A Secure Remote Authentication Scheme Preserving User Anonymity with Non-Tamper Resistant Smart Cards

WEN-BING HORNG[1], CHENG-PING LEE[2], and JIAN-WEN PENG[3]
[1,2]Department of Computer Science and Information Engineering
Tamkang University
151 Ying-Chuan Road, Tamsui, Taipei, Taiwan 25137
[3]Department of Commerce Automation and Management
Chihlee Institute of Technology
313, Section 1, Wunhua Road, Banciao, Taipei, Taiwan 22050
REPUBLIC OF CHINA
[1]horng@mail.tku.edu.tw, [2]89419038@s94.tku.edu.tw, [3]pchw8598@mail.chihlee.edu.tw

Abstract: - Anonymity is one of the important properties of remote authentication schemes to preserve user privacy. Besides, it can avoid unauthorized entities from using the user ID and other intercepted information to forge legal login messages. In 2004, Das et al. first proposed a remote user authentication scheme with smart cards using dynamic ID to protect user anonymity. Later, in 2005, Chien and Chen demonstrated that Das et al.'s scheme fails to preserve user anonymity and then presented a new scheme to remedy this problem. In 2007, Hu et al. pointed out that Chien-Chen's scheme cannot preserve user anonymity if the smart card is non-tamper resistant; i.e., the secret information stored in the smart card can be revealed. They then proposed an improved scheme to cope with this problem. In this paper, however, we will show that Hu et al.'s scheme still cannot preserve user anonymity under their assumption. In addition, their scheme is also vulnerable to the offline password guessing attack. We then present an improvement to overcome these weaknesses, while preserving all the merits of their scheme.

Key-Words: - Anonymity, non-tamper resistant, cryptanalysis, remote authentication, smart card.

1 Introduction

Remote user authentication is a mechanism for validating users' legitimacy to access the services provided by remote systems over an insecure network. Due to the convenience and the security of smart cards, plenty of remote user authentication schemes using smart cards have been proposed.

Of the proposed schemes, many of them [3, 4, 6, 9, 19, 22, 25, 27, 32, 33, 35–37] assume that the smart card is *tamper-resistant*; i.e., the secret information stored in the smart card cannot be revealed. However, recent research results [2, 11, 12, 20, 24, 30, 31] have shown that the secret data stored in the smart card could be extracted by some means, such as monitoring the power consumption or analyzing the leaked information. Therefore, such schemes based on the tamper-resistant assumption are vulnerable to some types of attacks, such as user-impersonation attacks, server-masquerading attacks, offline password guessing attacks, etc., once an adversary has obtained the secret information stored in a user's smart card and/or just some intermediate computational results in the smart card.

On the other hand, most of the proposed schemes [3, 5, 7, 8, 10, 13–17, 21, 23, 28, 29, 35] do not preserve *user anonymity*; i.e., the user's identity information, ID, is transmitted over an insecure public network in plaintext. Thus, it is possible for an adversary to intercept the user's ID easily along with other transmitted messages from the network to forge a legal login message. The leakage of the user ID may also cause an unauthorized entity to track the user's login history and current location [34]. Therefore, assuring anonymity does not only preserve user privacy but also make remote user authentication protocols more secure.

In 2004, Das et al. [6] first proposed a dynamic ID-based remote user authentication scheme with smart cards to protect user anonymity. The scheme allows users to choose their passwords freely and does not need any verification table in the remote server to validate users' legitimacy. However, Das et al.'s scheme does not provide session key exchange and mutual authentication, as reported in [1, 26, 27].

In 2005, Chien and Chen [4] pointed out that Das et al.'s scheme fails to protect user anonymity and

then presented a new scheme to cope with this weakness. The scheme preserves the merits of Das et al.'s scheme and offers the properties of mutual authentication, user anonymity, and session key agreement with perfect forward secrecy. Besides, it can also resist replay attacks, stolen-verifier attacks, and offline password guessing attacks.

Both of the above two schemes are based on the tamper-resistant assumption of the smart card. However, it is a challenge that the smart card is *non-tamper resistant* while preserving user anonymity. In 2007, Hu et al. [18] first showed that Chien-Chen's scheme is vulnerable to the strong masquerading server/user attack, if the smart card is no longer tamper-resistant; i.e., the secret information stored in the smart card can be extracted. Thus, the mutual authentication of Chien-Chen's scheme will not be achieved. In addition, Hu et al. also pointed out that Chien- Chen's scheme is subject to insider attacks, denial of service attacks, and restricted replay attacks as well. They then proposed an improved scheme to overcome these weaknesses to take such a challenge.

In this paper, however, we will show that Hu et al.'s scheme is still vulnerable to the strong masquerading server/user attack. In addition, their scheme is also vulnerable to the offline password guessing attack. We then propose an improvement over Hu et al.'s scheme to remedy their drawbacks, while preserving all the merits of their schemes. In summary, our scheme has the following advantages: (1) The server does not need password or verification tables for user validity checking. (2) Users can freely choose and change their own passwords. (3) Time synchronization is not needed between users and the server. (4) User anonymity is preserved. (5) Mutual authentication is supported. (6) Session key exchange with perfect forward secrecy is provided. (7) The scheme can resist various kinds of attacks, such as replay attacks, offline password guessing attacks, insider attacks, stolen verifier attacks, and masquerading server/user attacks, even if the smart card is non-tamper resistant; i.e., the secret information stored in the smart card can be extracted.

The rest of the paper is organized as follows. Section 2 briefly reviews Hu et al.'s scheme. Section 3 illustrates the security weaknesses of Hu et al.'s scheme. Our improved scheme is presented in Section 4, and its security analysis is given in Section 5. Finally, the paper is concluded in the last section.

2 Review of Hu et al.'s Scheme

In this section, we briefly review Hu et al.'s scheme. The security of the protocol is based on symmetric encryption/decryption and modular exponentiation to provide user anonymity and session key exchange. The scheme is composed of four phases: the registration, login, authentication, and password change phases. The notation used in Hu et al.'s scheme is listed below:

- U: the user
- ID: the identity of U
- PW: the password of U
- S: the remote system
- x: the secret key of S
- $h(\cdot)$: a secure one-way hash function
- $E_R[M]$: symmetric encryption of message M using secret key R
- N_s: the counter on the server's side
- N_u: the counter on the user's side
- p, g: the parameters of Diffie-Hellman key exchange protocol
- $\oplus$: the exclusive-OR (XOR) operation
- $\Rightarrow$: secure channel transfer
- $\rightarrow$: common channel transfer

Note that the counters N_s and N_u are set on the server's side and the user's side, respectively. They are synchronized normally, and their initial values are set to 0.

2.1 Registration phase

Whenever U initially registers or re-registers to S, the following steps are performed.

(R1) U selects his/her user identity ID, password PW, and a random number b, and then computes $h(b \oplus PW)$.
(R2) $U \Rightarrow S$: $\{ID, h(b \oplus PW)\}$.
(R3) If it is U's first registration, S sets $N_s = N_u = 0$ and stores ID and N_s in its account database. Otherwise, S updates the existing entry for U. Next, S computes $I = h(ID \oplus x)$, $M = I \oplus h(x)$, and $m = M \oplus h(b \oplus PW) = h(ID \oplus x) \oplus h(x) \oplus h(b \oplus PW)$.
(R4) $S \Rightarrow U$: S issues U a smart card containing ID, m, I, M, N_u, and the public parameters $\{h(\cdot), p, g\}$.
(R5) U enters and stores b into his/her smart card so that U does not need to remember b any more.

2.2 Login phase

Hu et al.'s scheme is shown in Fig. 1. If U wants to login to S, the following procedure is performed.

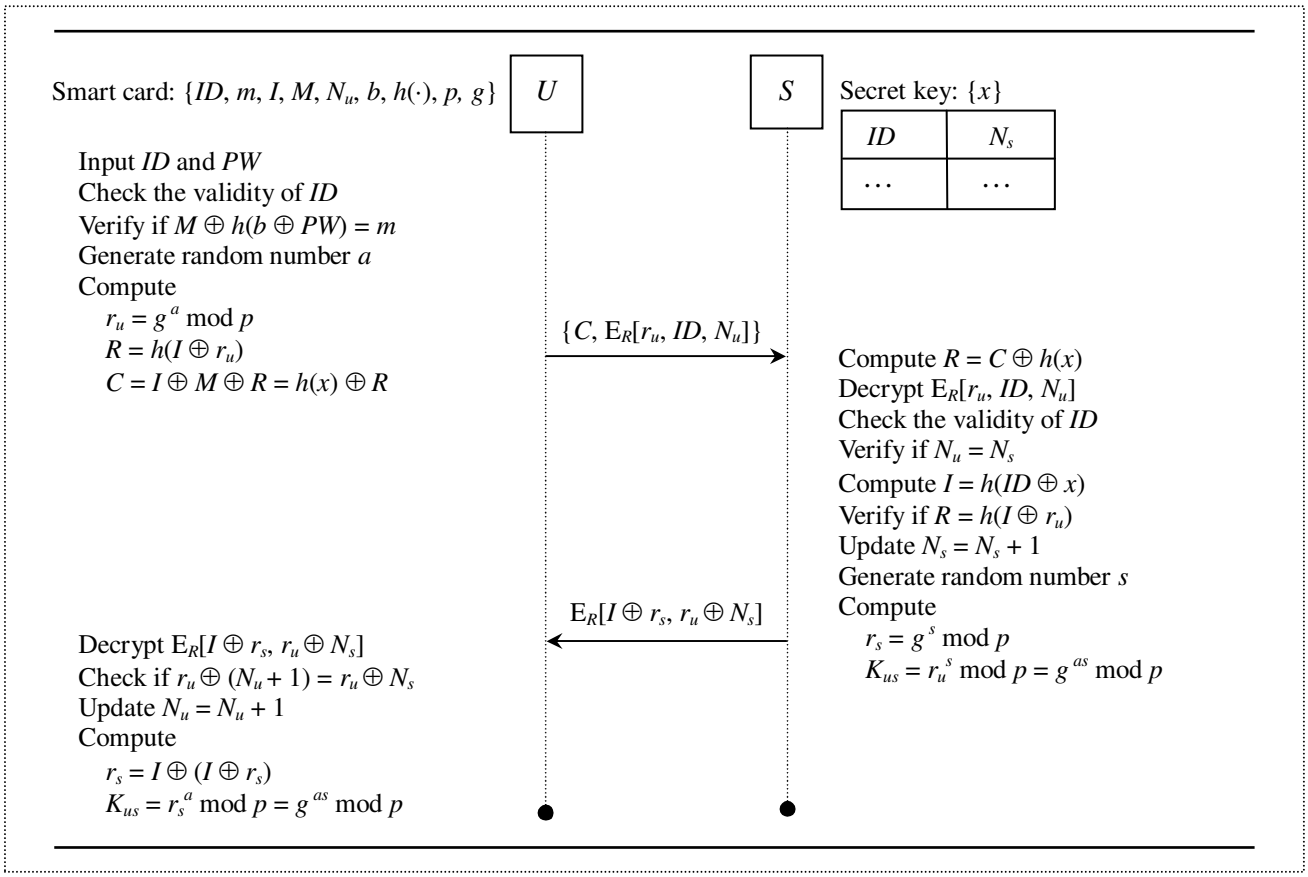

Fig. 1 Hu et al.'s authentication scheme

(L1) U inserts his/her smart card into the card reader of a terminal and inputs his/her ID and PW.

(L2) After checking the validity of the ID and verifying $M \oplus h(b \oplus PW)$ is equal to m, the smart card generates a random number a and then computes $r_u = g^a \bmod p$, $R = h(I \oplus r_u)$, and $C = I \oplus M \oplus R = h(x) \oplus R$.

(L3) $U \rightarrow S$: $\{C, E_R[r_u, ID, N_u]\}$, where $E_R[r_u, ID, N_u]$ is a ciphertext of $[r_u, ID, N_u]$ encrypted using the secret key R.

2.3 Authentication phase

After receiving U's login request message, the server S performs the following steps.

(A1) S computes $R = C \oplus h(x)$ and then decrypts the message $E_R[r_u, ID, N_u]$ using R to obtain the plaintext $[r_u, ID, N_u]$.

(A2) After checking the validity of the ID, S compares N_u with the corresponding N_s. If they are not equal, S gives a synchronization signal to U, and then U sends back an authentication request message to synchronize N_u with N_s.

(A3) The server S computes $I = h(ID \oplus x)$ and verifies whether R is equal to $h(I \oplus r_u)$. If they are equal, S accepts the login request and sets $N_s = N_s + 1$. Otherwise, S rejects the service request.

(A4) $S \rightarrow U$: $E_R[I \oplus r_s, r_u \oplus N_s]$, where $r_s = g^s \bmod p$ and s is a random number generated by S.

(A5) On receiving the reply message $E_R[I \oplus r_s, r_u \oplus N_s]$, U checks whether decrypted data contains the value $r_u \oplus (N_u + 1)$. If it does, U calculates $r_s = I \oplus (I \oplus r_s)$ and updates $N_u = N_u + 1$. Then, U and S can generate the session keys $K_{us} = r_s^a \bmod p = g^{as} \bmod p$ and $K_{us} = r_u^s \bmod p = g^{as} \bmod p$ for encrypting/decrypting subsequent transmitted messages.

2.4 Password change phase

If U wants to change his/her password PW with a new one PW^*, the following password change procedure is performed.

(P1) U first inserts his/her smart card into the card reader of a terminal for password changing.

(P2) The smart card checks whether $M \oplus h(b \oplus PW)$

equals the stored m. If they are equal, then the user U can enter his/her new password PW^*. Otherwise, the password change request is rejected.

(P3) U's smart card computes $m^* = m \oplus h(b \oplus PW) \oplus h(b \oplus PW^*) = M \oplus h(b \oplus PW^*)$, and then replaces m with m^*.

Because the password change procedure is performed only within U's smart card, U does not need to inform S.

3 Weaknesses of Hu et al.'s Scheme

In Hu et al.'s scheme, they assumed that the smart card is non-tamper resistant; that is, the secret data stored in the smart card can be revealed. Under this assumption, they claimed that their scheme could prevent (1) strong masquerading server/user attack, (2) insider attack, (3) denial of service attack, and (4) replay attack. Besides, the scheme can provide timely password verification and a secure password change phase.

In this section, however, we will show that Hu et al.'s scheme is still vulnerable to the strong masquerading server/user attack and, thus, fails to protect user anonymity. In addition, due to the early password verification mechanism, their scheme is subject to the offline password guessing attack, which causes the password change phase becoming insecure and is apt to the denial of service attack.

3.1 Strong masquerading server/user attack

A strong masquerading server/user attack means that if an adversary E has obtained the secret information stored in a legal user U's smart card or just some intermediate computational results, he/she can crash the mutual authentication scheme by masquerading as the server and/or other users. Hu et al. claimed that their scheme can resist such an attack. However, in the following, we will show that Hu et al.'s scheme is still vulnerable to the strong masquerading server/user attack by two possibilities: (1) legal users with their smart cards and (2) illegal users with stolen smart cards. Because of this, it fails to preserve user anonymity, one of the major security features the scheme was designed to support.

3.1.1 With legal smart cards

Assume that an adversary E is a legal user. He/she can derive $h(x)$ from the secret data M and I stored in his/her own smart card (i.e., $h(x) = M \oplus I$) or from the intermediate computational result R in the smart card and the intercepted C in the login request message (i.e., $h(x) = C \oplus R$). Note that only the legal user who enters the correct password PW can obtain the right intermediate computational value of R.

User impersonation attack: The adversary E can impersonate U as follows:

(1) Intercept a target user U's login request message $\{C, E_R[r_u, ID, N_u]\}$.
(2) Compute $R = C \oplus h(x)$.
(3) Decrypt $E_R[r_u, ID, N_u]$ using R. Then, U's ID is revealed. Hence, Hu et al.'s scheme fails to protect user anonymity.
(4) Whenever E wants to masquerade U, he can send a fake login request message $\{C, E_R[r_u, ID, N_u^*]\}$ to S with a proper N_u^*. It will pass the authentication process of S.

Note that the only thing E has to do is to verify the correctness of the counter N_u^*, because C, R, r_u, and ID can be replayed. E can update the new N_u^* by eavesdropping the communication between U and S. On the other hand, E can block all the transmissions between U and S to make sure that N_u^* can only be changed when E logins.

Server masquerading attack: To masquerade as S, the adversary E can perform the following steps:

(1) Intercept U's login request message $\{C, E_R[r_u, ID, N_u]\}$.
(2) Compute $R = C \oplus h(x)$.
(3) Intercept the reply message $E_R[I \oplus r_s, r_u \oplus N_s]$ from S and decrypt it using R to extract $I \oplus r_s$.
(4) Afterward, whenever U sends a new login request message $\{C', E_{R'}[r_u', ID, N_u']\}$, the adversary E intercepts and blocks it. Then, E can derive R' from $C' \oplus h(x)$ to obtain r_u', ID, and N_u' by decrypting $E_{R'}[r_u', ID, N_u']$.
(5) Finally, E can successfully impersonate S by sending $E_{R'}[I \oplus r_s, r_u' \oplus (N_u' + 1)]$ to the user U because $I \oplus r_s$ can be replayed.

3.1.2 With stolen smart cards

Suppose that the adversary E is not a legal user. He/she has stolen a user U's smart card. Then, he can extract ID, I, M, and N_u from U's smart card and compute $h(x) = M \oplus I$. Note that since E is not a legal user, he has no way to obtain the intermediate computational result R unless he knows the correct password PW. (However, in Section 3.2, we will show that Hu et al.'s scheme is vulnerable to the offline password guessing attack.)

User impersonation attack: The adversary E can masquerade as U as follows.

(1) Generate a random number e and compute $r_e = g^e \bmod p$.
(2) Compute $R = h(I \oplus r_e)$ and $C = h(x) \oplus R$.
(3) Send the forged login request message $\{C, E_R[r_e, ID, N_u]\}$ to S. The forged message will successfully pass the verification process performed on S. Moreover, E and S will derive the same session key $K_{es} = g^{es} \bmod p$.

Server masquerading attack: If E returns the smart card back to U, E can masquerade as S as follows:

(1) When U sends a login request message $\{C, E_R[r_u, ID, N_u]\}$, E intercepts and blocks it.
(2) Compute $R = C \oplus h(x)$.
(3) Decrypt $E_R[r_u, ID, N_u]$ using R.
(4) Generate a random number e and compute $r_e = g^e \bmod p$.
(5) Send U the forged reply message $E_R[I \oplus r_e, r_u \oplus (N_u + 1)]$. The message will pass the authentication of U.
(6) E and U can both derive the session key $K_{ue} = g^{ae} \bmod p$.

3.2 Offline password guessing attack

A remote user authentication scheme vulnerable to the offline password guessing attack must satisfy the following two conditions:

- the user's password is weak, and
- there exists a piece of password-related information used as a comparison target for password guessing.

In Hu et al.'s scheme, a user is allowed to choose his own password at will during the registration and password change phases; the user usually tends to select a password that is easily remembered for his convenience. Hence, these easy-to-remember passwords, called *weak passwords*, are potentially vulnerable to the password guessing attack, in which an adversary can try to guess the user's password from a dictionary of all possible weak passwords and then verify his guess.

On the other hand, Hu et al.'s scheme provides a timely password verification mechanism during the login phase as well as the password change phase to detect wrong password earlier, without the help from the server. The input password PW is verified by checking whether $M \oplus h(b \oplus PW)$ is equal to m stored in the smart card. However, if an adversary E has stolen U's smart card, he can perform the following procedure to guess U's password.

(1) Extract the secret data m, b, and M in U's smart card.
(2) Guess a password PW^* from a dictionary and check whether $M \oplus h(b \oplus PW^*)$ is equal to m. If they are equal, the correct password is PW^*. Otherwise, select another password and repeat the above process until a correct password is found.

Once the correct password is obtained, the adversary can change the password to a new one. This causes the password change phase becoming insecure. Moreover, if the adversary returns to the changed smart card to the original user U, then U cannot login to the remote server S. This leads to the denial of service attack.

4 Our Proposed Scheme

In this section, we present an enhancement over Hu et al.'s scheme to remedy their security flaws (i.e., vulnerabilities to the strong masquerading server/ user attack and the offline password guessing attack) while preserving user anonymity and other merits. Our scheme includes four different phases: the registration, login, authentication, and password change phases.

4.1 Registration phase

This phase is invoked whenever a user U initially registers to the remote server S. The following steps are performed:

(R1) The user U first chooses his/her identity ID, password PW, and a random number b.
(R2) $U \Rightarrow S$: $\{ID, h(b \| PW)\}$.
(R3) S computes
$W = h(ID \| x) \oplus h(b \| PW)$ and
$w = g^{h(ID \| x)\ h(x)} \bmod p$,
where x is the secret key of S.
(R4) $S \Rightarrow U$: a smart card containing W, w, and the public parameters $\{h(\cdot), p, g\}$.
(R5) After receiving the smart card from S, U inputs b into his/her smart card so that he/she does not need to remember b any more.

4.2 Login phase

Our scheme is shown in Fig. 2. When U wants to login to S, he/she inserts his/her smart card into the card reader of a terminal and inputs his/her ID and PW. Then, the smart card performs the following

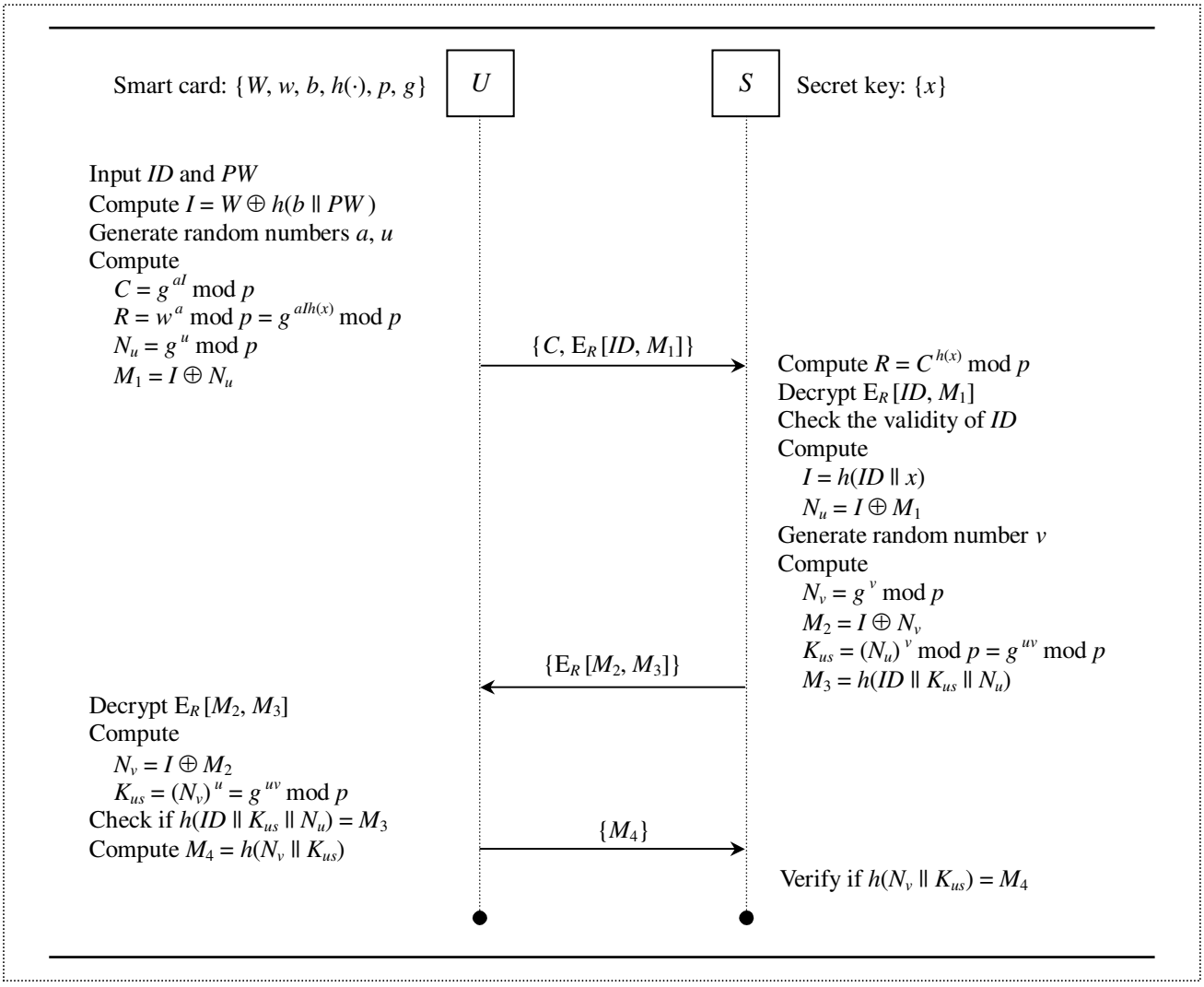

Fig. 2 Our proposed scheme

steps for login:

(L1) Compute $I = W \oplus h(b \| PW) = h(ID \| x)$.
(L2) Generate random numbers a and u, both of which are not 0.
(L3) Compute
$C = g^{aI} \bmod p$,
$R = w^a \bmod p = g^{aIh(x)} \bmod p$,
$N_u = g^u \bmod p$, and
$M_1 = I \oplus N_u$.
(L4) $U \rightarrow S$: $\{C, E_R[ID, M_1]\}$, where the $E_R[ID, M_1]$ is a ciphertext of $[ID, M_1]$ encrypted by using the generated one-time secret key R.

4.3 Authentication phase

On receiving the login request message from U, S performs the following steps:

(A1) Compute $R = C^{h(x)} \bmod p = g^{aIh(x)} \bmod p$, and then decrypt the message $E_R[ID, M_1]$ to obtain ID and M_1.
(A2) Check the validity of ID. If it is not valid, reject the login request.
(A3) Compute $I = h(ID \| x)$ and $N_u = I \oplus M_1$.
(A4) Generate a random number $v \neq 0$ and compute
$N_v = g^v \bmod p$,
$M_2 = I \oplus N_v$,
$K_{us} = (N_u)^v \bmod p = g^{uv} \bmod p$, and
$M_3 = h(ID \| K_{us} \| N_u)$,
where K_{us} is the session key.
(A5) $S \rightarrow U$: $\{E_R[M_2, M_3]\}$.

On receiving the reply message $E_R[M_2, M_3]$ from S, the smart card performs the following steps to authenticate S:

(A6) Decrypt $E_R[M_2, M_3]$ with R to obtain $[M_2, M_3]$.
(A7) Compute $N_v = I \oplus M_2$ and the session key $K_{us} = (N_v)^u \bmod p = g^{uv} \bmod p$. Check if $h(ID \|$

$K_{us} \| N_u$) equals M_3. If they are not equal, terminate the session.

(A8) $U \rightarrow S$: $\{M_4\}$, where $M_4 = h(N_v \| K_{us})$.

On receiving the message M_4 from U, the server S performs the following steps to authenticate U:

(A9) Check if $h(N_v \| K_{us})$ is equal to M_4. If it is, the authentication is complete.

4.4 Password change phase

If U wants to change his/her password, he/she inserts his/her smart card into the card reader of a terminal and inputs his/her ID and PW. Then, a mutual authentication between the server and the smart card is first performed as described above (steps (L1) to (L4) and (A1) to (A9)). Once the authentication is complete, the smart card proceeds as follows to change the password:

(P1) Ask U to enter a new password PW^*.

(P2) Compute $W^* = h(ID \| x) \oplus h(b \| PW^*)$ and replace W with W^*.

5 Security Analysis

The security of our proposed authentication scheme is based on the secure hash function, symmetric encryption/decryption, and the discrete logarithm problem. In this section, we analyze the security features our scheme provides.

5.1 User anonymity

To preserve user anonymity, user's ID will not be sent to the remote server in plaintext form over an insecure network. In both Hu et al.'s [18] and our scheme, ID is encrypted by the one-time secret key R. However, the server S has to derive R without knowing which user sends the login request message since ID is unknown. Thus, S must store some secret parameters in user's smart card to compute R such that it can easily derive R from the login request message of the anonymous user U.

For example, in both Chien-Chen's scheme [4] and Hu et al.'s scheme [18], the server S stores some parameters derived from $h(x)$ in U's smart card such that the smart card can easily compute $C = R \oplus h(x)$ from these parameters. The smart card can then encrypt U's ID and other authentication information using the secret key R along with C in the login request message. Upon receiving this anonymous login message, S can easily use $h(x)$ to obtain the secret key $R = C \oplus h(x)$ to decrypt the ciphertext in the login message without knowing ID.

However, recent research results [2, 11, 12, 20, 24, 30, 31] have shown that the secret information stored in the smart card could be extracted by some means. Therefore, if an adversary has obtained the secret information stored in the smart card or just some intermediate computational results, he/she might derive the secret key R. Once R is obtained, the adversary can use it to decrypt the ciphertext (such as $E_R[r_u, ID, T]$ in Chien-Chen's scheme [4] and $E_R[r_u, ID, N_u]$ in Hu et al.'s scheme [18]) in the login request message to discover ID.

To cope with this problem, the secret key R must not be derived from the secret information stored in the smart card. In our scheme, if an adversary E is a legal user, he/she can only know $W_E = h(ID_E \| x) \oplus h(b_E \| PW_E)$ and $w_E = g^{h(ID_E \| x)h(x)} \bmod p$ from his/her own smart card. It is computational infeasible for E to derive x from W_E, even if ID_E, PW_E, and b_E are known to the adversary E; this is due to the properties of one-way and collision resistance of the secure hash function $h(\cdot)$. On the other hand, it is computationally infeasible to derive $h(x)$ from w_E, even if $h(ID_E \| x)$, p, and g are known to E; this is because of the difficulty of the discrete logarithm problem in the modular exponentiation.

Similarly, if E is a legal user who can obtain the immediate computational result C_E and R_E from his/her own smart card, it is computationally infeasible for E to derive $h(x)$ from the formula $R_E = C_E^{h(x)} \bmod p$ owing to the discrete logarithm problem. Likewise, if E has obtained another user U's secret data, W and w, stored in U's smart card, it is computationally infeasible for E to derive x and $h(x)$ from W and w.

In our scheme, the user's ID is encrypted by $R = g^{aIh(x)} \bmod p = C^{h(x)} \bmod p$ in the login request message $\{C, E_R[ID, M_1]\}$, where x is a secret key of S, a is a random number generated by the smart card which is different at each login session, and $I = h(ID \| x)$. When E intercepts another user U's login request message $\{C, E_R[ID, M_1]\}$ from the network, there is no way for him/her to derive the secret key R to decrypt $E_R[ID, M_1]$ since E does not know a, $h(x)$, and I. Therefore, user anonymity is protected in our scheme.

5.2 Resistance to user impersonation attack

To impersonate a user U, an adversary E must fake a login request message $\{C, E_R[ID, M_1]\}$ and a reply message $\{M_4\}$ to deceive the server S. For the login message, since E does not know U's ID (as shown in Section 5.1), E cannot impersonate U by forging a

correct login request message.

On the other hand, E can replay a legal login request message previously sent by U. However, he still needs to forge $M_4 = h(N_v \| K_{us})$ to pass the authentication of S. This means that E has to extract N_v computed by S. As shown in Section 5.1, it is computationally infeasible for E to derive the one-time secret key $R = C^{h(x)} \bmod p$ from the intercepted C from the network to decrypt the ciphertext $E_R[M_2, M_3]$ transmitted over the network. Furthermore, without knowing I, E cannot derive $N_v = I \oplus M_2$, and thus E cannot forge M_4. Therefore, to impersonate user U is impossible.

5.3 Resistance to server spoofing attack

To masquerade as the server S, an adversary E has to send U a forged replay message $E_R[M_2, M_3]$ after receiving U's login request message $\{C, E_R[ID, M_1]\}$. As demonstrated in Section 5.1, E cannot derive R to decrypt the intercepted ciphertext $E_R[ID, M_1]$ to obtain ID and M_1. Without knowing M_1 and I, E cannot extract the correct value of $N_u = I \oplus M_1$. Therefore, E cannot compute the session key $K_{us} = (N_u)^v \bmod p$, where v is a random number which could be faked by E. Furthermore, because E does not know ID, K_{us}, and N_u, he/she cannot compute proper $M_3 = h(ID \| K_{us} \| N_u)$ to pass the authentication of U. Hence, our scheme can resist the masquerading server attack.

5.4 Resistance to offline password guessing attack

In Hu et al.'s scheme, they provided a timely password verification mechanism for wrong password detection in the login and password change phases by comparing whether $M \oplus h(b \oplus PW)$ is equal to m stored in the smart card. Because M, b, and m can be extracted from the smart card, it will suffer from offline password guessing attacks.

In our scheme, we do not use such an early password verification mechanism to detect wrong passwords. Instead, we need the help from the server to verify whether the input password is correct or not. As demonstrated in Section 5.1, an adversary E cannot derive x, $h(x)$, and ID. If the secret values (such as W, w, b) stored in the smart card were revealed, without knowing x or ID, it is computational infeasible to derive PW from $W = h(ID \| x) \oplus h(b \| PW)$ due to the one-way property of the secure hash function. Therefore, the offline password guessing attack is impossible to launch in our scheme.

5.5 Mutual authentication

In our scheme, a user U's smart card stores two shared secrets $W = h(ID \| x) \oplus h(b \| PW)$ and $w = g^{h(ID \| x)\ h(x)} \bmod p$. To authenticate U, the server S will validate both $E_R[ID, M_1]$ and M_4 sent from U. In Section 5.1, we have shown that our scheme can preserve user anonymity, so ID is only known to the server S and the user U itself. In Section 5.2, we have indicated that our scheme can resist user impersonation attacks; it is impossible for E to forge messages to masquerade as U in our scheme. To pass the authentication of S, the smart card needs U's password PW to calculate C and M_1 in the login phase. In Section 5.4, we have shown that our scheme can resist offline password guessing attacks. Besides, there is no password or verification table in S such that U's password could be stolen. In addition, the smart card needs U's ID to produce the correct ciphertext $E_R[ID, M_1]$. Therefore, only the legal user U who owns correct ID and PW can pass the authentication of S.

On the other hand, the user U authenticates S by checking the ciphertext $E_R[M_2, M_3]$ from S. In Section 5.3, it has been shown that it is impossible for E to forge $E_R[M_2, M_3]$ to masquerade as S. Only the legal server S who owns the secret key x can derive the correct $R = C^{h(x)} \bmod p$ to decrypt the login request message $E_R[ID, M_1]$ from U. Then, S can compute the proper $E_R[M_2, M_3]$ after obtaining U's ID and N_u, where $N_u = g^u \bmod p$ contains a fresh nonce u generated by U's smart card.

From the above analysis, we conclude that our scheme can achieve mutual authentication.

5.6 Secure session key agreement with perfect forward secrecy

An authentication scheme with perfect forward secrecy assures that even if a user U's password is compromised, it will never reveal any session keys used before. In this case, if an adversary E knows U's password PW, he/she can derive $I = W \oplus h(b \| PW) = h(ID \| x)$ from U's smart card in our scheme.

In addition, our scheme also provides a session key exchange during the verification phase between the user U and the server S. Both of them calculate the session key $K_{us} = (N_v)^u \bmod p = (N_u)^v \bmod p = g^{uv} \bmod p$ by using N_u and N_v, respectively, where u and v are random numbers. U's smart card and S keep u and v private, respectively, at each session. An adversary has no way to obtain them. However, both N_u and N_v are protected in $M_1 = I \oplus N_u$ and $M_2 = I \oplus N_v$ and encrypted by the one-time secret key R during transmissions. To obtain N_u and N_v, the

Table 1 Comparison of security features

Security Feature	Hu et al.'s Scheme	Our Scheme
Withstanding masquerading server attack	No	Yes
Withstanding masquerading user attack	No	Yes
Withstanding offline password guessing attack	No	Yes
Preserving user anonymity	No	Yes
Mutual authentication	No	Yes
Session key exchange	Yes	Yes
Perfect forward secrecy	Yes	Yes
No time synchronization	Yes	Yes

adversary E needs R to decrypt $E_R[ID, M_1]$ and $E_R[M_2, M_3]$ to compute $N_u = I \oplus M_1$ and $N_v = I \oplus M_2$, where I is known to E. As shown in Section 5.1, there is no way for E to derive the secret key R. Even if E has obtained N_u and N_v, it is impossible for him/her to derive u and v because of the discrete logarithm problem; thus, it is impossible to derive the session key K_{us}. Furthermore, due to the Diffie-Hellman assumption, it is computational infeasible for E to derive K_{us} from N_u and N_v. Therefore, our scheme provides the property of perfect forward secrecy.

Table 1 gives a comparison of the security features of our scheme and Hu et al.'s scheme.

6 Conclusion

It is a challenge that using non-tamper resistant smart cards to preserve user anonymity in a remote user authentication protocol. In 2007, Hu et al.'s first proposed an authentication scheme to meet this requirement. However, in this paper, we have demonstrated that Hu et al.'s scheme is vulnerable to the masquerading server/user attack and the offline password guessing attack. In addition, their scheme also fails to preserve user anonymity. In this paper, we proposed an improved scheme to overcome these weaknesses, while preserving all their merits, even if the secret information stored in the smart card is leaked.

References:

[1] A.K. Awasthi, Comment on 'a dynamic ID-based remote user authentication scheme', *Transaction on Cryptology*, Vol. 1, No. 2, 2004, pp. 15-17.

[2] E. Brier, C. Clavier, and F. Oliver, Correlation power analysis with a leakage model, *Lecture Notes in Computer Science,* Vol. 3156, 2004, pp. 135-152.

[3] Y.C. Chen, and L.Y. Yeh, An efficient nonce-based authentication scheme with key agreement, *Applied Mathematics and Computation*, Vol. 169, No. 2, 2005, pp. 982-994.

[4] H.Y. Chien and C.H. Chen, A remote authentication scheme preserving user anonymity, *IEEE International Conference on Advanced Information Networking and Applications*, Vol. 2, 2005, pp. 245-248.

[5] H.R. Chung, W.C. Ku, and M.J. Tsaur, Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments, *Computer Standards & Interface*, Vol. 31, No. 4, 2009, pp. 863-868.

[6] 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, 2004, pp. 629-631.

[7] M.L. Das, A. Saxena, V. Gulati, and D. Phatak, A novel remote user authentication scheme using bilinear pairings, *Computers & Security*, Vol. 25, No. 3, 2006, pp. 184-189.

[8] M.L. Das, V.L. Narasimhan, A simple and secure authentication and key establishment protocol, *First International Conference on Emerging Trends in Engineering and Technology*, 2008, pp. 844-849.

[9] M.L. Das and V.L. Narasimhan, EARS: efficient entity authentication in remote systems, *Fifth International Conference on Information Technology: New Generations*, 2008, pp. 603-608.

[10] C.I. Fan, Y.C, Chan, and Z.K. Zhang, Robust remote authentication scheme with smart cards, *Computer & Security*, Vol. 24, No. 8, 2005, pp. 619-628.

[11] Y. Han, X. Zou, Z. Liu, and Y. Chen, Improved differential power analysis attacks on AES hardware implementations, *International Conference on Wireless Communications, Networking and Mobile Computing*, 2007, pp. 2230-2233.

[12] N. Hanley, R. McEvoy, M. Tunstall, C. Whelan, C. Murphy, and W.P. Marnane, Correlation power analysis of large word sizes, *Irish Signals and Systems Conference*, 2007.

[13] M. Holbl and T. Welzer, Cryptanalysis and improvement of an 'improved remote authentication scheme with smart card', *Third International Conference on Availability, Reliability and Security*, 2008, pp. 1301-1305.

[14] W.B. Horng and C.P. Lee, Improvement of

Wang-Li's forward-secure user authentication scheme with smart cards, *Eighth International Conference on Intelligent System Design and Applications*, 2008, pp. 297-302.

[15] H.C. Hsiang and W.K. Shih, Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards, *Computer Communications*, Vol. 32, No. 4, 2009, pp. 649-652.

[16] H.C. Hsiang and W.K. Shih, A secure remote mutual authentication and key agreement without smart cards, *Information Technology Journal*, Vol. 8, No. 3, 2009, pp. 333-339.

[17] H.C. Hsiang and W.K. Shih, Efficient remote mutual authentication and key agreement with perfect forward secrecy, *Information Technology Journal*, Vol. 8, No. 3, 2009, pp. 366-371.

[18] L. Hu, Y. Yang and X. Niu, Improved remote user authentication scheme preserving user anonymity, *Fifth Annual Conference on Communication Networks and Services Research*, 2007, pp. 323-328.

[19] M.S. Hwang, C.C. Lee, and Y.L. Tang, A simple remote user authentication scheme, *Mathematical and Computer Modelling*, Vol. 36, No. 1, 2002, pp. 103-107.

[20] M. Joye, P. Paillier, and B. Schoenmakers, On second-order differential power analysis, *Lecture Notes in Computer Science*, Vol. 3659, 2005, pp. 293-308.

[21] M.K. Khan, An efficient and secure remote mutual authentication scheme with smart cards, *International Symposium on Biometrics and Security Technologies*, 2008, pp. 1-6.

[22] S. Kim, H.S. Rhee, J.Y. Chun, and D.H. Lee, Anonymous and traceable authentication scheme using smart cards, *Second International Conference on Information Security and Assurance*, 2008, pp. 162-165.

[23] S.K. Kim, M.G. Chung, More secure remote user authentication scheme, *Computer Communications*, Vol. 32, No. 6, 2009, pp. 1018-1021.

[24] P. Kocher, J. Jaffe, and B. Jun, Differential power analysis, *Lecture Notes in Computer Science*, Vol. 1666, 1999, pp. 388-397.

[25] W.C. Ku and S.M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, 2004, pp. 204-207.

[26] W.C. Ku and S.T. Chang, Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards, *IEICE Transactions on Communications*, Vol. E88-B, No. 5, 2005, pp. 2165-2167.

[27] I.E. Liao and C.C. Lee, Security enhancement for a dynamic ID-based remote user authentication scheme, *International Conference on Next Generation Web Services Practices*, 2005, pp. 204-207.

[28] I.E. Liao, C.C. Lee, and M.S. Hwang, A password authentication scheme over insecure networks, *Journal of Computer and System Sciences*, Vol. 72, No. 4, 2006, pp. 727-740.

[29] J.Y. Liu, A.M. Zhou, and M.X. Gao, A new mutual authentication scheme based on nonce and smart cards, *Computer Communications*, Vol. 31, No. 10, 2008, pp. 2205-2209.

[30] S. Mangard, N. Pramstaller, and E. Oswald, Successfully attacking masked AES hardware implementations, *Lecture Notes in Computer Science*, Vol. 3659, 2005, pp. 157-171.

[31] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, Examining smart card security and under the threat of power analysis attacks, *IEEE Transactions on Computers*, Vol. 51, No. 5, 2002, pp. 541-552.

[32] W.G. Shieh and W.B. Horng, Efficient and complete remote authentication scheme with smart cards, *IEEE International Conference on Intelligence and Security Informatics*, 2008, pp. 122-127.

[33] B. Wang and Z.Q. Li, A forward-secure user authentication scheme with smart cards, *International Journal of Network Security*, Vol. 3, No. 2, 2006, pp. 116-119.

[34] Y. Wei, H. Qiu and Y. Hu, Security analysis of authentication schemes with anonymity for wireless, *IEEE International Conference on Communication Technology*, 2006, pp. 1-4.

[35] C. Yang, W. Ma, B. Huang, and X. Wang, Password-based access control scheme with remote user authentication using smart cards, *Advanced Information Networking and Applications Workshops*, 2007, pp. 448-452.

[36] E.J. Yoon, E.K. Ryu, and K.Y. Yoo, Further improvement of an efficient password based remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, 2004, pp. 612-614.

[37] L. Zhang, J.P. Yin, and Y.B. Zhan, An anonymous digital cash and fair payment protocol utilizing smart card in mobile environments, *Fifth International Conference on Grid and Cooperative Computing Workshops*, 2006, pp. 335-340.