INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. 2003; **16**:799–808 (DOI: 10.1002/dac.617)

A new privacy and authentication protocol for end-to-end mobile users

Cheng-Chi Lee[1], Chao-Chen Yang[2] and Min-Shiang Hwang[3,*,†]

[1] *Department of Computer and Information Science, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C.*
[2] *Department of Computer and Information Science, Chaoyang University of Technology, 168 Gifeng E. Road, Wufeng, 413 Taichung County, Taiwan, R.O.C.*
[3] *Department of Management Information System, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.*

SUMMARY

In this papecr, we propose a new privacy and authentication scheme for end-to-end mobile users. There are three goals in our scheme. The first allows two end-to-end mobile users to communicate privately each other. The second allows two end-to-end mobile users to distribute a session key simply. The third allows two end-to-end mobile users to mutually authenticate. Copyright © 2003 John Wiley & Sons, Ltd.

KEY WORDS: authentication; mobile communication; privacy; security

1. INTRODUCTION

Recently, mobile communications technologies have undergone rapid development. Small mobile communication devices with numerous functions are becoming popular for people to transfer data at any place and any time. These devices provide convenience for people between destinations and far away from standard communications methods. This is bringing forth the important issue of information security, privacy and authentication in an open space. Privacy involves ensuring that an eavesdropper cannot intercept the communications information of mobile users. Authentication involves ensuring that the services are not obtained fraudulently [1–3].

In recent years, many literatures had been written on privacy and authentication for mobile communications [2,4–8]. A good security protocol for mobile communications must not only provide high security but also low computation. Recently, Yi, Okamoto, and Lam proposed an optimized protocol (denoted as the YOL protocol) for mobile network authentication and security. The YOL protocol is based on the ElGamal signature [9] and Diffie–Hellamn [10] key

[*] Correspondence to: Min-Shiang Hwang, Department of Management Information System, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
[†] E-mail: mshwang@mail.cyut.edu.tw

Contract/grant sponsor: National Science Council, Taiwan, R.O.C.; contract/grant number: NSC91-2213-E-324 003

Received 12 March 2003
Revised 27 May 2003
Accepted 14 July 2003

distribution scheme. The protocol has two advantages. The first is that the mobile users only keep two public parameters, a large prime (p) and a public key from the certification authority (CA). Therefore, the storage space of the mobile terminal for the protocol is smaller than that of other protocols. The other is that it uses a secret key cryptosystem to encrypt the communications between mobile user and base station. Therefore, the computation complexity of this protocol is smaller than that of other protocols, which use pubic key cryptosystems to encrypt communications.

However, the YOL protocol considers only that a mobile user will set up a communication session with a base station. When we extended their protocol for end-to-end mobile user communications, there existed either a security loophole or an inefficient processing problem. In this paper, we propose an efficient authentication and privacy protocol for end-to-end mobile user communications by adding a time-stamp to the YOL protocol. There are three goals in our scheme as follows.

1. It allows two end-to-end mobile users to communicate privately each other.
2. It allows two end-to-end mobile users to distribute a session key simply.
3. It allows two end-to-end mobile users to mutually authenticate.

In this paper, we extended YOL protocol for end-to-end mobile user communications. Two of our extended schemes and the YOL protocol have drawbacks shown in Section 3. Therefore, we then propose an efficient and secure authentication and privacy protocol for end-to-end mobile user communications. The proposed protocol do not only correct drawbacks shown in Section 3, but also achieve our above goals.

This paper is organized as follows. In the next section, we give an overview of the YOL protocol. In Section 3, we propose two straightforward protocols, which are extensions of the YOL protocol, to communicate privately and provide authentication for end-to-end mobile users. We also show that the two existing drawbacks in the YOL protocol, the security loophole and inefficient processing problem. In Section 4, we propose an efficient protocol to correct these drawbacks. In Sections 5, we analyse the security of our method. In Section 6, we give a discussion on our protocol. Finally, Section 7 presents our conclusions.

2. THE YOL PROTOCOL

The YOL protocol [7] used the ElGamal signature [9] and Diffie–Hellman key distribution protocol [10] for mobile network authentication and security. This is a good security protocol for mobile devices that use simple algebraic operations and have a small storage capacity. There are two procedures in this protocol. First, all mobile users and base stations must have certificates that are used to authenticate each other. In this procedure, each unit should get a certificate to be authenticated by others. To run next procedure, each unit must have a certificate which is issued by a trusted certification authority (CA). This procedure is generated by CA. Second, mutual authentication and key distribution between mobile user and base station must exist. The YOL protocol is summarized in the following:

2.1. Certification

They assumed that a mobile network includes a trusted third party (CA) which provides a public key certification service and issues a certificate to all mobile users and base stations. The CA should be a trusted third organization. When a unit wants to get a certificate, he/she generates his/her own key pair, gives the public key as well as some proof of his/her identification to CA. The CA plays the same role as the Government in the certificate issuing process, will check the person's identification to assure the identity of the unit.

1. Each participant (mobile user, base station, and CA) in the network generates a pair of public-secret keys. The pair of keys for a mobile user is (y_m, x_m), where $y_m = g^{x_m} \bmod p$. x_m is a secret number chosen randomly from $GF(q)^*$ by the mobile user. p is a large prime. q is a large factor of $(p-1)$; and $g = h^{(p-1)/q} \bmod p$ with h is an integer satisfying $1 < h < (p-1)$. The parameters (p, q, h, g) are generated by CA. In a similar way, the pairs of keys for the base station and CA are (y_b, x_b) and (y_{ca}, x_{ca}), respectively.
2. The CA generates certificates $\text{Cert}_{CA,b} = (C_b, s_b, t_b)$ and $\text{Cert}_{CA,m} = (C_m, s_m, t_m)$ for the base station and mobile user, respectively. Here, $s_b = g^{r_b} \bmod p$ with r_b is a random number chosen by the base station from $GF(p)^*$; $t_b = -s_b - h(C_b) \times r_b \times x_{ca}^{-1} \bmod q$; and C_b is a message which contains the certificate serial number, validity period, the identity (ID), the public key of the base station, etc. In a similar way, $s_m = g^{r_m} \bmod p$ with r_m is a random number chosen by the mobile user; $t_m = -s_m - h(C_m) \times r_m \times x_{ca}^{-1} \bmod q$; and C_m is a message which contains the certificate serial number, validity period, the identity (ID), the public key of the mobile user, etc.; $h(\cdot)$ is a one-way hash function [11].

2.2. Mutual authentication and key distribution

The procedures for mutual authentication between a mobile user, MS and a base station, BS, as well as the key distribution from BS to MS are shown in Figure 1. We briefly describe the procedures in the following.

1. MS sends a SETUP signal and his certification $\text{Cert}_{CA,m}$ to BS.
2. BS verifies the validity of MS by checking the following:

$$y_{ca}^{s_m+t_m} \times s_m^{h(C_m)} \bmod p = 1. \tag{1}$$

If the above equation holds, BS confirms that MS is a legal mobile user and then sends a CONNECT signal, his certification $\text{Cert}_{CA,b}$, and $(y_m^{-x_b} \times K \bmod p)$ to MS, where K is a session key which is shared by MS and BS.

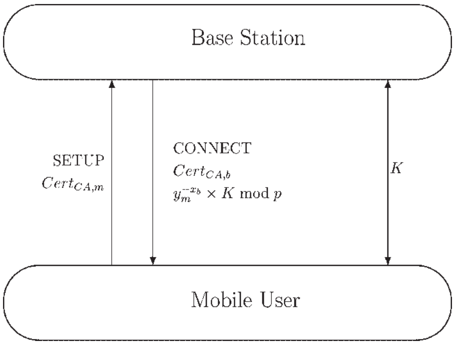


Figure 1. The YOL protocol.

3. MS verifies the validity of BS by checking the following: $y_b^{s_b+t_b} \times s_b^{h(C_b)} \bmod p = 1$. If the equation holds, MS confirms that BS is a legal base station and then derives the session key K by computing $y_b^{x_m} \times (y_m^{-x_b} \times K) \bmod p = K$.

Finally, MS and BS can commonly share this session key, K, to encrypt and decrypt confidential message using a block cipher.

3. EXTENSION OF YOL PROTOCOL

The YOL protocol [7] is designed to set up a communication session only between a mobile user and a base station. We extended this protocol for end-to-end mobile users with the following two schemes.

3.1. SCHEME 1: end-to-end mobile users communicate with three keys

A straightforward scheme to apply the YOL protocol for end-to-end mobile user communications is shown in Figure 2. This scheme uses three different keys for end-to-end mobile user communications. In Figure 2, we assume that mobile user 1 (denoted as MS_1) wants to communicate with the mobile user 2 (denoted as MS_2). Apply the YOL protocol for MS_1 to base station 1 (denoted as BS_1), both MS_1 and BS_1 can share a session key K_1. In a same way, both BS_1 and base station 2 (denoted as BS_2) can share a session key K_2, and both BS_2 and MS_2 can share a session key K_3.

There are three advantages in this method:

1. Communications privacy for end-to-end mobile users in a mobile network.
2. Key distribution for end-to-end mobile users.
3. Mutual authentication for end-to-end mobile users.

However, the disadvantage is related to the inefficiency of this scheme. If there are n base stations between MS_1 and MS_2, $(n+1)$ session keys are required. We must to do $2(n+1)$ times the encryption and decryption. It is thus inefficient for an on-line system.

3.2. SCHEME 2: end-to-end mobile users communicate with one key

In this scheme, we use only one key for end-to-end mobile users to communicate with in a mobile network. In this scheme, the main problem is key distribution; how to send the session key to each participant. When MS_1 wants to communicate with MS_2. Each participant must

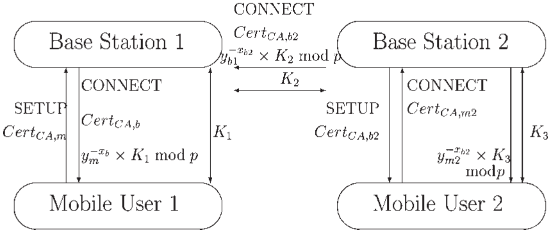


Figure 2. End-to-end mobile users communicate with three keys.

execute two procedures in the YOL protocol: certification, and mutual authentication and key distribution. As in Figure 3, MS_1 communicates with MS_2 using only one session key. This scheme can improve the inefficiency problem in the previous method, but there still exists a security loophole as follows

- Between MS_1 and BS_1, it is similar to SCHEME 1 for mutual authentication and key distribution.
- Between BS_1 and BS_2, it is similar to SCHEME 1 for mutual authentication. Then BS_1 sends $(y_{b2}^{-x_{b1}} \times K) \bmod p$ to BS_2, where K is decided by BS_1. When BS_2 receives it, he/she separates K from $y_{b2}^{-x_{b1}} \times K \bmod p$ by computing $(y_{b1}^{x_{b2}}) \times y_{b2}^{-x_{b1}} \times K \bmod p$.
- Between BS_2 and MS_2, it's similar to the method between BS_1 and BS_2.

Finally MS_1 can send confidential messages to MS_2 using a symmetrical cryptosystem [11] with the session key K as shown in Figure 3.

This scheme improves the disadvantage in SCHEME 1. It uses a key only for end-to-end mobile user communications in mobile network. The advantages in SCHEME 2 are the same as SCHEME 1. The disadvantage is insecurity. We explain it as follows

1. MS_1 to MS_2:

   When MS_1 communicates with MS_2, they use the mutual key K to encrypt and decrypt the confidential message. If MS_2 is an illegal user, he/she can intercept $y_{m1}^{-x_{b1}} \times K \bmod p$ from the transmission session and separate $y_{m1}^{-x_{b1}} \bmod p$ from it by computing:

$$\frac{y_{m1}^{-x_{b1}} \times K \bmod p}{K} = y_{m1}^{-x_{b1}} \bmod p.$$

2. MS_1 to MS_3:

   In the next session, when MS_1 wants to communicate with MS_3 (mobile user 3), they choose K_1 as their session key. The illegal user, MS_2, intercepts $y_{m1}^{-x_{b1}} \times K_1 \bmod p$ from this session and separates K_1 from it as follows.

$$\frac{y_{m1}^{-x_{b1}} \times K_1 \bmod p}{y_{m1}^{-x_{b1}} \bmod p} = K_1.$$

From now on, MS_2 uses the session key K_1 to wiretap the confidential messages between MS_1 and MS_3. The session key K is shared by MS_1 and MS_2, so MS_2 can derive the session key K_1

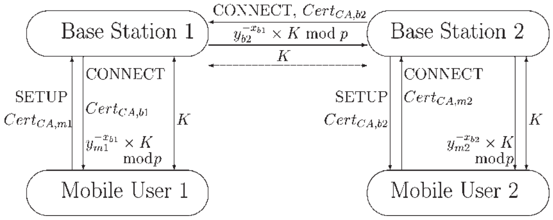


Figure 3. End-to-end mobile users communicate with one key.

shared by MS_1 and MS_3 by using above two equations. In the next section, we will propose an improved scheme to remedy this security loophole.

4. THE PROPOSED SCHEME

We have showed that the protocols for end-to-end mobile users are inefficient or insecure in Section 3. In this section, we propose a protocol to improve SCHEME 2, as discussed in Section 3. The main idea is that a time-stamp concept [12] is applied to our scheme. We added a time-stamp, T, and a public one-way hash function f in our scheme, as shown in Figure 4, to solve the inefficiency and insecurity problems as follows:

1. MS_1 to BS_1:
   (a) MS_1 sends a SETUP signal and his/her certification $\text{Cert}_{CA,m1}$ to BS_1.
   (b) BS_1 verifies the validity of the certification $\text{Cert}_{CA,m1}$ by checking Equation (1). If Equation (1) holds, BS_1 sends a CONNECT signal, his/her certification $\text{Cert}_{CA,b1}$, time-stamp T_1, and $y_{m1}^{-x_{b1}\times f(T_1,X)} \times K \bmod p$ to MS_1, where K is a random session key; X is equal to $y_{m1}^{x_{b1}}$ or $y_{b1}^{x_{m1}}$ and is shared by MS_1 and BS_1.
   (c) MS_1 verifies the validity of the time-stamp and the certification $\text{Cert}_{ca,b1}$ by checking Equation (1). If Equation (1) holds, MS_1 calculates the session key as follows:

$$y_{b1}^{x_{m1} f(T_1,X)} y_{m1}^{-x_{b1} f(T_1,X)} \times K \bmod p = K.$$

2. BS_1 to BS_2: This is similar to MS_1 to BS_1 for mutual authentication as shown above. BS_1 sends a new time-stamp T_2, and $(y_{b2}^{-x_{b1}\times f(T_2,Y)} \times K) \bmod p$ to BS_2, where Y is $y_{b1}^{x_{b2}}$ or $y_{b2}^{x_{b1}}$. Next, BS_2 calculates the session key K by computing

$$y_{b1}^{x_{b2} f(T_2,Y)} \times y_{b2}^{-x_{b1} f(T_2,Y)} \times K \bmod p = K.$$

3. BS_2 to MS_2: This is similar to BS_1 to BS_2 for mutual authentication as shown above. BS_2 sends a new time-stamp T_3, and $(y_{m2}^{-x_{b2}\times f(T_3,Z)} \times K) \bmod p$ to MS_2, where Z is $y_{m2}^{x_{b2}}$ or $y_{b2}^{x_{m2}}$. Next, MS_2 calculates the session key K by computing

$$y_{b2}^{x_{m2} f(T_3,Z)} \times y_{m2}^{-x_{b2} f(T_3,Z)} \times K \bmod p = K.$$

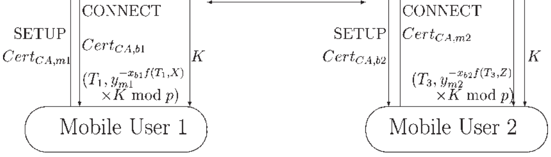


Figure 4. End-to-end mobile users communicate with one key and a time-stamp.

Finally, two mobile users, MS_1 and MS_2, get the session key K. They can use this session key to encrypt and decrypt confidential messages using a symmetrical cryptosystem [11].

5. CRYPTANALYSIS

Our scheme is an extension of the YOL protocol. For enhancing security, we added a time-stamp T and a one-way hash function f to the YOL protocol for end-to-end mobile users. Our scheme is secure against Martin and Mitchell's attack [13].

If an attacker does not know the secret key x, it is difficult to forge a valid signature pair (s, t) and obtain the session key K from $y_m^{-x_b \times f(T,X)} \times K \bmod p$. This is a discrete logarithm problem [9]. It is difficult to obtain X except that the attacker known the secret keys x_{m1} and x_{b1}.

Applying the time-stamp concept in our scheme, the security of the scheme is enhanced to defend and against a replay attack. Although an attacker can intercept the time stamp T and the end-to-end mobile user certification, he/she cannot pretend to be one of them by replaying these messages. An attacker may replay the certificates to pass authentication, he/she still cannot obtain their common session K without knowing the secret key x.

Furthermore, there is no way for an attacker to obtain the secret key, so he/she cannot obtain the session key K to wiretap the confidential messages. As in the description in Section 3, MS_2 is an attacker. He/She can intercept $y_{m1}^{-x_{b1} \times f(T_1,X)}$ and T_1, but he/she cannot get the session key K by computing

$$\frac{y_{m1}^{-x_{b1} \times f(T',X)} \times K \bmod x p}{y_{m1}^{-x_{b1} \times f(T_1,X)} \bmod p},$$

since the time-stamp T' is different from the time-stamp T_1 and the X is unknown to him/her.

6. DISCUSSIONS AND COMPARISONS

A good protocol for privacy and authentication in a mobile network should involve as simple an algebraic operation as possible and occupy as small a storage space as possible. The YOL protocol [7] can achieve these purposes. However, their protocol has the following drawbacks: (1) only communications between a mobile user and a base station are considered; (2) they cannot resist the certificate replaying attack; (3) the session key may be derived by another legal mobile user described in Section 3. Our scheme can remedy these drawbacks in Section 4. We added a time-stamp against replaying attack and a one-way hash function to solve the drawbacks (3). The security of our analysis is described in Section 5. Our end-to-end protocol has all of the necessary features.

Our method has the following improvements:

1. Traditionally, privacy and authentication for end-to-end mobile communication is a large topic [5]. In the YOL protocol, only communications between a mobile user and a base station are considered.
2. In SCHEME 1 of Section 3, $(n + 1)$ session keys and $2(n + 1)$ times of encryption and decryption computations are required for mobile communications. It is inefficient. In SCHEME 2 of Section 3, one session key for end-to-end mobile communications is used to avoid heavy encryption and decryption computations. This solves the inefficiency problem.

Table I. Comparisons among the four schemes.

	YOL scheme	SCHEME 1 in Section 3	SCHEME 2 in Section 3	End-to-end scheme
Simple algebraic operation	Yes	Yes	Yes	Yes
End-to-end	No	Yes	Yes	Yes
Security	No	No	No	Yes
Additional computational complexity	—	—	—	M + F*

*M: a multiplicative operation, F: a one-way hash function.

3. In the efficient scheme in Section 4, we added a time-stamp, T, and a one-way hash function f to solve a potential security loophole. Compared with the YOL protocol, only a multiplicative operation, $-x_b \times f(T,X)$, and $f(\cdot)$ were added. Therefore, the computational complexity was not increased. Communication between end-to-end mobile users was achieved and the security of the protocol was enhanced.

However, in our scheme, it also have a small shortcoming same as other mobile network that is base stations have the knowledge of that shared session key, which gives these base stations the capability to decrypting the encrypted message between the two mobile users.

In Table I, we compare the proposed schemes with YOL scheme. Although the computational complexity of our scheme is higher than YOL scheme, our scheme can achieve end-to-end security and improve the insecurity of YOL scheme. In addition, our scheme in Section 4 keeps the advantages of YOL scheme.

7. CONCLUSIONS

Yi, Okamoto and Lam proposed a good security protocol for a mobile network involving simple algebraic operations and small storage capacity. In their protocol, only mobile users setting up communications a base station was considered. In this paper, we extended their protocol to end-to-end mobile users communicating privately and authentically. Our scheme can achieve (1) privacy for end-to-end mobile users in a mobile network; (2) key distribution for end-to-end mobile users is achieved simply; (3) mutual authentication for end-to-end mobile users is also achieved. In addition the security of the protocol was also enhance.

ACKNOWLEDGEMENTS

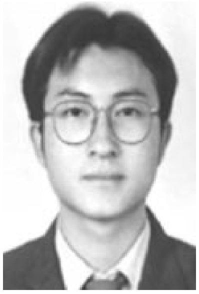
The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC91-2213-E-324-003.

REFERENCES

1. Min-Shiang Hwang, Cheng-Chi Lee, Wei-Pang Yang. An improvement of mobile users authentication in the integration environments. *International Journal of Electronics and Communications* 2002; **56**(5):293–297.
2. Min-Shiang Hwang, Chii-Hwa Lee. Authenticated key-exchange in a mobile radio network. *European Transactions on Telecommunications* 1997; **8**(3):265–269.

3. Chii-Hwa Lee, Min-Shiang Hwang, Wei-Pang Yang. Enhanced privacy and authentication for the global system of mobile communications. *Wireless Networks* 1999; **5**:231–243.
4. Aziz A, Diffie W. Privacy and authentication for wireless local area networks. *IEEE Personal Communications* 1994; **1**(1):24–31.
5. Beller MJ, Chang LF, Yacobi Y. Privacy and authentication on a portable communications system. *IEEE Journal on Selected Areas in Communications* 1993; **11**:821–829.
6. Min-Shiang Hwang, Wei-Pang Yang. Conference key distribution protocols for digital mobile communication systems. *IEEE Journal on Selected Areas in Communications* 1995; **13**(2):416–420.
7. Yi X, Okamoto E, Lam K.Y. An optimized protocol for mobile network authentication and security. *ACM Mobile Computing and Communications Review* 1998; **2**(3):37–39.
8. Zheng Y. An authentication and security protocol for mobile computing. In *Mobile Communication—Technology, Tools, Applications, Authentication and Security (Proceedings of IFIP World Conference on Mobile Communications)*, Encarnacao JL, Rabaey JM (eds). Chapman & Hall: Canberra, Australia, September 1996; 249–257.
9. ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory* 1985; **IT-31**:469–472.
10. Diffie W, Hellman ME. New directions in cryptography. *IEEE Transactions on Information Theory* 1976; **IT-22**: 644–654.
11. Schneier B. *Applied Cryptography* (2nd edn). John Wiley: New York, 1996.
12. Yae BH, Lee SC, Kim HS. A scheduling scheme for the heterogeneous multimedia services in mobile broadband systems. In *Proceedings of 8th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '97:* Helsinki; Finland, September*)*, 1997; 1059–1063.
13. Martin KM, Mitchell CJ, Comments on an optimized protocol for mobile network authentication and security. *ACM Mobile Computing and Communications Review* 1998; **3**(2):37.

AUTHORS' BIOGRAPHIES



Cheng-Chi Lee received the BS and MS in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and in 2001. He is currently pursuing his PhD in Computer and Information Science from National Chiao Tung University, Taiwan, Republic of China. His current research interests include information security, cryptography, and mobile communications.

Chao-Chen Yang received his BS in Industrial Education from the National Kaohsiung Normal University, in 1980, and his MS in Electronic Technology from the Pittsburg State University, in 1986, and his PhD in Computer Science from the University of North Texas, in 1994. He has been an associate professor in the Department of Information and Communication Engineering since 1994. His current research interests include network security, mobile communications, and distributed system.

Min-Shiang Hwang was born on August 27, 1960 in Tainan, Taiwan, Republic of China (R.O.C.). He received the BS in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, R.O.C., in 1980; the MS in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the PhD in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984 to 1986. Dr Hwang passed the National Higher Examination in the field 'Electronic Engineer' in 1988. He also passed the National Telecommunication Special Examination in the field 'Information Engineering', qualified as advanced technician in first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, R.O.C. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999–2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002–2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor of the department of Management Information Systems, National Chung Hsing University, Taiwan, R.O.C. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr Hwang has published 80 articles on the above research fields in international journals.