

An Improved Biometrics-based User Authentication Scheme without Concurrency System

Chin-Chen Chang
*Department of Information
Engineering and Computer
Science, Feng Chia
University, 100 Wenhwa Rd.,
Seatwen, Taichung 407,
Taiwan, R.O.C.
E-mail: alan3c@gmail.com*

Shih-Chang Chang
*Department of Computer
Science and Information
Engineering, National
Chung Cheng University,
160 San-Hsing, Ming-Hsiung,
Chiayi 621, Taiwan, R.O.C.
E-mail: chang.coby@gmail.com
doi: 10.4156/ijip.vol1.issue1.5*

Yu-Wei Lai
*Department of Computer
Science, National Tsing Hua
University, 101 Section 2,
Kuang-Fu Rd, Hsinchu
30013, Taiwan, R.O.C.
E-mail:
chrisxhades@gmail.com*

Abstract

Engineers have proposed many password authentication schemes for remote login systems in past decades. In recent years, the biometrics technology has become a new issue in computer science. This new technology has allowed us to develop a novel method of user authentication using a smart card. In addition, many authentication schemes need a system of synchronized clocks to withstand replay attacks and achieve mutual authentication. Since a system of synchronized clocks between the user and the remote server is an extra burden for both, we propose an improved scheme without a system of synchronized clocks to achieve mutual authentication. In addition to this improvement, our scheme does not require the use of a traditional password.

Keywords: *Biometrics, Mutual authentication, Smart card, Cryptography*

1. Introduction

In 1981, Lamport [15] first proposed a remote authentication scheme to allow communications between a remote system and users via an insecure channel. In Lamport's scheme, the remote server must maintain a password table for verifying legal users. However, the password table makes Lamport's scheme vulnerable to a stolen-verifier attack if an attacker is capable of accessing the remote server somehow [25, 27]. In 1990, Yamaguchi et al. [28] proposed a simple, but efficient, password authentication scheme. However, their scheme is vulnerable to password guessing attacks. Later, in 1994, Chang and Liao [7] proposed a novel remote authentication scheme based on ElGamal's signature. Their scheme has some design flaws that prevent users from choosing their preferred passwords, and it only provides one-way authentication. The same problems are also evident in many other schemes presented in the literatures [2, 4, 8, 9, 23, 26].

By using smart cards, engineers have recently proposed many password authentication schemes for remote login systems [3, 5-10, 14, 16, 17, 22, 24, 27]. Such schemes allow a legal user to use the combination of identity and password to log in to the remote server with a unique smart card. The main advantage of such schemes is that the remote server does not have to keep a password table in its database. Hence, the well-known stolen verifier attack can be resisted.

At the current time, biometrics is becoming more and more popular for user authentication and providing secure system [12, 13, 18, 20]. In 2004, Jin et al. proposed a novel, two-factor authentication scheme using fingerprint data and tokenized pseudo-random number, a process referred to as "biohashing [11]." Using this new technology, Li and Hwang [19] developed an efficient biometrics-based scheme for remote user authentication. Unfortunately, we found that their system has a weakness, which is discussed in Subsection 2.2. In addition, Li and Hwang's scheme needs to use personal biometrics and a password to achieve the essential requirements mentioned in their scheme. Because of the many applications that people use on the Internet, many passwords must be remembered. The large and growing number of passwords that people must remember is a serious problem. Based on this reason, we think that there might be a better way to achieve the remote user authentication.

Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic

physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. With the blooming development and advancement of computer technology, people's biometrics information, such as fingerprints, faces, and irises, can be used to confirm their identities. There are two main advantages of biometric keys. First, biometrics cannot be lost or forgotten. Second, biometrics information is very difficult to duplicate or copy.

Therefore, we present an improved method that solves the weaknesses of Li and Hwang's scheme by using only biometrics to develop a novel means of verifying the identity of any individual person. Further, our system can be implemented on wireless networks, such as Wi-Fi, WiMAX, and Mobile networks. Wi-Fi is a trademark of the Wi-Fi Alliance that manufacturers may use to brand certified products that belong to a class of wireless local area network (WLAN) devices based on the IEEE 802.11 standards. WiMAX is the term used to refer to wireless MANs and is covered in IEEE 802.16d/802.16e.

The remainder of this article is organized as follows. We are going to review Li and Hwang's scheme in Subsection 2.1 and present its weaknesses in Subsection 2.2. Then, we propose an improved method in Section 3. Next, we show our security analysis and discuss the status of our work in Sections 4 and 5, respectively. Finally, we present our conclusions in Section 6.

2. A Review of Li and Hwang's Scheme

In this section, we describe Li and Hwang's biometrics-based authentication scheme and show its weaknesses in Subsections 2.1 and 2.2, respectively.

2.1 Li and Hwang's Scheme

In Li and Hwang's scheme [19], there are three phases including registration phase, login phase, and authentication phase. We present the illustration in Figure 1 and the notations used in their scheme in Table 1. Then, more details about the three phases of their scheme are shown as follows.

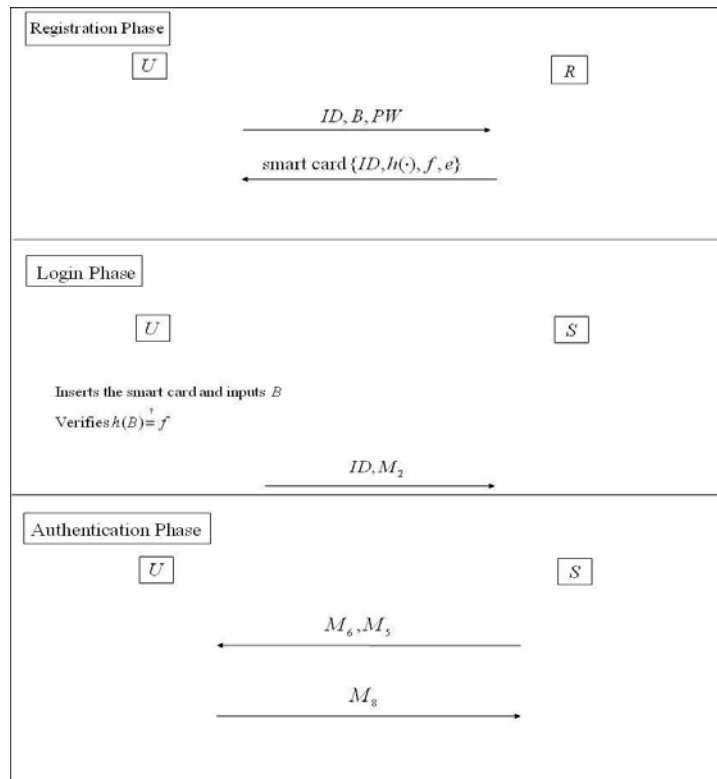


Figure 1. Li and Hwang's scheme

Table 1. The notations used in Li and Hwang's scheme

U	The user
S	The server
R	Trust registration center
ID	Identity of user
PW	Password shared between user and server
B	Biometric information of user
$h(\cdot)$	One-way hash function
X_S	Secret information kept by server
R_U	A random number chosen by user
R_S	A random number chosen by server
\parallel	Concatenation symbol
\oplus	XOR operation

Registration Phase

Before the user logs in to the remote server, he/she must first execute the following steps to obtain the smart card.

Step 1: The user firstly offers his/her identity ID , password PW , and the personal biometrics B to the registration center.

Step 2: After receiving the information, the registration center computes

$$r = h(PW \parallel f)$$

$$\text{and } e = h(ID \parallel X_S) \oplus r,$$

where $f = h(B)$ and X_S is a secret information kept by the server.

Step 3: Then, the registration center stores the information $\{ID, h(\cdot), f, e\}$ in the user's smart card and sends it to the user through a secure channel.

Login Phase

When the user wants to log in to the remote server, he/she executes the following steps.

Step 1: The user inserts his/her smart card into the device and inputs the personal biometrics B on the specific device to verify the user's biometric.

Step 2: Next, the smart card verifies the equation $h(B) \stackrel{?}{=} f$. If it holds, the process continues; otherwise, the user authentication scheme is terminated.

Step 3: After that, U inputs the password PW to perform the following procedures.

Step 4: The smart card computes

$$r' = h(PW \parallel f),$$

$$M_1 = e \oplus r' = h(ID \parallel X_S),$$

$$\text{and } M_2 = M_1 \oplus R_U,$$

where R_U is a random number chosen by the user.

Step 5: Then, U sends the message $\{ID, M_2\}$ to the remote server.

Authentication Phase

After receiving the request for login message, S executes the following steps to authenticate whether the user is legal or not.

Step 1: S firstly checks the format of ID .

Step 2: After passing the above step, S will compute the following message to provide the mutual authentication requirement.

$$M_3 = h(ID \parallel X_S),$$

$$M_4 = M_2 \oplus M_3 = R_U,$$

$$M_5 = M_3 \oplus R_S,$$

$$\text{and } M_6 = h(M_2 \parallel M_4).$$

Step 3: The server S sends the message $\{M_5, M_6\}$ to the user U .

Step 4: When receiving the message, U first verifies the equation

$$M_6 \stackrel{?}{=} h(M_2 \parallel R_U).$$

Step 5: If it holds, U believes that S is trusted and then computes the following message to provide the mutual authentication requirement.

$$M_7 = M_5 \oplus M_1 = R_S,$$

$$\text{and } M_8 = h(M_5 \parallel M_7).$$

Step 6: The user U sends the message $\{M_8\}$ to the server S .

Step 7: After that, S verifies the equation $M_8 \stackrel{?}{=} h(M_5 \parallel R_S)$.

Step 8: If the above step holds, S accepts U 's login request; otherwise, S rejects U 's login request.

2.2 Weaknesses

In this subsection, we introduce the weaknesses of Li and Hwang's scheme. In the authentication phase, we can easily intercept the information, M_5 and M_8 . Then, we use this information to perform the following algorithm.

Step 1: Select a random number R_A , where A means an attacker.

Step 2: Then, use R_A to verify the equation $M_8 \stackrel{?}{=} h(M_5 \parallel R_A)$.

Step 3: If Step 2 results in a successful verification, go to Step 4; otherwise, go back Step 1 to select a new random number.

Step 4: After that, we compute $M_5 \oplus R_A = h(ID \parallel X_S)$ and also create secret information X_A . Verify the equation $M_5 \oplus R_A \stackrel{?}{=} h(ID \parallel X_A)$. If it holds, then the important secret information is obtained; otherwise, redo this step.

Using the algorithm described above, we can get the secret information $X_A = X_S$. In Li and Hwang's scheme, this secret information is very important because it is long-term secret information. If an attacker acquires this secret information, he/she can use it to cheat everyone who wants to register with this system. Hence, we developed a novel system to solve this problem.

3. Our Proposed Scheme

In this section, we present our improved biometrics-based user authentication scheme that does not require the use of a traditional password. Our scheme could be divided into three phases: registration phase, login phase, and authentication phase. Then, we illustrate the flowchart of our scheme in Figure 2 and show the notations we used in Table 2. Detailed steps of the three phases are described as following.

Table 2. Notations used in the proposed scheme

U	The user
S	The server
R	Trust registration center
ID	Identity of user
Q	Biometric information of user
$h(\cdot)$	One-way hash function
X_S	Secret information kept by server
N_U	A nonce chosen by user
N_S	A nonce chosen by server
\parallel	Concatenation symbol
\oplus	XOR operation

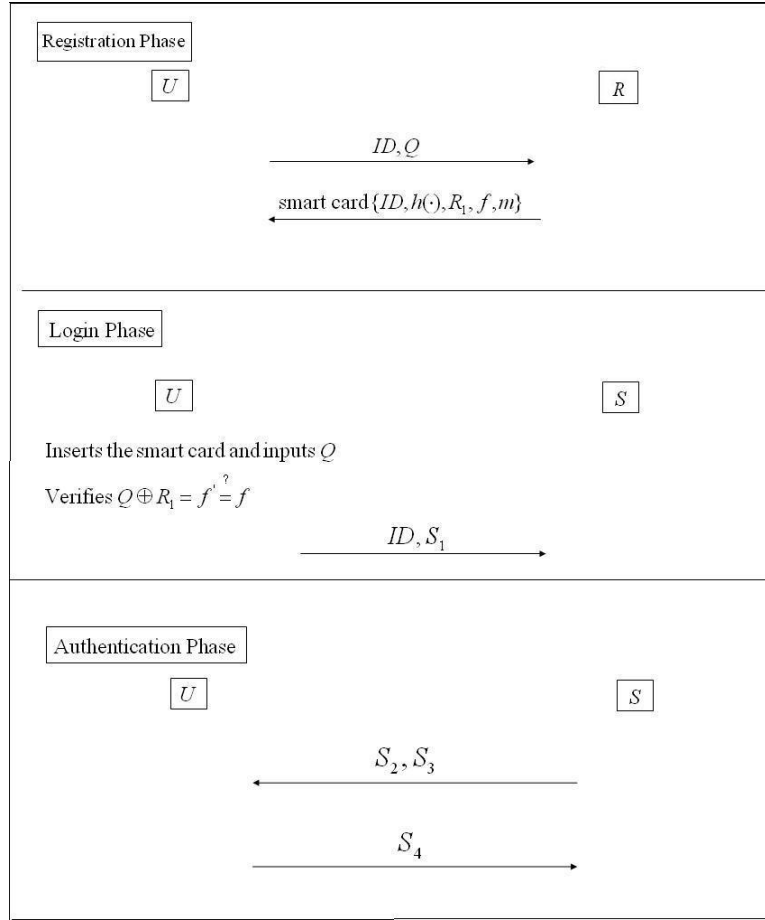


Figure 2. Our proposed scheme

Registration Phase

In this phase, the user registers the trust registration center to obtain the smart card, and the following actions occur.

Step 1: The user firstly offers his/her identity ID and the personal biometrics Q to the registration center.

Step 2: After receiving, the registration center firstly selects a random number R_1 and computes

$$f = Q \oplus R_1$$

$$\text{and } m = h(ID \| X_S) \oplus f,$$

where R_1 is the first time random secret to protect the personal biometrics and X_S is the secret information kept by the server.

Step 3: Next, the registration center stores the information $\{ID, h(\cdot), R_1, f, m\}$ in the user's smart card and sends it to the user through a secure channel.

Login Phase

When the user asks the service from the remote server, he/she performs the following steps.

Step 1: The user inserts his/her smart card into the device and provides the personal biometrics Q on the specific device.

Step 2: Next, the smart card verifies the equation $Q \oplus R_1 = f' = f$. If it holds, this phase continues; otherwise, this phase is terminated.

Step 3: Then, the user generates a nonce N_U and computes

$$S_1 = m \oplus f' \oplus N_U.$$

Step 4: U sends the message $\{ID, S_1\}$ to the remote server.

Authentication Phase

After receiving the request from login message, S performs the following steps.

Step 1: First, S checks the format of ID .

Step 2: After passing, S will compute $h(ID \| X_S)$ and uses it to obtain C_1 by the equation

$$C_1 = h(ID \| X_S) \oplus S_1, \text{ where } C_1 = N_U. \text{ Then, the server computes}$$

$$S_2 = h(h(ID \| X_S) \| C_1) \oplus N_S$$

$$\text{and } S_3 = h(h(ID \| X_S) \| C_1 \| N_S),$$

where N_S is a nonce selected by the server.

Step 3: The server S sends the message $\{S_2, S_3\}$ to the user U .

Step 4: When receiving the message, U obtains C_2 by computing

$$C_2 = h(m \oplus f' \| N_U) \oplus S_2,$$

where $C_2 = N_S$. After that, the user uses C_2 to verify this equation

$$S_3 \stackrel{?}{=} h(m \oplus f' \| N_U \| C_2).$$

Step 5: If it holds, U believes that S is trusted and then computes

$$S_4 = h(m \oplus f' \| C_2).$$

Step 6: The user U sends the message $\{S_4\}$ to the server S .

Step 7: Next, S verifies the equation $S_4 \stackrel{?}{=} h(h(ID \| X_S) \| N_S)$.

Step 8: If the above equation holds, S accepts U 's login request; otherwise, S sends a rejection message.

After the above three phases, our scheme can provide the mutual authentication between the user and the server. Besides, we change R_1 in the smart card every time and present the details according to the following procedure.

Step 1: The smart card selects a new random number R_2 .

Step 2: The smart card computes

$$f_{new} = f \oplus R_1 \oplus R_2$$

$$\text{and } m_{new} = m \oplus f \oplus f_{new}.$$

Step 3: The above information is replaced on the smart card.

4. Security Analysis

In this section, we analyze the security of our proposed scheme. We just use one-way hash function and XOR operation to develop our scheme, which can resist the well-known attacks. Then, we suppose that an attacker, named Eve, can monitor and intercept the communication messages in this method. Details are discussed as following.

The Smart Card Lost

If a legal user loses his/her smart card, no-one can use this smart card to pass the login phase in our scheme, because the adversary must provide the corresponding biometrics stored on the smart card. For instance, in the login phase of our scheme, the adversary first provides his biometrics Q_a on a specific device. In Step 2, we obviously know that the equation $Q_a \oplus R_1 = f^* = f$ is not validated. Hence, our scheme provides anyone other than the legal user from using the smart card.

Forgery Attack

Assume Eve wants to try to forge the login request message to fool the remote server into believing she is a legal user. Her attempt will fail. The details are shown in the following.

First, Eve generates the request message $\{ID, S_1^* = S_1 \oplus N_E\}$, where N_E is a random nonce selected by Eve, and sends it to the remote server. After receiving, the server checks the format of ID . If it holds, S will compute $h(ID \| X_S)$ and uses it to obtain $C_1^* = h(ID \| X_S) \oplus S_1^*$. Then, the server computes

$$S_2^* = h(h(ID \| X_S) \| C_1^*) \oplus N_S$$

$$\text{and } S_3^* = h(h(ID \| X_S) \| C_1^* \| N_S),$$

where N_S is a nonce selected by the server. The server sends the message $\{S_2^*, S_3^*\}$ to Eve. However, she can not compute the correct S_4 to pass Step 7 in authentication phase without knowing the random nonce N_S .

Also, for the same reason, Eve also can not fool the user into believing she is a legal server. Therefore, our scheme can achieve the desired security requirement.

Off-line Guessing Attack

Assume Eve obtains all communication messages such as $\{ID, S_1\}$, $\{S_2, S_3\}$, and $\{S_4\}$. If she wants to try to derive the secret information X_S from the intercepted messages, she must fail. The reason is that Eve can not know the random nonce N_U or the random nonce N_S . Besides, the secret information is protected by one-way hash function. Therefore, our scheme can withstand the off-line guessing attack.

Replay Attack

Suppose Eve intercepts the communication messages and wants to perform the replay attack. Then, she first sends this message $\{ID, S_1\}$ to the remote server. After receiving, the server computes and sends back this message $\{S_2, S_3\}$ to Eve. Next, she must obtain the important information C_2 from S_2 and use C_2 to compute S_4 to send it to the remote server for mutual authentication. However, Eve can not pass this authentication because she doesn't have the random nonce N_U generated by the legal user. In addition, the random nonce N_U or N_S is different in every session. Therefore, Eve can not guess them in our scheme. Again, it is obvious that the security requirement is achieved.

5. Discussions

In the following, we describe the performance comparisons between our scheme and other related schemes in Table 3 and also show the functionality comparisons in Table 4. Furthermore, we present the security requirements comparisons between Li and Hwang's scheme and ours in Table 5. Then, we denote the notations in Table 3. "H" means one-way hash function; "E" means the exponential operation. In Schneier [21], it mentioned that one modular exponentiation is similar to execute 600 hash functions.

Table 3. Performance comparisons

	Lin and Lai [20]	Lee and Chiu [16]	Yoon et al. [29]	Chang et al. [1]	Khan et al. [13]	Li and Hwang [19]	Our scheme
Registration Phase	1H+1E	2H+1E	1H	2H	2H	3H	1H
Login Phase	2H+2E	2H+1E	1H	2H	2H	2H	0H
Authentication Phase	1H+2E	2H	4H	6H	5H	5H	7H
Total	4H+5E	6H+2E	6H	10H	9H	10H	8H

The information in Table 3 shows that our scheme is more efficient than other related schemes. In Yoon et al.'s scheme, they just need six one-way hash functions. However, their scheme requires synchronized clocks between the user and the remote server because of the use of timestamps. We know that the system of synchronized clocks requires extra hardware to support this function. In our scheme, we just need two more one-way hash functions than their scheme and no extra hardware is needed. In real world usage, our scheme is more practical, and our main contribution is that we have developed an efficient, effective method that does not require the use of a traditional password.

Table 4. Functionality comparisons

	Lin and Lai [20]	Lee and Chiu [16]	Yoon et al. [29]	Chang et al. [1]	Khan et al. [13]	Li and Hwang [19]	Our scheme
Change password	YES	YES	YES	NO	YES	YES	YES
Mutual authentication	NO	NO	YES	YES	YES	YES	YES
Without synchronized clocks	NO	NO	NO	YES	NO	YES	YES
Provide non-repudiation	YES	NO	NO	NO	YES	YES	YES
Without traditional password	NO	NO	NO	NO	NO	NO	YES

In Table 5, we show the comparisons of withstanding the well-known attack, such as the smart card lost, forgery attack, off-line guessing attack, and replay attack, between Li and Hwang's scheme and ours. "I" means the smart card lost. "II" means the forgery attack. "III" means the off-line guessing attack. "IV" means the replay attack.

Table 5. Comparisons of security requirements

	I	II	III	IV
Li and Hwang's scheme	YES	YES	NO	YES
Our scheme	YES	YES	YES	YES

6. Conclusions

In this article, we propose an improved biometrics-based user authentication scheme without the use of a traditional password. This advantage is that the users just use their owned biometrics to be verified through the proposed system. They don't have to remember many passwords to pass any authentication protocol. To compare with other related schemes, our proposed scheme has higher efficiency and better functionality than others. Besides, we solve the weakness of Li and Hwang's scheme by employing just one factor to develop a novel method using the smart card. The comparisons show that our scheme is more secure, practical, and efficient than other related schemes. Hence, our novel method is most suitable for the wireless networks, such as mobile phone. In the future, we will apply our protocol to the different wireless networks.

7. References

- [1] Chang, Y. F., Chang, C. C., and Su, Y. W. "A secure improvement on the user-friendly remote authentication scheme with no time concurrency mechanism," *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06)*, Vienna, Austria, Vol. 2, pp. 741-745, Apr. 2006.
- [2] Chang, C.C. and Hwang, S.J. "Using smart cards to authenticate remote passwords," *Computers and Mathematical Applications*, Vol. 138, No. 3, pp. 165-168, 1993.
- [3] Chien, H.Y., Jan, J.K., and Tseng, Y.M. "An efficient and practical solution to remote authentication: smart card," *Computers and Security*, Vol. 21, No. 4, pp. 372-375, 2002.
- [4] Chang, C.C. and Liah, C.S. "Comment on remote password authentication with smart cards," *IEE Proceedings-Part E*, Vol. 139, No. 4, pp. 372-372, 1992.
- [5] Chang, C. C. and Lee, J. S. "An efficient and secure remote authentication scheme using smart cards," *Information & Security*, Vol. 18, pp. 122-133, 2006.
- [6] Chang, C.C. and Lee, W.B. "Cryptanalysis of an improved remote password authentication with smart card," *International Journal of Information Management and Engineering*, Vol. 2, No. 1, pp. 1-5, 1996.
- [7] Chang, C.C. and Liao, W.Y. "A remote password authentication scheme based upon ElGamal's signature scheme," *Computers and Security*, Vol. 13, No. 2, pp. 137-144, 1994.

- [8] Chang, C.C. and Wu, T.C. "Remote password authentication with smart cards," *IEE Proceedings-Part E*, Vol. 138, No. 3, pp. 165-168, 1991.
- [9] Hwang, M.S. and Li, L.H. "A new user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.
- [10] Hwang, M.S. and Liu, C.Y. "Authenticated encryption schemes: current status and key issues," *International Journal of Network Security*, Vol. 1, No. 2, pp. 61-73, 2005.
- [11] Jin, A.T.B., Ling, D.N.C., and Goh, A. "Biobhashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, Vol. 37, pp. 2245-2255, 2004.
- [12] Khan, M.K. and Zhang, J. "Improving the security of a flexible biometrics remote user authentication scheme," *Computer Standards and Interfaces*, Vol.29, No. 1, pp. 82-85, 2007.
- [13] Khan, M.K., Zhang, J., and Wang, X. "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," *Chaos, Solitons and Fractals*, Vol. 35, No. 3, pp. 519-524, 2008.
- [14] Kim, M. and Koc, C.K. "A simple attack on a recently introduced hash-based strong-password authentication scheme," *International Journal of Network Security*, Vol. 1, No. 2, pp. 70-80, 2005.
- [15] Lamport, L. "Password authentication with insecure communication," *Communications of ACM*, Vol. 24, pp. 770-772, 1981.
- [16] Lee, N.Y. and Chiu, Y.C. "Improved remote authentication scheme with smart card," *Computer Standards and Interfaces*, Vol. 27, No. 2, pp. 177-180, 2005.
- [17] Li, C.T. and Chu, Y.P. "Cryptanalysis of threshold password authentication against guessing attacks in ad hoc networks," *International Journal of Network Security*, Vol. 8, No. 2, pp. 166-168, 2009.
- [18] Li, C.T. and Hwang, M.S. "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, article in press, 2009.
- [19] Li, C.T. and Hwang, M.S. "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, Vol. 33, pp. 1-5, 2010.
- [20] Lin, C.H. and Lai, Y.Y. "A flexible biometrics remote user authentication scheme," *Computer Standards and Interfaces*, Vol. 27, No. 1, pp. 19-23, 2004.
- [21] Schneier, B. *Applied Cryptography, Protocols, Algorithms, and Source Code in C*, John Wiley and Sons Inc., 2nd Edition, New York, U.S.A., pp. 15, 1996.
- [22] Sun, H.M. "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, pp. 958-961, 2000.
- [23] Shen, J.J., Lin, C.W., and Hwang, M.S. "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 2, pp. 414-416, 2003.
- [24] Shen, J.J., Lin, C.Y., and Tang, H.W. "Cryptanalysis of a new efficient makeup for wireless communications," *International Journal of Network Security*, Vol. 1, No. 2, pp. 118-121, 2005.
- [25] Tan, K. and Zhu, H. "Remote password authentication scheme based on cross-product," *Computer Communications*, Vol. 18, pp. 390-393, 1999.
- [26] Wu, S.Y. and Chieu, B.C. "A user friendly remote authentication scheme with smart cards," *Computers and Security*, Vol. 22, No. 6, pp. 547-550, 2003.
- [27] Wu, T.C. "Remote login authentication scheme based on a geometric approach," *Computer Communications*, Vol. 18, No. 12, pp. 959-963, 1995.
- [28] Yamaguchi, S., Okayama, K., and Miyahara, H. "Design and implementation of an authentication system in WIDE internet environment," *Proceedings of IEEE Region Conference on Computer and Communication System*, Hong Kong, pp. 653-657, September 1990.
- [29] Yoon, E.J., Ryu, E.K., Yoo, K.Y. "An improvement of Hwang-Lee-Tang's simple remote user authentication scheme," *Computers and Security*, Vol. 24, No. 1, pp. 50-56, 2005.