A New Remote User Authentication Scheme for Multi-Server Architecture*

Iuon-Chang Lin [a] Min-Shiang Hwang [b] Li-Hua Li [b]

[a] *Department of Computer Science and Information Engineering, National Chung Cheng University, Chaiyi, Taiwan, R. O. C.* (Email:iclin@cs.ccu.edu.tw)

[b] *Department of Information Management, Chaoyang University of Technology, 168, Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.*
Email: mshwang@cyut.edu.tw Fax: 886-4-23742337

Abstract

Remote user authentication is used to validate the legitimacy of a remote login user. Conventional user authentication schemes are suited to solve the privacy and security problems for the single client/server architecture environment. However, the use of computer networks and information technology has grown spectacularly. More and more network architectures are used in multi-server environments. In this paper, we propose a new remote user authentication scheme. The scheme can be used in multi-server environments. In our scheme, the system does not need to maintain any verification table, and the users who have registered in the servers do not need to remember different login passwords for various servers. In addition, our scheme can also withstand replay and modification attacks. Furthermore, it allows users to choose their passwords freely, and a user can be removed from the system easily when the subscription expires.

Key words: Cryptography, user authentication, remote login, security

1 Introduction

In a multi-server network architecture, a network user must prove to the servers that he/her is a legitimate remote login user before he/she can get any service from the various servers. In conventional password authentication

⋆ This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-005.
Responsible for correspondence: Prof. Min-Shiang Hwang

methods, each network user does not only need to log in to various remote servers repetitively but also needs to remember various user IDs and passwords. Therefore, users often have to write down their numerous IDs and passwords. This is insecure, because these IDs and passwords may easily leak out. Another problem in using traditional remote login methods to authenticate a user is that the server often uses a verification table that stores each user's ID and password. Therefore, the server requires extra memory space to store the verification table.

Furthermore, the server must maintain and protect the table from being modified by an intruder. If the verification table can be read or altered by an intruder, then the intruder can also append a new ID and password to the table. Still another problem arises when the communication link between the terminal and the system is insecure. An intruder can discover a remote user's password and replay the message to break in the system later. Even if the password is encrypted during transmission [20,23], the intruder can still replay the previously intercepted login message to impersonate the legitimate user. An efficient, secure remote user authentication system must agree with the multi-server architecture and withstand these attacks [19].

According to the discussions here, an efficient remote password authentication scheme must not only perform the transaction correctly, but also meet the following requirements:

- It agrees with a multi-server network architecture without repetitive registration.
- It needs no password tables or verification tables.
- It can withstand the replay attack and guessing attack [13].
- It allows a user to choose his/her ID and password freely.

In this paper, we shall propose an efficient remote user authentication scheme based on the simple geometric properties of the Euclidean plane. This scheme can satisfy all of the requirements for authentication just above. Before describing the proposed scheme, we will first briefly review related works on remote password authentication schemes. Please note that the schemes to be reviewed have already solved the problems of remote user authentication in single-server network architectures. These reviewed schemes do not yet agree with multi-server network architectures. After the review, we shall propose our new remote password authentication scheme for multi-server architectures. Next, the security of our proposed scheme will be analyzed. Finally, we shall state our conclusions in the last section of the paper.

2 Literature Review

In this section, some related works in the area of remote password authentication schemes will be introduced. A typical remote password authentication system consists of two kinds of participants, a remote user and a server. The server verifies the password of the login user and provides service for a legitimate login user. Typically, a remote user authentication protocol consists of three phases: (1) registration phase, (2) login phase, and (3) server authentication phase. A new user must first register with the server. After registration and authorization, the user can login to the server for service.

The original concept of password authentication schemes is based on one-way hash functions [8,15,12,21,22,27]. In these schemes, the problems of impersonation and modification arise. An intruder can modify the passwords stored in the verification table. These schemes cannot withstand a replay attack. In 1981, a new remote password authentication scheme was proposed by Lamport [18]. His scheme can withstand the replay attack, but not the modification attack. Lamport's scheme requires a password table, stored in the computer system, which could be modified by an intruder. To solve the problems, Horng and Jan [9,16] proposed a password authentication scheme without verification tables or password tables.

Another interactive password authentication scheme, based on public-key cryptography, such as the Diffie-Hellman cryptosystem [6] and RSA cryptosystem [24], was proposed by Singh [26]. This scheme can withstand the replay attack, but it requires multiple communications between the user and the computer system. In [14], Hwang et al. they proposed an authentication scheme using a smart card. Their scheme was based on Shamir's ID-based signature scheme [25]. One year later, Chang and Wu proposed a similar scheme [5] also with a smart card based on the Chinese remainder theorem (CRT). Unfortunately, that scheme was vulnerable and was in fact broken by Chang and Laih [3]. In their scheme, each user holds a smart card in which the information could be read easily. Therefore, the secret encryption keys can easily be uncovered.

In [1], Chang et al. proposed an authentication scheme that introduced timestamps into the authentication algorithm. Although this scheme can guard against an attack that uses the replay of an intercepted login message, it has one major weakness. The user is not permitted to choose his/her identity and password freely. Similar problems also occurred in Chang and Hwang's scheme [2].

In 1995, Wu proposed an efficient remote login authentication scheme [29], which is based on the simple geometric property of the Euclidean plane. The primary advantage of this scheme is that users are permitted to choose and change their passwords freely. However, this scheme is vulnerable and broken in [11]. In addition, in this scheme, the authorization cannot be easily received from a legal user, and the scheme does not agree with a multi-server environment. Later, the proposed schemes in [4,28,30] also suffer from the similar problems. Recently, Hwang [10] proposed a new remote password authentication scheme based on the ElGamal digital signature method [7]. This new remote password scheme still does not agree with the multi-server environment.

Recently, Li et al. proposed a remote password authentication scheme by using neural networks [19]. It agrees with the multi-server environment. However, it spends too much time on training neural networks. In the next section, we shall propose a new, efficient user authentication scheme that allows password authentication in a multi-server architecture.

3 A New Authentication Scheme for Multi-Server Architecture

In this section, we shall propose an efficient remote user authentication scheme for multi-server architectures. There are three kinds of participants in our scheme: the login users, the various servers, and a central manager (CM). In this scheme, we assume the CM can be trusted. The CM sets up several public and secret parameters. Each legitimate user can get service granted from the servers where he/her has registered. The user does not need to do repetitive registrations with various servers.

The proposed password authentication scheme can be divided into four phases: (1) the initialization phase, (2) the registration phase, (3) the login phase, and (4) the authentication phase. In the initialization phase, the CM sets up and publishes some information. To obtain each server's secret and public keys, in the registration phase, a new user chooses his/her own identification name and password. In the login phase, when a legitimate user wants to log into the server, he/her must pass the identification. Then the server will verify the legitimacy of the login user in the authentication phase. The details of the proposed remote password authentication scheme for multi-server architectures are described as follows.

The initialization phase:
Assume that S_m is a set of servers in a multi-server environment, where S_m:{ $Ser_1, Ser_2, \ldots, Ser_m$}. Initially, CM chooses two system parameters p and g, where p is a large prime and g is a generator of order p in Z_p^*. To publish p and g, both p and g can be shared among the system of servers. CM then chooses a secret key d_i for each server Ser_i, where i is from 1 to m. These parameters all belong to the Galois field $GF(p)$. Up to this point, each server Ser_i has

a public key e_i and a secret key d_i. The security comes from the difficulty of solving the discrete logarithm problem in a finite field, which is similar to the ElGamal scheme [7]. The steps are as follows:

(1) CM selects a large prime p and a primitive number g of $GF(p)$.

(2) CM chooses each server's secret key d_i and calculates the public key e_i as follows:

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

Each server Ser_i has the key pair $(e_i,\, d_i)$.

The registration phase:

When a new user wants to log into the multi-server computer system, the user must register with the server first. Assume that the new user is granted registration only by a set S_n of servers, where $S_n \subseteq S_m$, the registration steps are as follows:

(1) Firstly, the new user chooses his/her own identity ID and password PW, then delivers ID and PW to CM.

(2) Suppose that S_n is a set of servers. With which the new user can register. CM calculates

$$X_i = ID^{e_i} \bmod p, \tag{2}$$
$$Y_i = ID^{d_i} \bmod p, \tag{3}$$
$$D_i = {e_i}^{ID} \bmod p, \quad \text{and} \tag{4}$$
$$W_i = {e_i}^{PW} \bmod p, \tag{5}$$

and (X_i, Y_i) is a point in the space of real numbers for server Ser_i while (D_i, W_i) is another point in the space of real numbers for the new user, where $Ser_i \in S_n$.

(3) According to the two points (X_i, Y_i) and (D_i, W_i), CM can construct a line L_i. Here, $L_i : Y = f(X) = aX + b \bmod p$, where $a = \frac{W_i - Y_i}{D_i - X_i} \bmod p$ and $b = Y_i - X_i(\frac{W_i - Y_i}{D_i - X_i}) \bmod p$.

(4) CM randomly chooses a line LS, where $LS = g(X) = a'X + b' \bmod p$. According to the two lines L_i and LS, CM can obtain an intersection point (K_i, Q_i) for each server $Ser_i \in S_n$.

(5) Assume that the server Ser_i provides service for the new user and that SP_i is the service period for each server Ser_i. SP includes the user's identity and the service expiration date. If the server does not provide service for the new user, the service period is zero. To sign each service period SP_i, we use ElGamal digital signatures [7]. To fulfill this, CM first chooses a random number k_i for server Ser_i such that k_i is relatively prime to $p-1$. Then CM keeps k_i secret. Next, we calculate

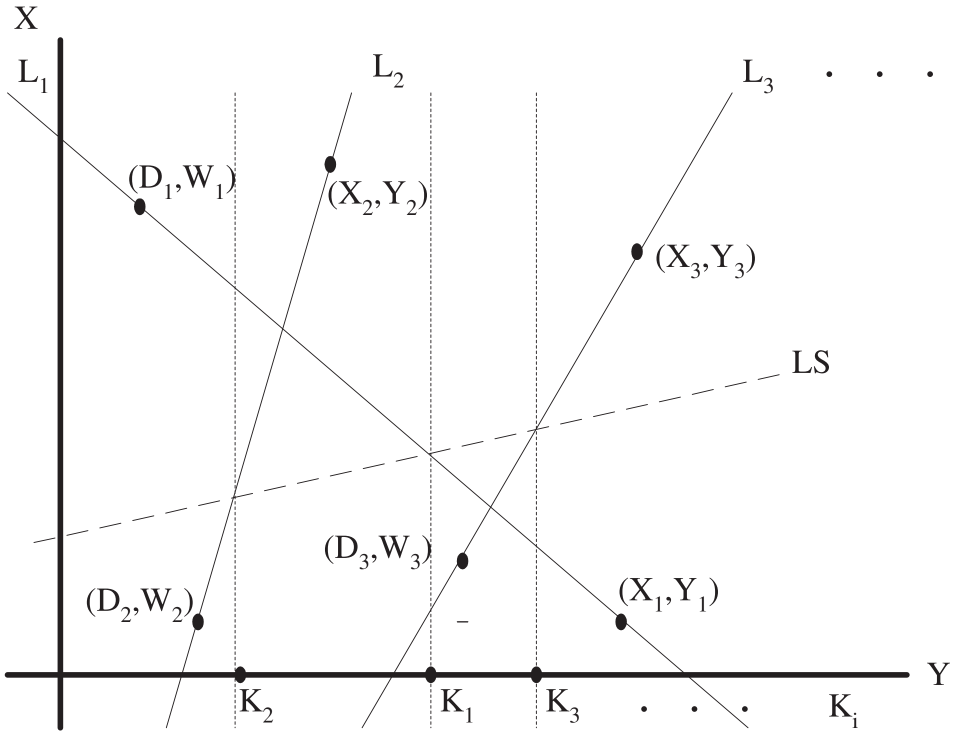


Fig. 1. The concept of the registration phase

$$r_i = g^{k_i} \bmod p. \tag{6}$$

By using the extended Euclidean algorithm, we obtain s_i in the following equation.

$$SP_i = (d_i \times r_i + k_i \times s_i) \bmod (p-1). \tag{7}$$

The signature of service period SP_i with server Ser_i is the pair (r_i, s_i).

(6) Once the registration phase is completed by CM, whose main role is to deliver the public parameters $\{SP_i, (r_i, s_i), K_i\}$ and LS to the registered user, these parameters can be stored in the smart card or other storage devices.

The concept of the registration phase is shown in Figure 1.

The login phase:

In this phase, users are authorized to use multiple servers once they have made their way through the password authentication. Assume that S_n is a set of servers that a registered user wants to log in. The user first keys in his/her ID and password, and then the authentication system will perform the following steps.

(1) The system obtains a time sequence T which is like a timestamp from the terminal.
(2) Afterwards, the system will generate a secret random number Ran_i and compute the two values A_i and B_i as follows:

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

(3) The value Q_i can be calculated from the line LS and K_i, where $LS : g(K_i) = Q_i$. Then the system will calculate (D_i, W_i) from Equations (4) and (5). According to the two points (K_i, Q_i) and (D_i, W_i), the system can reconstruct the line $L_i : f(X) = Y$.
(4) Then the system will calculate Z_i from L_i using B_i; i.e., $Z_i = f(B_i)$. Then, the system will send message M to Ser_i, where message M includes $[ID, (K_i, Q_i), Z_i, A_i, T, SP_i, (r_i, s_i)]$.

The user can also log into another registered server at the same time.

The authentication phase:
In the authentication phase, the server receives the message M at T' and performs the following tasks to authenticate the user's login request.

(1) The server shall check whether the time interval between T and T' is greater than ΔT, where ΔT denotes the expected legal time interval for transmission delay between the login terminal and the server Ser_i. If $(T' - T) \geq \Delta T$, the message M might have been replayed, and the server will reject the login request.
(2) Next, the server checks the correctness of ID. If the format of ID is incorrect, the server will reject the login request.
(3) Ser_i checks the validity of the service period SP_i. If the service period is overdue, the server will reject the login request. Otherwise, the server checks whether the following equation holds,

$$e_i^{r_i} \times r_i^{s_i} = g^{SP_i} \bmod p. \tag{8}$$

If the above equation does not hold, the server rejects the login request.
(4) Ser_i computes the value B_i,

$$\begin{aligned} B_i &= A_i^{d_i T} \bmod p, \\ &= (g^{Ran_i})^{d_i T} \bmod p, \\ &= e_i^{Ran_i T} \bmod p. \end{aligned} \tag{9}$$

According to the two points (K_i, Q_i) and (B_i, Z_i), Ser_i can reconstruct the original line L_i.
(5) Finally, the server Ser_i calculates the point (X_i, Y_i) following Equations (2) and (3). If the point is on the line $L_i(f(X_i) = Y_i)$, the server will

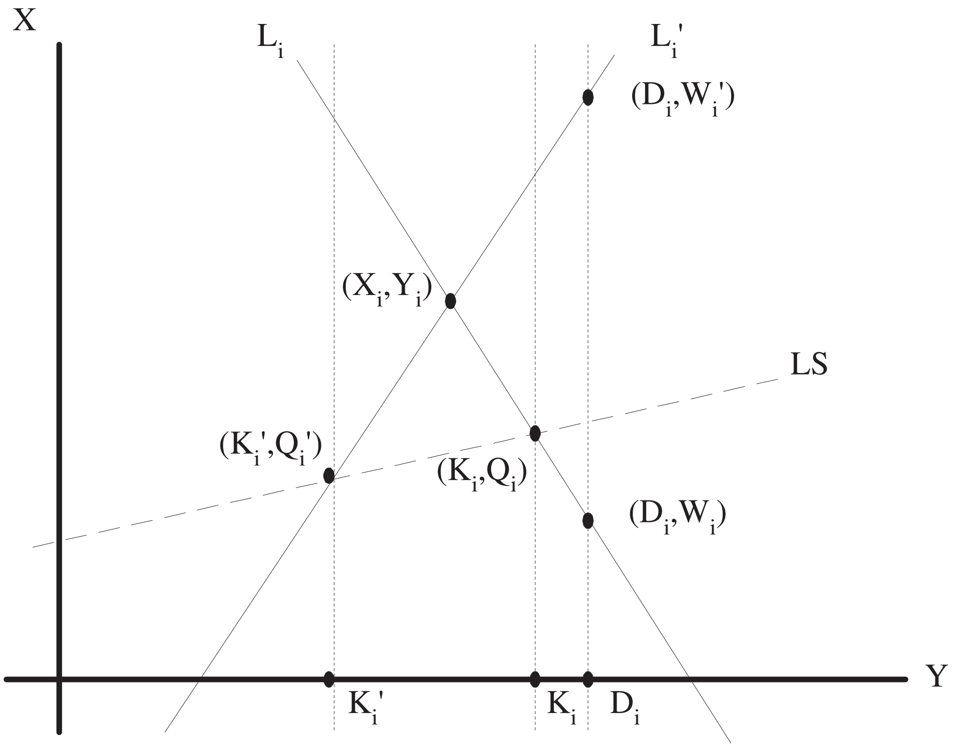


Fig. 2. The concept of the process changing passwords

accept the login request; otherwise, it will reject the login request.

To change password:
In this proposed scheme, users can choose and change their passwords freely. When a user wants to change his or her password at Server Ser_i, the steps are as follows.

(1) The user should type the old password and the new password.
(2) The system reconstructs the line $L_i : f(x) = y$ for the server Ser_i. The step is similar to step 3 as described in the login phase.
(3) Then we can calculate the value Y_i from $f(X_i)$, where X_i can be calculated through Equation (2). According to the new password, we obtain the new point (D_i, W_i') via Equation (5).
(4) The new line L_i' is reconstructed by the two points (D_i, W_i') and (X_i, Y_i). The new intersection point (K_i', Q_i') can be obtained from the lines L_i' and LS.
(5) Finally, we update the value K_i into K_i'.

In this process, we need no connection to the servers; that is, we can change passwords off line. The concept of the process is shown in Figure 2.

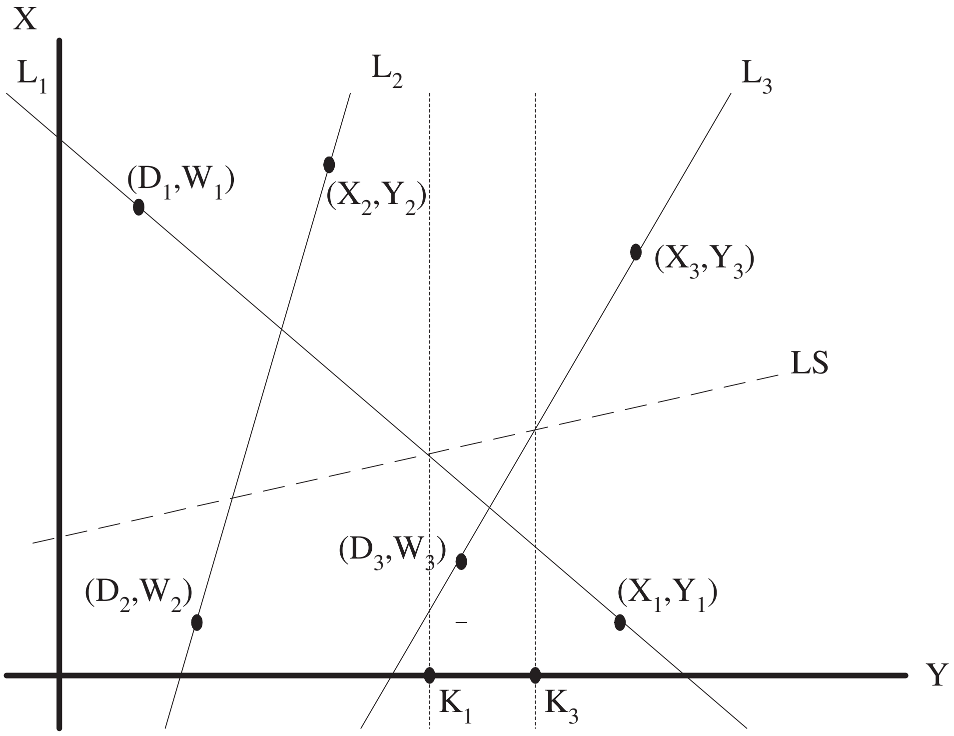


Fig. 3. An example in step 2 of the registration phase

4 Example

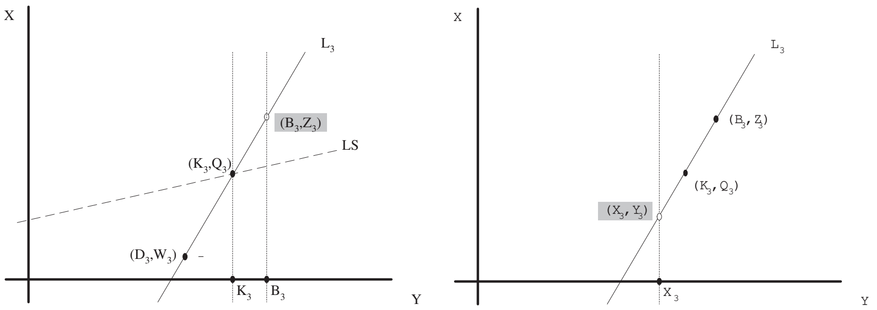
In this section, we give an example to illustrate how the proposed scheme works. We assume that there are three servers in this example.

The initialization phase:
In this phase, CM selects p, g and calculates the key pair (d_1, e_1), (d_2, e_2) and (d_3, e_3) for severs $Ser1, Ser2$ and $Ser3$ using.

$$e_i = g^{d_i} \bmod p, \quad i = 1, 2, 3.$$

The registration phase:
Assume that a new user U_1 is granted to register only from the servers Ser_1, Ser_3. The concept of registration is shown in Figure 3 and the process steps are as follows.

(1) The new user chooses his own identity ID and password PW, then sends the pair of (ID, PW) to CM.
(2) CM calculates the set of two points $[(X_1, Y_1), (D_1, W_1)]$ for Ser_1 and $[(X_3, Y_3), (D_3, W_3)]$ for Ser_3 using Equations (2), (3), (4), and (5).



(a) the login phase (b) the authentication phase

Fig. 4. The concepts of login and authentication phase

(3) According to the set of two points, CM constructs two lines; L_1 for $Ser1$ and L_3 for Ser_3.
(4) CM randomly chooses a line LS, $LS : g(x) = y$. According to the lines L_1, L_3 and LS, CM can obtain intersection points (K_1, Q_1) and (K_3, Q_3).
(5) The servers, Ser_1 and Ser_3, provide services for the new user and recall the service period for Ser_1 and Ser_3 with SP_1 and SP_3, respectively. CM uses ElGamal digital signatures scheme to sign each service period. The signatures for SP_1 and SP_3 are (r_1, s_1) and (r_3, s_3), respectively.
(6) CM delivers the parameters $[SP_1, (r_1, s_1), K_1]$, $[SP_3, (r_3, s_3), K_3]$, and the line LS to the new user.

The login phase:
In this phase, we assume that a user wants to log into the server Ser_3. The login phase perform the following steps.

(1) The user keys in his ID and password and system obtains the time sequence T.
(2) Then it generates a secret random number Ran_3 and calculates the values A_3 and B_3 using

$$A_3 = g^{Ran_3} \bmod p, \quad \text{and}$$
$$B_3 = e_3^{Ran_3 \times T} \bmod p.$$

Furthermore, system calculates Q_3 by using $LS : Q_3 = g(K_3)$.
(3) The system reconstructs the line L_3 from the two points (K_3, Q_3) and (D_3, W_3). The architecture is shown in Figure 4(a). Here, the point (D_3, W_3) are calculated using Equations (4) and (5).
(4) Finally, system computes $L_3 : Z_3 = f(B_3)$ and sends message $[ID, (K_3, Q_3), Z_3, A_3, T, SP_3, (r_3, s_3)]$ to Ser_3.

The authentication phase:
Assume that the server Ser_3 receives the message M at the time sequence T'. The server Ser_3 performs the following authentication phases.

(1) Ser_3 checks whether the time interval ΔT between login time (T) and the server system time (T').
(2) Ser_3 checks the correctness of ID.
(3) Verify the signature (r_3, s_3) with the service period SP_3 using Equation (8). If the signature is correct, Ser_3 will check whether the service period SP_3 is overdue.
(4) Ser_3 calculates B_3 as follows.

$$\begin{aligned} & A_3^{d_3 T} \bmod p, \\ = & (g^{Ran_3})^{d_3 T} \bmod p, \\ = & e_3^{Ran_3 T} \bmod p, \\ = & B_3. \end{aligned}$$

According to the two points (K_3, Q_3) and (B_3, Z_3), Ser_3 reconstructs the original line L_3 as shown in Figure 4(b).
(5) Ser_3 then computes the point (X_3, Y_3) using Equations (2) and (3). If the point is located on the line L_3, then Ser_3 will accept the login request of the user.

5 Security Analysis

In this section the security of the proposed remote password authentication scheme is examined.

Secrecy:
In our scheme, both the secret key d_i of server Ser_i and the password PW of the user must be kept secret. Furthermore, the user stores some important information, such as the users identity (ID), the service period (SP_i), the signature (r_i, s_i), (K_i) and the line LS.

If d_i or PW leaks out, then the system will become insecure because an intruder can reconstruct the line L_i and find the point (X_i, Y_i) of the server easily, and then he/she can impersonate the legal user. Thus, the two parameters d_i and PW must be kept secret. Our scheme is based on the ElGamal digital signature scheme. The security comes from the difficulty of calculating discrete logarithms. Therefore, to derive the secret key d_i from Equation (1) is difficult. In addition, only legal users can compute W_i and reconstruct the line L_i with Ser_i from the two points $(K_i, Q_i), (D_i, W_i)$. Then, they can derive the

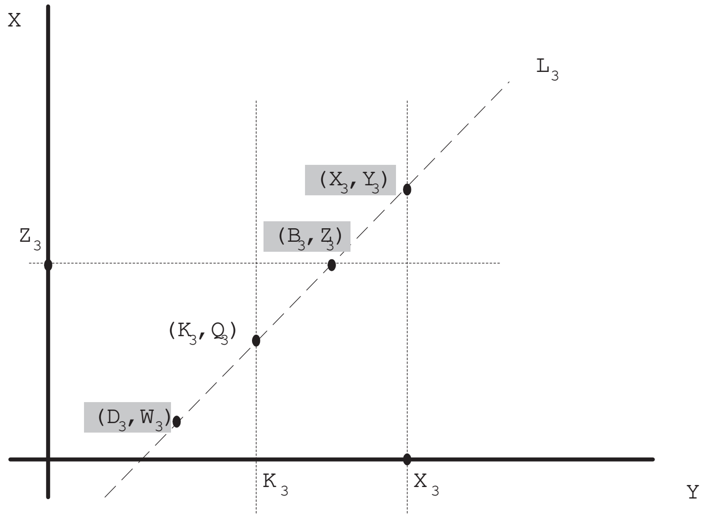


Fig. 5. It's difficult to reconstruct the line L_3

correct Z_i from the equation $f(B_i) = Z_i$. Thus, without the valid password, any illegal user, not knowing the point (D_i, W_i), cannot reconstruct the line L_i and the secret point (X_i, Y_i) of ser_i.

We have presented an example for examination in Section 4. Although the intruder can intercept the login request message M, however, without the secret parameter d_i, he/she cannot obtain B_i directly from Equation (9). Therefore, the intruder only knows the points (K_3, Q_3) and the parameters X_3, D_3, and Z_3. Obviously, the intruder does not have enough points to reconstruct the line L_i. It is difficult for the intruder to reconstruct the line L_3 as shown in Figure 5.

Non-forgery:
Assume that an intruder wants to pretend to be a legal user to login with the server Ser_i. For remote access, the intruder can previously intercept a login request including $[ID, (K_i, Q_i), SP_i, (r_i, s_i)]$. The intruder can also forge A'_i, B'_i and T'_i easily. However, the key point is that the intruder cannot obtain the line L_i; thus, Z_i cannot be solved in step 4 of the login phase. Supposing the intruder attempts to forge the value Z_i and sends the login message $[ID_j, (K_i, Q_i), A'_i, Z'_i, T'_i, SP_i, (r_i, s_i)]$ to the server. Although the server can recover B_i from Equation (9), the server will reject the login request in step 5 of the authentication phase. Therefore, the intruder cannot impersonate a legal user, which, again, shows our scheme can withstand the impersonation attack.

Replay resistance:
To resist the replay attack, our scheme uses the concept of timestamp. When the intruder replays the previously intercepted login messages and wants to masquerade as a legal user. In order to pass the test in step 1 of the authentication phase, the intruder must change T into a new time T^* such that

$(T'' - T^*) \leq \Delta T$, where T'' is the timestamp given at the time when the server receives the illegal login message. Once T is changed, the value of B_i is changed too. However, the intruder cannot acquire the valid Z_i because the line L_i is secret. This is the property of non-forgery. The intruder will fail the test in the authentication phase. Therefore, the proposed scheme is secure against the replay attack.

The proposed scheme detects replays of the login message by testing $(T' - T) \geq \Delta T$. However, this test may come to the two undesired results as follows. One result is that ΔT is small and the server denies legitimate authentication requests. This will result in a possible network delay or the loss of clock synchronization. The other is that ΔT is large and the server cannot resist the replay attack. Thus, it is important here to choose an appropriate ΔT. One of the solutions is to use a replay detection buffer which keeps the clock synchronization. The server can change ΔT according to the traffic loading and clock synchronization.

The resistance of extending the service period:
In our proposed scheme, the service period is used to manage the legal users. When the service period is exceeded, the user must re-register for extending the service period. Otherwise, the user will become an illegal user. To prevent the user from illegally extending the service period, we use the ElGamal digital signature scheme [7]. The security of this scheme comes from the difficulty of calculating discrete logarithms. Each server signs for the service period using the Equations (6) and (7). In the authentication phase, the server first tests the signature using Equation (8). In case that a user wants to extend his/her service period, that means the user has to modify his/her SP to SP'. However, the user cannot obtain the secret key from the server; therefore, he/she cannot calculate the correct s_i for Equation (7), $SP_i' = (d_i \times r_i + k_i \times s_i')(\bmod\ P-1)$, and for Equation (8). Obviously, the test will be failed. Therefore, the service period cannot be modified by any user in our proposed scheme.

6 Conclusions and Discussion

In this paper, we have proposed an efficient remote user authentication scheme. The server stores only its key pair (e_i, d_i), and each registered user stores the information $[SP_i, (r_i, s_i), K_i]$, and a linear formula LS. This scheme is constructed based on the ElGamal digital signature scheme and the simple geometric properties on the Euclidean plane. This scheme authenticates the validity of a login user without using any verification table or password file. The scheme uses the timestamp technique to work against the replay attack. It is proven that our new scheme can withstand both the modification attack and the replay attack. The major breakthrough of this scheme is that it agrees not only with multi-user networks but also with multi-server networks. The user can log into various servers at the same time without repetitive registrations with all the servers. Furthermore, the system can manage user's privileges by using the service period. When the service period of a user expires, the central authority will stop the service for that user. Another advantage of this scheme is that users can freely choose and change their passwords off line.

Acknowledgements

The author wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-005.

References

[1] C. C. Chang, R. J. Hwang, and J. B. Daniel, "Using smart cards to authenticate passwords," *IEEE International Carnahan Conference on Security Technology* pp. 154–156, 1993.

[2] C. C. Chang and S. J. Hwang, "Using smart cards to authenticate remote passwords," *Computers and Mathematics with Applications*, vol. 26, no. 7, pp. 19–27, 1993.

[3] C. C. Chang and C. S. Laih, "Remote password authentication with smart cards (correspondence)," *IEE Proceedings-E*, vol. 139, no. 4, p. 372, 1992.

[4] C. C. Chang, S. M. Tsu, and C.Y. Chen, "Remote scheme for password authentication based on theory of quadratic residues," *Computer Communications*, vol. 18, pp. 936–942, Dec. 1995.

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

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, pp. 644–654, 1976.

[7] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[8] A. J. Evans, W. Kantrowiz, and E. Weiss, "A user authentication scheme not requiring secrecy in the computer," *Communications of the ACM*, vol. 17, pp. 437–442, 1974.

[9] G. Horng, "Password authentication without using password table," *Information Processing Letters*, vol. 55, pp. 247–250, 1995.

[10] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," *International Journal of Computer Mathematics*, vol. 70, pp. 657–666, 1998.

[11] M. S. Hwang, "Cryptanalysis of remote login authentication scheme," *Computer Communications*, vol. 22, no. 8, pp. 742–744, 1999.

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

[13] M. S. Hwang, C. C. Lee, Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack," *International Journal of Informatica*, vol. 12, no. 2, pp. 297–302, 2001.

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

[15] T. J. Hwang, "Password authentication using public-key encryption," *IEEE Proceedings International Carnahan Conference Security Technology*, pp. 141–144, 1983.

[16] J. K. Jan and Y. Y. Chen, "'paramita wisdom' password authentication scheme without verification tables," *The Journal of Systems and software*, vol. 42, pp. 45–57, 1998.

[17] H. P. Konigs, "Cryptographic identification methods for smart card in the process of standardization," *IEEE Communications Magazine*, pp. 42–48, June 1991.

[18] L. Lamport, "Password authication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[19] L. H. Li, I. C. Lin, and M. S. Hwang, "A remote password authentication scheme for multi-server architecture using neural networks," in: *IEEE Transactions on Neural Networks*, to appear.

[20] R. E. Lennon, S. M. Matyas, and C. H. Meyer, "Cryptographic authentication of time-invariant quantities," *IEEE Transactions on Communications*, vol. 29, no. 6, pp. 773–777, 1981.

[21] R. Morris and K. Thompson, "Password security: a case history," *Communications of the ACM*, vol. 22, pp. 594–597, 1979.

[22] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Communications of the ACM*, vol. 21, pp. 993–999, 1978.

[23] P. G. Neumann, "Risks of passwords," *Communications of the ACM*, vol. 37, p. 126, 1994.

[24] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[25] A. Shamir, "Identity based on cryptosystems and signature schemes," *Advances in Cryptology, CRYPTO'84*, pp. 47–53, 1984.

[26] K. Singh, "On improvements to password security," *Operation System Review*, vol. 19, pp. 53–60, 1985.

[27] M. Udi, "A simple scheme to make passwords based on one-way function much harder to crack," *Computers & Security*, vol. 15, no. 2, pp. 171–176, 1996.

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

[29] T. C. Wu, "Remote login authentication scheme based on a geometric approash," *Computer Communications*, vol. 18, no. 12, pp. 959–963, 1995.

[30] T. C. Wu and H. S. Sung, "Authentication passwords over an insecure channel," *Computers & Security*, vol. 15, no. 5, pp. 431–439, 1996.