Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006

# TWO SECURE REMOTE USER AUTHENTICATION SCHEMES USING SMART CARDS

**XUE-GUANG WANG[1], ZHEN-CHUAN CHAI[2]**

[1]School of Information Science and Technology, East China University of Politics and Law, 505 Long Yuan Road Shanghai 201620, P. R. China
[2]Department of Computer Science and Engineering, Shanghai Jiao Tong University, 1954 Hua Shang Road Shanghai 200030, P. R. China
E-MAIL: wangxueguang@ecupl.edu.cn , zhenchuanchai@163.com

**Abstract:**

**Remote user authentication is essential in network environment to protect unauthorized access of a networked system. Over the past years, many remote user authentication schemes have been put forth. In 2003, to prevent from forgery attacks encountered in Hwang-Li's scheme, a modified remote user authentication scheme was proposed by Shen, Lin and Hwang. However, Leung, Chang, Fong and Chen showed the modified scheme is still insecure. Therefore, in the paper, we would like to improve Shen et al. scheme and propose another secure remote user authentication scheme from bilinear pairings.**

**Keywords:**

**Information security; password authentication; remote login; smart card; bilinear pairings**

## 1. Introduction

Remote user authentication schemes are very useful in networked systems since they can guarantee only the legal users have right to visit the resources provided by the remote servers. Therefore, over the past years, many remote user authentication schemes [1,4-16] have been proposed.

In 1981, Lamport [11] proposed the first well-known password authentication scheme using a password table to achieve user authentication. However, Lamport's scheme suffers from the risk of a modified password table and the cost of protecting and maintaining the password table. In Lamport's scheme, if the password table is stolen by the adversary, the system will be totally broken. To overcome the weakness, Hwang and Li [10] proposed a new remote user authentication scheme in 2000, in which the remote system only keeps a secret key $x_s$ for computing the user passwords and doesn't need to maintain password or verification tables for verifying legal user. However, Chan and Cheng [4] soon pointed out there is a weakness in Hwang-Li's scheme. In 2003, to overcome this weakness, Shen, Lin and Hwang [15] introduced the concept of "shadowed" identity, proposed a modified version and claimed it is secure against Chan-Cheng's attack. However Leung, Cheng, Fong and Chan [13] have showed the weakness still exists in Shen-Lin-Hwang scheme recently. Therefore, from this viewpoint, the remote user authentication deserves further studying in network security field.

Motivated by the above mentioned, in this paper, we point out the homomorphism is the main insecure factor in Shen-Lin-Hwang scheme [15], and propose an improved version using one-way hash function. Furthermore, based on the bilinear pairings [2], we also propose another remote user authentication scheme.

The rest of this paper is organized as follows. In Section 2, we first review Shen-Lin-Hwang's remote user authentication scheme. Then, we give an improved version and propose another remote user authentication scheme in Section 3 and Section 4, respectively. We also give some performance evaluations of our schemes in Section 5. And in the end, we draw our conclusions in Section 6.

## 2. Review of Shen-Lin-Hwang's scheme

In the literature [15], Shen, Lin and Hwang employed the concept of hiding identity and proposed an enhanced scheme to prevent from forgery attack [10]. For reader's convenience, we first briefly review Shen-Lin-Hwang's scheme [15] in this section.

The Shen-Lin-Hwang's scheme involves the registration phase, the login phase and the authentication phase. In the registration phase, each user sends his identity to the remote server. After the user identity is affirmed, the remote server will issue a smart card, a 'shadowed' identity and a password to him via a secure channel. When the user

wants to access the remote system, he attaches his smart card to an input device, and keys in his 'shadowed' identity and a corresponding password. Then, the remote server will verify it in the authentication phase.

The details are described below.

*Registration phase*: The remote server first prepares some system parameters as follows:

- $p$ : a secure large prime.
- $x_s$ : the secret key owned by the remote server
- $h(.)$ : a public secure one-way hash function
- Red(.):a 'shadowed' identity of the device only processed with the remote server

Suppose a new user $U_i$ wants to register the system, he first submits his identity $ID_i$ to the remote server. After the identity is identified, the server computes the 'shadowed' identity $SID_i$ and password $PW_i$ for $U_i$.

$$SID_i = \mathrm{Re}\,d(ID_i)$$

$$PW_i = SID_i^{x_s} \bmod p$$

At last, the server issues the smart card, which contains the public parameters ( $p, h()$ ), and ( $SID_i, PW_i$ ) to the user $U_i$ via a secure channel.

*Login phase*: When $U_i$ wants to login to the remote server, he inserts his smart card into the terminal, and keys in his $SID_i$ and $PW_i$. Then the smart card can perform the following operations:

1. Select a random number $r \in [1,..., p-1]$;
2. Compute $C_1 = SID_i^r \bmod p$;
3. Pick up the current date and time $T$ of the login device, and compute $t = h(T \oplus PW_i) \bmod p - 1$, where $\oplus$ is XOR operation;
4. Compute $M = SID_i^t \bmod p$;
5. Compute $C_2 = M \cdot PW_i^r \bmod p$;
6. Send the message $C = (C_1, C_2, T, SID_i)$ to the remote server.

*Authentication phase*: Suppose that the remote server receives the message $C$ at $T'$, where $T'$ is the current date and time of the system. Then the following operations are performed to facilitate the authentication.

1. Check the validity of 'shadowed' identity $SID_i$, if the format is incorrect, the login request will be rejected;
2. Check the time interval between $T$ and $T'$, if $(T'-T) \geq \Delta T$, where $\Delta T$ is the expected legal time interval for transmission delay, the system will reject the login request;
3. Check $C_2 \cdot C_1^{-x_s} = SID_i^{h(T \oplus PW_i)} \bmod p$. If it does hold, the system will accept the login request. Otherwise, the request will be rejected.

Although Shen-Lin-Hwang's scheme employs the concept of hiding identity, yet it still suffers from the forgery attack. In the literature [4], Leung, Cheng, Fong and Chan presented an attack on Shen-Lin-Hwang's scheme. The attack is similar to Chan-Cheng's attack [2]. Here let us review it.

As an enhanced version of Hwang-Li's scheme [10], Shen-Lin-Hwang's scheme [15] also does not keep any user or password table in the remote system. Therefore, an evil user can freely login to the remote system successfully if he gets a valid pair $(SID_v, PW_v)$. In Leung et al.'s attack [13], a legitimate user $U_i$ with a valid pair $(SID_i, PW_i)$ can impersonate other legal users by the following tricks:

$$SID_v = SID_i^r \bmod p,$$

$$\begin{aligned} PW_v &= SID_v^{x_s} \bmod p \\ &= SID_i^{rx_s} \bmod p \\ &= PW_i^r \bmod p \end{aligned}$$

where $r$ is a random number chosen by the user $U_i$. Obviously, $(SID_v, PW_v)$ is a valid pair and can pass the remote system's authentication.

Like Hwang-Li's scheme, the homomorphic property is also the main insecure factor in Shen-Lin-Hwang's scheme. Therefore, in what follows, we will make a slight modification to propose an improved scheme.

## 3. Scheme 1: an improved scheme

In this section, we will present our improved scheme and show that the scheme can resist above mentioned attacks.

### 3.1. Improved scheme

The improved scheme is composed of three phases: the registration phase, the login phase and the authentication phase. In below, we will describe each of

them in detail.

*Registration phase:* The remote server first prepares some system parameters as follows:

- $p$ : a secure large prime.
- $x_s$ : the secret key owned by the remote server
- $h(.)$ : a public secure one-way hash function
- $f(.)$ : a public secure one-way hash function

When a new user $U_i$ submits his identity $ID_i$ to the remote server for registration, the remote server first checks its validity and then computes the password $PW_i$ as follows:

$$PW_i = f(ID_i)^{x_s} \bmod p$$

Then, the server stores the public parameters $(p, h(), f())$ to a smart card. Finally, the server issues the smart card and $PW_i$ to the user $U_i$ via a secure channel.

*Login phase:* When $U_i$ wants to login to the remote server, he inserts his smart card into the terminal, and keys in his $ID_i$ and $PW_i$. Then the smart card will perform as follows:

1. Select a random number $r \in [1,..., p-1]$;
2. Compute $C_1 = f(ID_i)^r \bmod p$;
3. Pick up the current date and time $T$ of the login device, and compute $t = h(T \oplus PW_i) \bmod p - 1$;
4. Compute $M = f(ID_i)^t \bmod p$;
5. Compute $C_2 = M \cdot PW_i^r \bmod p$;
6. Send the message $C = (C_1, C_2, T, ID_i)$ to the remote server.

*Authentication phase*: Suppose that the remote server receives the message $C$ at $T'$, where $T'$ is the current date and time of the system. Then the following operations are performed to facilitate the authentication.

1. Check the validity of identity $ID_i$, if the format is incorrect, the login request will be rejected;
2. Check the time interval between $T$ and $T'$, if $(T'-T) \geq \Delta T$, where $\Delta T$ is the expected legal time interval for transmission delay, the system will reject the login request;
3. Check $C_2 \cdot C_1^{-x_s} = f(ID_i)^{h(T \oplus PW_i)} \bmod p$. If it does hold, the system will accept the login request. Otherwise, the request will be rejected.

### 3.2. Security analysis

The improved scheme is similar to Shen-Lin-Hwang's scheme, and the main difference is that $f(.)$ is a public one-way hash function. Just as this one-way hash function, it eliminates homomorphic property. Therefore, the improved scheme can withstand Chan-Cheng's attack [4] and Leung et al.'s attack [13].

Suppose a legitimate user $U_i$ with a valid pair $(ID_i, PW_i)$ can use Chan-Cheng's attack or Leung et al.'s attack to impersonate other legal users. For instance, he can obtain a new password $PW_v$ from $PW_i$, i.e. $PW_v = PW_i^r = h(ID_v)^{x_s} = h(ID_i)^{x_s r} \bmod p$, where $r \geq 2$, and then to derive the corresponding user identity $ID_v$ from the equality $h(ID_v) = h(ID_i)^r \bmod p$. However, since $h()$ is a secure one-way hash function, he can't obtain the identity $ID_v$ from $h(ID_v)$. Therefore, the improved scheme can withstand the impersonation attack.

Although the improved scheme can withstand the forgery attack, it still requires high communication overhead, since the length of the modulus $p$ should reach at least 1024 bits to ensure the discrete logarithm problem in $Z_p^*$ is hard.

## 4. Scheme 2: pairing based scheme

In this section, we will introduce another remote user authentication scheme from bilinear pairings. First, we review some basic concepts of bilinear pairings.

### 4.1. Bilinear pairings

Let $G_1$ be a cyclic additive group and $G_2$ be a cyclic multiplicative group of the same prime order $q$. We assume that the discrete logarithm problems in both $G_1$ and $G_2$ are hard. A bilinear pairing is a map $e: G_1 \times G_2 \to G_2$, which satisfies the following properties:

- *Bilinear:* for any $P, Q \in G_1$ and $a, b \in Z_q^*$, we have $e(aP, bQ) = e(P, Q)^{ab}$.

- *Non-degenerate:* there exists $P \in G_1$ and $Q \in G_1$ such that $e(P,Q) \neq 1$.
- *Computability:* Given $P, Q \in G_1$, there is an efficient algorithm to compute $e(P,Q) \in G_2$.

Such a bilinear pairing may be realized using the modified Weil pairing and Tate pairing associated with super singular elliptic curve. And a more comprehensive description can refer to [2].

### 4.2. Pairing-based scheme

Now we introduce our pairing-based remote user authentication scheme. The scheme includes three phases: registration, login and authentication. In the following, each phase will be described in detail.

*Registration phase:* The remote server first prepares some system parameters as follows:

- $q$ : A secure large prime.
- $G_1$ : A cyclic additive group of order $q$
- $G_2$ : A cyclic multiplicative group of order $q$
- $P$ : a specific point in $G_1$ :
- $e : G_1 \times G_2 \rightarrow G_2$ : a bilinear map
- $x_s$ : The secret key owned by the remote server
- $H(.) : \{0,1\}^* \rightarrow G_1$ : A secure one-way *MapToPoint* hash function

When a new user $U_i$ submits his identity $ID_i$ to the remote server for registration, the remote server first checks its validity and then computes the password $PW_i$ as follows:

$$PW_i = x_s \cdot H(ID_i)$$

Then, the remote server stores the public parameters $(q, G_1, P)$ to a smart card. Finally, the server issues the smart card and $PW_i$ to the user $U_i$ via a secure channel.

*Login phase:* When $U_i$ wants to login to the remote server, he inserts his smart card into the terminal, and keys in his $ID_i$ and $PW_i$. Then the smart card will perform as follows:

1. Select a random number $r \in Z_q^*$;
2. Compute $C_1 = r \cdot P$;
3. Pick up the current date and time $T$ of the login device;
4. Compute $C_2 = \frac{1}{T+r} \cdot PW_i$ ;
5. Send the message $C = (C_1, C_2, T, ID_i)$ to the remote server.

*Authentication phase:* Suppose that the remote server receives the message $C$ at $T'$, where $T'$ is the current date and time of the system. Then the following operations are performed to facilitate the authentication.

1. Check the validity of identity $ID_i$, if the format is incorrect, the login request will be rejected;
2. Check the time interval between $T$ and $T'$, if $(T'-T) \geq \Delta T$, where $\Delta T$ is the expected legal time interval for transmission delay, the system will reject the login request;
3. Check $e(T \cdot P + C_1, C_2) = e(P, x_s H(ID_i))$. If it holds, the system will accept the login request. Otherwise, the request will be rejected. Since

$$\begin{aligned} & e(T \cdot P + C_1, C_2) \\ &= e((T+r) \cdot P, \frac{1}{T+r} PW_i) \\ &= e(P, PW_i)^{(T+r)\frac{1}{T+r}} \\ &= e(P, PW) \\ &= e(P, x_s H(ID_i)) \end{aligned}$$

### 4.3. Security analysis

The security of the scheme is based on the one-way hash function and the hardness of discrete logarithm problem. In below, let us examine the security from viewpoints of various known attacks. Firstly, we define two security terms as follows:

*Definition 1:* Let $H(\cdot)$ be a one-way MapToPoint hash function. We say $H(\cdot)$ is a secure one-way hash function, if, given $y = H(x)$, it is hard to compute $x$ from $y$.

*Definition 2:* Let $Q, P$ be two elements in $G_1$, where $Q = aP$ for some $a \in Z_q^*$. We say the discrete logarithm problem is hard if it is hard to compute such an $a$.

Based upon the above definitions, we analyze the security of our scheme by the following three theorems.

*Theorem 1:* The proposed scheme can resist the replay attacks.

*Proof:* An adversary may execute the replay attack by replaying the intercepted login message in a late time. However, the replay attack here cannot work, since the remote server will check $(T'-T) \geq \Delta T$ in the authentication phase, where $T'$ is the current date and time of the system and $\Delta T$ is the expected legal time interval caused by transmission delay. Thereby, the proposed scheme can resist the replay attacks.

*Theorem 2:* The proposed scheme can resist the stolen-verifier attacks.

*Proof*: Many remote user authentication schemes maintain a password table in the server to store the shared passwords used for the user authentication. However, once an attacker steals the password table, he may successfully masquerade as any legal user to login the server. In our proposed scheme, since it doesn't need to maintain a password table in the server, nobody could obtain any useful information from the server to threaten the protocol. Therefore, stolen-verifier attacks will not occur in our scheme.

*Theorem 3:* The proposed scheme can resist the impersonation attacks.

*Proof:* Firstly, any legal user $U_i$ can't derive the system secret $x_s$ from his password $PW_i = x_s H(ID_i)$. If he could, the discrete logarithm problem will be solved. Secondly, any attacker also can't forge another valid message $C' = (C_1', C_2', T', ID_i)$ from an existing message $C = (C_1, C_2, T, ID_i)$, where $T' \neq T$, $C_1' = r \cdot P$ and $C_2' = \frac{1}{T'+r} PW_i$. If he could, then from the fact that $C_2' = \frac{T+r}{T'+r} C_2$, he must have known $r$, but it will contradict with the assumption that the discrete logarithm problem is hard.

Besides, since it adopts the one-way hash function $H()$ on $ID_i$, the proposed scheme also can withstand Chan-Cheng's attack [4] and Leung et al.'s attack [13]. Hence, the impersonation attacks also can't follow.

From what has been analyzed above, we are fully convinced that the proposed scheme is a secure remote user authentication scheme.

## 5. Performance evaluation

As smart cards are lower-powered and resource-constrained devices, we should keep the computation cost down at smart card side. Besides, low communication overhead also should be cared for in our scheme. Therefore, here we mainly discuss our schemes' performance from the computation cost and the communication overhead's view.

First, the following notations are used to analyze the computation and communication costs: EXP denotes the time for modular exponentiation; MUL is the time for modular multiplication; Hash is the time for hash operation; Inv is the time for modular inversion; PMul is the time for point multiplication. Then, we use Table.1 to compare three schemes' performance at smart card side.

Table 1. Performance comparisons at smart card side

| | Comput.cost | Comm.cost |
|---|---|---|
| S-L-H Scheme[15] | 3Exp+Hash+Mul | High |
| Scheme 1 | 3Exp+2Hash+Mul | High |
| Scheme 2 | 2PMul+Inv | Low |

Generally, in order to make the discrete logarithm problem infeasible in $Z_p^*$, the modulus $p$ is usually assumed to be 1024 bits in both Shen-Lin-Hwang's scheme [15] and our Scheme-1. While for our Scheme-2, to offer approximately the same security level of the discrete logarithm problem over elliptic curve, the prime order of some elliptic curve groups, such as super singular curve groups used to construct the short signature scheme [3], may be chosen very small. Therefore, from Table 1, we can see, under the same security level, our Scheme-1 is almost as efficient as Shen-Lin-Hwang's scheme, and our Scheme-2 is also acceptable, especially in communication cost.

## 6. Conclusions

In this paper, we first reviewed Shen-Lin-Hwang's modified remote user authentication scheme, and pointed out the homomorphism is the main insecure factor. Then, we presented a corresponding improved version, which eliminates the homomorphism. Furthermore, we also presented another pairing-based scheme. By analysis, both our two schemes can resist the impersonation attacks encountered in Shen-Lin-Hwang's scheme, and the performances of them are also acceptable.

**Acknowledgements**

This work is supported by ECUPL Young Science Foundation under Grant BM518222.

**References**

[1] A.K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy", IEEE Trans. Consum. Electron. Vol 49, No.4, pp. 1246 - 1248, 2003.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", SIAM J. Computing, Vol 32 No.3, pp. 586 - 615, 2003.

[3] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing", Proceedings of Asiacrypt 2001, LNCS 2248, pp. 514 - 532, Springer-Verlag, 2001.

[4] C.K. Chan and L.M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards", IEEE Trans. Consum. Electron. Vol 46, No 4, pp. 992 - 993, 2000.

[5] H.Y. Chien and C.H. Chen, "A remote authentication scheme preserving user anonymity", Proceedings of the 19th International Conference on Advanced Information Networking and Applications - AINA 2005, pp. 245 - 248, 2005.

[6] C.C. Chan and K.F. Hwang, "Some forgery attacks on a remote user authentication scheme using smart cards", Informatics Vol 14, No. 3, pp. 289 - 294, 2003.

[7] H.Y. Chien, J. Jan, and Y. Tseng, "An efficient and practical solution to remote authentication: smart card", Computer Security, Vol 21, No 4, pp. 372 - 375, 2002.

[8] C.C. Chang and T.C. Wu, "Remote password authentication with smart cards", IEE Proceddings-E. Vol 138 No. 3, pp.165 - 168, 1993.

[9] M.L. Das, A. Saxena, and V.P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE Trans. Consum. Electron., Vol 50, No 2, pp. 629 - 631, 2004.

[10] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart cards", IEEE Trans. Consum. Electron. Vol 46, No 1, pp. 28 - 30, 2000.

[11] L. Lamport, "Password authentication with insecure communication"}, Communication of ACM, Vol 24 No 11, pp. 770 -772, 1981.

[12] R.X. Lu, Z.F. Cao, "Efficient remote user authentication scheme using smart card", Computer Networks, Vol.49 No 4,, pp.535-540. 2005.

[13] K.C. Leung, L.M. Cheng, A.S. Fong, and C.K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards"}, " IEEE Trans. Consum. Electron. Vol 49 No 4, pp. 1243 - 1245, 2003.

[14] H.M. Sun, "An efficient remote user authentication scheme using smart cards", IEEE Trans. Consum. Electron. Vol 46 No 4, pp. 958 - 961, 2000.

[15] J.J. Shen, C.W. Lin, and M.S. Hwang, "A modified remote user authentication scheme using smart cards", IEEE Trans. Consum. Electron. Vol49 No 2, pp. 414 - 416, 2003.

[16] W.H. Yang and S.P. Shieh, "Password authentication schemes withsmart card", Computer Security, Vol, 18 No.8, pp. 727 - 733, 1999.