) \in G_1$ and a key exchange between user A and B can be accomplished as follows:

- A generates a random number $a \in Z_q^*$, calculates $D_A = a*P$ and sends D_A to B.
- B generates a random number $b \in Z_q^*$, calculates $D_B = b*P$ to A.
- A can calculate key $sk_A = a*D_B$ and B can calculate key $sk_B = b*D_A$

Since, $a*D_B = a*b*P = b*a*P = b*D_A$, thus $sk_A = sk_B$. To break this scheme, an attacker would face ECDLP, which is assumed hard.

三. The proposed scheme

In this section, we propose a bilinear pairings based remote user authentication scheme for multi-server environment. After receiving the login message, the remote server can compute the bilinear parings associated with user's identity and published public key to authenticate the users. Besides, the mutual authentication and session key agreement are also taken into consideration. There are three kinds of participants in this scheme, including the user (U_i), the remote server (S_j) and key distributing center (KDC) . We assume that KDC is a trusty party responsible for generating the secret keys among the participants. Let ID_i denotes a unique identification of the user U_i and SID_j denotes a unique identification of the remote server S_j. The proposed scheme consists of some phases, including setup phase, registration phase, login phase, mutual verification and session key agreement phase. Moreover, we provide the password change phase to change the user's password as his favorite strings without the help of KDC . Different phase works as follows:

(一) Setup Phase

Define $h:\{0,1\}^* \to Z_q^*$, $H_1:\{0,1\}^* \to G_1$ and $H_2:\{0,1\}^* \times G_1 \to Z_q^*$ be a cryptographic hash functions. Suppose KDC is a third trust party responsible for the secret key management in whole system. As such, KDC regards $Pub_{KDC} = s * P$ as public key and distributes the secret key $P_{s_j} = s * H_1(SID_j)$ to each registered service provider S_j . Then, KDC publishes the system parameters $(G_1, G_2, \hat{e}, q, P, Pub_{KDC}, h(.), H_1(.), H_2(.))$, where these parameters have been defined above.

(二) Registration phase

If the user U_i wants to access the sources of multi-server environment, he must submit identity ID_i and password PW_i to KDC . Then, KDC performs the following steps:

1. Compute $t_i = h(ID_i \| PW_i)$, $Q_i = H_1(ID_i)$, $\mathrm{Re}\, g_{ID_i} = s * Q_i$, $X_i = PW_i * Q_i \oplus \mathrm{Re}\, g_{ID_i}$ and $y_i = h(\mathrm{Re}\, g_{ID_i}^x) \oplus s$, where $\mathrm{Re}\, g_{ID_i}^x$ denotes the x coordinate of the point $\mathrm{Re}\, g_{ID_i}$.
2. Issue the smart card with $(t_i, X_i, y_i, h(.), H_1(.))$ to the user U_i over a secure channel.

(三) Login phase

When the user U_i want to access the sources of the remote server S_j, he insert the smart card and enters ID_i^* and PW_i^* . Then the smart card executes the following steps:

1. Compute $t_i^* = h(PW_i^* \| ID_i^*)$, and then check whether t_i^* is equal to t_i stored in the smart card. If yes, the legality of the user can be assured and proceed with next step; otherwise, terminated the login phase.
2. Generate a nonce n_i , and compute the login parameters according to following equations:

$$Q_i = H_1(ID_i)$$
$$\mathrm{Re}\, g_{ID_i} = X_i \oplus PW_i * Q_i$$
$$s = y_i \oplus \mathrm{Re}\, g_{ID_i}^x$$
$$B_i = n_i * P$$
$$C_i = H_2(ID_i, B_i) * \mathrm{Re}\, g_{ID_i} + n_i * Q_i$$
$$D_i = B_i \oplus s * H_1(SID_j)$$

Finally, send the login request $< ID_i, C_i, D_i >$ to the remote server S_j .

(四) Mutual verification phase

Upon receiving the login request message $< ID_i, C_i, D_i >$ from the user U_i , the remote server S_j verifies the user U_i with the following steps:

3. Compute $B_i^* = D_i \oplus P_{S_j} = n_i * P$
4. Check the validity of ID_i and whether the following equation holds or not.

$$\hat{e} < C_i, P >=$$
$$\hat{e} < H_1(ID_i), H_2(ID_i, B_i^*) > * Pub_{KDC} + B_i^*) \qquad (1\ )$$

If both of them hold, it indicates that the legality of the user can be verified and the remote server can obtain $B_i (= n_i * P)$. Then the remote server S_j accepts the login request, otherwise rejects it.

$\hat{e} < C_i, P) >$ can be deduced as follows:

$$\hat{e} < C_i, P >= \hat{e} < H_2(ID_i, B_i) * \mathrm{Re}\, g_{ID_i\, i} + n_i * Q_i, P >$$
$$= \hat{e} < H_2(ID_i, B_i) * s * Q_i + n_i * Q_i, P >$$
$$= \hat{e} < Q_i, H_2(ID_i, B_i) * s * P + n_i * P >$$
$$= \hat{e} < Q_i, H_2(ID_i, B_i) * Pub_{KDC} + B_i >$$
$$= \hat{e} < H_1(ID_i), H_2(ID_i, B_i^*) * Pub_{KDC} + B_i^* >$$

5. Generate a nonce n_s , and compute $E_s = n_s * P$ and $f_s = h(B_i^x \parallel E_s^x)$, where B_i^x and E_s^x denotes the x coordinate of point B_i and E_s . Finally, send (E_s, f_s) back to the user U_i .

After receiving S_j acknowledge message (E_s, f_s) , the user U_i verifies the service provider S_j by working as following steps:

6. Compute $h(B_i^x \parallel F_s^x)$ and compare it with f_s . If they are equivalent, then the user U_i successfully authenticates the remote server S_j ; otherwise, the connection is disconnected.
7. Compute $g_i = H_2(ID_i, B_i)$ and respond to the remote server S_j .
8. Upon receiving g_i from the user U_i , the remote server S_j compare g_i with $H_2(ID_i, B_i)$. If it holds, the mutual verification phase is finished.

(五) Session key agreement phase

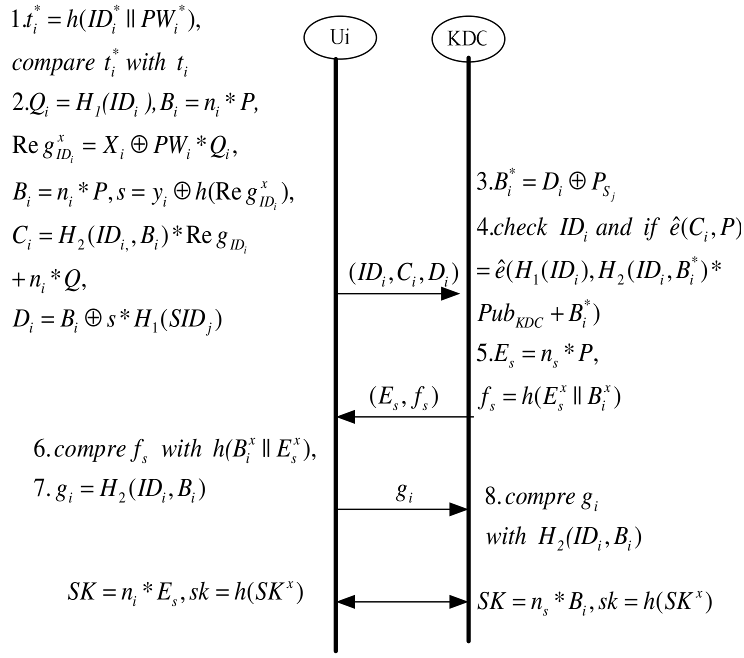
After completing the mutual authentication, the user U_i and the remote server S_j can negotiate the session key as follows:

$$SK = n_i * n_s * P,\ sk = h(SK^x) \qquad (3)`$$

, where SK^x denotes the x coordinate of point SK . The security of session key agreement phase is based on the ECDHKES. In this phase, the common session key is associated to protect the sensitive data between the user U_i and the remote server S_j . Thus, the user and the remote server can encrypt and decrypt the transmitting data within each session.

(六) Password change phase

When the user U_i wants to update password without the help of KDC , he inserts his smart card to card reader and inputs ID_i^* and PW_i^* corresponding to the smart card. To avoid the cardholder updating password freely by way of stealing the user's smart card, the smart card first works as the step1 of login phase. After assuring the legality of the cardholder, the smart card allows the cardholder to resubmit a new password PW_i^{new} , and then computes $t_i^{new} = h(PW_i^{new} \parallel ID_i)$ and $X_i^{new} = X_i \oplus PW_i * Q_i \oplus PW_i^{new} * Q_i$. Finally, (t_i^{new}, X_i^{new}) is replace of (t_i, X_i) stored in the smart card.



Ui
KDC
$1.t_i^* = h(ID_i^* \parallel PW_i^*)$,
$compare\ t_i^*\ with\ t_i$
$2.Q_i = H_1(ID_i), B_i = n_i * P$,
$\mathrm{Re}\, g_{ID_i}^x = X_i \oplus PW_i * Q_i$,
$B_i = n_i * P, s = y_i \oplus h(\mathrm{Re}\, g_{ID_i}^x)$,
$C_i = H_2(ID_{i,}, B_i) * \mathrm{Re}\, g_{ID_i}$
$+ n_i * Q$,
$D_i = B_i \oplus s * H_1(SID_j)$
(ID_i, C_i, D_i)
$3.B_i^* = D_i \oplus P_{S_j}$
$4.check\ ID_i\ and\ if\ \hat{e}(C_i, P)$
$= \hat{e}(H_1(ID_i), H_2(ID_i, B_i^*) *$
$Pub_{KDC} + B_i^*)$
$5.E_s = n_s * P$,
$f_s = h(E_s^x \parallel B_i^x)$
(E_s, f_s)
$6.compre\ f_s\ with\ h(B_i^x \parallel E_s^x)$,
$7.g_i = H_2(ID_i, B_i)$
g_i
$8.compre\ g_i$
$with\ H_2(ID_i, B_i)$
$SK = n_i * E_s, sk = h(SK^x)$
$SK = n_s * B_i, sk = h(SK^x)$

Figure1. The protocol of mutual authentication and session key agreement

四. Security analysis

In this section, we analyze the security of our scheme. We will show that the proposed scheme can withstand the various possible attacks.

(一) Withstanding attacks

- Replay attack

The replay attack is replaying the same message of the receiver or the sender again. If the adversary replies an old message $< ID_i, C_i^*, D_i^* >$ to the remote server S_j, the replay attack must fail. Without knowing the secret key s of KDC, the adversary can not obtain B_i^* from D_i^*. Thus, the adversary cannot respond to a valid g_i to the remote serve S_j. On the other hand, the adversary sends an old verification message (E_s^*, f_s^*) to launch replay attack, where f_s^* is related to n_i^*. The user U_i compares f_s^* with $h(B_i^x \| E_s^x)$. It is obvious that the equality does not hold since nonce is usually used once.

- Forgery attack

When the adversary wants to masquerade the legal user U_i to pass the verification of the remote server S_j, he must construct a valid login message $< ID_i, C_i, D_i >$. Without the knowledge of the secret key s of KDC, the adversary cannot compute $\mathrm{Re}\,g_{ID_i} (= s * H_1(ID_i))$ to forge a valid $C_i (= H_2(ID_i, B_i) * \mathrm{Re}\,g_{ID_i} + n_i * Q_i)$ and $D_i (= B_i \oplus s * H_1(SID_j))$. Similarly, the severing spoofing attack does not succeed because the adversary cannot compute a valid B_i from $D_i (= B_i \oplus s * H_1(SID_j))$ unless he knows the secret key P_{S_j} of the remote server S_j.

- Stolen verifier attack

Since the scheme has no verification table, nobody could obtain any verifiable information from the remote server to threaten the protocol. So the scheme can prevent stolen-verifier attack.

- Smart card lost attack:

When the smart card is lost or stolen, the cardholder tries to obtain either the password corresponding to the smart card or other secret information. If it works, anyone can impersonate the legal user's to login the service provider. The possible ways are described as follows:

[1] Secret information leaked

According the analysis of forgery attack, the system can be attacked by way of leaking the secret key s or secret parameter $\mathrm{Re}\,g_{ID_i}$. Although the adversary can extract $X_i (= PW_i * Q_i \oplus \mathrm{Re}\,g_{ID_i})$ with some ways, he can not obtained $\mathrm{Re}\,g_{ID_i}$ without knowing PW_i. Similarly, the secret key s can not extracted form $y_i (= h(\mathrm{Re}\,g_{ID_i}^x) \oplus s)$

[2] Offline dictionary attack

The adversary can extract t_i, X_i and y_i stored in the smart card through some ways [28]. However, it is feasible to guess PW_i and ID_i from smart card parameters since it will face the security of one-way hashing function and ECDLP. That is, our scheme can withstand the offline dictionary attack.

[3] Online guessing attack

To pass the examination of the remote server S_j, the adversary may guess the password corresponding to the smart card. Before that, our scheme can check the valid of the password via the smart card. So, the smart card can restrict the numbers of input to withstand online guessing attack.

(二) Session key security

- Known-key security

The known-key security is defined as the assurance that any future session keys will not compromised if the current session key will be known to an attacker. In our scheme, the user U_i and the remote server S_j should generate a unique session key, which is based on ECDHKES. Thus, the session key generated in each session is independent and should not be exposed if other session keys are compromised.

- Forward secrecy

The forward secrecy is defined as the assurance that any previous session keys will not compromised if the secret information is leaked. In our scheme, any session keys are related to nonces, which are different in each session. If the secret key s is compromised between the user U_i and the remote server S_j, it is not helpful to deduce the session keys used in the past. Thus, the session keys used in the past should not be recovered.

(三) Robust updating password

In the password change phase, the cardholder can freely change his password as the favorite stings without the help of KDC . Before that, he must submit his identity and password corresponding to the smart card. In other word, anyone even having the smart card can not update his password without knowing the original identity and password.

五. Performance and functionality analysis

In this section, we will evaluate the performance of the proposed scheme and make comparison with the others. Typically, the efficiency evolution can be divided into communication cost and computation cost. Table 1 denotes the notation for various operations used in all related schemes. Before that, we use the following facts and assumptions. Assume the identity ID_i , password PW_i , timestamp and nonces are all 128-bit length; a point on ECC is 320-bit length since 160-bit ECC is equivalent in security to 1024-bit RSA for practical implementation [29]. Moreover, we also assume the output sizes of various hashing functions are 128-bit.

In our scheme, the parameters stored in the smart card are (t_i, X_i, y_i) , so memory needed in the smart card is 576 bits (=128+320+128). The communication cost of authentication includes the capacity of transmitting message involved in the authentication scheme. At the user part, the capacity of transmitting message is 896 bits (=128+320+320+128), including $< ID_i, C_i, D_i >$ and g_i . As for the service provider part, that is 448(=320+128) bits, including E_s and f_s . Thus, the communication cost is 1344bits. The computation cost of registration is defined as the total time of various operations executed in the registration phase. According to the definition, the computation cost of registration is $3T_H + 2T_{EC-MUL}$. Similarly, the computation cost of the user and the service provider are focused on the time spent by both the user and the service provider in the process of authentication. Therefore, the computation cost of the user and the remote server are $7T_H + T_{EC-ADD} + 6T_{EC-MUL}$ and $4T_H + T_{EC-ADD} + 2T_{EC-MUL} + 2T_{BP}$ respectively. In view of the efficiency computation, the computation cost at user's part is a crucial issue due to the limited resource of smart card. As such, our scheme only uses efficient elliptic curve operations instead of costly bilinear pairings at the user's part. It implies that our scheme is apply well to smart card based scheme. The comparison of performance evaluation with the others is given in Table 2. Seemingly, our scheme is not more efficient than Wu et al.'s scheme [26] and Das et al.'s scheme [21] in all respects, but Wu et al.'s scheme and Das et al.'s scheme can not apply to business transactions due to lacking for the mechanism of mutual authentication and session key agreement. Moreover, our scheme can withstand various possible attacks effectively. Although the computation cost of server side in our scheme mainly involves the pairing operations, which is complex and costly, the computation cost is done by the service provider with large computation power. Therefore, our scheme is well suited to smart card applications for multi-server environment. In addition to the comparison of performance, we also demonstrate the functionality between our scheme and the others in Table3. In Wu et al.'s scheme, the server must store $s*P$ to verify the legality of the user. Therefore, their scheme cannot resist the impersonation attack by leaking $s*P$. Furthermore, although Das et al.'s scheme provides the password change phase, the adversary can use the false password to update the owner's password freely. Thus, our scheme can not only satisfy all listed functions but also enhance security level.

Table 1 Notation of time complexity for various operations

Notation	Definitions
T_{BP}	the time for bilinear pairing operation.
T_{EXP}	the time for the modular exponentiation
T_{EC-MUL}	the time for the multiplication of a number and an elliptic curve point
T_{EC-ADD}	the time for the addition of two points in

	an elliptic curve
T_H	the time for executing the one-way hash function, including $h(.)$, $H_1(.)$ and $H_2(.)$

Table 2 Efficiency comparison between our scheme and the others

	Ours	Wu et al. [26]	Das et al.[21]
E1	576bits	448bits	448bits
E2	1344bits	896bits	896bits
E3	$3T_H + 2T_{EC-MUL}$	$T_H + 2T_{EC-MUL}$	$2T_H + T_{EC-MUL}$
E4	$7T_H + T_{EC-ADD}$ $+ 6T_{EC-MUL}$	$T_H + T_{EC-ADD}$ $+ 4T_{EC-MUL}$	$T_H + 2T_{EC-MUL}$
E5	$4T_H + T_{EC-ADD}$ $+ 2T_{EC-MUL}$ $+ 2T_{BP}$	$T_H + T_{EC-ADD}$ $+ T_{EC-MUL}$ $+ 2T_{BP}$	$T_H + T_{EC-ADD}$ $+ T_{EXP}$ $+ 2T_{BP}$

E1: Memory needed in the smart card
E2: Communication cost of the authentication
E3: Computation cost of the registration
E4: Computation cost of the user
E5: Computation cost of the service provider

Table3 The functionality comparison between our scheme and the others

	Ours	Wu et al.	Das et al.
F1	Yes	Yes	No
F2	Yes	No	No
F3	Yes	No	No
F4	Yes	No	No
F5	Yes	Yes	No
F6	Yes	No	No
F7	Yes	No	No

F1: Multi-server environment
F2: Mutual authentication
F3: Session key agreement
F4: Robust updating password
F5: No time synchronization
F6: Fast detect the wrong password
F7: Withstand impersonation attack

六. Conclusion

In this paper, we propose a secure and efficient scheme of remote user authentication based on bilinear pairings for multi-server environment. The proposed scheme achieves a complete authentication scheme, including mutual authentication and session key agreement. The proposed scheme uses nonce to withstand replay attack. Moreover, our scheme also provides a robust mechanism in password change phase without any help of the third trusty party.

七. References

[1] L. Lamport, “Password Authentication with Insecure Communication”, Communication of the ACM, vol. 24, no. 11, pp. 770-772, 1981.

[2] Chang and T. C. Wu, “Remote password authentication with smart cards,” IEE Proceedings-E, vol. 138, no. 3, pp. 165-168, 1993.

[3] W. H. Yang and S.P. Shien, “Password authentication schemes with smart cards,” Computer and Security, vol. 18, no. 8, pp. 727-733, 1999.

[4] M. S. Hwang and L. H. Li, “A new remote user authentication scheme using smart cards,” IEEE Trans. Consumer Electron., vol. 46, No. 1, pp. 28-30, 2000.

[5] H. M. Sun, “An efficient remote user authentication scheme using smart cards,” IEEE Trans. On Consumer Electronics, vol. 46, no. 4, pp. 958-961, 2000.

[6] H.Y. Chien, J.K. Jan and Y.M. Tseng, “An efficient and practical solution to remote authentication using smart card,” Computers and Security, vol. 21, no. 4, pp. 372-375, 2002

[7] C.W. Lin, J.J Shen and M. S. Hwang, “Security Enhancement for Optional Strong-Password Authentication Protocol”, ACM Operating Systems Review, 29, No. 3, pp. 12-16, 2003.

[8] W. S. Juang, “Efficient password authenticated key agreement using smart card,” Computer and Security, vol. 23, pp. 167-173, 2004.

[9] C.I. Fan, Y.C. Chan and Z.K. Zhang, “Robust remote authentication scheme with smart cards,” Computer and Security, vol. 24, pp. 619-628, 2005.

[10] W. B. Lee, C.C. Chang, User identification and

key distribution maintaining anonymity for distributed computer network, Computer System Science , vol 15, No.4, pp. 113-116, 2000.

[11] W. J. Tsuar, C. C. Wu, W. B. Lee, A flexible User Authentication for Multi-server Internet Services, Networking-JCN2001LNCS, Springer-Verlag, 2093 pp. 174-183, 2001.

[12] C. Lin, M. S. Hwang and L, H. Li, A new remote user authentication scheme for multi-server architecture, Future Generation Computer Systems, vol. 1, No. 19, pp. 13-22, 2003.

[13] W. J. Tsuar, An enhanced user authentication scheme for multi-server internet services, Applied Mathematical and computation, vol. 170, pp. 258-266, 2005.

[14] T. S. Wu, C. L. Hsu, Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks, Computer and Security, vol. 23 pp. 120-125, 2004

[15] Y.Yang, S. Wang, F.Bao, J. Wang, R. Deng, New efficient user identification and key distribution scheme providing enhanced security, Computer and Security, vol. 23, No. 8, pp. 697-704, 2004.

[16] W. S. Juang, Efficient multi-server password authenticated key agreement using smart cards, IEEE. Transactions on Consumer Electronics, vol. 50, No.1, pp. 251-255, 2004.

[17] C. Lin, M. S. Hwang and L, H. Li, A new remote user authentication scheme for multi-server architecture, Future Generation Computer Systems, vol.19, No.1, pp. 13-22, 2003.

[18] C. Chang, J. S. Lee, An efficient and secure multi-server password authentication scheme using smart cards, IEEE. Proceeding of the 2004 International Conference on Cyberworlds.

[19] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, Proceedings of CRYPTO 2001, LCNCS, Springer-Verlag, 2139, pp. 213-219, 2001.

[20] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, Advances in Cryptology Proceedings of EUROCRYPT 2001, LNCS, Springer-Verlag, 2656 , pp. 416-432, 2003.

[21] M. L. Das, A. Saxena, V. P. Gulati and D. B. Phatak, "A novel remote user authentication scheme using bilinear pairings," Computers and Security, vol. 25, no. 3, pp. 184-189, 2006

[22] J. S. Chou, Y. Chen, J. Y. Lin "Improvement of Manik et al.'s remote user authentication scheme", http://eprint.iacr.org/2005/450.pdf

[23] G. Thulasis, Manik Lal Das, Ashutosh Saxena "Ceyptanalysis of recently proposed Remote user authentication Schemes", http://eprint.iacr.org/2006/028.pdf

[24] G. Fang and G. Huang, "Improvement of recently proposed Remote User Authentication Schemes", http://eprint.iacr.org/2006/200.pdf

[25] Debasis Giri and P.D. Srivastava, "An Improvement Remote User Authentication Scheme with Smart Cards using Bilinear Pairings", http://eprint.iacr.org/2006/274.pdf

[26] Shyi-Tsong Wu, Jung-Hui Chiu and Bin-Chang Chieu, "ID-based remote authentication with smart card on open distributed system from elliptic curve cryptography," Electro Information Technology, 2005 IEEE International Conference on, 22-25 May 2005.

[27] Duc-Liem Vo, Kwangjo Kim, "Cryptanalysis of ID-Based Remote Authentication with Smart Cards on Open Distributed System from Elliptic Curve Cryptography ", The 2007 Symposium on Cryptography and Information Security Sasebo, Japan, Jan. 23-26, 2007.

[28] T. S. Messergers, E. A. Dabbish, and R. H. Sloan, Examining smart card security under the threat of power analysis attacks," IEEE Trans. Comput., vol. 51, No. 5, pp. 541-552, 2002.

[29] N. Koblitz, Elliptic curve cryptosystems, Math. Comp., 48, pp. 203-209, 1987.