J Med Syst (2013) 37:9941
DOI 10.1007/s10916-013-9941-8

ORIGINAL PAPER

A Secure and Efficient Password-Based User Authentication Scheme Using Smart Cards for the Integrated EPR Information System

Tian-Fu Lee · I-Pin Chang · Tsung-Hung Lin · Ching-Cheng Wang

Received: 19 November 2012 / Accepted: 18 March 2013 / Published online: 4 April 2013

Abstract The integrated EPR information system supports convenient and rapid e-medicine services. A secure and efficient authentication scheme for the integrated EPR information system provides safeguarding patients' electronic patient records (EPRs) and helps health care workers and medical personnel to rapidly making correct clinical decisions. Recently, Wu et al. proposed an efficient password-based user authentication scheme using smart cards for the integrated EPR information system, and claimed that the proposed scheme could resist various malicious attacks. However, their scheme is still vulnerable to lost smart card and stolen verifier attacks. This investigation discusses these weaknesses and proposes a secure and efficient authentication scheme for the integrated EPR information system as alternative. Compared with related approaches, the proposed scheme not only retains a lower computational cost and does not require verifier tables for storing users' secrets, but also solves the security problems in previous schemes and withstands possible attacks.

Keywords Integrated EPR information system · Network security · Password · Mutual authentication

T.-F. Lee (✉)
Department of Medical Informatics, Tzu Chi University,
No. 701, Zhongyang Road, Sec. 3,
Hualien 97004, Taiwan, Republic of China
e-mail: jackytflee@mail.tcu.edu.tw

T.-F. Lee
e-mail: tflee@ismail.csie.ncku.edu.tw

I.-P. Chang · C.-C. Wang
Institute of Manufacturing Information and Systems,
National Cheng Kung University, No. 1, Ta-Hsueh Road,
Tainan 70101, Taiwan, Republic of China

I.-P. Chang
Department of Digital Applications, Kang Ning University,
No. 188, Sec. 5, Anzhong Road,
Tainan 70970, Taiwan, Republic of China

T.-H. Lin
Department of Computer Science and Information Engineering,
National Chin-Yi University of Technology, Taichung County
411, Taiwan, Republic of China

Introduction

Nowadays, with the development of internet, the integrated EPR information system makes it be possible to share the patients' medical histories such as patients' privacy, diagnosis records and reports among hospitals. The security and privacy issues of EPRs are important for the patients to understand how the hospitals control the use of their personal information, such as name, telephone, address, e-mail and medical records, etc [1, 2]. Secure and efficient authentication schemes for the integrated EPR information system can realize the goals described above and can help health care workers and medical personnel to rapidly making correct clinical decisions.

Recently, many related authentication approaches for the integrated EPR information system were proposed in succession. For example, Takeda et al. [3] in 2000 proposed the architecture for networked electronic patient record systems. Lee et al. [4] in 2002 proposed a fingerprint-based remote user authentication scheme by using smart cards and biometrics. Lin and Lia [5] in 2004 pointed out that the scheme of Lee et al. was vulnerable to masquerade attacks and proposed an improved flexible scheme to enhance the security problem.

Lee and Chiu [6] in 2005 proposed an improved remote authentication scheme based on the remote authentication scheme using smart cards of Wu and Chieu [7]. Wu et al. [8] in 2010 used pre-computing concepts to develop an efficient authentication scheme for telecare medicine information systems. Later, He et al. [9] stated the weaknesses of the scheme proposed by Wu et al., and proposed an improved scheme to improve the weaknesses in security. In 2012, Wei et al. [10] stated that both of the authentication schemes of Wu et al. and He et al. cannot achieve a two-factor authentication. Wei et al. also proposed an improved authentication scheme and claimed their scheme could withstand various attacks. However, the scheme of Wei et al. still had weaknesses, which was showed by Zhu [11]. In 2012, Wu et al. [12] proposed a reliable user authentication and key agreement scheme for HAI surveillance information system.

Additionally, Wu et al. [2] in 2012 used lower computational operations including hash, exclusive-or and multiplication operations to develop an efficient password-based authentication scheme for the integrated EPR information system. They also claimed their scheme could resist various malicious attacks. However, in the scheme of Wu et al., if an adversary steals a copy of the verifier in the authentication server's database, then can derive all secrets and successfully masquerade as a legitimate user. Additionally, if an adversary steals a user's smart card and, then he/she knows all the user's secrets and easily masquerade as a legitimate user. That is, the scheme of Wu et al. is vulnerable to lost smart card and stolen verifier attacks.

This investigation will discuss the weaknesses of the scheme proposed by Wu et al. Also, a secure and efficient authentication scheme for the integrated EPR information system is proposed. There are many approaches were proposed for overcoming the possible attacks described above. For example, Song in 2010 [13] presented a smart card based password authentication protocol based on the Discrete Logarithm Problem (DLP) [14]. Kumar et al. in 2011 [15] demonstrated the weaknesses of the remote password authentication schemes proposed by Yoon and Yoo [16] and Xiang et al. [17] and presented an improved authentication scheme, which was also based on the Discrete Logarithm Problem (DLP), as alternative. In addition, Ramasamy and Muniyandi [18] in 2012 developed a smart card based password authentication protocol based on RSA [19]. However, all these authentication schemes required some heavy exponential computations. In order to solve the security problems and provide lower computational cost, the proposed authentication scheme protects the user's password with a secret key in the user's smart cards, and uses the one-way hash function to protect users' passwords for server's authentications such that the server cannot directly derive them from the revealed messages. Thus, the proposed scheme not only keeps the advantages of the scheme of Wu et al. including a lower computational cost and no verifier tables in the server, but also solves the security problems in previous schemes and withstands possible attacks.

The rest of this paper is organized as follows. The next section defines the notation used in this paper and reviews the scheme of Wu et al. Section "The weaknesses of the scheme of Wu et al." shows the possible attacks against the scheme of Wu et al. The subsequent section introduces the proposed authentication scheme. The security and performance analyses are described in "Security analyses" and "Performance analyses". Finally, Section "Conclusions" concludes the paper.

Review of the authentication scheme of Wu et al.

This section first lists the notation used throughout this work and then briefly reviews the authentication scheme created by Wu et al. [2] and its weaknesses. In this work, *U* denotes the medical service requester (user); *ID* denotes the identifier of *U*; and *S* denotes the integrated EPR information system server, which *U* registers in. Table 1 lists the notations used throughout this work.

Wu et al. [2] in 2012 proposed a password-based user authentication scheme for the integrated EPR information system. Their scheme comprises four phases including registration, login, verification and password change phases, which works as follows.

Registration phase

A user *U* registers his/her identity *ID* and password *pw* to the integrated EPR information system *S* by performing the following steps:

Step 1: User *U* submits the registration request *ID* and *pw* to the server *S*.

Step 2: The server *S* verifies the validity of the user *ID*, and then computes $v = h(K \oplus ID)$, where *K* is the secret number belonging to *S*.

Table 1 Notation

pw	The password of *U*.
h( )	The secure one-way hash function.
⊕	The bitwise XOR operation.
⇒	The secure channel.
→	The common channel.
||	The bit concatenation operator.

Step 3: S finds N such that the sum of $v{\cdot}pw + N$ equals a constant secret value H. Then S computes $s = h(pw||K)$.

Step 4: S personalizes U's medical smart card included with the above parameters $\{h(\bullet), N, s, pw\}$. The number s is stores into smart card.

Step 5: $S \Rightarrow U$: Finally, the server S returns the medical smart card to user U through a secure channel.

Login phase

Whenever a user U wants to login the integrated EPR information system server S, U inserts his smart card into the smart card reader of a terminal, enters ID and pw, and then executes the following steps.

Step 1: U's smart card chooses a random number r_1, and then computes $C_1 = h(s||r_1)$ and $C_2 = r_1{\cdot}pw$.

Step 2: $U \rightarrow S$ with parameters (N, ID, C_1, C_2).

Verification phase

After receiving the request message (N, ID, C_1, C_2) from U, S executes the following steps.

Step 1: If S successfully verifies the validity of ID, then accepts the user U request; otherwise, rejects this service request.

Step 2: Compute $v = h(K \oplus ID)$ and $pw = (H - N){\cdot}v^{-1}$.

Step 3: Compute $r_1' = pw^{-1}{\cdot}C_2 = pw^{-1}{\cdot}pw{\cdot}r_1$ and $s' = h(pw||K)$.

Step 4: If $h(s'||r_1')$ equals to C_1, go to Step 5; otherwise, stop and reply the error message to U.

Step 5: Generate the message pair (a, b) for a mutual authentication between S and U, where $a = r_2 \oplus h(s')$, $b = h(pw \,||\, r_2 \,||\, r_1')$, and r_2 is a random number.

Step 6: $S \rightarrow U$ with (a, b).

After receiving the reply message (a, b) from S, U executes the following steps.

Step 1: Restore r_2' through $r_2' = \mathrm{a} \oplus h(s)$.

Step 2: Check $b = h(pw \,||\, \mathrm{r}_2' \,||\, r_1)$. If successful, user U confirms that S is valid.

Step 3: $U \rightarrow S$ with $c = h(pw \,||\, r_1 \,||\, r_2')$ for another side authentication.

After receiving the message c from U, S executes the following steps.

Step 1: Check $c = h(pw \,||\, r_1' \,||\, r_2)$. If successful, U is authenticated. Finally, U and S can generate a common session key $sk = h(r_1'||r_2) = h(r_1||r_2')$ used for later secure transmission.

Password change phase

The legal user U changes his/her password by executing the following steps.

Step 1: $U \Rightarrow S$ with parameters (ID, pw, pw_{new}).

Step 2: S computes $v = h(K \oplus ID)$ and finds another appropriate N^* such that the value $v{\bullet}pw_{new} + N^*$ equals the secret value H. Then S computes $s = h(pw_{new} \,||\, K)$, and sends it with the N^* to U through the secure channel.

The weaknesses of the scheme of Wu et al.

Wu et al. presented an efficient authentication scheme in order to solve the weaknesses of the previous authentication schemes. However, in the authentication scheme of Wu et al., if an adversary steals a copy of the verifier in S's database, then can derive all secrets and thus can masquerade as a legitimate user. Additionally, if an adversary steals U's smart card and, then he/she knows all U's secrets, and can easily masquerade as a legitimate user U. Thus, the scheme of Wu et al. is vulnerable to lost smart card and stolen verifier attacks. The scenarios are described as follows.

Security against lost smart card attacks

If an adversary $\mathcal{A}$ steals U's smart card and obtains the message $\{h(\cdot), N, s, pw\}$, then he/she can easily compute and send out the request message (N, ID, C_1, C_2), where r_1 is a random number, $C_1 = h(s||r_1)$ and $C_2 = r_1{\cdot}pw$. Since $\mathcal{A}$ knows all U's secrets and thus can masquerade as a legitimate user U. Therefore, the scheme of Wu et al. is vulnerable to the lost smart card attacks

Security against stolen verifier attacks

An adversary $\mathcal{A}$ steals a copy of the verifier $\{K, H, h(.)\}$ in S's database and records $\{ID, N\}$ from a successful authentication of a certain user U. Then $\mathcal{A}$ computes $v = h(K \oplus ID)$, $pw = (H - N){\cdot}v^{-1}$ and $s = h(pw|| K)$. $\mathcal{A}$ has $\{h(), N, s, pw\}$ and thus can masquerade as a legitimate user. Therefore, the scheme of Wu et al. is vulnerable to the stolen verifier attacks.

The proposed secure and efficient authentication scheme

This section presents a secure and efficient authentication scheme, which protects the password with a secret key in the user's smart cards. In order to prevent that the adversary steals a user's smart card and obtains the valuable message, and masquerades as a legitimate user, the proposed authentication scheme protects the user's password with a secret key in the user's smart cards. Additionally, the proposed scheme uses the one-way hash function to protect users' passwords for server's authentications such that the server is able to verify users' passwords, but cannot directly derive them from the revealed messages. We adopt lower computational operations, such as XOR and hash operations, to develop the proposed scheme. Thus, it can avoid the weaknesses described above and have a lower computational cost. The proposed scheme also comprises registration, login, verification and password change phases, which works as follows.

Registration phase

A user U registers his/her identity ID and password pw to the integrated EPR information system S by performing the following steps.

Step 1: User U submits the registration request ID and pw to the server S via a secure channel.
Step 2: The server S verifies the validity of the user ID, and then computes $v = h(K \oplus ID)$, where K is the secret number of S.
Step 3: S computes $s_1 = h(pw\|K)$, $s_2 = h(h(pw\|s_1))$ and $N = v \oplus s_2 \oplus H$, where H is a constant secret value.
Step 4: S personalizes U's medical smart card included with the above parameters $\{ID, h(\cdot), N, s_1\}$.
Step 5: $S \Rightarrow U$: Finally, the server S returns the medical smart card to user U through a secure channel.

Figure 1 illustrates the login and verification phases of the proposed authentication scheme, which functions as follows.

Login phase

Whenever a user U wants to login the integrated EPR information system server S, U inserts his smart card into the smart card reader of a terminal, enters ID and pw, and then executes the following steps.

Step 1: U's smart card chooses a random number r_1, and then computes $s_2 = h(h(pw\|s_1))$ and $C_1 = r_1 \oplus s_2$.
Step 2: $U \rightarrow S$ with parameters (N, ID, C_1).

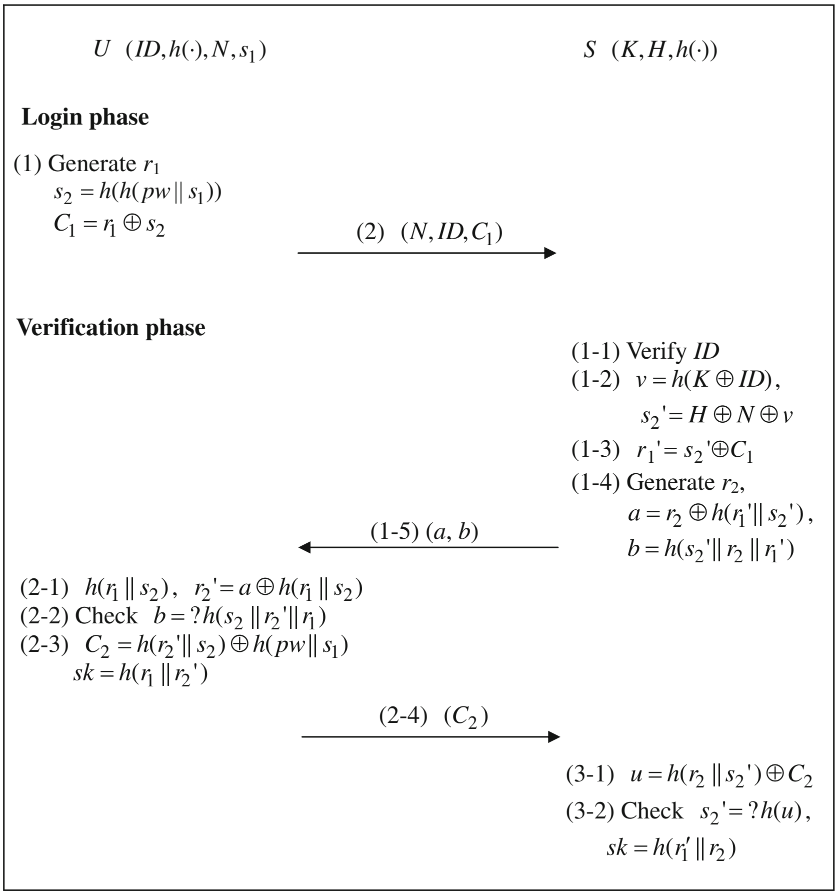
$U \ (ID, h(\cdot), N, s_1)$
$S \ (K, H, h(\cdot))$
Login phase
(1) Generate r_1
$s_2 = h(h(pw \| s_1))$
$C_1 = r_1 \oplus s_2$
(2) (N, ID, C_1)
Verification phase
(1-1) Verify ID
(1-2) $v = h(K \oplus ID)$,
$s_2' = H \oplus N \oplus v$
(1-3) $r_1' = s_2' \oplus C_1$
(1-4) Generate r_2,
$a = r_2 \oplus h(r_1' \| s_2')$,
$b = h(s_2' \| r_2 \| r_1')$
(1-5) (a, b)
(2-1) $h(r_1 \| s_2)$, $r_2' = a \oplus h(r_1 \| s_2)$
(2-2) Check $b = ?h(s_2 \| r_2' \| r_1)$
(2-3) $C_2 = h(r_2' \| s_2) \oplus h(pw \| s_1)$
$sk = h(r_1 \| r_2')$
(2-4) (C_2)
(3-1) $u = h(r_2 \| s_2') \oplus C_2$
(3-2) Check $s_2' = ?h(u)$,
$sk = h(r_1' \| r_2)$

Fig. 1 The login and verification phases of proposed authentication scheme

Verification phase

After receiving the request message (N, ID, C_1) from U, the integrated EPR information system server S executes the following steps.

Step 1-1: If S successfully verifies the validity of ID, then accepts the user U request; otherwise, rejects this service request.
Step 1-2: Compute $v = h(K \oplus ID)$ and $s_2' = H \oplus N \oplus v$.
Step 1-3: Compute $r_1' = s_2' \oplus C_1 = s_2' \oplus (s_2 \oplus r_1)$.
Step 1-4: Generate the message pair (a, b) for a mutual authentication between S and U, where $a = r_2 \oplus h(r_1' \| s_2')$, $b = h(s_2' \| r_2 \| r_1')$, and r_2 is a random number.
Step 1-5: $S \rightarrow U$ with (a, b).

After receiving the reply message (a, b) from S, U executes the following steps.

Step 2-1: Compute $h(r_1 \| s_2)$ and $r_2' = a \oplus h(r_1 \| s_2)$.
Step 2-2: Check $b = h(s_2 \| r_2' \| r_1)$. If successful, U confirms that S is valid.
Step 2-3: Compute $C_2 = h(r_2' \| s_2) \oplus h(pw \| s_1)$.
Step 2-4: $U \rightarrow S$ with C_2 for S's authentication.

After receiving C_2 from U, S executes the following steps.

Step 3-1: Compute $u = h(r_2 \| s_2') \oplus C_2 = h(r_2 \| s_2')(\oplus h(r'_2 \| s_2) \oplus h(pw \| s_1))$.
Step 3-2: If S successfully checks $s_2' = h(u)$, U is authenticated. Finally, U and S can generate a common session key $sk = h\left(r_1' || r_2\right) = h\left(r_1 || r_2'\right)$ used for later secure transmission.

Password change phase

Any legal user U can change the password by using the following steps.

Step 1: $U \Rightarrow S$ with parameters (ID, pw, pw_{new}).
Step 2: S computes $v = h(K \oplus ID)$, $s_1^* = h(pw_{new} \| K)$, $s_2^* = h\left(h\left(pw \| s_1^*\right)\right)$ and $N^* = v \oplus s_2^* \oplus H$. Then, S sends $\left(s_1^*,\ N^*\right)$ to U through the secure channel. Finally, U updates his/her medical smart card as $\left\{ID, h(\cdot), N^*, s_1^*\right\}$.

Security analyses

This section shows that the proposed authentication scheme can resist possible attacks including off-line password guessing attacks, undetectable on-line password guessing attacks, stolen verifier attacks, and lost smart card attacks. For data transmission security, user masquerading detection and server spoofing detection, the analyses of the proposed scheme are similar to those of the scheme of Wu et al. Thus these analyses are not presented here.

Resistance to off-line password guessing attacks

In the proposed scheme, no information helps to verify directly the correctness of the guessed passwords based on C_1, (a, b) and C_2, where $C_1 = r_1 \oplus s_2$, $a = r_2 \oplus h(r_1 \| s_2)$, $b = h(s_2 \| r_2 \| r_1)$ and $C_2 = h(r_2 \| s_2) \oplus h(pw \| s_1)$, $s_1 = h(pw \| K)$ and $s_2 = h(h(pw \| s_1))$, because that r_1 and r_2 are two random numbers and are protected by the secret keys s_1 and s_2. Thus, offline password guessing attacks are unsuccessful against the proposed protocol.

Resistance to undetectable on-line password guessing attacks

In proposed scheme, an adversary $\mathcal{A}$, who disguises as U, sends a request message (N, ID, C_1^*) to S, where C_1^* may be a previous used message or a random number. Then, S computes v, s_2' and $r_1' = s_2' \oplus C_1^*$, generates a random number r_2 , computes and sends (a, b) to U, where $a = r_2 \oplus h(r_1' \| s_2')$ and $b = h(s_2' \| r_2 \| r_1')$. After receiving ($a$, b), $\mathcal{A}$ cannot correct compute $C_2 = h(r_2' \| s_2) \oplus h(pw \| s_1)$ for S' authentication without the random secrets r_1, r_2, and the secret keys s_1, s_2; then a failed guess must be detected by S in Step 2-4 of the verification phase.

Table 2 The performance comparisons of the related schemes and the proposed scheme

	Lin-Lia [5]	Lee-Chiu [6]	Lu et al. [20]	Wang et al. [21]	Wu et al. [2]	Proposed scheme
Computations in registration phase	1H+1E	2H+1E	1H	2H	2H	4H
Computations in login phase	2H+2E	2H+2E	1EC	2H	1H+1M	2H
Computations in verification phase	1H+2E	2H	3H+2EC	6H	10H+1M	10H
Resisting possible attacks	Yes	Yes	No	No	No	Yes

H one way hash function operations; *M* multiplication operations; *E* exponential operations; *EC* elliptic curve exponential operations

Resistance to stolen verifier attacks

An adversary $\mathcal{A}$ steals a copy of the verifier $\{K, H, h(.)\}$ in S's database and records $\{ID, N\}$ from a successful authentication of a certain user U. Although $\mathcal{A}$ can obtain s_2 by computing $v = h(K \oplus ID)$ and $s_2 = H \oplus N \oplus v$, $\mathcal{A}$ cannot derive the correct pw because of the one-way hash property, where $s_1 = h(pw||K)$, $s_2 = h(h(pw||s_1))$. He/she cannot compute and send out the correct messages (N, ID, C_1) in the login phase and $C_2(= h(r_2'||s_2) \oplus h(pw||s_1))$ in Step 2-4 of the verification phase, and thus cannot masquerade as a legitimate user. Therefore, the proposed scheme can resist the stolen verifier attacks.

Resistance to lost smart card attacks

If an adversary $\mathcal{A}$ steals U's smart card and obtains the message $\{ID, h(\cdot), N, s_1\}$, then he/she cannot compute and send out the correct messages (N, ID, C_1) in the login phase and C_2 in Step 2-4 of the verification phase, without the correct pw, where r_1 is a random number, $s_2 = h(h(pw||s_1)) = h^2(pw||s_1)$ and $C_1 = r_1 \oplus s_2$, and $C_2 = h(r_2'||s_2) \oplus h(pw||s_1)$. A fail login will be detected by S in Step 3-2 of the authentication phase, and thus the proposed scheme can resist lost smart card attacks.

Performance analyses

Table 2 lists the performance comparisons of related schemes and the proposed scheme. Both the scheme of Wu et al. and the proposed scheme do not require heavy exponential operations and elliptic curve exponential operations, and thus more efficient than other related schemes. Although the scheme of Wu et al. requires fewer hash function operations than the proposed scheme, the scheme of Wu et al. employs multiplication operations and requires more computations to find the inverses of some numbers. Moreover, the proposed scheme solves the security problems in previous schemes and withstands possible attacks. Thus, the proposed scheme is superior to other related schemes.

Conclusions

This investigation addresses the weaknesses of the authentication scheme of Wu et al., including suffering from the stolen verifier attacks and lost smart card attacks. This investigation also presents a secure and efficient authentication scheme for the integrated EPR information system. The proposed authentication scheme still retains lower computational cost and does not require verifier tables for storing users' secrets. Additionally, the proposed scheme solves the security problems in previous schemes and withstands possible attacks. Thus, the proposed authentication scheme for the integrated EPR information system can provide users with a secure and efficient practical environment.

Acknowledgment The authors would like to thank the editor and the anonymous referees for their valuable comments. This work was supported in part by the National Science Council of the Republic of China under the Grant NSC 100-2221-E-320-004.

References

1. Chen, T. L., Chung, Y. F., and Lin, F. Y. S., A study on agent-based secure scheme for electronic medical record system. *J. Med. Syst.* 2012. doi:10.1007/s10916-010-9595-8.
2. Wu, Z. P., Chung, Y., Lai, F., and Chen, T. S., A password-based user authentication scheme for the integrated EPR information system. *J. Med. Syst.* 36(2):631–638, 2012.
3. Takeda, H., Matsumura, Y., and Kuwata, S., Architecture for networked electronic patient record systems. *Int. J. Med. Inform.* 60(2):161–167, 2000.
4. Lee, J. K., Ryu, S. R., and Yoo, K. Y., Fingerprint-based remote user authentication scheme using smart cards. *Electron. Lett.* 38(12):554–555, 2002.
5. Lin, C. H., and Lai, Y. Y., A flexible biometrics remote user authentication scheme. *Comput. Stand. Interfaces* 27(1):19–23, 2004.
6. Lee, N. Y., and Chiu, Y. C., Improved remote authentication scheme with smart card. *Comput. Stand. Interfaces* 27(2):177–180, 2005.
7. Wu, S. T., and Chieu, B. C., A user friendly remote authentication scheme with smart cards. *Comput. Secur.* 22(6):547–550, 2003.
8. Wu, Z. Y., Lee, Y. C., Lai, F., Lee, H. C., and Chung, Y., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 2010. doi:10.1007/s10916-010-9614-9.
9. He, D. B., Chen, J. H., and Zhang, R., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 2011. doi:10.1007/s10916-011-9658-5.
10. Wei, J., Hu, X., and Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 2012. doi:10.1007/s10916-012-9835-1.
11. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 2012. doi:10.1007/s10916-012-9856-9.
12. Wu, Z. Y., Tseng, Y. J., Chung, Y., Chen, Y. C., and Lai, F., A reliable user authentication and key agreement scheme for Web-based Hospital-acquired Infection Surveillance Information System. *J. Med. Syst.* 36:2547–2555, 2012.
13. Song, R., Advanced smart card based password authentication protocol. *Comput. Stand. Interfaces* 32(5–6):321–325, 2010.
14. Stallings, W., *Cryptography and network security: principles and practice*, 2nd edition. Prentice Hall, Upper Saddle River, 1999.
15. Kumar, M., Gupta, M. K., and Kumari, S., An improved efficient remote password authentication scheme with smart card over insecure network. *Int. J. Netw. Secur.* 13(3):167–177, 2011.
16. Yoon, E. J., and Yoo, K. Y., Drawbacks of Liao et al.'s password authentication scheme. *International Conference on Next Generation Web Services Prac-tices (NWeSP 2006)*, Seoul, Korea, 2006.
17. Xiang, T., Wong, K. W., and Liao, X., Cryptanalysis of a password authentication scheme over insecure networks. *J. Comput. Syst. Sci.* 74(5):657–661, 2008.

18. Ramasamy, R., and Muniyandi, A. P., An efficient password authentication scheme for smart card. *Int. J. Netw. Secur.* 14(3):180–186, 2012.
19. Rivest, R. L., Shamir, A., and Adleman, L., A method for obtaining digital signature and public key cryptosystems. *Commun. ACM* 21(2):120–126, 1978.
20. Lu, R., Cao, Z., Chai, Z., and Liang, X., A simple user authentication scheme for grid computing. *Int. J. Netw. Secur.* 7(2):202–206, 2008.
21. Wang, Y. Y., Liu, J. Y., Xiao, F. X., and Dan, J., A more efficient and secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* 32:583–585, 2009.