An Improvement of Mobile Users Authentication in the Integration Environments*

Min-Shiang Hwang, Cheng-Chi Lee and Wei-Pang Yang

Abstract **This paper shows that Tzeng and Tzeng's protocol has a drawback that the protocol can be easily crashed by an evil *VLR* attack. Therefore, we propose a slight modification to their protocol to improve their shortcoming. As a result, our protocol does not only enhance the security of Tzeng and Tzeng's protocol but also improves the efficiency.**

Keywords **Authentication, Certificate-based, Mobile Communication, Security**

1. Introduction

Generally speaking, there are two kinds of key-based cryptosystem algorithms: symmetric and asymmetric. The two cryptosystems lead to different research strategies, especially in mobile communication systems. Some symmetric cryptosystems in mobile communication systems [8–10] have been proposed for authenticating mobile users in GSM, IS-41, and DECT. Since symmetric cryptosystems were first used, the power consumption and computational cost of handsets have both been reduced in these systems. However, these systems only offer one-way authentication. On the other hand, as for asymmetric cryptosystems, some protocols [4, 11] have been proposed with quite some advantages including achieving two-way authentication as well as being equipped with the mechanism of detecting clone. However, the major disadvantage of these protocols is higher computational cost.

To combine both the advantages of symmetric and asymmetric cryptosystems, some hybrid schemes [1–3, 5, 7, 12, 13, 15] have also been proposed. These schemes have succeeded in enhancing the security level and reducing the computational cost at the same time. However, there are still some shortcomings in their schemes. In Beller et. al.'s scheme [1], in order to authenticate mobile users, they have decided to send secret information via the network, which is very dangerous because an evil network operator may clone the user. Similar problems have also occurred in Park's scheme [12]. In Carlsen [3] and Tatebayashi's [13] schemes, a trust center has been additionally added to the system to distribute a session key for mobile users. In Yi et. al.'s scheme [15], they have proposed an efficient computation method with less storage requirement in the mobile device. This scheme is, however, insecure [6].

Recently, Tzeng and Tzeng [14] have proposed a hybrid scheme of efficient authentication protocol for the third-generation mobile communication system. Their protocol has both enhanced the security and improved the performance of the second-generation mobile communication system. Their protocol can satisfy some security requirements as follows: key exchange, mutual authentication, location privacy, anonymity, avoidance of clone, perfect forward secrecy, minimized long-distance real-time signaling, and minimized bilateral pre-arrangements between service providers and network operators. Furthermore, their protocol can verify mobile users for international roaming.

However, this Tzeng-Tzeng protocol has a drawback that the protocol can be easily crashed by an evil *VLR* (Visitor Location Register) attack. An evil *VLR* can impersonate MS (Mobile Station) to access services for the use in the repeated authentication protocol in the Tzeng-Tzeng protocol because he/she can obtain the *Ticket* and session key of *MS* for the use in another *VLR*. The reason is that if an evil *VLR* knows another legal *VLR* is providing services to an *MS*, the evil *VLR* can intercept the transmitted messages and forward his/her forged messages to the *MS*. The *MS* would believe that he/she is communicating with a perfectly normal *VLR* because the *VLR* has a legal certificate issued by *HLR* (Home Location Register), and thus the *MS* would reply his/her messages (such as temporal secret key and session key). Once the evil *VLR* receives the *MS*'s messages, he/she can replay it to another legal *VLR* and then impersonate the *MS* to communication with another legal *VLR* in the repeated authentication protocol in the Tzeng-Tzeng protocol. In this paper, we shall point out this shortcoming more clearly later. Then, we shall propose a slight modification of the Tzeng-Tzeng protocol to improve the performance. Our protocol can not only enhance the se-

Received August 16, 2001. Revised November 8, 2001.

M.-S. Hwang, Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.; Fax: 886-4-23742337
E-mail: mshwang@cyut.edu.tw
C.-C. Lee, W.-P. Yang, Department of Computer and Information Science, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu 300, Taiwan, R.O.C.;
E-mail: cclee@cis.nctu.edu.tw, wpyang@cis.nctu.edu.tw
Correspondence to M.-S. Hwang.

* This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-005.

curity of the Tzeng-Tzeng protocol but also improve their protocol's efficiency.

The content of this paper is organized as follows: in the next section, we shall review Tzeng-Tzeng protocol. In Section 3, we shall analyze Tzeng-Tzeng protocol to show its weakness. Then, our improved protocol will be introduced in Section 4 and analyzed in Section 5. Finally, we shall conclude this paper with Section 6.

2. Review of the Tzeng-Tzeng protocol

Tzeng and Tzeng proposed an authentication protocol in the integration environments [14]. Technically, their protocol can be divided into two sub-protocols: the certificate-based authentication protocol and the repeated authentication protocol. The certificate-based authentication protocol is responsible for the registration procedure, handover procedure, and the procedure for international roaming. The repeated authentication protocol is responsible for authorizing the requested services by the *MS* always staying at the same *VLR*. In this section, we only briefly review the certificate-based authentication protocol. In Table 1, we list the abbreviations and notations used in their protocol. The statement $\{A \rightarrow B : messages\}$ denotes that the messages are transmitted from *A* to *B*.

Table 1. The abbreviations and notations.

HLR	Home Location Register
VLR	Visitor Location Register
MS	Mobile Station
TID/*TMSI*	Temporary mobile subscriber's unique identity/ Temporary Mobile Subscriber Identity
ID_x	Identity of the entity *x*
R_i	Random number
KU_A	Public key of the entity *A*
KR_A	Private key of the entity *A*
$(x)_y$	Encryption of *x* under key *y*
||	Concatenation
Date	Issue date of the certificate or ticket
L	Live time of the certificate or ticket
$Cert_A$	Entity *A*'s certificate $(ID_A, KU_A, Date_A, L_A, (ID_A, KU_A, Date_A, L_A)_{KR_{HLR}})$
K_{VLR}	The key of generating message authentication code of *VLR*
K_s	A temporal secret key
$\bigoplus$	*XOR* operation

The Certificate-based Authentication protocol:

When each entity is to be authenticated by others in the mobile network, the certificate-based method is used. *HLR* issues the certificate $Cert_{MS}$ and $Cert_{VLR}$ to *MS*s and *VLR*s. *MS* stores $Cert_{MS}$, KR_{MS}, and $Cert_{HLR}$ in their memory or SIM cards, and *VLR* stores the $Cert_{VLR}$, KR_{VLR}, K_{VLR}, and $Cert_{HLR}$ in their memory. K_{VLR} means the secret key of *VLR*. The protocol is described in the following steps:

1. $VLR \rightarrow MS : Cert_{VLR}, R_1$
   To authenticate *MS*, *VLR* generates R_1 and then sends his/her $Cert_{VLR}$ and R_1 to *MS*.
2. $MS \rightarrow VLR : (K_s)_{KU_{VLR}}, (Cert_{MS} \| (R_1 \| R_2)_{KR_{MS}})_{K_s}$
   Upon receiving $Cert_{VLR}$ and R_1 from *VLR*, *MS* verifies whether $Cert_{VLR}$ is a legitimate certificate using the public key of *HLR*. *MS* then generates an R_2 and a temporal secret key K_s and stores K_s, R_1, R_2, and $Cert_{VLR}$ in his/her memory or SIM card. *MS* encrypts K_s using KU_{VLR} and sends it along with $(Cert_{MS} \| (R_1 \| R_2)_{KR_{MS}})_{K_s}$ to *VLR*. Upon receiving these messages, *VLR* decrypts K_s using KR_{VLR} and then uses K_s to decrypt $Cert_{MS}$ and $(R_1 \| R_2)_{KR_{MS}}$. *VLR* can obtain KU_{MS} from $Cert_{MS}$ to decrypt R_1 and R_2. *VLR* then verifies whether R_1 is the same as the one previously sent. If it is correct, *VLR* computes the session key $R_1 \bigoplus R_2$ and stores it.
3. $VLR \rightarrow MS : (Ticket \| (R_1 \| R_2)_{KR_{VLR}})_{K_s}$
   VLR can authenticate $Cert_{MS}$ using the public key of *HLR*. After verifying *MS*, *VLR* generates a *TID* and a *Ticket* to *MS*, where the *Ticket* is a MAC (Message Authentication Code). The MAC is derived from $(TID, Date, L)_{K_{VLR}}$. Then *VLR* sends $(Ticket \| (R_1 \| R_2)_{KR_{VLR}})_{K_s}$ to *MS*.

After receiving these messages, *MS* decrypts *Ticket* and $(R_1 \| R_2)_{KR_{VLR}}$ using K_s. *MS* can recover $(R_1 \| R_2)$ using the public key of *VLR* and check whether it is correct. If it is, then the session key $R_1 \bigoplus R_2$ is computed. Finally, *MS* stores the *Ticket* and session key for the use in the repeated authentication protocol [14].

3. Cryptanalysis of the Tzeng-Tzeng protocol

In this section, we shall show that the Tzeng-Tzeng authentication protocol is not robust enough against the attack from an evil *VLR*. An evil *VLR* can impersonate an *MS* to request services in another *VLR* in the Tzeng-Tzeng repeated authentication protocol. Once the evil *VLR* obtains the *Ticket* and session key pair of an *MS*, he/she can impersonate this *MS* to access services for the use in the repeated authentication protocol in another *VLR*. In order to obtain the *Ticket* and session key pair of an *MS*, an evil *VLR* can intercept and modify messages during the communication sessions between the *MS* and another *VLR*. The detailed steps of this attack are shown in Figure 1 and as follows:

1. Assume that VLR' is an attacker. To forge *MS* communicating with *VLR*, VLR' can intercept $Cert_{VLR}$ and R_1 when *VLR* sends them to *MS* and then modify them to $Cert_{VLR'}$ and R_1. Then VLR' sends $Cert_{VLR'}$ and R_1 to *MS*.
2. After receiving $Cert_{VLR'}$ and R_1 from VLR', *MS* believes that he/she is communicating with a legitimate *VLR* when making a call. *MS* follows the usual proced-

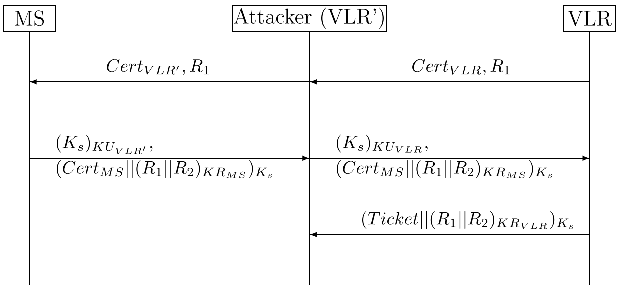

MS
Attacker (VLR')
VLR
$Cert_{VLR'}, R_1$
$Cert_{VLR}, R_1$
$(K_s)_{KU_{VLR'}}$,
$(Cert_{MS}||(R_1||R_2)_{KR_{MS}})_{K_s}$
$(K_s)_{KU_{VLR}}$,
$(Cert_{MS}||(R_1||R_2)_{KR_{MS}})_{K_s}$
$(Ticket||(R_1||R_2)_{KR_{VLR}})_{K_s}$

Fig. 1. Attack on the Tzeng-Tzeng protocol.

ure in the Tzeng-Tzeng protocol; he/she produces the messages $(K_s)_{KU_{VLR'}}$, $(Cert_{MS} \parallel (R_1 \parallel R_2)_{KR_{MS}})_{K_s}$ and sends them to VLR'.

3. Upon receiving these messages from *MS*, VLR' can also follow the same procedure in the Tzeng-Tzeng protocol and decrypt K_s using his/her private key. Thus, VLR' re-encrypts K_s using the public key of *VLR* and sends the encrypted message and $(Cert_{MS} \parallel (R_1 \parallel R_2)_{KR_{MS}})_{K_s}$ to *VLR*.
4. After receiving these messages from VLR', *VLR* follows the usual procedure in the Tzeng-Tzeng protocol. *VLR* can verify whether $Cert_{MS}$ is a legitimate *MS*. If it is correct in this case, yes, *VLR* believes that he/she is communicating with a legitimate *MS*. *VLR* produces a *Ticket* and computes a session key to store them. *VLR* sends $(Ticket \parallel (R_1 \parallel R_2)_{KR_{VLR}})_{K_s}$ to *MS*.
5. VLR' can intercept these messages and decrypt them because he/she has the key K_s. Finally, VLR' has a *Ticket* of *MS* and a session key $R_1 \bigoplus R_2$ of *MS*. Once having these messages, the attacker (VLR') can pretend to be the *MS* to communicate with *VLR* in the Tzeng-Tzeng repeated authentication protocol until the *Ticket* is out of date.

4. Our improved protocol

In our modified protocol, we can overcome the attack from an evil *VLR*. Since the *Ticket* and session key of *MS* can be in no way obtained, an attacker cannot impersonate *MS* to communicate with *VLR* any longer in our modified Tzeng-Tzeng repeated authentication protocol.

As in the original Tzeng-Tzeng protocol, *HLR* is distributes a certificate and a private key to each entity. For example, *MS* has $Cert_{MS}$, KR_{MS}, and $Cert_{HLR}$, and *VLR* has $Cert_{VLR}$, KR_{VLR}, K_{VLR}, and $Cert_{HLR}$, where K_{VLR} means the secret key of *VLR*. Here, we also use the same abbreviations and notations in Table 1. The statement "$A \rightarrow B$: *messages*" denotes that the messages are transmitted from A to B.

In our improved protocol, we propose some slight modification to the certificate-based authentication part of the Tzeng-Tzeng protocol. The other parts of the Tzeng-Tzeng protocol, such as the repeated authentication protocol and the authentication protocol for international roaming, stay the same as they are. The steps of our improved protocol are shown in Figure 2 and as follows:

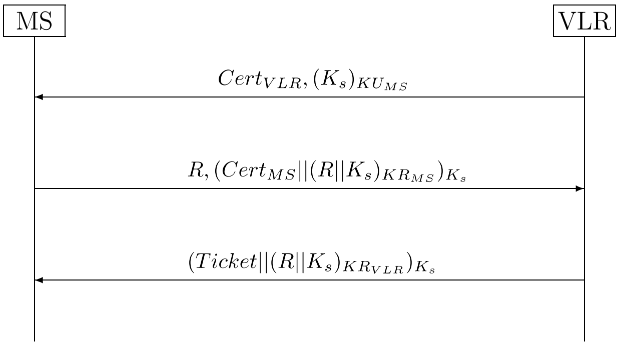

MS
VLR
$Cert_{VLR}, (K_s)_{KU_{MS}}$
$R, (Cert_{MS}||(R||K_s)_{KR_{MS}})_{K_s}$
$(Ticket||(R||K_s)_{KR_{VLR}})_{K_s}$

Fig. 2. Our improved protocol.

1. $VLR \rightarrow MS : Cert_{VLR}, (K_s)_{KU_{MS}}$
   To authenticate *MS*, *VLR* generates a temporal secret key K_s and then sends his/her $Cert_{VLR}$ and $(K_s)_{KU_{MS}}$ to *MS*.
2. $MS \rightarrow VLR : R, (Cert_{MS} \parallel (R \parallel K_s)_{KR_{MS}})_{K_s}$
   Upon receiving $Cert_{VLR}$ and $(K_s)_{KU_{MS}}$ from *VLR*, *MS* verifies whether $Cert_{VLR}$ is a legitimate certificate using the public key of *HLR*. *MS* decrypts K_s using his/her private key. *MS* then generates an R and stores K_s, R, and $Cert_{VLR}$ in his/her memory or SIM card. *MS* sends R and $(Cert_{MS} \parallel (R \parallel K_s)_{KR_{MS}})_{K_s}$ to *VLR*. Upon receiving these messages, *VLR* decrypts $Cert_{MS}$ and $(R \parallel K_s)_{KR_{MS}}$ using the key K_s. *VLR* can obtain KU_{MS} from $Cert_{MS}$ to decrypt R and K_s. *VLR* then verifies whether K_s is the same as the one previously sent and verifies whether R remains the same too. If and only if both are yeses, *VLR* computes the session key $R \bigoplus K_s$ and stores it.
   Note that no one can forge R even if R is in plaintext. If an attacker wants to forge it, he/she has to know K_s and KR_{MS} to compute $(Cert_{MS} \parallel (R \parallel K_s)_{KR_{MS}})_{K_s}$. In an asymmetric cryptosystem, the private key KR_{MS} is only known to *MS*. Therefore, no one can forge R.
3. $VLR \rightarrow MS : (Ticket \parallel (R \parallel K_s)_{KR_{VLR}})_{K_s}$
   VLR can authenticate the $Cert_{MS}$ using the public key of *HLR*. After verifying the *MS*, *VLR* generates a *TID* and a *Ticket* for the *MS*, where the *Ticket* is a MAC. The MAC is computed from $(TID, Date, L)_{K_{VLR}}$. Then *VLR* sends $(Ticket \parallel (R \parallel K_s)_{KR_{VLR}})_{K_s}$ to *MS*.

After receiving this message, *MS* decrypts *Ticket* and $(R \parallel K_s)_{KR_{VLR}}$ using K_s. *MS* can recover $(R \parallel K_s)$ using the public key of *VLR* and check whether it is correct. If it is, then *VLR* computes the session key $R \bigoplus K_s$. Finally, *MS* stores the *Ticket* and session key for later use in the repeated authentication protocol [14].

5. Analysis

Our protocol is a slight modification of the Tzeng-Tzeng protocol [14]. The security and efficiency of the Tzeng-

Tzeng protocol have already been discussed and demonstrated in [14]. In this session, we shall only discuss the difference between their protocol and ours.

Security analysis:

Our protocol can overcome the attack from an evil *VLR* that the Tzeng-Tzeng protocol falls for. In the Tzeng-Tzeng protocol, an attacker can intercept and modify the messages between *MS* and *VLR* and then impersonate *MS* to fool *VLR*. However, this attack will surely be detected by our *VLR*. The reason for that is only *MS* and *VLR* know the temporal secret key K_s. Since K_s is not known to any others, an attacker cannot obtain *Ticket* and $(R \parallel K_s)$ of *MS*. Therefore, there will be no way to fool *VLR* in the repeated authentication protocol.

Efficiency:

In Table 2, we can see that our protocol is more efficient than the original Tzeng-Tzeng protocol. In our protocol, one unit of computation time is reduced because *MS* does not generate a K_s. Therefore, the computation cost is low, and the power consumption of *MS* is of course reduced in our protocol. Here, $T(\cdot)$ stands for the computation time. For example, $T(Symmetric)$ and $T(Asymmetric)$ indicate respectively the computation time the symmetric cryptosystem spends and that the asymmetric cryptosystem spends; $T(K_s)$, $T(TID)$, $T(Ticket)$, and $T(Random)$ indicate respectively the computation time for the generation of K_s, *TID*, *Ticket*, and random numbers (R_1, R_2, R); and $T(XOR)$ indicates the computation time the *XOR* operation spends. We divide $T(Asymmetric)$ into two processes, signing S and verifying V, which use private key and public key respectively. $T(Asymmetric - S)$ and $T(Asymmetric - V)$ indicate respectively the computing time the asymmetric cryptosystem the spending on signing process and the computing time the verifying process takes. In general, the verifying process is mostly faster than the signing process in an asymmetric cryptosystem. That is to say, in terms of the computations in the asymmetric cryptosystem in *VLR*, our protocol is more efficient than the Tzeng-Tzeng protocol, and in terms of the computations in the computing asymmetric cryptosystem in *MS*, the Tzeng-Tzeng protocol is more efficient than of our protocol. Overall, Our protocol is more secure and efficient than that of the Tzeng-Tzeng protocol.

Table 2. The computational costs.

	Tzeng-Tzeng Protocol	Our Protocol
VLR	$2T(Symmetric)$	$2T(Symmetric)$
	$2T(Asymmetric\text{-}V)$	$3T(Asymmetric\text{-}V)$
	$2T(Asymmetric\text{-}S)$	$1T(Asymmetric\text{-}S)$
	$1T(Random)$	$1T(K_s)$
	$1T(TID)$	$1T(TID)$
	$1T(Ticket)$	$1T(Ticket)$
	$1T(XOR)$	$1T(XOR)$
MS	$2T(Symmetric)$	$2T(Symmetric)$
	$3T(Asymmetric\text{-}V)$	$2T(Asymmetric\text{-}V)$
	$1T(Asymmetric\text{-}S)$	$2T(Asymmetric\text{-}S)$
	$1T(Random)$	$1T(Random)$
	$1T(K_s)$	None
	$1T(XOR)$	$1T(XOR)$

6. Conclusions

In this paper, we have pointed out that the Tzeng-Tzeng protocol is not strong enough against the attack from an evil *VLR* and thus is not a secure protocol. Therefore, we have proposed an improvement of the Tzeng-Tzeng protocol which is a slight modification. The proposed protocol does not only achieve their original security requirements but also enhances the security by withstanding the attack from an evil *VLR*. In addition, the efficiency of our protocol is even higher than that of the original Tzeng-Tzeng protocol.

Acknowledgement

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. NSC90-2213-E-324-005.

References

[1] Beller, M.J.; Chang, L.F.; Yacobi, Y.: "Privacy and authentication on a portable communications system," *IEEE Journal on Selected Areas in Communications*, vol. 11, pp. 821–829, Aug. 1993.

[2] Brown, D.: "Techniques for privacy and authentication in personal communication systems," *IEEE Personal Communications*, pp. 6–10, Aug. 1995.

[3] Carlsen, U.: "Optimal privacy and authentication on a portable communications system," *ACM Operation System Review*, vol. 28, pp. 16–23, July 1994.

[4] Frankel, Y.; Herzberg, A.; Karger, P.A.; Krawczyk, H.; Kunzinger, C.A.; Yung, M.: "Security issues in a CDPD wireless network," *IEEE Personal Communications*, vol. 4, no. 16–27, p. 1995, 2.

[5] Hwang, M.-S.; Lee, C.H.: "Authenticated key-exchange in mobile radio network," *European Transactions on Telecommunications*, vol. 8, pp. 265–269, May/June 1997.

[6] Hwang, M.-S.; Tang, Y.-L.; Lee, C.-C.: "A new protocol using time-stamp for mobile network authentication and security," *Proceedings of the Six Workshop on Mobil Computing*, pp. 61–65, 2000.

[7] Hwang, M.-S.; Yang, W.P.: "Conference key distribution protocols for digital mobile communication systems," *IEEE*

Journal on Selected Areas in Communications, vol. 13, pp. 416–420, Feb. 1995.

[8] Hwang, T.: "Scheme for secure digital mobile communications based on symmetric key cryptography," *Information Processing Letters*, vol. 48, pp. 35–37, 1993.

[9] Lee, C.H.; Hwang, M.-S.; Yang, W.P.: "Enhanced privacy and authentication for the global system for mobile communications," *Wireless Networks*, vol. 5, pp. 231–243, July 1999.

[10] Mohan, S.: "Privacy and authentication protocols for PCS," *IEEE Personal Communications*, vol. 35, pp. 34–38, Oct. 1996.

[11] Park, C.; Kurosawa, K.; Okamoto, T.; Tsujii, S.: "On key distribution and authentication in mobile radio networks," in *Advances in Eurocryptology, Proceedings of Eurocrypt'93*, pp. 131–138, 1993.

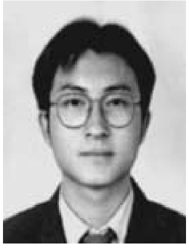
[12] Park, C.S.: "On certificate-based security protocols for wireless mobile communication systems," *IEEE Network*, pp. 50–55, 1997.

[13] Tatebayashi, M.; Matsuzaki, N.; Newman, Jr. D.B.: "Key distribution protocol for digital mobile communication systems," in *Advances in Cryptology, Proceedings of Crypto'89*, pp. 324–334, 1989.

[14] Tzeng, Z.-J.; Tzeng, W.-G.: "Authentication of mobile users in the integration environments," in *International Symposium on Communications (ISCOM'99)*, pp. 195–199, Kaohsiung, Taiwan, Nov. 1999.

[15] Yi, X.; Okamoto, E.; Lam, K.Y.: "An optimized protocol for mobile network authentication and security," *ACM Mobile Computing and Communications Review*, vol. 2, no. 3, pp. 37–39, 1998.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. 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 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the 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, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.



Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and in 2001. He is currently pursuing his Ph.D. 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.

Wei-Pang Yang was born on May 17, 1950 in Hualien, Taiwan, Republic of China. He received the B.S. degree in mathematics from National Taiwan Normal University in 1974, and the M.S. and Ph.D. degrees from the National Chiao Tung University in 1979 and 1984, respectively, both in computer engineering. Since August 1979, he has been on the faculty of the Department of Computer Science and Information Engineering at National Chiao Tung University, Hsinchu, Taiwan. In the academic year 1985-1986, he was awarded the National Postdoctoral Research Fellowship and was a visiting scholar at Harvard University. Prom 1986 to 1987, he was the Director of the Computer Center of National Chiao Tung University. In August 1988, he joined the Department of Computer and Information Science at National Chiao Tung University, and acted as the Head of the Department for one year. Then he went to IBM Al-maden Research Center in San Jose, California for another one year as visiting scientist. From 1990 to 1992, he was the Head of the Department of Computer and Information Science again. His research interests include database theory, database security, object-oriented database, image database, and Chinese database retrieval systems.

Dr. Yang is a senior member of IEEE, and a member of ACM. He was the winner of the 1988, and 1992 AceR Long Term Award for Outstanding M.S. Thesis Supervision, 1993 AceR Long Term Award for Outstanding Ph. D. Dissertation Supervision, and the winner of 1990 Outstanding Paper Award of the Computer Society of the Republic of China. He also obtained the Outstanding Research Award of National Science Council of the Republic of China.