# An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards

Chun-Ta Li[1] and Min-Shiang Hwang[2]

[1] Department of Information Management, Tainan University of Technology, 529 Jhong Jheng Road, Yongkang, 710 Tainan, Taiwan, R.O.C.
th0040@mail.tut.edu.tw

[2] Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
mshwang@nchu.edu.tw

**Abstract.** In this paper, we propose an efficient biometric-based remote user authentication scheme using smart cards, in which the computation cost is relatively low compared with other related schemes. The security of the proposed scheme is based on the one-way hash function, biometrics verification and smart card. Moreover, the proposed scheme enables the user to change their passwords freely and provides mutual authentication between the users and the remote server. In addition, many remote authentication schemes use timestamps to resist replay attacks. Therefore, synchronized clock is required between the user and the remote server. In our scheme, it does not require synchronized clocks between two entities because we use random numbers in place of timestamps.

*Keywords:* Biometrics; Cryptography; User authentication; Smart cards; Security.

## 1 Introduction

In 1981, Lamport [30] first proposed a remote authentication scheme in which the remote server could authenticate the remote user based on identity and password over an insecure network. However, Lamport's scheme has to store verification tables. In 1998, Jan and Chen [26] proposed a password authentication scheme without storing verification tables in the system. It is ineffective for the server to maintain the verification tables due to the size of the verification tables are proportional to the number of users. Later, Hwang and Li [24] proposed a new remote user authentication scheme using smart cards based on ElGamal's [7] public-key cryptosystem in 2000. The Hwang-Li scheme has to maintain only one secret key and no password table is required to keep in the system. Note that the smart card is a temper-resistant device and the primary properties are: (1) it is unable to get the information in it unless the user passes the verification; (2) it will have great trouble in performing complex computations for the smart card in each ongoing session due to its constrained computational capability.

In traditional remote identity-based remote authentication schemes [18, 25, 29, 32, 34], the security of the remote user authentication is based on the passwords, but simple passwords are easy to break by simple dictionary attacks. So, the cryptographic secret keys are used as they are long and random (e.g., 128 bits for the advanced encryption standard, AES [1, 5]). However, the cryptographic keys are difficult to memorize and they must be stored somewhere. Thus, they are expensive to maintain. Furthermore, both passwords and cryptographic keys are unable to provide non-repudiation because they can be forgotten, lost or when they are shared with other people, there is no way to know who the actual user is. Therefore, biometric keys [17, 27, 28, 33] are proposed which are based on physiological and behavioral characteristics of persons such as fingerprints, faces, irises, hand geometry, and palmprints etc. In the following, we shall present some advantages of biometric keys as follows:

- Biometric keys can not be lost or forgotten.
- Biometric keys are very difficult to copy or share.
- Biometric keys are extremely hard to forge or distribute.
- Biometric keys can not be guessed easily.
- Someone's biometrics is not easy to break than others.

Accordingly, biometrics-based authentication is inherently more reliable than traditional password-based authentication. Recently, in 2002, Lee et al. [31] proposed a fingerprint-based remote user authentication scheme using smart cards, but this scheme could not withstand impersonation attack [9, 33]. In 2004, Lin et al. [33] further proposed a flexible biometrics remote user authentication scheme. However, this scheme is susceptible to the server spoofing attack [27]. In this article, we shall present a secure and efficient biometric-based remote authentication scheme and compare it with other related schemes in terms of functionality requirements and computation costs. To do so, we shall list some essential requirements and the goal of the proposed scheme must satisfy these requirements of a secure user authentication scheme which will be mentioned in Section 2.

The remainder of this paper is organized as follows: Section 2 shows some related requirements for our scheme. In Section 3, our biometric-based authentication scheme is proposed. The security and the efficiency of our scheme will be analyzed in Section 4. Finally, we conclude this article in Section 5.

## 2 Essential Requirements

According to the previous researches, in this section, we list some essential requirements for evaluating a new remote user authentication scheme. The following criteria are crucial and these requirements solve all problems in smart card-oriented schemes. For a protection mechanism for remote user authentication, each requirement is a fundamental and independent requirement. The purpose of this paper is to propose a new remote user authentication scheme to meet the following essential requirements so as to establish a standard for our biometrics-based remote user authentication scheme.

**Security requirements:**

- Withstand masquerade attacks: An adversary may try to masquerade as a legitimate user to communicate with the valid system or masquerade as a valid system to communicate with the legal users [11, 16, 20, 21, 36, 38].
- Withstand replay attacks: An attacker would try to hold up the messages between two communication parties and impersonating other legal party to replay the fake messages for further deceptions [22].
- If user loses the smart card, the secret information and the password can not be derived by adversary [36].
- Withstand parallel session attacks [10].

**Functionality requirements:**

- Allow users to freely choose and change the passwords in local without notifying the server, thus, it can decrease the communication overheads and some possible attacks between two communication parties over an insecure network [39].
- Provide mutual authentication between two communication parties [13, 14, 19, 35].
- Without storing password tables and identity tables in the system [37].
- Without synchronized clock: Some authentication schemes used timestamps to prevent replaying attacks. However, it may cause some problems by employing timestamps [4, 8].
- Provide non-repudiation because of employing personal biometrics [2, 3, 6, 23].

**Performance requirements:**

- Efficiency (With low computation cost): In general, the smart card usually does not support powerful computational capability. Hence, the exponential operation will not be used in our proposed scheme because its computational cost is relatively high [12, 15].

## 3 The Proposed Scheme

In this section, we shall present our biometrics-based remote user authentication scheme. The notations in Table 1 are used in the proposed scheme.

There are three phases in our scheme including registration phase, login phase and authentication phase. Detailed steps of these phases of the proposed scheme are described as follows and are in Figure 1.

### 3.1 Registration Phase

Before the remote user logins to the system, the user needs to perform the following steps.

**Step 1** : Firstly, the user inputs his/her personal biometrics, $B_i$, on the specific device and offering the password, $PW_i$, identity of the user, $ID_i$ to the registration center in person.

*Registration phase*

$C_i$ $\qquad$ $R_i$

1. $ID_i, B_i, PW_i$ $\longrightarrow$

2. Computes $r_i$ and $e_i$

3. Smart card$(ID_i, h(\cdot), f_i, e_i)$ $\longleftarrow$

---

*Login phase*

$C_i$ $\qquad$ $S_i$

1. Inserts the smart card and inputs $B_i$
2. Verifies $h(B_i) \stackrel{?}{=} f_i$
3. If it holds, $C_i$ inputs $PW_i$
4. Computes $r_i` = h(PW_i \| f_i)$

   Computes $M_1 = e_i \oplus r_i`$

   Computes $M_2 = M_1 \oplus Rc$

5. $ID_i, M_2$ $\longrightarrow$

---

*Authentication phase*

$C_i$ $\qquad$ $S_i$

1. Checks the format of $C_i$'s $ID_i$
2. If above holds, $S_i$ computes

   $M_3 = h(ID_i \| Xs)$

   $M_4 = M_2 \oplus M_3$

   $M_5 = M_3 \oplus Rs$

   $M_6 = h(M_2 \| M_4)$

3. $M_6, M_5$ $\longleftarrow$

4. Verifies $M_6 \stackrel{?}{=} h(M_2 \| Rc)$
5. If above holds, $C_i$ computes

   $M_7 = M_5 \oplus M_1$

   $M_8 = h(M_5 \| M_7)$

6. $M_8$ $\longrightarrow$

7. Verifies $M_8 \stackrel{?}{=} h(M_5 \| Rs)$
8. If it holds, $S_i$ accepts $C_i$'s login request
9. Otherwise, $S_i$ rejects $C_i$'s login request

**Fig. 1.** The proposed scheme

**Table 1.** Notations used in the proposed scheme

| | |
|---|---|
| $C_i$ | Client(User) |
| $S_i$ | Server |
| $R_i$ | Trust registration center |
| $ID_i$ | Identity of user |
| $PW_i$ | Password shared between $C_i$ and $S_i$ |
| $B_i$ | Biometric template of the user |
| $h(\cdot)$ | One-way hash function |
| $Xs$ | A secret information maintained by the server |
| $Rc$ | A random number chosen by the client |
| $Rs$ | A random number chosen by the server |
| $\|\|$ | Concatenation of messages |
| $\oplus$ | XOR operation |

**Step 2** : Next, the registration center computes $r_i$ and $e_i$ as follows:

$$r_i = h(PW_i \| f_i)$$
$$e_i = h(ID_i \| Xs) \oplus h(PW_i \| f_i)$$

where $f_i = h(B_i)$ and $Xs$ is a secret information generated by the server. Note that the secret information $Xs$ of server node and the passwords of corresponding users are undisclosed to any others for securing all future authentications.

**Step 3** : Lastly, the registration center stores ($ID_i$, $h(\cdot)$, $f_i$, $e_i$) on the user's smart card and sends it to the user via a secure channel.

### 3.2 Login Phase

Whenever the user wants to logon to the remote server, he/she must perform the following steps.

**Step 1** : First, $C_i$ inserts his/her smart card into the card reader and inputs the personal biometrics, $B_i$, on the specific device to verify the user's biometrics.

**Step 2** : Then, verifies $h(B_i) \stackrel{?}{=} f_i$.

**Step 3** : If the above mentioned does not hold, it means $C_i$ does not pass the biometric verification and the remote user authentication scheme is terminated. On the contrary, if it holds, $C_i$ passes the biometrics verification. Then $C_i$ inputs the $PW_i$ to perform the following operations in Step 4.

**Step 4** : After receiving $C_i$'s password, the smart card will compute the following messages:

$$r_i` = h(PW_i \| f_i)$$
$$M_1 = e_i \oplus r_i` = h(ID_i \| Xs)$$
$$M_2 = M_1 \oplus Rc$$

where $Rc$ is a random number generated by the user. For this step, the random value $Rc$ is introduced to mask the hash of the secret value $h(ID_i \| Xs)$.

**Step 5** : Finally, $C_i$ sends the message $(ID_i, M_2)$ to the remote server, $S_i$.

### 3.3 Authentication Phase

After receiving the request login message, $S_i$ will perform the following steps to authenticate that the user is legal or not.

**Step 1** : First, $S_i$ checks whether the format of $ID_i$ is valid or not.

**Step 2** : If Step 1 holds, $S_i$ then computes the following messages to provide mutual authentication between $C_i$ and $S_i$. For this step, $M_4$ is in fact the random value $Rc$ of the client $C_i$ and that only $S_i$ can unmask the value, because only it can compute $h(ID_i \| Xs)$.

$$M_3 = h(ID_i \| Xs)$$
$$M_4 = M_2 \oplus M_3 = Rc$$
$$M_5 = M_3 \oplus Rs$$
$$M_6 = h(M_2 \| M_4)$$

**Step 3** : Then, $S_i$ sends the message $(M_5, M_6)$ to $C_i$.

**Step 4** : After receiving $S_i$'s message, $C_i$ first verifies whether $M_6 \stackrel{?}{=} h(M_2 \| Rc)$.

**Step 5** : If it holds, $C_i$ believes that $S_i$ is authenticated and then computes the following messages to provide mutual authentication between $S_i$ and $C_i$. For this step, $M_7$ is in fact the random value $Rs$ of the server $S_i$ and only the client, which knows $M_1 = h(ID_i \| Xs)$ can send back the correct hashed value of $M_8 = h((h(ID_i \| Xs) \oplus Rs) \| Rs)$.

$$M_7 = M_5 \oplus M_1 = Rs$$
$$M_8 = h(M_5 \| M_7)$$

**Step 6** : $C_i$ sends the message $M_8$ to $S_i$.

**Step 7** : After receiving $C_i$'s message, $S_i$ verifies whether $M_8 \stackrel{?}{=} h(M_5 \| Rs)$.

**Step 8** : If the above mentioned holds, $S_i$ accepts $C_i$'s login request.

**Step 9** : Otherwise, $S_i$ rejects $C_i$'s login request.

### 3.4 Change Password

According to the above-mentioned requirements, user $C_i$ can freely change the password, $PW_i$, to a new password, $PW_i^n$. First, $C_i$ inserts the smart card and inputs his/her biometric template, $B_i$ on the specific device to verify the user's biometrics. If $C_i$ passes the biometric verification $(h(B_i) = f_i)$, then he/she inputs the old password, $PW_i$, and the new password, $PW_i^n$. Next, the smart card will perform the following operations:

$$r_i` = h(PW_i \| f_i)$$
$$e_i` = e_i \oplus r_i` = h(ID_i \| Xs)$$
$$e_i" = e_i` \oplus h(PW_i^n \| f_i)$$

Finally, replace the $e_i$ with $e_i$" on the smart card.

## 4 Security Analysis and Comparisons

In this section, we will analyze the security of the proposed scheme and further compare Lin-Lai's scheme [33], Lee-Chiu's scheme [32], Yoon et al.'s scheme [40], Chang et al.'s scheme [4], Khan et al.'s scheme [28], and our scheme in terms of functionality and efficiency.

### 4.1 Security Analysis

The security of our scheme is analyzed in the following:

- In our scheme, the remote server only has to maintain a secret information, $Xs$, without storing the password tables. An attack may try to derive $Xs$ from the intercepted messages, $(ID_i, M_2)$, $(M_5, M_6)$, and $M_8$. But it is computationally infeasible because of the property of the one-way hashing function and random values.
- If the legal user lost his/her smart card, it is difficult for any adversary to derive or change the password because he/she can not pass the biometric verification. On comparing adversary's biometric template with the biometric template stored on the smart card, the illegal request will be rejected. Besides, the secret information stored on the smart card is as secure as the password.
- An illegal user may try to fabricate fake request login messages to cheat the remote server into believing it is a legal remote login request (masquerade attack) in the login phase. It does not work unless he/she could modify $M_2$ correctly. However, it is difficult for the user to modify $M_2$ without knowing $M_1$ and the random number $Rc$. In addition, during the login phase, if a fake user intercepts the message $(ID_i, M_2)$ and modifies the message to $(ID_i, M_2 \oplus Rx)$, where $Rx$ is a random number chosen by the fake user. For the server, this is a valid request with a different random number $Rc \oplus Rx$. However, this attack is still not work because the fake user is unable to compute the message $M_8$ to convince $S_i$ unless he/she knows $C_i$'s random number $Rc$.
- If the illegal user intercepts the message $(ID_i, M_2)$ from $C_i$ and try to masquerade as the remote server. It is impossible for the user to compute the message $M_6$ to convince $C_i$ unless he/she knows the secret information $Xs$. Furthermore, in our protocol, the server does not store all random values ever sent by the client.
- In our proposed protocol, the server does not store all random values ever sent by the client and parallel session attack is completely solved by generating the random number between user and remote server. During login phase, user sends login message $(ID_i, M_2)$ to the remote server. If an attacker resends it to the remote server, it well be verified in steps 1 and 2 of the authentication phase. However, remote server responses differential $Rs$ in every session. As a result, parallel session attempt will be failed in the step 5 of the authentication phase, because an attacker is unable to compute $M_3$,

derive the valid value of $Rs$ and response mutual authentication message $M_8$ to the remote server.

**Table 2.** Comparison with other related schemes

| | Lin-Lai [33] | Lee-Chiu [32] | Yoon et al. [40] | Chang et al. [4] | Khan et al. [28] | Our scheme |
|---|---|---|---|---|---|---|
| Computational operations in registration phase | 1H+1E | 2H+1E | 1H | 2H | 2H | 3H |
| Computational operations in login phase | 2H+2E | 2H+1E | 1H | 2H | 2H | 2H |
| Computational operations in authentication phase | 1H+2E | 2H | 4H | 6H | 5H | 5H |
| Change password | Yes | Yes | Yes | No | Yes | Yes |
| Mutual authentication | No | No | Yes | Yes | Yes | Yes |
| Without synchronized clocks | No | No | No | Yes | No | Yes |
| Provide non-repudiation | Yes | No | No | No | Yes | Yes |

*Notes.* H: One-way hashing operation; E: Exponential operation.

### 4.2 Performance Comparisons

In the following, the comparisons of our scheme and other related schemes are summarized in Table 2. From Table 2, Lin-Lai's scheme and Lee-Chiu's scheme requires some exponential operations because the security of their schemes is based on solving discrete logarithm problems. However, in terms of efficiency, the exponential computation is very high-powered and time-consuming. Contrary to ours, Yoon et al.'s, Chang et al.'s, and Khan et al.'s scheme, the computation costs are very low, only a few hashing function computations are needed. Therefore, this feature makes our scheme effective.

### 4.3 Functionality Comparisons

For functionality comparisons, though Chang et al.'s scheme allows users to freely choose the initial passwords during the registration phase, their scheme does not provide the functionality of change password in local. Thus, the user must notify the server if he/she wants to change the password. It will increase the communication overheads and some possible attacks between the user and the remote server over an insecure network. In addition, from Table 2 shows, only ours, Yoon et al.'s, Chang et al.'s, and Khan et al.'s scheme provide mutual authentication between two communication parties. However, Yoon et al.'s and

Chang et al.'s scheme does not provide non-repudiation and ours and Khan et al.'s scheme achieves non-repudiation because of employing personal biometrics.

On the other hand, Yoon et al.'s and Khan et al.'s schemes required synchronized clocks between the user and the remote server because of using timestamps. In fact, it is fairly complicated to achieve time concurrency and some disadvantages exist such as the delivery latency and the different time zone, and so forth [4, 8]. As a result, in our scheme, it not only provides non-repudiation, it also does not require synchronized clocks because we use random numbers in place of timestamps.

## 5 Conclusions

In this article, an efficient biometrics-based remote user authentication scheme is proposed. By comparison with other related schemes, the proposed scheme not only keeps good properties (e.g. without synchronized clock, freely changes password, low computation costs, mutual authentication) but also provides non-repudiation because the characteristics of personal biometrics. Thus, it is suitable for various authentication cryptosystems in distributed computing environments since it provides security, reliability, and efficiency.

## References

1. Advanced Encryption Standard. http://csrc.nist.gov/encryption/aes/.
2. Arslan Broemme. A risk analysis approach for biometric authentication technology. *International Journal of Network Security*, 2(1):52–63, 2006.
3. Andrew Burnett, Fergus Byrne, Tom Dowling, and Adam Duffy. A biometric identity based signature scheme. *International Journal of Network Security*, 5(3):317–326, 2007.
4. Ya-Fen Chang, Chin-Chen Chang, and Yu-Wei Su. A secure improvement on the user-friendly remote authentication scheme with no time concurrency mechanism. In *Proceedings of 20th International Conference on Advanced Information Networking and Applications*, IEEE CS, 2006.
5. J. Daemen and V. Rijmen. Rijndael, the advanced encryption standard. *Dr. Dobb's Journal*, 26(3):137–139, 2001.
6. Christos K. Dimitriadis and Siraj A. Shaikh. A biometric authentication protocol for 3G mobile systems: modelled and validated using CSP and rank functions. *International Journal of Network Security*, 5(1):99–111, 2007.
7. T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31(4):469–472, 1985.
8. Li Gong. A security risk of depending on synchronized clocks. *ACM Operating Systems Review*, 26(1):49–53, 1992.
9. B. T. Hsieh, H. Y. Yeh, H. M. Sun, and C. T. Lin. Cryptanalysis of a fingerprint-based remote user authentication scheme using smart cards. In *Proceedings of 37th IEEE Conference on Security Technology*, pages 349–350, 2003.
10. C. L. Hsu. Security of chien et al.'s remote user authentication scheme using smart cards. *Computer Standards & Interfaces*, 26(3):167–169, 2004.

11. Chun-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu. Further improvement on a novel privacy preserving authentication and access control scheme for pervasive computing environments. *Computer Communications*, 31(18):4255–4258, 2008.
12. Chun-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communications*, 31(12):2803–2814, 2008.
13. Chun-Ta Li, Min-Shiang Hwang, and Chi-Yu Liu. An electronic voting protocol with deniable authentication for mobile ad hoc networks. *Computer Communications*, 31(10):2534–2540, 2008.
14. Chun-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu. Improving the security of a secure anonymous routing protocol with authenticated key exchange for ad hoc networks. *International Journal of Computer Systems Science and Engineering*, 23(3):227-234, 2008.
15. Chun-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu. An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks. *International Journal of Innovative Computing, Information and Control*, 5(8):2107-2124, 2009.
16. Chun-Ta Li, C. H. Wei, and Y. H. Chin . A secure event update protocol for peer-to-peer massively multiplayer online games against masquerade attacks. *International Journal of Innovative Computing, Information and Control*, accepted, 2009.
17. Chun-Ta Li and Min-Shiang Hwang. An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards. *International Journal of Innovative Computing, Information and Control*, accepted, 2009.
18. Chun-Ta Li and Yen-Ping Chu. Cryptanalysis of threshold password authentication against guessing attacks in ad hoc networks. *International Journal of Network Security*, 8(2):166–168, 2009.
19. Chun-Ta Li. An enhanced remote user authentication scheme providing mutual authentication and key agreement with smart cards. In *Proceedings of 5th International Conference on Information Assurance and Security*, IEEE CS, 2009.
20. Chun-Ta Li and Min-Shiang Hwang. "Improving the security of non-PKI methods for public key distribution. In *Proceedings of 6th International Conference on Information Technology: New Generations*, IEEE CS, pages 1695–1696, 2009.
21. Ching-Yung Liu. A lightweight security mechanism for ATM networks. *International Journal of Network Security*, 1(1):32–37, 2005.
22. Rongxing Lu, Zhenfu Cao, Zhenchuan Chai, and Xiaohui Liang. A simple user authentication scheme for grid computing. *International Journal of Network Security*, 7(2):202–206, 2008.
23. Deholo Nali, Carlisle Adams, and Ali Miri. Using threshold attribute-based encryption for practical biometric-based access control . *International Journal of Network Security*, 1(3):173–182, 2005.
24. Min-Shiang Hwang and Li-Hua Li. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(1):28–30, 2000.
25. Min-Shiang Hwang and Chi-Yu Liu. Authenticated encryption schemes: Current status and key issues. *International Journal of Network Security*, 1(2):61–73, 2005.
26. J. K. Jan and Y. Y. Chen. Paramita wisdom password authentication scheme without verification tables. *The Journal of Systems and Software*, 42(1):45–57, 1998.
27. Muhammad Khurram Khan and Jiashu Zhang. Improving the security of 'a flexible biometrics remote user authentication scheme'. *Computer Standards & Interfaces*, 29(1):82–85, 2007.

28. Muhammad Khurram Khan, Jiashu Zhang, and Xiaomin Wang. Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. *Chaos, Solitons and Fractals*, 35(3):519–524, 2008.
29. Minho Kim and Çtin Kaya Koç. A simple attack on a recently introduced hash-based strong-password authentication scheme. *International Journal of Network Security*, 1(2):77–80, 2005.
30. L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, November 1981.
31. J. K. Lee, S. R. Ryu, and K. Y. Yoo. Fingerprint-based remote user authentication scheme using smart cards. *Electronic Letters*, 38(12):554–555, 2002.
32. Narn-Yih Lee and Yu-Chung Chiu. Improved remote authentication scheme with smart card. *Computer Standards & Interfaces*, 27(2):177–180, 2005.
33. Chu-Hsing Lin and Yi-Yi Lai. A flexible biometrics remote user authentication scheme. *Computer Standards & Interfaces*, 27(1):19–23, 2004.
34. Jau-Ji Shen, Ching-Ying Lin, and Hung-Wen Yang. Cryptanalysis of a new efficient makep for wireless communications. *International Journal of Network Security*, 1(2):118–121, 2005.
35. Da-Zhi Sun and Zhen-Fu Cao. New cryptanalysis paradigm on a nonce-based mutual authentication scheme. *International Journal of Network Security*, 6(1):116–120, 2008.
36. Xiaojian Tian, Robert W. Zhu, and Duncan S. Wong. Improved efficient remote user authentication schemes. *International Journal of Network Security*, 4(2):149–154, 2007.
37. Chwei-Shyong Tsai, Cheng-Chi Lee, and Min-Shiang Hwang. Password authentication schemes: current status and key issues. *International Journal of Network Security*, 3(2):101–115, 2006.
38. Ren-Chiun Wang and Chou-Chen Yang. Cryptanalysis of two improved password authentication schemes using smart cards. *International Journal of Network Security*, 3(3):283–285, 2006.
39. Bin Wang and Zheng-Quan Li. A forward-secure user authentication scheme with smart cards. *International Journal of Network Security*, 3(2):116–119, 2006.
40. Eun-Jun Yoon, Eun-Kyung Ryu, and Kee-Young Yoo. An improvement of hwang-lee-tang's simple remote user authentication scheme. *Computers & Security*, 24(1):50–56, 2005.