Security Analysis of a Remote User Authentication Scheme Using Euclidean Plane for Multi-Server Architecture

Wei-Chi Ku
Department of Computer Science and Information Engineering
Fu Jen Catholic University
Email: wcku@csie.fju.edu.tw

Shen-Tien Chang
Department of Computer Science and Information Engineering
Fu Jen Catholic University
Email: figo@wcku1.csie.fju.edu.tw

Min-Hung Chiang
Department of Computer Science and Information Engineering
Fu Jen Catholic University
Email: grievous@wcku1.csie.fju.edu.tw

Abstract*-Recently, Lin, Hwang, and Li proposed an efficient user authentication scheme using smart cards for multi-server architecture based on the geometric property of the Euclidean plane. However, we find that their scheme is vulnerable to two forgery attacks and a password-guessing attack, and is not reparable. Herein, we first review Lin-Hwang-Li's scheme, and then describe its weaknesses.*

Keywords: Euclidean plane, forgery attack, multi-server architecture, password authentication, smart card.

1. Introduction

One of the common features of conventional remote user password authentication schemes is that a verification table, which contains the verifiers of users' passwords, should be securely maintained in the server. If the verification table is stolen or modified by the adversary, the system will be breached. In 1990, Hwang, Chen, and Laih [1] initially proposed a non-interactive password authentication scheme that does not require storing verifiers in the server. However, the authors themselves showed that this scheme is vulnerable to a replay attack, and then described an enhanced version, which additionally uses smart cards. Unfortunately, Hwang-Chen-Laih's enhanced scheme still has several drawbacks and weaknesses. Since then, many verifier-free password authentication schemes using smart cards have been proposed, and each has its pros and cons. In 1991, Chang and Wu [2] also proposed a verifier-free password authentication scheme using smart cards based on the Chinese remainder theorem (CRT). However, Chang-Wu's scheme is vulnerable to a forgery attack [3]. In 1995, Wu [5] proposed a verifier-free password authentication scheme using smart cards based on the geometric property of the Euclidean plane. The merits of his scheme are its simplicity of geometry and the property that users can freely choose passwords. Unfortunately, Wu's scheme has been found to be flawed as indicated in [7], [13]. In 1996, Wang and Chang [6] proposed a verifier-free password authentication scheme using smart cards based on the difficulties of factoring a large number and discrete logarithm problem. In their scheme, users can also freely choose passwords. However, Wang-Chang's scheme was found to be vulnerable to a replay attack and a forgery attack [8], [12]. In 1999, Yang and Shieh [8] proposed two verifier-free password authentication schemes using smart cards, one uses timestamps and the other uses nonces. In their schemes, users can freely choose passwords. However, their nonce-based scheme is inefficient while their timestamp-based scheme was found to be vulnerable to several forgery attacks [18], [19], [21]. Later, Fan, Li, and Zhu [18] proposed an improved version of Yang-Shieh's timestamp-based scheme. Unfortunately, Fan-Li-Zhu's scheme was found to be vulnerable to two forgery attacks [23], [26].

In 2000, Hwang and Li [9] proposed a verifier-free password authentication scheme using smart cards based on the ElGamal's public-key technique. However, Hwang-Li's scheme does not allow users freely choosing and changing their passwords. Furthermore, Hwang-Li's scheme was found to be vulnerable to various forgery attacks [10], [22], [27], [28]. To solve the security problems of Hwang-Li's scheme, Shen, Lin, and Hwang [22] proposed a modified scheme. However, since the user's password is a pseudo-random number, the user can not easily remember it. Additionally, Shen-Lin-Hwang's scheme was found to be vulnerable to a forgery at-

tack [25]. In 2003, Awasthi and Lal [24] proposed a verifier-free password authentication scheme using smart cards, and claimed that their scheme can achieve forward secrecy. In Awasthi-Lal's scheme, users can not freely choose and change passwords. In addition, Awasthi-Lal's scheme was found to be potentially vulnerable to a forgery attack [30].

To avoid using high-complexity operations such as modular exponentiation, Sun [11] proposed an efficient verifier-free password authentication scheme using smart cards based on cryptographic hash functions. The major drawbacks of Sun's scheme are that the password is not easily memorable and users can not freely choose and change passwords. In 2002, Lee, Hwang, and Yang [16] also proposed a hash-based verifier-free password authentication scheme using smart cards as an improved version of Sun's scheme in that users are allowed to freely choose and change passwords. However, Lee-Hwang-Yang's scheme is potentially vulnerable to an insider attack and is not reparable [4]. Same security problems can also be found in the similar scheme proposed by Hwang, Lee, and Tang [15]. In 2002, Chien, Jan, and Tseng [17] criticized that Sun's scheme only achieves unilateral user authentication, and then proposed a hash-based verifier-free password authentication scheme using smart cards that can achieve mutual user authentication. In addition, users can freely choose and change passwords. Unfortunately, Ku and Chen [29] found that Chien-Jan-Tseng's scheme is vulnerable to a reflection attack, an insider attack, and is not reparable once a user's permanent secret is compromised, and then proposed an improved scheme with better security.

All previously mentioned schemes are designed for the single-server architecture. If there are multiple servers to access, the user has to register with each server individually and possibly should remember different identities and passwords for accessing different servers. In 2001, Li, Lin, and Hwang [14] described a verifier-free password authentication scheme for the multi-server architecture by using neural networks. The user does not need to individually register with each server. However, Li-Lin-Hwang's scheme is inefficient because it spends too much time training neural networks. Later, Lin, Hwang, and Li [20] described an efficient verifier-free password authentication scheme using smart cards for the multi-server architecture based on the geometric property of the Euclidean plane. Their scheme allows users freely choosing and changing passwords. The service period for accessing each server can be assigned to each user independently, and the ElGamal's digital signature technique is employed to prevent the user from illegally extending the service period. Additionally, Lin-Hwang-Li's scheme was claimed to be resistant to the replay attack, the forgery attack, the guessing attack, and the modification attack. Unfortunately, we find that Lin-Hwang-Li's scheme is vulnerable to two forgery attacks and a password-guessing attack, and is not reparable. In this paper, we will describe the weaknesses of Lin-Hwang-Li's scheme.

2. Review of Lin-Hwang-Li's Scheme

For reader's convenience, we first review Lin-Hwang-Li's scheme [20] before demonstrating its weaknesses. In the multi-server architecture of Lin-Hwang-Li's scheme, there are three kinds of participants: the login users, m servers, and a central manager (*CM*), where *CM* is assumed to be trusted and is responsible for setting up several public/secret parameters and publishing some system information. The user only has to register with *CM* once and then can obtain the services from a set of servers. That is, the user does not need to individually register with each server. The notations used throughout this paper can be summarized as follows:

- U denotes the user.
- ID denotes the identity of U.
- PW denotes the password of U.
- S_m denotes the set of all m servers.
- Ser_i denotes the server with identity i.
- p denotes a large prime.
- g denotes a primitive element of GF(p).
- e_i denotes Ser_i's public key.
- d_i denotes Ser_i's private key.
- SP_i denotes the service period, which contains ID and the expiration time, for accessing Ser_i assigned to U.

Lin-Hwang-Li's scheme involves the initialization phase, the registration phase, the login phase, the authentication phase, and the password change phase, which can be described as in the following.

Initialization Phase

This phase is invoked for the initialization of the whole system.

Step I1. *CM* selects a large prime p and a primitive element of GF(p), say g.

Step I2. For each server $Ser_i \in S_m$, *CM* selects the private key d_i and computes the corresponding public key e_i as follows:

$$e_i = g^{d_i} \bmod (p-1)$$

Then, *CM* delivers (e_i, d_i) to Ser_i through a secure channel.

Registration Phase

This phase is invoked when U requests to register with CM. Assume that U is granted registration by a set of n servers S_n, where $S_n \subseteq S_m$.

Step R1. U chooses his own identity ID and password PW, and then delivers ID and PW to CM through a secure channel.

Step R2. For each $Ser_i \in S_n$, CM computes the following items:

$$X_i = ID^{e_i} \bmod p$$
$$Y_i = ID^{d_i} \bmod p$$
$$D_i = e_i^{ID} \bmod p$$
$$W_i = e_i^{PW} \bmod p$$

(X_i, Y_i) and (D_i, W_i) are two points for U with respect to Ser_i on the Euclidean plane.

Step R3. With respect to Ser_i, CM constructs a line L_i passing through (X_i, Y_i) and (D_i, W_i), i.e., L_i: $Y = f(X) = aX + b \bmod p$, where $a = (W_i - Y_i) / (D_i - X_i) \bmod p$ and $b = Y_i - X_i ((W_i - Y_i) / (D_i - X_i)) \bmod p$.

Step R4. CM chooses a line LS: $Y = g(X) = a'X + b' \bmod p$, where a' and b' are randomly selected in GF(p). With respect to Ser_i, CM computes the intersection point (K_i, Q_i) of lines L_i and LS.

Step R5. With respect to Ser_i, CM chooses a random number k_i that is relatively prime to $p-1$, and then computes $r_i = g^{k_i} \bmod p$. In addition, CM assigns the service period SP_i for accessing Ser_i to U. By using the extended Euclidean algorithm, the following equation can be solved for s_i:

$$SP_i = (d_i \times r_i + k_i \times s_i) \bmod (p-1)$$

Then, the signature of service period SP_i with respect to Ser_i is (r_i, s_i).

Step R6. CM delivers a smart card containing

$$\{SP_i, (r_i, s_i), K_i, LS\}$$

for all i such that $Ser_i \in S_n$ to U through a secure channel.

Login Phase

This phase is invoked whenever U requests to login Ser_i ($\in S_n$).

Step L1. U inserts his smart card into the smart card reader of a terminal, and then enters ID and PW.

Step L2. U's smart card generates a secret random number Ran_i, and computes A_i and B_i:

$$A_i = g^{Ran_i} \bmod p$$
$$B_i = e_i^{Ran_i \times T} \bmod p$$

where T denotes the current time-stamp.

Step L3. U's smart card uses the stored K_i to compute Q_i based on the stored LS. Next, U's smart card computes $D_i = e_i^{ID} \bmod p$ and $W_i = e_i^{PW} \bmod p$, and then uses (K_i, Q_i) and (D_i, W_i) to reconstruct L_i.

Step L4. U's smart card uses B_i to compute Z_i based on L_i, and then outputs (K_i, Q_i), Z_i, A_i, T, SP_i, and (r_i, s_i).

Step L5. U sends $\{ID, (K_i, Q_i), Z_i, A_i, T, SP_i, (r_i, s_i)\}$ to Ser_i through a common channel.

Authentication Phase

This phase is invoked whenever Ser_i ($\in S_n$) receives U's login request. Let T' denote the time Ser_i receives U's login request.

Step A1. If the difference between T' and T is greater than the acceptable legal time interval for the transmission delay and the inconsistency of clocks, Ser_i rejects U's login request.

Step A2. If the format of ID is incorrect, Ser_i rejects U's login request.

Step A3. If either service period SP_i is invalid or the equation $e_i^{r_i} \times r_i^{s_i} \equiv g^{SP_i} \bmod p$ does not hold, Ser_i rejects U's login request.

Step A4. Ser_i computes B_i:

$$\begin{aligned} B_i &= A_i^{d_i \times T} \bmod p \\ &= (g^{Ran_i})^{d_i \times T} \bmod p \\ &= (g^{d_i})^{Ran_i \times T} \bmod p \\ &= e_i^{Ran_i \times T} \bmod p \end{aligned}$$

Based on (K_i, Q_i) and (B_i, Z_i), Ser_i reconstructs L_i.

Step A5. Ser_i uses ID, e_i, and d_i to compute (X_i, Y_i). If (X_i, Y_i) is on L_i, Ser_i accepts U's login request. Otherwise, Ser_i rejects U's login request.

Password Change Phase

This phase is invoked whenever U requests to change his password with respect to Ser_i for all i such that $Ser_i \in S_n$.

Step C1. U inserts his smart card into the smart card reader of a terminal, and then enters ID, PW, and his new password $PW_{(new)}$.

Step C2. U's smart card uses K_i to compute Q_i based on LS, computes $D_i = e_i^{ID} \bmod p$ and $W_i = e_i^{PW} \bmod p$, and then reconstructs L_i based on (K_i, Q_i) and (D_i, W_i).

Step C3. U's smart card computes $X_i = ID^{e_i} \bmod p$ and $Y_i = f(X_i)$, and then computes $D_i = e_i^{ID} \bmod p$ and $W_{i(new)} = e_i^{PW_{(new)}} \bmod p$.

Step C4. U's smart card constructs the new line $L_{i(new)}$ based on $(D_i, W_{i(new)})$ and (X_i, Y_i), and then computes the intersection point $(K_{i(new)}, Q_{i(new)})$ of $L_{i(new)}$ and LS.

Step C5. U's smart card updates K_i with $K_{i(new)}$.

Note that U can simultaneously login multiple servers belonging to S_n in the login and authentication phase, and U's password is changed off-line in the password change phase.

3. Weaknesses of Lin-Hwang-Li's Scheme

Now, we will show that Lin-Hwang-Li's scheme is vulnerable to two forgery attacks, the unspecified forgery attack and the specified forgery attack. The former one is similar to Chan-Cheng's attack [10], Chang-Hwang's attack [27], and Leung-Cheng-Fong-Chan's attack [25] while the latter one is similar to Shen-Lin-Hwang's attack [22] and Yeh-Sun-Hsieh's attack [28]. Additionally, we will also demonstrate that Lin-Hwang-Li's scheme is vulnerable to a password-guessing attack and is not reparable [4].

3.1. Forgery Attacks

The unspecified forgery attack and the specified forgery attack that can be mounted on Lin-Hwang-Li's scheme are described as in the following.

Unspecified Forgery Attack

Suppose that the adversary is also a legal user, say U_a with identity ID_a and password PW_a. In the login phase, U_a enters ID_a and PW_a into his smart card which will then output $K_{i,a}$ and $Q_{i,a}$. In addition, U_a can compute $D_{i,a} = e_i^{ID_a} \bmod p$ and $W_{i,a} = e_i^{PW_a} \bmod p$, and then construct the line $L_{i,a}$ passing through $(K_{i,a}, Q_{i,a})$ and $(D_{i,a}, W_{i,a})$. Based on $L_{i,a}$, U_a can use $X_{i,a}$ $(= ID_a^{e_i} \bmod p)$ to compute $Y_{i,a}$. If $(ID_a \times ID_a) \bmod p$ equals the identity of any legal user, say U_b, i.e., $ID_b = (ID_a \times ID_a) \bmod p$, U_a can compute $X_{i,b}$ and $Y_{i,b}$ as in the following:

$$X_{i,b} = ID_b^{e_i} \bmod p$$

$$Y_{i,b} = ID_b^{d_i} \bmod p = (ID_a^2)^{d_i} \bmod p$$

$$= (ID_a^{d_i})^2 \bmod p = Y_{i,a}^2 \bmod p$$

Since U_a can intercept the $K_{i,b}$ and $Q_{i,b}$ previously sent from U_b, he can construct the line $L_{i,b}$ passing through $(X_{i,b}, Y_{i,b})$ and $(K_{i,b}, Q_{i,b})$. Consequently, U_a can successfully use $L_{i,b}$ to impersonate U_b to login the remote server Ser_i. Similarly, U_a can compute $L_{j,b}$, for all j such that $Ser_j \in S_n$, to impersonate U_b to login the remote server Ser_j. However, if $(ID_a \times ID_a) \bmod p$ does not equal the identity of any legal user, we can further extend our attack by checking whether $ID_a^r \bmod p$, where r is an integer within the interval $[3, p-1]$, equals the identity of a legal user [27]. Alternatively, two legal users, say U_a and U_c can conspire to check whether $(ID_a \times ID_c) \bmod p$ equals any legal user's identity. If $ID_b = (ID_a \times ID_c) \bmod p$, U_a and U_c can cooperate to perform the following computations:

$$X_{i,b} = ID_b^{e_i} \bmod p$$

$$Y_{i,b} = ID_b^{d_i} \bmod p = (ID_a \times ID_c)^{d_i} \bmod p$$

$$= (ID_a^{d_i} \times ID_c^{d_i}) \bmod p = Y_{i,a} \times Y_{i,c} \bmod p$$

Then, U_a and U_c can construct $L_{i,b}$, for all i such that $Ser_i \in S_n$, based on the computed $(X_{i,b}, Y_{i,b})$ and the intercepted $(K_{i,b}, Q_{i,b})$. That is, U_a and U_c can use $L_{i,b}$ to impersonate U_b to login the remote server Ser_i, for all i such that $Ser_i \in S_n$. Note that the difficulty of the above described unspecified forgery attack to succeed depends on the redundancy contained in the identity format [27] and the number of legal users.

Specified Forgery Attack

Suppose that the attack target of the adversary is the specific valid user U_b. The adversary can try to find ID_a with valid format such that $ID_a = ID_b^r \bmod p$, where r is an integer within the interval $[2, p-1]$. If the adversary succeeds in finding such an ID_a, he can select PW_a, and then register ID_a and PW_a to CM as U_a. Clearly, the adversary can compute $D_{i,a} = e_i^{ID_a} \bmod p$ and $W_{i,a} = e_i^{PW_a} \bmod p$. In addition, the adversary can obtain the $(K_{i,a}, Q_{i,a})$ sent out from his smart card during the login phase. Hence, the adversary can reconstruct the line $L_{i,a}$ passing through $(D_{i,a}, W_{i,a})$

and ($K_{i,a}$, $Q_{i,a}$). After computing $X_{i,a} = ID_a^{e_i} \bmod p$, the adversary can use $X_{i,a}$ to compute $Y_{i,a}$ based on $L_{i,a}$. Next, the adversary can compute $X_{i,b}$ and $Y_{i,b}$ as in the following:

$$X_{i,b} = ID_b^{e_i} \bmod p$$

$$Y_{i,b} = ID_b^{d_i} \bmod p = (ID_a^{-r})^{d_i} \bmod p$$

$$= (ID_a^{d_i})^{-r} \bmod p = Y_{i,a}^{-r} \bmod p$$

Since the adversary can intercept the $K_{i,b}$ and $Q_{i,b}$ previously sent from U_b, he can construct the line $L_{i,b}$ passing through ($X_{i,b}$, $Y_{i,b}$) and ($K_{i,b}$, $Q_{i,b}$). Then, the adversary can successfully use $L_{i,b}$ to impersonate the specific user U_b to login the remote server Ser_i. Similarly, the adversary can compute $L_{j,b}$, for all j such that $Ser_j \in S_n$, to impersonate the specific user U_b to login the remote server Ser_j. Note that the difficulty of the above described specified forgery attack to succeed is not closely related to the number of legal users.

3.2. Password-Guessing Attack

If any of the above described two forgery attacks succeeds, the adversary U_a can also perform a password-guessing attack as follows. Since U_a can construct $L_{i,b}$ and compute $D_{i,b} = e_i^{ID_b} \bmod p$, he can use $D_{i,b}$ to compute $W_{i,b}$ based on $L_{i,b}$. Next, U_a guesses a candidate password PW_b' and computes $e_i^{PW_b'} \bmod p$. If the computed result equals $W_{i,b}$, U_a has correctly guessed $PW_b' = PW_b$. Otherwise, U_a tries another candidate password. If U_b also uses PW_b to access the servers outside this system for his convenience, it is likely that U_a can impersonate U_b to access these servers [29].

3.3. Poor Reparability

In real application environments, it is impractical to assume that the secrets will never be compromised. Suppose that the adversary U_a has learned U_b's password PW_b, possibly by the above described password-guessing attack or some other means, and intercepted ($K_{i,b}$, $Q_{i,b}$) for any $Ser_i \in S_n$. Knowing PW_b, U_a can compute ($D_{i,b}$, $W_{i,b}$) and construct $L_{i,b}$ based on ($D_{i,b}$, $W_{i,b}$) and ($K_{i,b}$, $Q_{i,b}$), and then use $L_{i,b}$ to impersonate U_b to login Ser_i. Next, we will show that such a fraud can not be prohibited even if U_b has detected that PW_b has been compromised and replaced it with a new one, say $PW_{b(new)}$, by invoking the password change phase. Clearly, U_a can compute $X_{i,b} = ID_b^{e_i} \bmod p$, and then use $X_{i,b}$ to compute $Y_{i,b}$ based on $L_{i,b}$. Since $X_{i,b}$ and $Y_{i,b}$ are irrelevant to U_b's password, their values will remain unchanged after completing the password change phase. Then, U_a still can use ($X_{i,b}$, $Y_{i,b}$) and ($K_{i(new)}$, $Q_{i(new)}$), which can be obtained by interception, to construct $L_{i,b(new)}$. Henceforth, U_a can use $L_{i,b(new)}$ to impersonate U_b to login any remote server $Ser_i \in S_n$. On the other hand, if any of the previously described two forgery attacks succeeds, U_a can always impersonate U_b to login $Ser_i \in S_n$ no matter U_b has changed his password or not. Recall that the values of $X_{i,b}$ and $Y_{i,b}$ are determined only by U_b's identity ID_b and Ser_i's permanent key pair (e_i, d_i). Therefore, CM can not change ($X_{i,b}$, $Y_{i,b}$) for U_b unless either ID_b or (e_i, d_i) can be changed. However, since (e_i, d_i) is commonly used for all users rather than specifically used for only U_b, it is unreasonable and inefficient that (e_i, d_i) should be changed to recover the security for U_b only. Additionally, it is also impractical to change ID_b, which should be tied to U_b uniquely in most application systems. Therefore, Lin-Hwang-Li's scheme is not reparable [4].

4. Conclusion

Lin-Hwang-Li's verifier-free password authentication scheme using smart cards is interesting and novel in that it is specifically designed for the multi-server architecture based on the geometric property of the Euclidean plane. Lin-Hwang-Li's scheme was claimed to be resistant to the replay attack, the forgery attack, the modification attack, and the guessing attack. Additionally, the ElGamal's digital signature technique is used to prevent the user from illegally modifying the service period. In this paper, we have demonstrated that Lin-Hwang-Li's scheme is still vulnerable to two forgery attacks and a password-guessing attack, and is not reparable.

Acknowledgment

This work was partly supported by the National Science Council, R.O.C., under Grant NSC-93-2213-E-030-017.

References

[1] T. Hwang, Y. Chen, and C. S. Laih, "Non-interactive password authentications without password tables," *IEEE Region 10 Conference on Computer and Communication Systems*, Hong Kong, pp. 429-431, Sept. 1990.

[2] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, no. 3, pp. 165-168, May 1991.

[3] C. C. Chang and C. S. Laih, "Correspondence: Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 139, no. 4, pp. 372, July 1992.

[4] T. Hwang and W. C. Ku, "Reparable key distribution protocols for Internet environments," *IEEE Transactions on Communications,* vol. 43, no. 5, pp. 1947-1949, May 1995.

[5] T. C. Wu, "Remote login authentication scheme based on a geometric approach," *Computer Communications*, vol. 18, no. 12, pp. 959-963, Dec. 1995.

[6] S. J. Wang and J. F. Chang, "Smart card based secure password authentication scheme," *Computers & Security*, vol. 15, no. 3, pp. 231-237, 1996.

[7] M. S. Hwang, "Cryptanalysis of a remote login authentication scheme," *Computer Communications*, vol. 22,

no. 8, pp. 742-744, 1999.

[8] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computers & Security*, vol. 18, no. 8, pp. 727-733, 1999.

[9] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart card," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28-30, Feb. 2000.

[10] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 992-993, Nov. 2000.

[11] H. M. Sun, "An efficient remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958-961, Nov. 2000.

[12] C. K. Chan and L. M. Cheng, "Remarks on Wang-Chang's password authentication scheme," *Electronics Letters*, vol. 37, no. 1, pp. 22-23, Jan. 2001.

[13] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "A modified remote login authentication scheme based on geometric approach," *The Journal of Systems and Software*, vol. 55, no. 3, pp. 287-290, Jan. 2001.

[14] L. H. Li, I. C. Lin, and M. S. Hwang, "A remote password authentication scheme for multiserver architecture using neural networks," *IEEE Transactions on Neural Networks*, vol. 12, no. 6, pp. 1498-1504, Nov. 2001.

[15] M. S. Hwang, C. C. Lee, and Y. L. Tang, "A simple remote user authentication scheme," *Mathematical and Computer Modelling*, vol. 36, no. 1-2, pp. 103-107, July 2002.

[16] C. C. Lee, M. S. Hwang, and W. P. Yang, "A flexible remote user authentication scheme using smart cards," *ACM Operating Systems Review*, vol. 36, no. 3, pp. 46-52, July 2002.

[17] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers & Security*, vol. 21, no. 4, pp. 372-375, Aug. 2002.

[18] L. Fan, J. H. Li, and H. W. Zhu, "An enhancement of timestamp-based password authentication scheme," *Computers & Security*, vol. 21, no. 7, pp. 665-667, Nov. 2002.

[19] C. K. Chan and L. M. Cheng, "Cryptanalysis of a timestamp-based password authentication scheme," *Computers & Security*, vol. 21, no. 1, pp. 74-76, 2002.

[20] I. C. Lin, M. S. Hwang, and L. H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13-22, Jan. 2003.

[21] H. M. Sun and H. T. Yeh, "Further cryptanalysis of a password authentication scheme with smart cards," *IEICE Transactions on Communications*, vol. E86-B, no. 4, pp. 1412-1415, April 2003.

[22] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414-416, May 2003.

[23] B. Wang, J. H. Li, and Z. P. Tong, "Cryptanalysis of an enhanced timestamp-based password authentication scheme," *Computers & Security*, vol. 22, no. 7, pp. 643-645, Oct. 2003.

[24] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1246-1248, Nov. 2003.

[25] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1243-1245, Nov. 2003.

[26] K. F. Chen and S. Zhong, "Attacks on the (enhanced) Yang-Shieh authentication," *Computers & Security*, vol. 22, no. 8, pp. 725-727, Dec. 2003.

[27] C. C. Chang and K. F. Hwang, "Some forgery attacks on a remote user authentication scheme using smart cards," *Informatica*, vol. 14, no. 3, pp. 289-294, 2003.

[28] H. T. Yeh, H. M. Sun, and B. T. Hsieh, "Security of a remote user authentication scheme using smart cards," *IEICE Transactions on Communications*, vol. E87-B, no. 1, pp. 192-194, Jan. 2004.

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

[30] W. C. Ku, S. M. Chen, and H. M. Chuang, "A study of hash-based password authentication schemes without storing verifiers," *Proc. 14th Information Security Conference*, Taiwan, pp. 429-435, June 2004.