J Med Syst (2014) 38:42
DOI 10.1007/s10916-014-0042-0

MOBILE SYSTEMS

A More Secure Anonymous User Authentication Scheme for the Integrated EPR Information System

Fengtong Wen

Received: 4 November 2013 / Accepted: 18 March 2014 / Published online: 24 April 2014

Abstract Secure and efficient user mutual authentication is an essential task for integrated electronic patient record (EPR) information system. Recently, several authentication schemes have been proposed to meet this requirement. In a recent paper, Lee et al. proposed an efficient and secure password-based authentication scheme used smart cards for the integrated EPR information system. This scheme is believed to have many abilities to resist a range of network attacks. Especially, they claimed that their scheme could resist lost smart card attack. However, we reanalyze the security of Lee et al.'s scheme, and show that it fails to protect off-line password guessing attack if the secret information stored in the smart card is compromised. This also renders that their scheme is insecure against user impersonation attacks. Then, we propose a new user authentication scheme for integrated EPR information systems based on the quadratic residues. The new scheme not only resists a range of network attacks but also provides user anonymity. We show that our proposed scheme can provide stronger security.

Keywords Integrated EPR information systems · Authentication · Smart card · Anonymity · Quadratic residues

Introduction

Nowadays, with the increase of people's average life span, more and more chronic patients require long-term follow-ups, such that most of them are required to go to hospital for checkups and treatments. Such treatments not only consume huge human and material resources but also reduce patients' quality of life. In order to solve this kind of situation, wireless network technology was used by many hospitals to transmit information instead of using labor power. Patients can send or access their health information for health monitoring and healthcare related services by the network technology. Their physiological information can be monitored instantly.

A integrated EPR information system can help health care workers and medical personnel to make correct clinical decision rapidly. The registered user can get various services from the medical server. In integrated EPR information system, with the rapid development of computer and information technologies, the control of the access to remote medical server's resources has become a crucial challenge [2]. A secure remote authentication scheme is needed to protect confidentiality and data integrity. Recently, a lot of research work (e.g. [5, 6, 8, 9, 11, 15–18, 21, 24–26, 29]) has been done in the design and analysis of user authentication protocols for integrated EPR information systems. However, most of the existing protocols were broken shortly after they were proposed.

Most of Current integrated EPR information systems are smart-card-based password authentication; it involves a server S and a client U_i. At first, S securely issues a smart-card to U_i with the smart-card being personalized with respect to ID_i and an initial password in the registration phase. This phase is carried out only once for each client. Later on, U_i can access S in the login-and-authentication phase based on his/her smart card and password, and this phase can be carried out as many times as needed. However, in login-and-authentication phase, there could have various kinds of passive and active adversaries in the

---

This article is part of the Topical Collection on *Mobile Systems*

F. Wen (✉)
School of Mathematical Sciences, University of Jinan,
Jinan 250022, China
e-mail: wftwq@163.com

communication channel between U_i and S. They can eavesdrop on messages and even modify, remove or insert messages into the channel. One famous attack is off-line guessing attack (also known as off-line dictionary attack). The purpose of off-line guessing attack is to compromise a client's password through exhaustive search of all possible password values. If the adversary also obtains the information stored in the smart card, the probability of getting the password will greatly increase. Therefore, one security requirement for smart-card-based password authentication is security against off-line guessing attack. In particular, an adversary should not launch off-line guessing attack against the client's password even if a client's smart-card is compromised. In practice, the adversary may steal the smart-card and extract all the information stored in it through reverse engineering [7, 13]. So, for a secure smart-card-based password authentication scheme, we require that the client's password should remain secure even after the client's smart-card is compromised.

In 2012, Wu et al. [23] 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, Lee et al. [10] pointed out that their scheme is vulnerable to lost smart card attack and stolen verifier attack. Then, Lee et al. proposed a new scheme and claimed that it can resist those attacks.

User anonymity and untraceability are very important security features. They are desirable to keep users' identities anonymous and not to be traced in the remote user authentication process in integrated EPR information system. Recently, some research work (e.g. [1, 2, 12, 19, 20, 22, 28]) have been done in the design and analysis of anonymous authentication protocols. However, most of them exists some flaws.

Our contributions First, we analyzed Lee et al.' scheme and claimed that their scheme is still vulnerable to lost smart card attack. If the adversary obtained the secret information stored in user's smart card, he/she can obtain the user's password by off-line password guessing attack. Then, the adversary can impersonate the user to fool the server.

Second, in this paper, we propose a novel anonymous user authentication protocol based smart card for integrated EPR information system that can achieve the following properties: resist lost smart card attack; provide user anonymity; provide mutual authentication.

Organization of the paper The rest of this paper is organized as follows. We provide some mathematical preliminaries in section"Mathematical preliminaries", which will be used throughout the paper. In section "Review Lee et al.'s scheme", we briefly review Lee et al.'s scheme. Subsequently, we show its weaknesses in section "Flaws of Lee et al.'s scheme". Then, we proceed with proposing our scheme in section "The proposed scheme", together with analyzing its security in section "Security analysis". In section "Performance comparison", we compare the performance of our new protocol with others previous scheme [3, 10, 23, 27]. Section "Conclusion" concludes the paper.

Notations In Table 1, we list the notations used throughout this paper.

Table 1 Notations used in this paper

U_i	The user
ID_i	Identity of U_i
pw_i	Password of U_i
S	the remote medical server for the EPR
K	secret key of S
ctr_i	A counter maintained by U_i
$h(\cdot)$	A secure collision-free one-way hash function
$\oplus$	the bitwise XOR operation
$\|$	the concatenation operation

Mathematical preliminaries

In this section, we discuss quadratic residue problem which will be used in the proposed scheme.

Quadratic residue problem Assume that $n = pq$, where p and q are two large primes. If $y = x^2 \ mod \ n$ has a solution, i.e., there exists a square root for y, then y is called a quadratic residue $mod \ n$. The set of all quadratic residue numbers in $[1, n-1]$ is denoted by QR_n. Then the quadratic residue problem states that, for $y \in QR_n$, it is hard to find x without the knowledge of p and q due to the difficulty of factoring n [14]. Some related authentication schemes are designed based on quadratic residues [3, 27].

Review Lee et al.'s scheme

There are four phases in Lee et al.'s scheme.

Registration phase

A user U_i registers his/her identity ID_i and password pw_i to the integrated EPR information system S by performing the following steps.

Step 1: The patient U_i submits his/her registration request (ID_i, pw_i) to the server S via a secure channel.

Step 2: The server S verifies the legitimacy of ID_i and computes $v = h(K \oplus ID_i)$, where K is the secret number of S.

Step 3: S computes $s_1 = h(pw_i \| K)$, $s_2 = h(h(pw_i \| s_1))$ and $N = v \oplus s_2 \oplus H$, where H is a constant secret value.

Step 4: S issues the smart card, containing $ID_i, h()$, N, s_1.

Step 5: S sends the smart card to U_i over a secure channel.

Login phase

Whenever a user U_i wants to login the integrated EPR information system server S, he/she proceeds the following steps:

Step 1: U_i's smart card chooses a random number r_1 and computes $s_2 = h(h(pw_i \| s_1))$ and $C_1 = r_1 \oplus s_2$.

Step 2: U_i sends (N, ID_i, C_1) to S.

Verification phase

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

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

Step 1–2: Compute $v = h(K \oplus ID_i)$ and $s_2' = H \oplus N \oplus v$.

Step 1–3: Compute $r_1' = s_2' \oplus C_1 = s_2' \oplus s_2 \oplus r_1$.

Step1–4: Compute $a = r_2 \oplus h(r_1' \| s_2')$, $b = h(s_2' \| r_2 \| r_1')$, where r_2 is a random number.

Step 1–5: S sends $(a,\ b)$ to U_i.

After receiving the reply message $(a,\ b)$ from S, U_i 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_i confirms that S is valid.

Step 2–3: $C_2 = h(r_2' \| s_2) \oplus h(pw_i \| s_1)$.

Step 2–4: U_i sends C_2 to S.

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

Step 3–1: Compute $u = h(r_2 \| s_2') \oplus C_2 = h(r_2 \| s_2') \oplus h(r_2' \| s_2) \oplus h(pw_i \| s_1)$.

Step 3–2: If S successfully checks $s_2' = h(u)$, U_i is authenticated.

Finally, U_i 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

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

Step 1: U_i sends $(ID_i,\ pw_i,\ pw_{new})$ to S.

Step 2: S computes $v = h(K \oplus ID_i)$, $s_1^* = h(pw_{new} \| K)$, $s_2^* = h(h(pw_{new} \| s_1^*))$ and $N^* = v \oplus s_2^* \oplus H$. Then, S sends $(s_1^*,\ N^*)$ to U_i through the secure channel. Finally, U_i updates his/her medical smart card as $(ID_i, h(),\ N^*,\ s_1^*)$.

Figure 1 illustrates the login and verification phases of Lee et al.'s scheme.

Flaws of Lee et al.'s scheme

Security against lost smart card attack

Lee et al. proposed a secure and efficient password-based authentication scheme and claimed that it can resist off-line password guessing attack and lost smart card attack.

In this section, we show that Lee et al.'s scheme is vulnerable to lost smart card attack. If an adversary A obtains the message $ID_i, h(.), N, s_1$ stored in U_i's smart card and the transmitted message C_1, (a, b), then he/she can get the U_i's password pw_i by the following steps:

Step 1. The adversary A chooses pw_i^* and computes $s_2^* = h(h(pw_i^* \| s_1)), r_1^* = C_1 \oplus S_2^* = C_1 \oplus h(h(pw_i^* \| s_1))$.

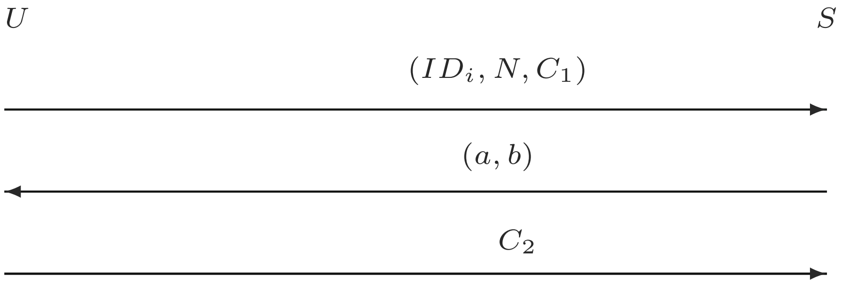

Fig. 1 Message flows in login and authentication phase

Step 2. The adversary A computes $r_2^* = a \oplus h(r_1^* \| s_2^*) = a \oplus h(C_1 \oplus h(h(pw_i^* \| s_1)) \| \, h(h(pw_i^* \| s_1)))$.

Step 3. The adversary A computes $b^* = h(s_2^* \| r_2^* \| r_1^*) = h(h(h(pw_i^* \| s_1)) \| (a \oplus h(C_1 \oplus h(h(pw_i^* \| s_1)) \| h(h(pw_i^* \| s_1)))) \| (C_1 \oplus h(h(pw_i^* \| s_1))))$.

Step 4. The adversary A verifies whether $b^* = b$ or not. If it holds, the adversary obtains the correct password pw_i of legal user U_i. Otherwise, the adversary A repeats the above steps until the correct password is found.

When an adversary obtains the password of user U_i, he/she can impersonate U_i to cheat the server S. Hence, Lee et al's scheme cannot resist impersonation attack and provide mutual authentication.

The proposed scheme

In this section, we propose a new authentication scheme with privacy preservation for integrated EPR information system. The new scheme can resist against a range of attacks, such as off-line password guessing attack, stolen verifier attack, and lost smart card attack, etc.

Before the system begins, S generates two secret large primes p, q and computes the number $n = pq$. The new protocol has four phases: registration, login phase, authentication phase, password change phase.

Registration phase

To initialize, the patient U_i registers with the medical server S.

Step 1: The patient U_i submits his/her registration request (ID_i, pw_i) to the server S via a secure channel.

Step 2: The server S verifies the legitimacy of ID_i and computes $v = h(K \oplus ID_i)$, where K is the secret number of S.

Step 3: S computes $s_1 = h(pw_i \| K)$, $s_2 = h(h(pw_i \| s_1))$ and $N = v \oplus s_2$. S then initiates a counter $ctr_i = 0$ for U_i and creates a record (ID_i, ctr_i) in its database.

Step 4: S issues the smart card, containing $h()$, N, s_1, ctr_i.

Step 5: S sends the smart card to U_i over a secure channel.

Login phase

In this phase, when a legal user wants to login the EPR information system, he/she will proceed the following steps:

Step 1. U_i inserts his/her smart card into the device and enters his/her identity ID_i and password pw_i. The smart card computes $s_2 = h(h(pw_i \| s_1))$ and generates a random number r.

Step 2. The smart card computes $ctr_i = ctr_i + 1$, $M_1 = (ID_i \| N \| s_2 \| r \| ctr_i)^2 \ mod \ n$. Finally, U_i sends a login message M_1 to S.

Authentication phase

After receiving the message M_1, S executes the following Steps:

Step 1. S solves M_1 by using the Chinese Remainder Theorem with p and q to get ID_i, N, s_2, r, ctr_i. Then, the S verifies the retrieved ctr_i with the stored ctr_i' corresponding to ID_i. If $ctr_i > ctr_i'$, then the S replaces ctr_i' with new counter ctr_i in its database and proceeds the next step. Otherwise, the S rejects this message and considers it as a replay message.

Step 2. After that, S computes $v = h(K \oplus ID_i)$, $s_2' = N \oplus v$ and compares it with the received s_2. If they are equal, the authenticity of U_i is ensured. S computes the session key $SK = h(s_2 \| r \| 1)$ shared with U_i.

Step 3. S computes $M_2 = h(s_2 \| r \| 0)$ and sends M_2 to U_i.

Step 4. U_i computes $M_2' = h(s_2 \| r \| 0)$ and checks whether $M_2 = M_2'$. If they are not equal, U_i stops the session. Otherwise, U_i authenticates the server S and computes the session key $SK = h(s_2 \| r \| 1)$.

Password change phase

The legal user U_i can change the password by using the following steps.

Step 1: U_i sends ID_i, pw_i, pw_{new} to S via a secure channel.

Step 2: S computes $v = h(K \oplus ID_i)$, $s_1^* = h(pw_{new} \| K)$, $s_2^* = h(h(pw_{new} \| s_1^*))$ and $N^* = v \oplus s_2^*$. Then, S sends (s_1^*, N^*) to U_i through the secure channel. Finally, U_i updates his/her medical smart card as $(ID_i, h(), N^*, s_1^*)$.

Figure 2 illustrates the login and authentication phases of the proposed authentication scheme.

Security analysis

In this section, we analyze the security of the proposed scheme and show that it can resist against different types of attacks and also it provides user anonymity.

We assumed that an attacker may have the following capabilities. First, the attacker has total control over the

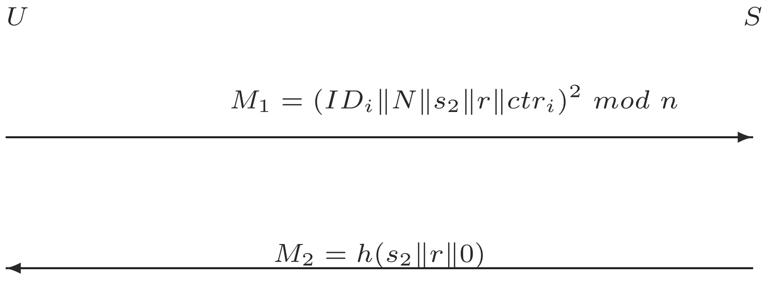

Fig. 2 Message flows in login and authentication phase

communication path between the user and the server. That is, the attacker can intercept, insert, delete, or modify any message through the path. Second, the attacker may extract the secret parameters from the smart card [7, 13].

User anonymity

Firstly, we can see that the communication transcript reveals no information about the identity ID_i of the user. In our proposed scheme, ID_i is concealed in M_1. If the attacker wants to get the ID_i from M_1, he/she should solve the quadratic residue problem by knowing the secret key p, q which only kept by the server S. Therefore, the attacker cannot identify the U_i from the login message. Secondly, if the attacker wants to obtain the ID_i from the information N stored in the smart card, he/she should know the $S's$ secret key K and user $U_i's$ password pw_i. Hence, our proposed scheme protects the user's anonymity.

Replay attack

In our scheme, we used the counter based authentication mechanism to prevent replay attack. If the adversary replays the previous login message, then S will detect the attack when examining the counter ctr_i of the user U_i. The concrete step is as follows: During the authentication phase, when the S receives a message M_1', it verifies the retrieved the counter ctr_i' with the stored counter ctr_i according to the ID_i. If the message M_1' is a replay message, then the S will find that $ctr_i' < ctr_i$. Then S simply rejects this message. Hence, our scheme prevents the replay attack.

Impersonation attack

In our scheme, in order to impersonate the U_i, the adversary must obtain the value of ID_i, N, s_2. When the smart card is stolen and compromised, the adversary can learn the values of (N, s_1, ctr_i). However, the adversary knows neither ID_i, pw_i nor K, and he/she cannot compute the value of s_2. Hence, the adversary can not forge a valid message M_1' to cheat S.

On the other hand, if an adversary wants to impersonate the server S to cheat the user U_i, he/she should forge valid information M_2 by knowing the value s_2, r which is concealed in M_1. If the adversary wants to get the s_2, r from M_1, he/she should solve the quadratic residue problem by knowing the secret key p, q which only kept by the server S.

Hence, our proposed scheme can resist the impersonation attack and provide mutual authentication.

Stolen verifier attack

An adversary A steals the secret information K stored in S's database and records M_1 from a successful authentication of a certain user U_i. He/She cannot get any information about U_i, because he/she cannot solve the message M_1. Thus, he/she cannot masquerade as a legitimate user. On the other hand, the adversary cannot masquerade as S to cheat user U_i, because he/she cannot compute s_2, r by knowing K. Therefore, the proposed scheme can resist the stolen verifier attack.

Off-line password guessing attack

Assumed that the adversary obtains the secret values of (N, s_1, ctr_i) stored in the smart card and the transmitted message M_1, M_2, he/she wants to get the password pw_i. Firstly, we can see that the adversary cannot get the password pw_i by the equations $s_1 = h(pw_i \| K)$ and $N = v \oplus s_2 = h(K \oplus ID_i) \oplus h(h(pw_i \| s_1))$, because he/she doesn't know the secret value K stored by S. Secondly, he/she cannot get password pw_i by the equations $M_1 = (ID_i \| N \| s_2 \| r \| ctr_i)^2 \ mod \ n$, $M_2 = h(s_2 \| r \| 0)$, because he/she doesn't know the secret value K, ID_i, r. Hence, our proposed scheme can prevent the off-line password guessing attack.

Lost smart card attack

If an attacker steals the smart card of user U_i and wants to use the obtained smart card to login to the server, he/she has to input the correct information ID_i, pw_i of the user U_i. However, the attacker does not know U_i's ID_i and pw_i, he/she cannot successfully be authenticated by the server.

We further assume that the attacker can retrieve all the information $\{h(), N, s_1, ctr_i\}$ stored in the smart card by monitoring the power consumption [7, 13]. Note that the user's identity ID_i is not stored in the smart card, and the attacker knows neither ID_i nor pw_i. Suppose the attacker wants to obtain pw_i, ID_i from the retrieved message. From $N = h(ID_i \oplus K) \oplus h(h(pw_i \| h(pw_i \| K)))$, the attacker has no feasible way to obtain pw_i, because he/she doesn't know the secret key K known by server S. Similarly, the attacker cannot obtain pw_i from the information $s_1 = h(pw_i \| K)$, because he/she doesn't know the value of K.

Therefore, our proposed scheme can resist lost smart card attack.

Performance comparison

We compare our new scheme with other previous authentication schemes [3, 10, 23, 27]. In Table 2, we provide the comparison based on the key security, while we compare their efficiency in terms of computation and communication cost in Table 3. The following notations are used in Table 3. t_h: The time complexity of the hash computation; t_m: The time complexity of the modular squaring computation; t_{qr}: The time complexity of computing a square root modulo n. Modular squaring computation is cheaper than traditional hash function, such as MD5. The computation of a square root modulo n is as efficient as that of modular exponentiation [4].

From Table 2, we can conclude that our proposed scheme provides better security and usability than the other two schemes [10, 23]. Wu et al.'s scheme in [23] satisfies two of the six criterions. Lee et.al.'s scheme in [10] only satisfies one of the six criterions. Our scheme can achieve the entire criterion listed in Table 2.

Table 2 Security and Usability Comparison

Feature	Lee et al. [10]	Wu et al. [23]	Ours
F1	No	No	Yes
F2	Yes	Yes	Yes
F3	No	Yes	Yes
F4	No	No	Yes
F5	No	No	Yes
F6	No	No	Yes

F1: User Anonymity
F2: Correct Password Update
F3: Mutual Authentication
F4: Stolen verifier attack resistance
F5: Lost smart card attack prevention
F6: off-line guessing attack prevention

Table 3 Efficiency Comparison in login phase and authentication phase

	Chen [3]	Lee [10]	Yeh [27]	Ours
C1	$7t_h + 2t_m$ $+1t_{qr}$	$7t_h$	$4t_h + 3t_m$	$3t_h + 1t_m$
C2	$9t_h + 1t_m$ $+2t_{qr}$	$6t_h$	$13t_h + 3t_{qr}$	$3t_h + 1t_{qr}$
C3	7	6	8	2

C1: Computation cost of the $U_i(Tag)$
C2: Computation cost of the S
C3: Total messages transmitted between $U_i(Tag)$ and S

In Table 3, we summarize the efficiency comparison between our scheme and other schemes in [3, 10, 27] in case of the login phase and authentication phase. Our scheme requires two less Modular squaring computation and two less computation of a square root modulo n than Chen et al.'s scheme [3] and Yeh et al.'s schme [27]. Moreover, our proposed scheme saves thirteen, fourteen and seven hash operations compared with Chen et al.'s scheme [3], Yeh et al.'s scheme [27] and Lee et al.'s scheme [10], respectively. Our scheme also reduces five, six and four transmitted message compared with Chen et al.'s scheme [3], Yeh et al.'s scheme [27] and Lee et al.'s scheme [10], respectively. Although our scheme requires one extra Modular squaring computation and one computation of a square root modulo n than Lee et al.'s scheme [10], our scheme achieves stronger security than Lee etal.'s scheme, as is shown in Table 2.

Conclusion

In this paper, we discussed several security weaknesses in a recently proposed smart card based user authentication scheme for EPR information system. We showed that this scheme is vulnerable to lost smart card attack. In order to withstand its security flaws, we proposed a novel anonymous user authentication protocol based on quadratic residue problem for EPR information system. Our scheme is secure even if the secret information stored in the smart card is compromised. Our scheme uses counter based authentication mechanism to prevent replay attack.

Acknowledgments The author would like to thank the anonymous referees for their valuable comments and suggestions. This work is supported by Natural Science Foundation of Shandong Province(NO.ZR2013FM009).

References

1. Chang, Y.F., Lin, S.C., Chang, P.Y., A location-privacy-protected RFID authentication scheme. In: *IEEE International Conference on Communications*, pp. 1–4, 2011.
2. Chen, H.M., Lo, J.W., Yeh, C.K., An efficient and secure dynamic ID-based authentication scheme for Telecare medical information systems. *J. Med. Syst.* 36(6):3907–3915, 2012.
3. Chen, Y., Chou, J., Sun, H., A novel mutual-authentication scheme based on quadratic residues for RFID systems. *Comput. Netw.* 52(12):2373–2380, 2008.
4. Cheng, Z.Y., Liu, Y., Chang, C.C., Liu, C.X., A novel biometric-based remote user authentication scheme using quadratic residues. *Int. J. Inf. Electron. Eng.* 3(4):419–422, 2013.
5. He, D.B., Chen, J.H., Zhang, R., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1989–1995, 2012.
6. Kumar, M., A new secure remote user authentication scheme with smart cards. *Int. J. Netw. Secur.* 11(2):88–93, 2010.
7. Kocher, P.C., Jaffe, J., Jun, B., Differential power analysis. In: *Proceedings of 19th International Advances in Cryptology*, pp. 388-397, Santa Barbara, 1999.
8. Lee, N.Y., and Chiu, Y.C., Improved remote authentication scheme with smart card. *Comput. Stand. Interfaces* 27(2):177–180, 2005.
9. Lee, S.W., Kim, H.S., Yoo, K.Y., Improvement of Chien et al.s remote user authentication scheme using smart cards. *Comput. Stand. Interfaces* 27(2):181–183, 2005.
10. Lee, T.F., Chang, I.P., Lin, T.H., Wang, C.C., A secure and efficient password-based user authentication scheme using smart cards for the integrated EPR information system. *J. Med. Syst.* 37(3):9941, 2013. doi:10.1007/s10916-013-9941-8.
11. Lee, T.F., An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. *J. Med. Syst.* 37(6):9985, 2013. doi:10.1007/s10916-013-9985-9.
12. Li, X., Qiu, W., Zheng, D., Chen, K., Li, J., Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards. *IEEE Trans. Ind. Electron.* 57(2): 793–800, 2010.
13. Messerges, T.S., Dabbish, E.A., Sloan, R.H., Examining smart card security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51(5):541–552, 2002.
14. Rosen, K. *Elementary number theory and its applications*. *Reading*. MA: Addison-Wesley, 1988.
15. Takeda, H., Matsumura, Y., Kuwata, S., Architecture for networked electronic patient record systems. *Int. J. Med. Inform.* 60(2):161–167, 2000.
16. Wang, B., and Li, Z.Q., A forward-secure user authentication scheme with smart cards. *Int. J. Netw. Secur.* 3(2):116–119, 2006.
17. Wei, J., Hu, X., Liu, W.: An improved authentication scheme for telecare medicine information systems. In: *Journal of Medical System*, 36(6):3597–3604, 2012.
18. Wen, F.T., Susilo, W., Yang, G.M., A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. In: *Wireless personal communicationx*, **73**(3):993–1004, 2013.
19. Wen, F.T., A robust uniqueness and anonymity preserving remote user authentication scheme for connected health care. *J. Med. Syst.* 37(6):9980, 2013.
20. Wen, F.T., Susilo, W., Yang, G.M., A robust smart card-based anonymous user authentication protocol for wireless communications. In: *Security and Communication Networks*, 2013. doi:10.1002/sec.816.
21. Wu, Z.P., Chung, Y., Lai, F., Chen, T.S., A password-based user authentication scheme for the integrated EPR information system. *J. Med. Syst.* 36(2):631–638, 2012.
22. Wu, S., Zhu, Y., Pu, Q., Robust smart-cards-based user authentication scheme with user anonymity. *Secur. Commun. Netw.* 5(2):236–248, 2012.
23. Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C., Chung, Y., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1529–1535, 2012.
24. Xu, J., Zhu, W.T., Feng, D.G., An improved smart card based password authentication scheme with provable security. *Comput. Stand. Interfaces* 31(4):723–728, 2009.
25. Yang, G., Wong, D., Wang, H., Deng, X., Two-factor mutual authentication based on smart cards and passwords. *J. Comput. Syst. Sci.* 74(7):1160–172, 2008.
26. Yau, W.C., Raphael, C., Phan, W., Security analysis of a chaotic map-based authentication scheme for telecare medicine information systems. *J. Med. Syst.* 37(6):9993, 2013. doi:10.1007/s10916-013-9993-9.
27. Yeh, T.C., Wu, C.H., Tseng, Y.M., Improvement of the RFID authentication scheme based on quadratic residues. *Comput. Commun.* 34:337–341, 2011.
28. Youn, T., Park, Y., Lim, J., Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks. *IEEE Commun. Lett.* 13(7):471–473, 2009.
29. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012.