An Efficient Two-Pass Anonymous Identity Authentication Protocol Using a Smart Card

Jue-Sam Chou[1]*, Yalin Chen[2]

[1]Department of Information Management, Nanhua University Chiayi 622 Taiwan,
*: corresponding author, jschou@mail.nhu.edu.tw,
Tel: 886+ (0)5+272-1001 ext.56536
[2]Institute of information systems and applications, National Tsing Hua University
yalin78900@gmail.com

Abstract

Recently, Khan *et al*. proposed an enhancement of a remote authentication scheme designed by Wang *et al*., which emphasizes on using dynamic identity. They claimed that their improvement could avoid insider attacks. However, we found that the scheme lacks the anonymity property. Further, Madhusudhan *et al*. indicated that their scheme also suffers the insider attack. More recently, in 2013, there have been several studies on this field. Nevertheless, only Ding *et al*.'s scheme has the anonymity property, but it uses an unchanged RSA value whenever the same user logs in. This makes their scheme computationally intensive and traceable for a specific user, thus violating the eighth requirement in Liao *et al*.'s proposal. Inspired by this observation, in this paper, we propose a novel scheme that can anonymously authenticate a remote user with only two passes of very efficient hash and x-or operations. Moreover, this scheme satisfies all ten requirements (proposed by Liao *et al*.) of an authentication scheme using card.

Keywords: smart card, anonymity, insider attack, remote authentication, password-guessing attack

1. Introduction

Password-based authentication protocols are widely used for users logging into remote servers. If designed appropriately, they can provide authentication between the client and the server and thus ensure the legality of both parties. However, an attacker can compromise passwords after their long-time usage. Therefore, a designer usually accommodates such a scheme with password-changing function. There have been many protocols developed in this area [1–13, 15, 17–24, 26–30, 32–34, 37–40, 44], and several of these are as recent as 2013 [41–43]. However, other than the schemes in [6, 17, 22, 31, 39], which are anonymous, all the others in the literature do not satisfy three important properties simultaneously: (1) two passes to reduce the network traffic and increase system performance to be applied to specific circumstances, (2) anonymity, and (3) the ten security features proposed by Liao *et al*. [9]. Inspired by this observation, in this paper, we attempt to propose a scheme that satisfies all these three properties. In the scheme, the secret keys of both the user and the server are denoted as x and y, respectively, and are embedded in related parameters to fulfill the three properties. After various security analyses, we found that we can achieve the stated goal.

The rest of this paper is organized as follows. In Section 2, we review the weaknesses of Song, Khan *et al*., and Ding *et al*.'s schemes. Section 3 presents the proposed scheme. Section 4 analyzes its security, and Section 5 makes comparisons between our work and others in the literature, and briefly describes its applications. Finally, a conclusion is given in Section 6.

2. Weaknesses in Song, Khan et al., and Ding et al.'s schemes

In the following, we examine three protocols in this password authentication field. First, Song [37] claimed that their scheme is efficient and strong, but we found that the scheme is still vulnerable to a password-guessing attack if the card is lost. Second, Khan *et al*.'s scheme [1] concerns anonymous identity authentication. They emphasized that their schemes possess the demanded anonymity, but Madhusudhan *et al*. [34] found that Khan *et al*.'s scheme is susceptible to an insider attack. In addition, we also found that the scheme indeed cannot authenticate anonymously. Third, Ding *et al*. [39] claimed that their scheme is secure and efficient for practical applications, but we found that their scheme is traceable and not efficient enough. We describe the reasons briefly in the following. For more details (including the definitions of used notations), the reader can refer to the original articles.

- Song's scheme is vulnerable to a lost-smart-card password-guessing attack, and it also does not have anonymity. If an attacker obtains the card, he knows B_A. He can then guess the card holder's password PW_A as PW_A' and compute $K_A' = B_A \oplus h(PW_A')$. This can then be followed by a calculation of $R_A'' = D_{KA}'(W_A) \oplus T_A$ and a comparison of $h(ID_A \| R_A'' \| T_S)$ with C_S. If they are equal, then the attacker has guessed ID_A's password correctly.
- Khan *et al*.'s scheme is flawed because Madhusudhan *et al*. [34] indicated that it is susceptible to an insider attack. Moreover, we further found that an attacker can get AID_i from the transmitted message and thus can obtain the user's identity ID_i by

computing $ID_i = AID_i \oplus h(y \| T_i \| d)$ from the value y stored in the smart card. Therefore, their scheme is not anonymous.

- Ding *et al.*'s scheme [39] is traceable and not efficient enough because of its usage of an unchanged RSA value, C_1, which is computationally intensive. Therefore, their scheme is traceable for a specific user and not efficient enough.

3. Proposed Scheme

From the above mentioned, we know that there is no valid anonymous mutual authentication scheme in the literature, so we propose a novel one. Our scheme consists of three phases: a registration phase, a login and authentication phase, and a password change phase. In the following, we first define the notations we use and then describe the three phases.

U: user,
S: server,
ID_u: identity of U,
PW_u: password of U,
ID_s: identity of S,
x: U's secret value,
y: S's secret value,
N_s: random number selected by S,
T: timestamp,
$\|$: concatenation operation,
C_v: random number selected by U,
N_u: random number selected by the smart card,
PW_u': new password chosen by U in the password change phase,
pc: random number selected by U for changing the password,
h: collision free one-way hash function, mapping from $\{0,1\}^*$ to $\{0,1\}^n$.

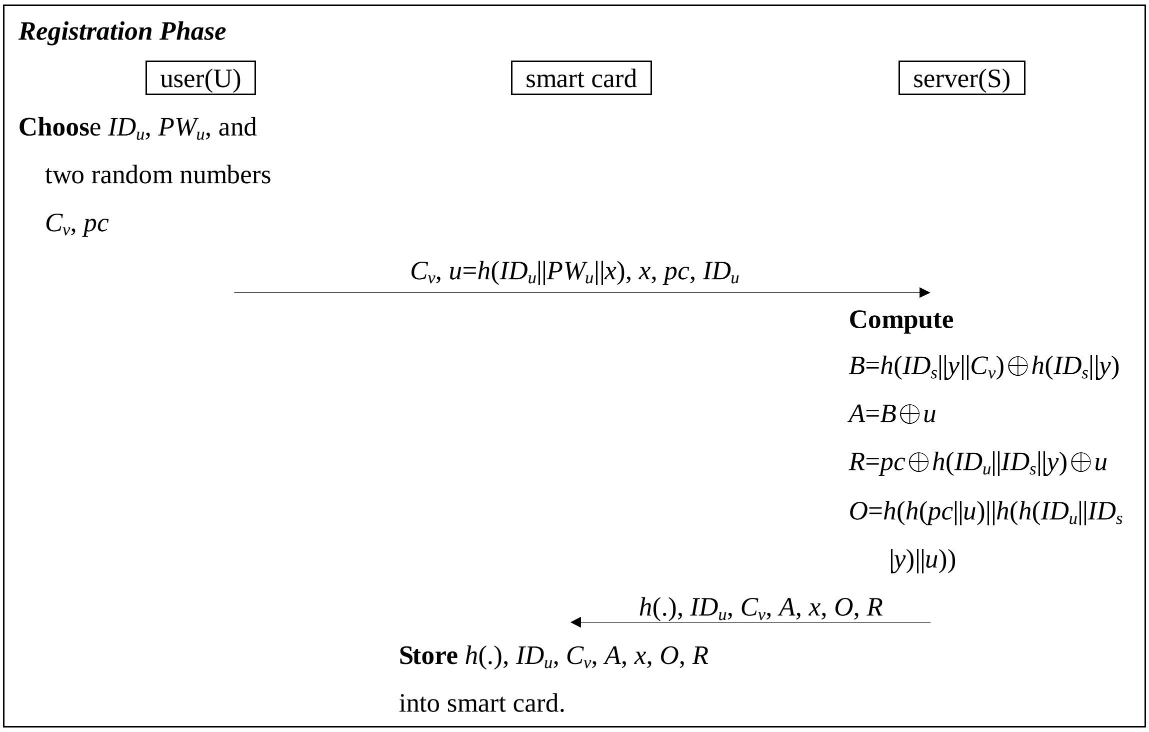
3.1 Registration Phase

In this phase, a user U carries out two steps to register with the server S in order to obtain a smart card:

Step 1. U chooses his ID_u, PW_u, and two random numbers, C_v and pc, and computes $u = h(ID_u \| PW_u \| x)$. He then sends $\{C_v, u, x, pc, ID_u\}$ to S through a secure channel.

Step 2. After receiving the message from U, S computes $B = h(ID_s \| y \| C_v) \oplus h(ID_s \| y)$, $A = B$ $(= h(ID_s \| y \| C_v) \oplus h(ID_s \| y)) \oplus u$ $(= h(ID_u \| PW_u \| x))$, $R = pc \oplus h(ID_u \| ID_s \| y) \oplus u$, and $O = h(h(pc \| u) \| h(h(ID_u \| ID_s \| y) \| u))$, and then stores $\{h(.), ID_u, C_v, A, x, O, R\}$ in the smart card. Later, U will use the parameters O and R in the password change phase if he wishes to.

The flowchart of the registration phase is shown in Figure 1.



Registration Phase

user(U)

smart card

server(S)

Choose ID_u, PW_u, and two random numbers C_v, pc

C_v, $u=h(ID_u||PW_u||x)$, x, pc, ID_u

Compute

$B=h(ID_s||y||C_v)\oplus h(ID_s||y)$

$A=B\oplus u$

$R=pc\oplus h(ID_u||ID_s||y)\oplus u$

$O=h(h(pc||u)||h(h(ID_u||ID_s||y)||u))$

$h(.)$, ID_u, C_v, A, x, O, R

Store $h(.)$, ID_u, C_v, A, x, O, R into smart card.

Figure 1: Registration phase

3.1 Login And Authentication Phase

When U wants to login into S, he first inserts his smart card and then executes the following steps together with S to allow mutual authentication.

Step 1. The smart card selects a random number N_u, computes $u = h(ID_u \,||\, PW_u \,||\, x)$ and $F = u \oplus N_u$, and acquires the current timestamp T from the system. It then computes $B = A \oplus u$, $N = h(N_u \,||\, u) \oplus ID_u$, $M = h(T \,||\, u \,||\, h(B \,||\, N))$, and $Q = h(u \,||\, h(N_u \,||\, u))$.

Step 2. U then sends the message $\{C_v, A, F, M, N, Q, T\}$ to S for authentication.

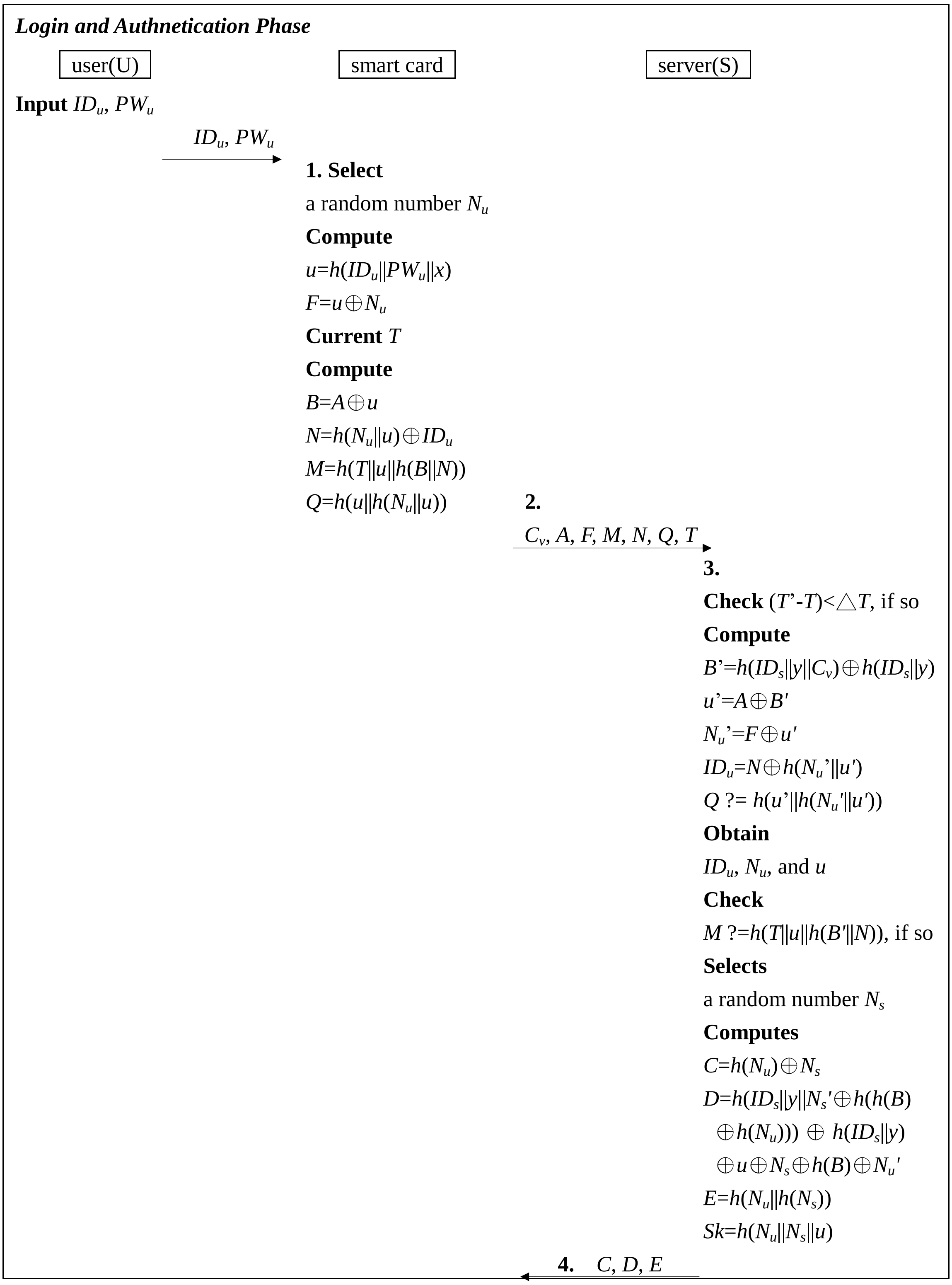
Step 3. S checks to see whether $(T' - T) > \Delta T$, where T' is the current system time. If so, S rejects the login request; otherwise, it computes $B' = h(ID_s \,||\, y \,||\, C_v) \oplus h(ID_s \,||\, y)$, $u' = A \oplus B'$, $N_u' = F \oplus u'$, $ID_u = N \oplus h(N_u' \,||\, u')$, and checks whether the equation $Q = h(u' \,||\, h(N_u' \,||\, u') \,||\, u'))$ holds. If it does, S confirms that the values of ID_u, N_u, and u are valid. It then checks whether equation $M = h(T \,||\, u \,||\, h(B' \,||\, N))$ holds. If it does, S selects a random number N_s and computes $C = h(N_u) \oplus N_s$, $D = h(ID_s \,||\, y \,||\, N_s) \oplus h(ID_s \,||\, y) \oplus u \oplus N_s$, $E = h(N_u \,||\, h(N_s))$, and session key $Sk = h(N_u \,||\, N_s \,||\, u)$.

Step 4. S sends the message $\{C, D, E\}$ to the smart card.

Step 5. Upon receiving the message from S, the smart card computes $N_s' = C \oplus h(N_u)$, and checks, whether $E = h(N_u \,||\, h(N_s'))$ holds. If it does, the smart card replaces A

and C_v by $D \oplus N_s' \oplus h(B) \oplus N_u$ and $N_s' \oplus h(B) \oplus h(N_u)$, respectively, for the next login, and then computes the common session key $Sk = h(N_u \| N_s' \| u)$. Now, U and S share the same session key, Sk.

The flowchart of the login and authentication phase is shown in Figure 2.



Login and Authnetication Phase

user(U)

smart card

server(S)

Input ID_u, PW_u

ID_u, PW_u →

1. Select
a random number N_u
Compute
$u=h(ID_u\|PW_u\|x)$
$F=u\oplus N_u$
Current T
Compute
$B=A\oplus u$
$N=h(N_u\|u)\oplus ID_u$
$M=h(T\|u\|h(B\|N))$
$Q=h(u\|h(N_u\|u))$

2.
C_v, A, F, M, N, Q, T →

3.
Check $(T'-T)<\triangle T$, if so
Compute
$B'=h(ID_s\|y\|C_v)\oplus h(ID_s\|y)$
$u'=A\oplus B'$
$N_u'=F\oplus u'$
$ID_u=N\oplus h(N_u'\|u')$
$Q \mathrel{?=} h(u'\|h(N_u'\|u'))$
Obtain
ID_u, N_u, and u
Check
$M \mathrel{?=} h(T\|u\|h(B'\|N))$, if so
Selects
a random number N_s
Computes
$C=h(N_u)\oplus N_s$
$D=h(ID_s\|y\|N_s'\oplus h(h(B)$
$\oplus h(N_u))) \oplus h(ID_s\|y)$
$\oplus u\oplus N_s\oplus h(B)\oplus N_u'$
$E=h(N_u\|h(N_s))$
$Sk=h(N_u\|N_s\|u)$

← **4.** C, D, E

5. Compute

$N_s'=C\oplus h(N_u)$

Check

E ?= $h(N_u||h(N_s'))$, if so,

Compute

$Sk=h(N_u||N_s'||u)$

/*For next login, the smart card updates A, C_v */

$A=D\oplus N_s'\oplus h(B)\oplus N_u$

$C_v=N_s'\oplus h(h(B)\oplus h(N_u))$

Figure 2: Login and authentication phase

3.3 Password Change Phase

When U wants to change his password from PW_u to PW_u', he performs the following steps.

Step 1. U inserts his smart card and inputs his ID_u, PW_u, the new password PW_u', and pc.

Step 2. The smart card computes $u = h(ID_u \,||\, PW_u \,||\, x)$, $h(ID_u \,||\, ID_s \,||\, y) = R \oplus pc \oplus u$, and checks to see whether $O = h(h(pc \,||\, u) \,||\, h(h(ID_u \,||\, ID_s \,||\, y) \,||\, u))$ holds. If it does, the smart card computes $u' = h(ID_u \,||\, PW_u' \,||\, x)$, $R' = pc \oplus h(ID_u \,||\, ID_s \,||\, y) \oplus u'$, $O' = h(h(pc \,||\, u') \,||\, h(h(ID_u \,||\, ID_s \,||\, y) \,||\, u'))$, and $A' = A \oplus h(ID_u \,||\, PW_u \,||\, x) \oplus h(ID_u \,||\, PW_u' \,||\, x)$, and then updates R, O, A as R', O', A', respectively.

The flow chart of the password change phase is shown in Figure 3.

Password Change Phase

user(U) smart card

1. ID_u, PW_u, PW_u', pc →

2. Compute

$u=h(ID_u||PW_u||x)$

$h(ID_u||ID_s||y)=R\oplus pc\oplus u$

Check

O ?= $h(h(pc||u)||h(h(ID_u||ID_s||y)||u))$, if so

Compute

$u'=h(ID_u||PW_u'||x)$

$R'=pc\oplus h(ID_u||ID_s||y)\oplus u'$

$O'=h(h(pc||u')||h(h(ID_u||ID_s||y)||u')$

$A'=A\oplus h(ID_u||PW_u||x)\oplus h(ID_u||PW_u'||x)$

updates R, O, A **with** R', O', A', **respectively**

Figure 3: Password change phase

4. Security analyses

In this section, we demonstrate that our scheme satisfies Liao *et al.'*s ten requirements [9] for a smart-card-based password authentication protocol.

- **Satisfying the ten security requirements (R1 through R10)**

R1. It requires no password or verifier tables.

Our scheme requires no verifier tables stored on the server's memory. Therefore, it meets this requirement.

R2. The user can choose and change his/her password at will.

In our scheme, a password change request can be accepted after the smart card has successfully authenticated the user. This guarantees that only the real card holder can safely and liberally change his password. In other words, our password change protocol lets the user choose and change his password freely and securely.

R3. The user needs not to reveal his/her password to the administrator of the server.

Obviously, the password is not revealed to the administrator of the server in either the login and authentication phase or the password change phase of our scheme.

R4. The password is not transmitted in plain text over the Internet.

As shown in Section 3, the password in our scheme is not transmitted in clear form. Therefore, our scheme satisfies this requirement.

R5. It can resist insider attacks.

An insider attack means that a legal user, J, can impersonate another user, U, to gain the service of server S. Suppose that J wants to impersonate U to login to S. Without the knowledge of U's password PW_u and $u(=h(ID_u||PW_u||x))$, he cannot deduce A, M, or Q to pass S' verification.

R6. It can resist the replay, password-guessing, modification-verifier-table, and stolen-verifier attacks.

Our scheme can resist the modification-verifier-table attack and stolen-verifier attack because it requires no verifier table. In addition, our scheme is robust against replay attacks because it chooses two fresh nonces, N_u and N_s, for each protocol run.

Additionally, an on-line password-guessing attack will fail because without the values ID_u, PW_u, *y*, and *x*, the attacker cannot compute *B* and *u*, which are required to generate the necessary parameters *A*, *F*, *M*, *N*, and *Q* to pass *S*' examinations.

R7. The length of a password is appropriate for memorization.

In our scheme, PW_u is included in $u = (ID_u \parallel PW_u \parallel x)$, and then used to generate parameters *A*, *F*, *M*, *N*, and *Q* in the message flow. Hence, our scheme's strength does not rely on the length of the password. The user, therefore, can choose a password of any length for easy memorization.

R8. It is efficient and practical.

Our scheme has the advantages that it simply demands two passes, requires no complex computation, and makes use of only hash functions and x-or operations. Therefore, our scheme is efficient and practical.

R9. It achieves mutual authentication.

Mutual authentication [14] means both the server and the user can confirm each other's identity before generating the common session key. In the following, we first demonstrate that our protocol can achieve this goal and then show that our scheme can resist the man-in-the-middle attack (MIMA).

(a) Mutual authentication:

In the login and authentication phase, to validate *U*, *S* has to verify the validity of *Q* and *M*, and *U* must check the validity of $E = h(N_u \parallel h(N_s'))$ to authenticate *S*. In other words, when both party complete validity checks on the corresponding parameters, they successfully authenticate each other.

(b) Man-In-the-Middle attack:

In the man-in-the-middle attack, an active attacker might intercept a communication between a legal user and the server and next use some means to successfully masquerade as both the server (to the user) and the user (to the server). The user will then believe that he is talking to the intended server, and vice versa.

We now describe what happens when an MIMA is launched on our protocol, as shown in Figure 4. In the figure, after having intercepted the communication between *S* and *U*, the attacker *AE* impersonates *U* by sending $\{C_v', A', F', M', N', Q', T'\}$ to *S* and masquerades as *S* by sending $\{C', D', E'\}$ to *U*. If *S* can successfully verify *Q*', *M*', and *U* can successfully confirm *E*', *AE* will then be regarded as authentic by both communicating parties and will have the two common session keys shared by U and S, respectively. However, in order to verify Q' and M', S should compute $Q' = h(u' \parallel h(N_u' \parallel u'))$, and $M' = h(T \parallel u \parallel h(B' \parallel N))$, where $u' = A \oplus B'$, $B' = h(ID_s \parallel y \parallel C_v)$. Without the knowledge of N_u, u, and y, AE cannot send valid Q' and M'. Similarly, to verify E', U should compute $E{=}h(N_u \parallel h(N_s'))$, where $N_s' = C \oplus h(N_u)$. However, without the knowledge of N_u and N_s, AE cannot send a genuine E'. Hence, the MIMA fails.

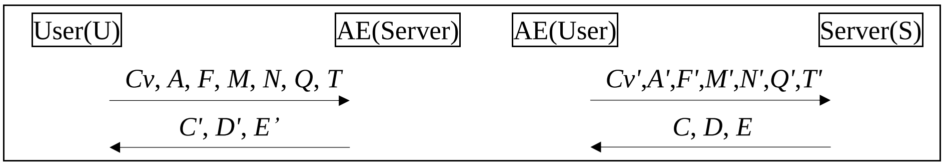


Figure 4: MIMA on our scheme as shown in Figure 1

R10. It resists password-guessing attacks, even if the smart card is lost.

In a lost-smart-card attack, an attacker AE can launch various attacks when he obtains a legal user’s smart card [23]. In the following, under such a situation, we discuss the most common attack—the offline password-guessing attack—to demonstrate that our scheme can resist such an attack. We show it in two cases: (1) U’s smart card is obtained by AE after registration, and (2) U’s smart card is obtained by AE after the login and authentication phase.

(1). Suppose that U’s smart card is obtained by AE after registration.

Although AE can read the stored values $\{h(\bullet), ID_u, C_v, A\ (= B \oplus u = h(ID_s \parallel y \parallel C_v)) \oplus h(ID_s \parallel y)) \oplus h(ID_u \parallel PW_u \parallel x)\ ), x, O, R\}$, he cannot, without the knowledge of $u = h(ID_u \parallel PW_u \parallel x)$, confirm whether his guessed password is correct. Therefore, he cannot launch an off-line password-guessing attack. For example, AE may guess a password PW_u as PW_{AE} and compute $h(ID_u \parallel PW_{AE} \parallel x)$; yet, without the knowledge of value u, AE cannot confirm the validity of his guess.

(2). Suppose U’s smart card is obtained by AE after the login and authentication phase.

As in the former case, AE cannot have any advantage in deducing any helpful result. Not to mention, C_v and A are further randomized in this case. From the preceding description, we conclude that such an attack by AE cannot succeed.

5. Comparisons and Applications

- **Comparisons**

In the following, we compare our scheme with other existing 2PAKE protocols [1, 3–6, 9, 11, 17, 21, 22, 26, 27, 29, 30–33, 35, 37, 39] in terms of both the number of required passes and whether the ten security features (STSF) proposed by Liao *et al*. are satisfied. The results are summarized in Table 1. For convenience, we use notations i(1)-[35] to denote the first improvement over [35].

Table 1. Comparison with some smart card password-based schemes in terms of passes and STSF

Schemes	i(1)-[35]	[1]	[3]	[4]	[5]	[6]	[9]	[11]	[17]	[21]	[22]
Passes	2	2	2	2	3	4	3	3	2	2	3
Anonymity	N	N	N	N	N	Y	N	N	Y	N	Y
STSF	Y	N	Y	Y	Y	N	N	N	N	N	N

Table 1- continued. Comparison with some smart card password-based schemes in terms of passes and STSF

Schemes	[26]	[27]	[29]	[30]	[31]	[32]	[33]	[37]	[39]	Ours
Passes	2	2	3	2	4	4	3	2	2	2
Anonymity	N	N	N	N	Y	N	N	N	Y	Y
STSF	N	N	N	N	N	Y	Y	N	N	Y

From Table 1, we conclude that our scheme outperforms the others in three aspects: passes, anonymity, and STSF.

- **Application: Smart Grid**

Based on our two-pass one-to-one (server-user) authentication protocol, (which not only meets Liao *et al.*'s ten requirements but also is more secure and efficient than other relevant works from the literature), in our future work, we will adapt and apply our scheme to a smart grid network. A smart grid network consists of multiple users (customers), electrical equipment, and one operation center. It is prone to security vulnerabilities and requires a large computational overhead [36]. Our work requires only hash and x-or operations. Therefore, it is well suited for adaptation and application in a smart grid network or future mobile communication networks, which may contain more servers than other networks to cope with multiple users.

6. Conclusion

This paper discussed the weaknesses of Khan *et al*., Song, and Ding *et al*.'s authentication protocols and then demonstrated our scheme, which satisfies the ten security requirements proposed by Liao *et al*. for remote user authentications; it was also shown that our scheme can prevent insider attacks and password-guessing attacks when a smart card is lost. Finally, we compared our scheme with other proposed works on the literature in terms of three factors: (1) the required number of passes, (2) ten security features, and (3) anonymity property. We concluded that our scheme outperforms the others. The single concern with our scheme is a denial-of-service (DOS) attack, which is a common attack for all the protocols discussed. However, our scheme uses only hash and x-or operations, and these are very efficient. To counter a DOS attack, we can further set the number of login users to some number. Therefore, our scheme is better suited than others for use in real implementations, such as smart grid or future mobile communication networks.

References

[1] Muhammad Khurram Khan, soo-Kyun Kim, Khaled Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'", Journal of Computer Communications, Vol. 6, No. 4, pp. 305-309, 2011.

[2] Daojing He, Maode Ma, Yan Zhang, Chun Chen, Jiajun Bu, "A Strong user authentication scheme with smart card for wireless communications", Journal of Computer Communications, Vol. 34, No. 3, pp. 367-374, 2011.

[3] Ronggong Song, "Advanced smart card based password authentication protocol", Journal of Computer Standards & Interfaces, Vol. 32, No. 5-6, pp. 321-325, 2010.

[4] Xiong Li, Jian-Wei Niu, Jian Ma, Wen-Dong Wang, Cheng-Lian Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications, Vol. 34, No. 1, pp. 73-79, 2011.

[5] Amit K. Awasthi, Keerti Srivastava, R.C. Mittal, "An improved timestamp-based remote user authentication scheme", Journal of Computers and Electrical Engineering, Vol. 37, No. 6, pp. 869-874, 2011.

[6] [6] SK. Hafizul Islam, G.p. Biswas, "A more efficient for secure ID- based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem", Journal of Systems and Software, Vol. 84, No. 11, pp. 1892-1898, 2011.

[7] Sandeep K. Sood, Anil K. Sarje, Kuldip Singh, "A secure dynamic identity based

authentication protocol for multi-server architecture", Journal of Network and Computer Applications, Vol. 34, No. 2, pp. 609-618, 2011.

[8] Hui Li, Chuan-Kun Wu, Jun Sun, "A general compiler for password-authentication group key exchange protocol", Journal of Information Processing Letters, Vol. 110, No. 4, pp. 160-167, 2010.

[9] I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang, "A password authentication scheme over insecure networks", Journal of Computer and System Sciences, Vol. 72, No. 4, pp. 727-740, 2006.

[10] J-Han Yang, Tian-Jie Cao, "Provably secure three-party password authenticated key exchange protocol in the standard model", The Journal of Systems and Software, Vol. 85, No. 2, pp. 340-350, 2012.

[11] Ren-Chiun Wang, Wen-Sheng Juang, Chin-Laung Lei, "Robust authentication and key agreement scheme preserving the privacy of secret key", Journal of Computer Communications, Vol. 34, No. 3, pp. 274-280, 2011.

[12] Junghyun Nam, Juryon Paik, Dongho Won, "A security weakness in Abdalla et al.'s generic construction of a group key exchange protocol", Journal of Information Science, Vol. 181, No. 1, pp. 234-238, 2011.

[13] Ting-Yi Chang, Min-Shiang Hwang, Wei-Pang Yang, "A communication- efficient three-party password authenticated key exchange protocol", Journal of Information Sciences, Vol. 181, No. 1, pp. 217-226, 2011.

[14] Yunho Lee, Seungjoo Kim, Domgho Won, "Enhancement of two- factor authemticated key exchange protocols in public wireless LANs", Journal of Computers and Electrical Engineering, Vol. 36, No. 31, pp. 213-223, 2010.

[15] Binod Vaidya, Jong Hyuk Parkm, Sang-Soo Yeo, Joel J.P.C. Rodrigues, "Robust one-time password authentication scheme using smart card for home network environment", Journal of Computer Communications, Vol. 34, No. 3, pp. 326-336, 2011.

[16] Qiang Tang, Liqun Chen, "Extended KCI attack against two-party key establishment protocols", Joutnal of Information Processing Letters, Vol. 111, No. 15, pp. 744-747, 2011.

[17] Kuo-Hui Yeh, Chunhua Su, N.W. Lo, Yingjiu Li, Yi-Xiang Hung, "Two robust remote user authentication protocols using smart cards", The Journal of Systems and Software, Vol. 83, No. 12, pp. 2556-2565, 2010.

[18] Jonathan Katz, Philip Mackenzie, Gelareh Taban, Virgil Gligor, "Two-server password-only authenticated key exchange", Journal of Computer and System Sciences, Vol. 78, No. 2, pp. 651-669, 2012.

[19] S.K. Hafizul Islam, G.P. Biswas, "Design of improved password authentication

and update scheme based on elliptic curve cryptography", Journal of Mathematical and Computer Modelling, 2010.

[20] Yi-Pin Liao, Shuenn-Shyang Wang, "A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves", Journal of Computer Communications, Vol. 33, No. 3, pp. 372-380, 2010.

[21] Tien-Ho Chen, Han-Cheng Hsiang, Wei-Kuan Shih, "Security enhancement on an improvement on two remote user authentication scheme using smart cards", Journal of Future Generation Computer Systems, Vol. 27, No. 4, pp. 377-380, 2011.

[22] Cheng-Chi Leem Tsung-Hung Lin, Rui-Xiang Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards", Journal of Expert Systems with Applications, Vol. 38, No. 11, pp. 13863-13870, 2011.

[23] Ren-Chiun Wang, Wen-Shenq Juang, Chin-Laung Lei, "Provably secure and efficient identification and key agreement protocol with user anonymity", Journal of Computer and System Sciences, Vol. 77, No. 4, pp. 790-798, 2011.

[24] Tian-Fu Lee, Tzonelih Hwang, "Simple password-based three-party authenticated key exchange without server public keys", Journal of Information Sciences, Vol. 180, No. 9, pp. 1702-1714, 2010.

[25] A.M. Rossudowski, H.S. Venter, J.H.P. Eloff, D.G. Kourie, "A security privacy aware architecture and protocol for a single smart card used for multiple services", ScienceDirect Computers & Security, Vol. 29, No. 4, pp. 393-409, 2010.

[26] Sang-Kyun Kim, Min Gyo Chung, "More secure remote user authentication scheme", Computer Communications, Vol. 32, No. 6, pp. 1018-1021, 2009.

[27] Yan-yan Wang, Jia-yong Liu, Feng-xia Xiao, Jing Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communications, Vol. 32, No. 4, pp. 583-585, March 2009.

[28] Xiong Li, Yongping Xiong, Jian Ma, Wendong Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards", Journal of Network and Computer Applications, Vol. 35, No. 2, pp. 763-769, 2012.

[29] Chun-TaLi, Min-ShiangHwang, "An efficient biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications, Vol. 33, No. 1, pp. 1-5, 2010.

[30] Han-Cheng Hsiang, Wei-Kuan Shih, "Weaknesses and improvements of the Yoon–Ryu–Yoo remote user authentication scheme using smart cards", Computer Communications, Vol. 32, No. 4, pp. 649-652, 2009.

[31] Chun-Ta Li, Cheng-Chi Lee, “A novel user authentication and privacy preserving scheme with smart cards for wireless communications”, Mathematical and Computer Modeling, Vol. 55, No. 1-2, pp. 35-44, 2012.

[32] Min-Shiang Hwang, Song-Kong Chong, Te-Yu Chen, “DoS-resistant ID-based password authentication scheme using smart cards”, Journal of Systems and Software, Vol. 83, No. 1, pp. 163-172, 2010.

[33] Hao-Rung Chung, Wei-Chi Ku, Maw-Jinn Tsaur, “Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments”, Computer Standards & Interfaces, Vol. 31, No. 4, pp. 863-868, 2009.

[34] R. Madhusudhan, R.C. Mittal, “Dynamic ID-based remote user password authentication schemes using smart cards: A review”, Journal of Networks and Computer Applications, Vol. 35, No. 4, pp. 1235-1248, 2012.

[35] Yalin Chen, Jue-Sam Chou, Chun-Hui Huang, “Improvements on two password-based authentication protocols”, http://eprint.iacr.org/2009/561 Cryptology ePrint Archive.

[36] R. Lu, X. Liang, X. Li, X. Lin, X. Shen, “EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications”, IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 9, 2012.

[37] R. Song, “Advanced smart card based password authentication protocol”, Computer Standards & Interfaces, Vol. 32, No. 5-6, 2010.

[38] Tsu-Yang Wu, Yuh-Min Tseng, “An efficient user authentication and key exchange protocol for mobile client–server environment”, Computer Networks, Vol. 54, No. 9, pp. 1520-1530, 2010.

[39] W. Ding and C.G. Ma,” Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards”, The Journal of China Universities of Posts and Telecommunications, Volume 19, Issue 5, October 2012, Pages 104–114.

[40] D. He, S., Wu , and J. Chen, ”note on 'design of improved password authentication and update scheme based on elliptic curve cryptography”, Mathematical and Computer Modelling, Vol. 55(3–4), Pages 1661– 1664, 2012.

[41] L. Gong, J. Pan, B. Liu, S. Zhao, “A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords”, Journal of Computer and System Sciences, Vol. 79 Issue 1, Pages 122-130, February, 2013

[42] S. H. Islam and G.P. Biswas, “Design of improved password authentication and update scheme based on elliptic curve cryptography”, Mathematical and Computer Modelling, Volume 57, Issues 11–12, June 2013, Pages 2703–2717.

[43] X. Li, J. Niu, M. Khurram Khan, J. Liao, “An enhanced smart card based remote user password authentication scheme ”, Journal of Network and Computer, Available online 5 March 2013.

[44] Q. Xie,”Improvement of a security enhanced one-time two-factor authentication and key agreement scheme”, Scientia Iranica, Vol. 19, Issue 6, December 2012, Pages 1856–1860.