

## A Bilateral Remote User Authentication Scheme that Preserves User Anonymity\*

Huei-Ru Tseng, Rong-Hong Jan, and Wu Yang<sup>†</sup>

Department of Computer Science, National Chiao Tung University, Hsinchu, 30010,  
Taiwan

### Abstract

Smart card-based authentication is one of the most widely used and practical solutions to remote user authentication. Compared to other authentication schemes, our proposed scheme aims to provide more functionalities and to resist well-known attacks. These crucial merits include (1) a user can freely choose and change his passwords; (2) our scheme provides mutual authentication between a server and a user; (3) it achieves user anonymity; (4) a server and a user can generate authenticated sessions keys; (5) it is suitable for decentralized servers. Moreover, our scheme can resist replay attacks, forgery attacks, insider attacks, reflection attacks, and parallel session attacks.

**Keywords:** Smart card, Authentication, Password, Anonymity.

---

\*This work was supported by the National Science Council, Taiwan, Republic of China, under grant NSC 96-2752-E-009-005-PAE, NSC 96-2219-E-009-012, NSC 96-2219-E-009-006, NSC 96-2219-E-009-008, and NSC-96-3114-P-001-002-Y.

<sup>†</sup>Corresponding Author. Phone: +886-3-5712121 ext. 31247; fax: +886-3-5721490; e-mail: wuyang@cs.nctu.edu.tw

# 1 Introduction

A remote user authentication scheme is a mechanism that authenticates remote users and allows legitimate users to access network services over an insecure communication network. In a distributed network, when a remote user requests for a service, the server should authenticate the user first. Due to high portability, low cost, and limited cryptographic capabilities of smart cards, a number of smart card-based remote authentication schemes have been proposed [1-22]. In 1981, Lamport [1] proposed the first password authentication scheme for remote users over an insecure channel. Since then, several schemes [2-22] have been proposed to improve security, efficiency, and functionality. Past experience has shown that constructing a secure user authentication scheme is not trivial because lots of proposed schemes were subsequently broken by well-known attacks [3, 6, 7, 8, 10, 11, 13, 16].

Traditionally, if a remote user wants to log into a server, he has to submit his identity and password to the server. On receiving the login request, the server first checks the validity of the identity and computes a one-way hash value of the received password, and then checks the computed value against the server's verification table. Since this approach clearly incurs the risk of tampering and the cost of managing the table, several schemes [2, 4, 5, 9, 12, 14, 15, 17-22] have been proposed that do not depend on a verification table.

Due to the constrained resources in smart cards, the computation and communication overhead must be low in practical implementation. Sun [19] proposed an efficient authentication scheme that adopts only simple hashing operations. In 2002, Chien et al. [4] proposed another authentication scheme that improves on Sun's in two ways: it achieves mutual authentication and it allows users to choose their passwords freely.

After a user is authenticated, the messages between the user and the server must be encrypted when transmitted over the public network. They have to agree

on a session key. Juang [9] proposed an authentication scheme that provides a key agreement function. In various e-commerce applications, user anonymity is also crucial. Das et al. [5] first proposed a dynamic identity-based authentication scheme that preserves user anonymity. However, Chien and Chen [2] pointed out that Das et al.'s scheme [5] fails to protect user anonymity.

In order to reduce the risk of single-point failures, Choi and Youn [23] proposed a novel data encryption and distribution approach based on LU decomposition in 2004. The scheme allows higher security and availability compared with the mirroring scheme [24, 25, 26], and provides a solution for failures and malicious compromises of storage nodes, client systems, and user account. Pathan et al. [17, 18] also proposed two bilateral authentication schemes based on LU decomposition. However, their schemes have several security weaknesses, including (1) they cannot resist replay attacks; (2) passwords could be revealed by the server; (3) they cannot preserve user anonymity; and (4) the server and users cannot agree on a session key.

To conquer these weaknesses, we propose a bilateral user-authentication scheme that not only fixes these weaknesses, but also aims to achieve more functionality and resists well-known attacks. These crucial merits include (1) users can freely choose and change their passwords; (2) it provides mutual authentication between a server and a user; (3) it achieves user anonymity; (4) a server and a user can generate authenticated sessions keys; (5) it is suitable for decentralized servers. Moreover, the scheme is secure against replay attacks, forgery attacks, insider attacks, reflection attacks, and parallel session attacks.

The rest of this paper is organized as follows: In Section 2, we state the basic terms and preliminaries for our scheme. Our proposed scheme is presented in Section 3. Then, we shall analyze our proposed scheme, show that our scheme can resist several attacks, and provide a comparative study with other authentication schemes in Section 4. Finally, we will conclude our paper in Section 5.

## 2 Preliminaries

Our scheme is based on LU decomposition of matrices [27]. The decomposition re-writes a matrix as the product of a lower and an upper triangular matrices. In the LU decomposition, an  $n \times n$  matrix  $A$  is written as

$$A = L \cdot U \quad (1)$$

where  $L$  is a nonsingular lower triangular matrix, and  $U$  is a nonsingular upper triangular matrix.

In our scheme, a symmetric key matrix  $A_{n \times n}$  is generated by the server during system initialization, where  $n$  is the number of users that could be supported. This matrix is a secret of the server.

Each element  $a_{ij}$  is a key from a key pool. We assume that  $a_{ij} = a_{ji}$ , for  $1 \leq i \leq n$  and  $1 \leq j \leq n$ . Since  $A$  is symmetric, the product of the  $x$ -th row of matrix  $L$  and  $y$ -th column of matrix  $U$  is as same as that of the  $y$ -th row of matrix  $L$  and  $x$ -th column of matrix  $U$ .

For example, given  $A$  as follows:

$$A = \begin{pmatrix} 1 & 2 & 4 & 5 \\ 2 & 5 & 8 & 9 \\ 4 & 8 & 15 & 17 \\ 5 & 9 & 17 & 20 \end{pmatrix} \quad (2)$$

we perform elementary row operations to get the lower matrix  $L$  and upper matrix  $U$  as follows:

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 4 & 0 & -1 & 0 \\ 5 & -1 & 0 & -3 \end{pmatrix} \text{ and } U = \begin{pmatrix} 1 & 2 & 4 & 5 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 2 \end{pmatrix} \quad (3)$$

Given  $x = 2$  and  $y = 3$ , we can compute  $a_{23}$  and  $a_{32}$  as follows:

$$a_{23} = L_R(2) \times U_C(3) = \begin{pmatrix} 2 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 4 & 0 & 1 & 1 \end{pmatrix}^T = 8 \quad (4)$$

$$a_{32} = L_R(3) \times U_C(2) = \begin{pmatrix} 4 & 0 & -1 & 0 \end{pmatrix} \times \begin{pmatrix} 2 & 1 & 0 & 0 \end{pmatrix}^T = 8 \quad (5)$$

Since matrix  $A$  is symmetric,  $a_{23} = a_{32}$ .

Table 1: Notations

Symbol	Definition
$U_i$	User $i$
$ID_i$	User $i$ 's identity
$PW_i$	User $i$ 's chosen password
$K_s$	The server's secret key
$AK_i$	The authenticated session key computed by the server and $U_i$
$n$	The number of users that could be supported by the system
$A_{n \times n}$	A symmetric key matrix
$T$	The timestamp
$h(\cdot)$	A one-way hash function
$p$	A prime number and $p$ is divisible by $q - 1$
$g$	A generator of order $q$
$\oplus$	An XOR operation

### 3 Our Proposed Scheme

Our bilateral user authentication scheme is divided into four phases: registration, login, authentication, and password-changing phases. The notations and their corresponding definitions are listed in Table 1.

#### 3.1 Registration phase

Suppose a new user  $U_i$  with the identity  $ID_i$  wants to register with a server for remote-access services.  $U_i$  randomly chooses his password  $PW_i$  and sends the pair  $(ID_i, h(PW_i))$  to the server. These private data should be submitted in person or via a secure channel [3, 7, 10, 11, 12, 13, 15, 17, 18, 19, 20, 22]. Upon receiving the registration message, the server takes the following steps:

1. Generate two random numbers  $x_i, y_i$  between 1 and  $n$ , and select the  $x_i$ -th row from matrix  $L$  (denoted as  $L_R(x_i)$ ), the  $x_i$ -th column from matrix  $U$  (denoted as  $U_C(x_i)$ ), and the  $y_i$ -th column from matrix  $U$  (denoted as  $U_C(y_i)$ ).

2. Compute the pair  $(K_{x_i y_i}, \theta_i)$  as follows: ( $\oplus$  means the exclusive-or operation)

$$K_{x_i y_i} = L_R(x_i) \times U_C(y_i) \quad (6)$$

$$\theta_i = h(ID_i \oplus K_{x_i y_i}) \oplus h(PW_i) \oplus h(K_s) \quad (7)$$

3. Issue a smart card containing  $(K_{x_i y_i}, \theta_i, U_C(x_i), v_i, h(\cdot), g, p)$  to  $U_i$ , where  $v_i = h(K_s) \oplus y_i$ .

### 3.2 Login phase

When  $U_i$  wants to log in to the system,  $U_i$  first attaches the smart card and inputs his password  $PW_i^*$ . The smart card performs the following operations:

1. Generate a random number  $r$ .
2. Compute the pair  $(H_i, S_i)$  as follows:

$$H_i = K_{x_i y_i} \oplus h(r \oplus T) \quad (8)$$

$$S_i = \theta_i \oplus h(PW_i^*) \oplus r \quad (9)$$

where  $T$  is the current timestamp.

3. Generate a random number  $a$  and compute the pair  $(r_i, R_i)$  as follows:

$$r_i = g^a \text{ mod } p. \quad (10)$$

$$R_i = h(\theta_i \oplus r_i) \quad (11)$$

4. Encrypt  $(ID_i, r_i, U_C(x_i), v_i, T)$  with  $R_i$  and compute  $C_i$  as follows:

$$\begin{aligned} C_i &= \theta_i \oplus h(ID_i \oplus K_{x_i y_i}) \oplus h(PW_i^*) \oplus R_i \\ &= h(K_s) \oplus R_i \end{aligned} \quad (12)$$

5. Send the login message  $M_i = (C_i, E_{R_i}(ID_i, r_i, U_C(x_i), v_i, T), H_i, S_i, T)$  to the server.

### 3.3 Authentication phase

Upon receiving the login request  $M_i$ , the server performs the following operations.

1. Compute  $R_i = C_i \oplus h(K_s)$ , and decrypt  $E_{R_i}(ID_i, r_i, U_C(x_i), v_i, T)$  with  $R_i$ .
2. Check the validity of  $ID_i$ . If  $ID_i$  is invalid, the server rejects the login request.
3. Verify if the time interval  $(T' - T) \leq \Delta T$ , where  $T'$  is the current timestamp and  $\Delta T$  is the allowed time interval for transmission delay. If  $(T' - T) > \Delta T$ , the login request is considered out-of-date and is rejected.
4. Compute  $(v_i \oplus h(K_s))$ , which is denoted as  $y_i$ .
5. Compute the triple  $(K_{y_i x_i}, t, r')$  as follows:

$$K_{y_i x_i} = L_R(y_i) \times U_C(x_i) \quad (13)$$

$$t = h(ID_i \oplus K_{y_i x_i}) \quad (14)$$

$$r' = S_i \oplus T \oplus h(K_s) \oplus t \quad (15)$$

6. Verify if the following equation holds:

$$K_{x_i y_i} = H_i \oplus h(r') \quad (16)$$

If not, the server rejects the login request. Otherwise, it proceeds to the next step.

7. Generate a random number  $b$  and compute  $r_s$  as follows:

$$r_s = g^b \text{ mod } p. \quad (17)$$

8. Construct the authenticated session key  $AK_i$ :

$$AK_i = r_i^b = g^{ab} \text{ mod } p. \quad (18)$$

9. Send  $E_{R_i}(K_{y_i x_i} \oplus r_s, r_i + 1, T'')$  to the new user  $U_i$ .

After receiving the message  $E_{R_i}(K_{y_i x_i} \oplus r_s, r_i + 1, T'')$ , the new user  $U_i$  performs following operations:

1. Decrypt the message, obtain  $K_{y_i x_i} \oplus r_s$ , and verify whether  $(T''' - T'') \leq \Delta T$ , where  $T'''$  is the current timestamp. If so,  $U_i$  proceeds to the next step.
2. Check whether decrypted data contains the value  $r_i + 1$ . If so,  $U_i$  uses  $K_{x_i y_i}$  to compute  $r_s$  as follows:

$$r_s = (K_{y_i x_i} \oplus r_s) \oplus K_{x_i y_i} \quad (19)$$

3. Generate the authenticated session key  $AK_i$  as follows:

$$AK_i = r_s^a = g^{ba} = g^{ab} \pmod{p}. \quad (20)$$

Then  $U_i$  uses  $AK_i$  to communicate with the server.

### 3.4 Password-changing phase

When  $U_i$  wants to change his password  $PW_i$  to  $PW'_i$ , he sends the triple  $(ID_i, h(PW_i), h(PW'_i))$  to the server. As in the registration phase, these private data should be submitted in person or via a secure channel. Upon receiving the password-changing message, the server takes the following steps:

1. Compute  $\theta'_i$  as follows:

$$\begin{aligned} \theta'_i &= \theta_i \oplus h(PW_i) \oplus h(PW'_i) \\ &= h(ID_i \oplus K_{x_i y_i}) \oplus h(PW'_i) \oplus h(K_s) \end{aligned} \quad (21)$$

2. Replace  $\theta_i$  with  $\theta'_i$  in the smart card.

## 4 Analysis of our scheme

In this section, we analyze our scheme and show that our scheme can resist several well-known attacks. In addition, we provide a comparative study with other authentication schemes.

## 4.1 Correctness

According to equation (15), we first derive the equation as follows:

$$\begin{aligned}
r' &= S_i \oplus T \oplus h(K_s) \oplus t \\
&= \theta_i \oplus h(PW_i^*) \oplus r \oplus T \oplus h(K_s) \oplus t \\
&= h(ID_i \oplus K_{x_i y_i}) \oplus h(PW_i) \oplus h(K_s) \oplus h(PW_i^*) \oplus r \oplus T \oplus h(K_s) \oplus t \\
&= h(ID_i \oplus K_{x_i y_i}) \oplus r \oplus T \oplus t \\
&= h(ID_i \oplus K_{x_i y_i}) \oplus r \oplus T \oplus h(ID_i \oplus K_{y_i x_i}) \\
&= r \oplus T
\end{aligned} \tag{22}$$

Using equation (22), we verify equation (16) as follows:

$$\begin{aligned}
K_{x_i y_i} &= H_i \oplus h(r') \\
&= K_{x_i y_i} \oplus h(r \oplus T) \oplus h(r \oplus T) \\
&= K_{x_i y_i}
\end{aligned} \tag{23}$$

## 4.2 Security analysis

We now analyze the security properties of our scheme. We first introduce a few terms used in this paper [28].

**Definition 1.** *The discrete logarithm problem (DLP) is defined as follows: given a prime  $p$ , a generator  $g$  of  $Z_p^*$ , and an element  $\beta \in Z_p^*$ , find the integer  $\alpha$ ,  $0 \leq \alpha \leq p - 2$ , such that  $g^\alpha \equiv \beta \pmod{p}$ .*

**Definition 2.** *The Diffie-Hellman problem (DHP) is defined as follows: given a prime  $p$ , a generator  $g$  of  $Z_p^*$ , and elements  $g^c \pmod{p}$  and  $g^s \pmod{p}$ , find  $g^{cs} \pmod{p}$ .*

The security of the proposed scheme is based on the difficulty of DLP and DHP, which are believed infeasible to solve in polynomial time. We will show that our scheme can resist replay attack, forgery attack, insider attack, reflection attack, and parallel session attack. We will also analyze the following security properties: anonymity, mutual authentication, forward secrecy, and known-key security.

**Theorem 1.** *The proposed scheme can resist a replay attack.*

*Proof.* Assume an adversary eavesdrops the login message sent by  $U_i$  and uses it to impersonate  $U_i$  when logging into the system in a later session. However, the replay of  $U_i$ 's previous login message will be detected by the server since the user has already bound the timestamp  $T$  into the login message according to equation (8), and the server will verify the validity of the timestamp  $T$  used by  $U_i$ . Therefore, the adversary cannot replay the login message. However, there seems to be one potential security threat common to most existing timestamp-based user authentication schemes. That is, an adversary could impersonate a legitimate user by replaying that user's previous login message within the allowed time interval  $\Delta T$ . This threat can be solved by the additional requirement that  $T$  is not reused by  $U_i$  within  $\Delta T$ .  $\square$

**Theorem 2.** *The proposed scheme can resist a forgery attack.*

*Proof.* If the adversary wants to impersonate  $U_i$ , he has to create a valid login message  $(C_i^*, E_{R_i^*}(ID_i, r_i^*, U_C(x_i), v_i, T^*), H_i^*, S_i^*, T^*)$ , where  $T^*$  is the current timestamp. First he has to choose a random number  $r^*$  and compute the pair  $(H_i^*, S_i^*)$  as follows.

$$H_i^* = K_{x_i y_i} \oplus h(r^* \oplus T^*) \quad (24)$$

$$S_i^* = \theta_i \oplus h(PW_i) \oplus r^* \quad (25)$$

Because having no idea about  $K_{x_i y_i}$ ,  $\theta_i$ , and  $PW_i$ , the adversary cannot forge a valid login message and hence cannot launch a forgery attack.  $\square$

**Theorem 3.** *The proposed scheme can resist an insider attack.*

*Proof.* In our proposed scheme, when  $U_i$  wants to register with a server for remote-access services, he has to submit  $(ID_i, h(PW_i))$  instead of  $(ID_i, PW_i)$ , as in Pathan et al.'s schemes [17] [18]. Due to the employment of the one-way hash function  $h$ , it is considered practically impossible for the server to derive the user's password  $PW_i$  from the hashed value [29]. That is, even the server does not know  $PW_i$ . Obviously, the proposed scheme can prevent the insider attack.  $\square$

**Theorem 4.** *The proposed scheme can resist a reflection attack.*

*Proof.* A reflection attack is one in which, when a user sends a login message to a server, the adversary eavesdrops the message and sends it (or a modified version of the message) back to the user. In the proposed scheme, the adversary cannot fool the server since he has to know the server's secret key  $K_s$  in computing  $R_i$ , which is used to decrypt the ciphertext  $E_{R_i}(ID_i, r_i, U_C(x_i), v_i, T)$  sent by  $U_i$ . Therefore, it is ensured that our scheme can withstand the reflect attack.  $\square$

**Theorem 5.** *The proposed scheme can resist a parallel-session attack.*

*Proof.* In the proposed scheme, an adversary cannot impersonate a legitimate user by creating a valid login message in another on-going run from the honest run since the server's response message  $E_{R_i}(K_{y_i x_i} \oplus r_s, r_i + 1, T'')$  is encrypted with  $R_i$ , which is unknown to the adversary. Therefore, the proposed scheme can resist the parallel-session attack.  $\square$

**Theorem 6.** *The proposed scheme can provide user anonymity.*

*Proof.* If an adversary eavesdrops the login message, he cannot extract the user's identity from the ciphertext  $E_{R_i}(ID_i, r_i, U_C(x_i), v_i, T)$  since it is encrypted with  $R_i$ , which is unknown to the adversary. In addition, due to the use of the nonce and the timestamp in the login phase, the login messages submitted to the server are different in the login sessions. Hence, it is difficult for the adversary to discover a user's identity. Clearly, the proposed scheme can provide user anonymity.  $\square$

**Theorem 7.** *The proposed scheme can provide mutual authentication.*

*Proof.* The proposed scheme uses the Diffie-Hellman key exchange algorithm to achieve mutual authentication between the server and a user.  $U_i$  and the server securely exchange  $r_i$  and  $r_s$  in the login and authentication phases, respectively. As a result, the authenticated session key is established as follows:

$$AK_i = r_i^b = r_s^a = g^{ab} \pmod{p} \quad (26)$$

Therefore,  $U_i$  and the server can use the authenticated session key  $AK_i$  in subsequent communications.  $\square$

**Theorem 8.** *The proposed scheme can provide perfect forward secrecy.*

*Proof.* Perfect forward secrecy means that the disclosure of the long-term secret key material (e.g., server’s secret key  $K_s$  and user’s password  $PW_i$ ) does not compromise the secrecy of the agreed keys in earlier runs. In the proposed scheme, perfect forward secrecy is ensured since the Diffie-Hellman key exchange algorithm is used to establish the authenticated session key  $g^{ab}$ . Even if the adversary knows the server’s secret key  $K_s$ , he is only able to obtain  $g^a$  and  $g^b$  from earlier runs. However, based on the difficulty of the discrete logarithm problem and the Diffie-Hellman problem, it is computationally infeasible to compute the authenticated session key  $g^{ab}$  from  $g^a$  and  $g^b$ . Thus, our proposed scheme provides perfect forward secrecy.  $\square$

**Theorem 9.** *The proposed scheme can provide known-key security.*

*Proof.* Known-key security means that the compromise of a session key will not lead to further compromise of other secret keys or session keys. Even if a session key  $g^{ab}$  is revealed to an adversary, he still cannot derive other session keys since they are generated from the random numbers  $g^{a'}$  and  $g^{b'}$  based on Diffie-Hellman key exchange algorithm. Hence, the proposed scheme can achieve known-key security.  $\square$

### 4.3 Functionality

We summarize the functionality of our proposed scheme in this subsection. The crucial criteria in a user authentication scheme are listed below:

**C1.** *Freely chosen password:* A user can choose his password freely in the registration phase.

**C2.** *Mutual authentication:* The server and a user can authenticate each other.

**C3.** *User anonymity:* A user’s identity is protected when he logs into the system. No one knows the user’s identity except the server.

**C4.** *Session key agreement:* While mutual authentication is established between the server and a user, they can agree on a session key for use in subsequent com-

Table 2: Comparison of authentication schemes

	<b>C1</b>	<b>C2</b>	<b>C3</b>	<b>C4</b>	<b>C5</b>	<b>C6</b>
Our scheme	Yes	Yes	Yes	Yes	Yes	Yes
Pathan et al.(2007)	Yes	Yes	No	No	Yes	No
Hu et al.(2007)	Yes	Yes	Yes	Yes	No	Yes
Pathan et al.(2006)	Yes	Yes	No	No	Yes	Yes*
Chien and Chen(2005)	Yes	Yes*	Yes	Yes	No	No
Das et al.(2004)	Yes	No	Yes*	No	No	No
Juang(2004)	Yes	Yes	No	Yes	No	No
Chien et al.(2002)	Yes	Yes	No	No	No	No

C1: freely chosen password; C2: mutual authentication; C3: user anonymity; C4: session key agreement; C5: key separability; C6: secure password change.

Yes\*: Authors claimed such a security property but the property actually failed.

munications.

**C5. Key separability:** To avoid single-point failures, copies of the symmetric key matrix generated in the server can be stored in other servers.

**C6. Secure password change:** After the registration, a user can change his password freely.

We summarized the functionality of related authentication and key distribution protocols in Table 2.

#### 4.4 Efficiency analysis

Now we examine the performance of our proposed scheme. The evaluation parameters are defined in Table 3. The time requirement of the proposed scheme is summarized in Table 4. We use the computational overhead as the metrics to evaluate the performance of the proposed scheme.

## 5 Conclusions

In this paper, we present a bilateral user authentication scheme based on LU decomposition. The scheme can withstand well-known attacks and possesses many merits, including freely changeable passwords, mutual authentication, user

Table 3: Evaluation parameters

Symbol	Definition
$T_H$	Time for performing a one-way hash function
$T_M$	Time for performing a vector multiplication operation
$T_{XOR}$	Time for performing an XOR operation
$T_{EXP}$	Time for performing an exponentiation operation
$T_{ENC}$	Time for performing a symmetric encryption operation
$T_{DEC}$	Time for performing a symmetric decryption operation

Table 4: Performance of the proposed scheme

Phase	the server	a user
Registration	$1T_M + 2T_H + 4T_{XOR}$	$1T_H$
Login	—	$3T_H + 9T_{XOR} + 1T_{EXP} + 1T_{ENC}$
Authentication	$1T_M + 2T_H + 8T_{XOR} + 2T_{EXP} + 1T_{ENC} + 1T_{DEC}$	$2T_{XOR} + 1T_{DEC} + 1T_{EXP}$
Total	$2T_M + 4T_H + 12T_{XOR} + 2T_{EXP} + 1T_{ENC} + 1T_{DEC}$	$4T_H + 11T_{XOR} + 2T_{EXP} + 1T_{ENC} + 1T_{DEC}$

anonymity, session key agreement, and key separability. In addition, the proposed scheme is secure against replay attacks, forgery attacks, insider attacks, reflection attacks, and parallel session attacks. Moreover, compared with other authentication schemes, our scheme achieves more functionalities.

## References

- [1] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, Nov. 1981, pp. 770-772.
- [2] H. Y. Chien and C. C. Chen, "A remote authentication scheme preserving user anonymity," *In Proceedings of the IEEE International Conference on Advanced Information Networking and Applications (AINA '05)*, Mar. 2005, pp. 245-248.

- [3] Y. F. Chang, C. C. Chang, and Y. W. Su, "A secure improvement on the user-friendly remote authentication scheme with no time concurrency mechanism," *In Proceedings of the IEEE International Conference on Advanced Information Networking and Applications (AINA '06)*, vol. 2, Apr. 2006.
- [4] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers and Security*, vol. 21, no. 4, Aug. 2002, pp. 372-375.
- [5] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, May 2004, pp. 629-631.
- [6] C. L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 26, no. 3, May 2004, pp. 167-169.
- [7] C. L. Hsu, "A user friendly remote authentication scheme with smart cards against impersonation attacks," *Applied Mathematics and Computation*, vol. 170, no. 1, Nov. 2005, pp. 135-143.
- [8] L. Hu, Y. Yang, and X. Niu, "Improved remote user authentication scheme preserving user anonymity," *In Proceedings of the IEEE International Conference on Communication Networks and Services Research (CNSR '07)*, May 2007, pp. 323-328.
- [9] W. S. Juang, "Efficient password authenticated key agreement using smart cards," *Computers and Security*, vol. 23, no. 2, Mar. 2004, pp. 167-173.
- [10] W. C. Ku, H. M. Chuang, and M. J. Tsaur, "Vulnerabilities of Wu-Chieu's improved password authentication scheme using smart cards," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E88-A, no. 11, Nov. 2005, pp. 3241-3243.

- [11] W. C. Ku, S. T. Chang, H. H. Chen, and M. J. Tsaur, "Weakness and simple improvement of a password authentication scheme based on geometric approach," *In Proceedings of the IEEE Conference on Local Computer Networks (LCN '05)*, Nov. 2005, pp. 472-473.
- [12] K. W. Kim, J. C. Jeon, and K. Y. Yoo, "Efficient and secure password authentication schemes for low-power devices," *In Proceedings of International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2005)*, Dec. 2005, pp. 73-82.
- [13] S. W. Lee, H. S. Kim, and K. Y. Yoo, "Improvement of Chien et al.'s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 27, no. 2, Jan. 2005, pp. 181-183.
- [14] H. T. Liaw, J. F. Lin, and W. C. Wu, "An efficient and complete remote user authentication scheme using smart card," *Mathematical and Computer Modelling*, vol. 44, no. 1-2, Jul. 2006, pp. 223-228.
- [15] Y. Lee, J. Nam, S. Kim, and D. Won, "Two efficient and secure authentication schemes using smart cards," *In Proceedings of International Conference on Computational Science and its Applications (ICCSA 2006)*, May. 2006, pp. 858-866.
- [16] C. J. Mitchell and Q. Tang, "Security of the Lin-Lai smart card based user authentication scheme," *Technical Report*, RHUL-MA-2005-1, Royal Holloway, University of London, Jan. 2005.
- [17] A. K. Pathan and C. S. Hong, "An efficient bilateral remote user authentication scheme with smart cards," *In Proceedings of the 33rd Korea Information Science Society Fall Conference*, Oct. 2006, pp. 132-134.
- [18] A. K. Pathan, C. S. Hong, and T. Suda, "A novel and efficient bilateral remote user authentication scheme using smart cards," *In Proceedings of the IEEE*

- International Conference on Consumer Electronics (ICCE '07)*, Jan. 2007, pp. 1-2.
- [19] H. M. Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, Nov. 2000, pp. 958-961.
- [20] S. T. Wu and B. C. Chieu, "A user friendly remote authentication scheme with smart cards," *Computers and Security*, vol. 22, no. 6, Sept. 2003, pp. 547-550.
- [21] E. J. Yoon and K. Y. Yoo, "Robust secret key based authentication scheme using smart cards," *In Proceedings of Pacific Rim Conference on Multimedia (PCM 2005)*, Nov. 2005, pp. 723-734.
- [22] E. J. Yoon and K. Y. Yoo, "New authentication scheme based on a one-way hash function and Diffie-Hellman key exchange," *In Proceedings of International Conference on Cryptology and Network Security (CANS 2005)*, Dec. 2005, pp. 147-160.
- [23] S. J. Choi and H. Y. Youn, "A novel data encryption and distribution approach for high security and availability using LU decomposition," *In Proceedings of the International Conference on Computational Science and Its Applications (ICCSA '04)*, May 2004, pp. 637-646.
- [24] H. I. Hsiao and D. J. DeWitt, "A performance study of three high availability data replication strategies," *In Proceedings of the First International Conference on Parallel and Distributed Information Systems (ICPDIS)*, Dec. 1991, pp. 18-28.
- [25] D. D. E. Long, "A technique for managing mirrored disks," *In Proceedings of the IEEE International Conference on Performance, Computing, and Communications*, Apr. 2001, pp. 272-277.

- [26] J. Menon, J. Riegel, and J. Wyllie, "Algorithms for software and low-cost hardware RAIDS," *In Proceedings of the 40th IEEE Computer Society International Conference (COMPCON)*, Mar. 1995, pp. 411-418.
- [27] C. J. Zarowski, *An introduction to numerical analysis for electrical and computer engineers*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2004, pp. 148.
- [28] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1997.
- [29] B. Schneier, *Applied Cryptography*, John Wiley & Sons Inc. Publication, New York, second edition, 1996.