Conference Key Distribution Schemes for Secure Digital Mobile Communications

Min-Shiang Hwang and Wei-Pang Yang, *Senior Member, IEEE*

***Abstract*—In this paper, we propose a new service for digital mobile communication systems. The service enables two or more users to hold a secure conference. Two requirements must be considered: privacy and authentication. Privacy involves ensuring that an eavesdropper cannot intercept the conversations of the parties holding the conference. Authentication involves ensuring that service is not obtained fraudulently in order to avoid usage charges. We present two new conference key distribution schemes for digital mobile communication systems. In these schemes, a group of users can generate a common secret key over a public channel so that they may hold a secure conference.**

I. Introduction

MOBILE satellite communications have been implemented for many systems, including maritime, aeronautical, and land systems. A main characteristic of mobile satellite communication systems is that they provide wireless access to traditional wireline networks for a large number of access services, such as telephone calls. But wireless transmission is vulnerable to relatively easy interception [7], such as fraudulent call attempts and intrusion or listening-in by third parties. Thus, we action must be taken to prevent various kinds of intrusion. For example, sensitive data must be protected against disclosure to an unauthorized person. Fraudulent modification of messages, repeating old messages, or one user masquerading as another must also be prevented. Data are particularly vulnerable when transferred in networks, especially in mobile communication networks. For this reason, a feasible solution for implementation of secure mobile communication systems is needed.

A simple but effective method for secure digital communications is the use of encryption methods. Two types of encryption methods are available: private-key cryptosystems, such as DES [14], [20] and FEAL-32 [13], and public-key cryptosystems, such as RSA [17]. In public-key cryptosystems the degree of computational complexity increases with the level of security. As a result, public-key cryptosystem cannot be used in low-cost and low-power mobile (portable) communication systems, because no existing protocol provides acceptable call-setup time performance [6]. Private-key cryptosystems are simpler and faster than public-key cryptosystem as far as computational complexity is concerned. But private-key cryptosystems require a tremendous amount of effort for key management and distribution [3]. Private-key cryptosystems require that parties (portable) to the conversation share knowledge of a secret key and that unauthorized users not have access to this key. Key agreement is the process by which the parties agree upon the proper key.

In this paper, we propose a new service for digital mobile communication systems. This service enables two or more users to hold a secure electronic conference. Two requirements must be considered: privacy and authentication. Privacy involves ensuring an eavesdropper cannot intercept conversations during a conference or information about conferees' locations. Authentication involves ensuring that service is not obtained fraudulently in order to avoid charges for usage. We thus have the following four security goals for the mobile communication system:

1) Privacy of conversation content during the conference.
2) Privacy of information about conferees' locations during the conference.
3) Prevention of fraud by ensuring that the portable units are authentic.
4) Prevention of replaying attacks, so that intruders are not able to obtain sensitive data by replaying a previously intercepted message.

Since the portable units must operate over long periods of time on small, low-power batteries, low complexity implementation of the encryption function is critical. Private-key cryptosystems meet such criteria [2]. As mentioned above, private-key cryptosystems require a session key agreed upon by the conferees in the conference.

In this paper, we present two new conference key distribution schemes for digital mobile communication systems. In these schemes, a group of conferees can obtain a common secret key over a public channel and use it to hold a secure conference. Since the computation needed to obtain the common secret session key is relatively simple, our scheme can be used in low-cost, low-power mobile communications. The complexity of our schemes will be analyzed in Section V.

This paper is organized as follows. In the next section, we review previous key distribution schemes and the problems that arise when they are applied to mobile communication systems. In Section III, we present two new schemes for mobile communication systems. In Section IV, we analyze the security of our schemes. In Section V, we discuss and evaluate

Manuscript received January 15, 1994; revised September 5, 1994. This work was supported by the National Science Council, Taiwan, China, under Contract no. NSC83-0408-E-009-039. This paper was presented at the Conference of IEEE APCCAS'94, Taipei, 1994.

M.-S. Hwang is with the Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 300, China. He is also Directorate General of Telecommunication Laboratories, Ministry of Transportation and Communications, Chung-Li, Taiwan 320, China.

W.-P. Yang is with the Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 300, China.

IEEE Log Number 9407520.

the complexity of the proposed schemes. Finally, Section VI presents our conclusions.

II. Related Key Distribution Schemes

A key distribution protocol for mobile communication systems was first proposed in [21]. Mobile communication systems may be regarded as star-type networks. For convenience, let the word "portable" denote a user terminal. Each user terminal in the network communicates with another user via a network center. In order to eliminate the need for key management at a network center and to enable hardware-limited user terminals to obtain a common secret key in a reasonable amount of time, Tatebayashi *et al.* [21] employed a public key cryptosystem such as the RSA cryptosystem for uplink channels (from a user terminal to a network center), and a secret key cryptosystem such as the Vernam cipher for downlink channels (from a network center to user terminals). Unfortunately, this method was successfully attacked by Park *et al.* [15]. Recently, Hwang proposed another scheme based on symmetric key cryptography [8]. This method requires key management at the network center. Beller, Chang, and Yacobi of Bellcore proposed three elegant public-key/private-key hybrid key agreement and authentication protocols [1], [2]. Their methods are based on the modular square root technique [16] and the Diffie-Hellman technique [4].

The above key distribution schemes, however, can be used only by two user terminals. If three or more user terminals want to communicate in order to hold an electronic conference, they have to derive one communication key for each link in the digital mobile communication systems. Doing so requires $(m-1)$ times more computations than that needed for two users, where m is the number of user terminals.

The concept of conference key distribution was first proposed by Ingemarsson *et al.* [9]. A number of studies have been carried out concerning conference key distribution systems [10], [11], [12]. Since these schemes involve a high computational complexity (modular exponentiation) as the fundamental arithmetic, they are not suitable for use in low-cost, low-power mobile communication systems. Below two new conference key distribution schemes are proposed for low complexity digital mobile communication systems. In our schemes, a group of conferees can generate a common secret key over the public channel to hold a secure conference.

III. Two New Efficient Schemes

In this section we present two conference key distribution protocols for digital mobile communications. The first is based on public-key cryptography. In this scheme, the network center need not keep the secret keys of all conferees. The other is based on private-key cryptography. The scheme can easily be implemented using hardware-limited terminals, but the network center needs to keep the secret keys of all conferees.

Without loss of generality, let user terminal T_1 be the terminal logged in by the chairperson U_1, who initiates the secure electronic conference with m conferees, $U_1, U_2, \cdots, U_m$. Moreover, let NC be the network center; T_i the user terminal logged in by U_i; ID_i the unique identity of U_i; CK_1 and

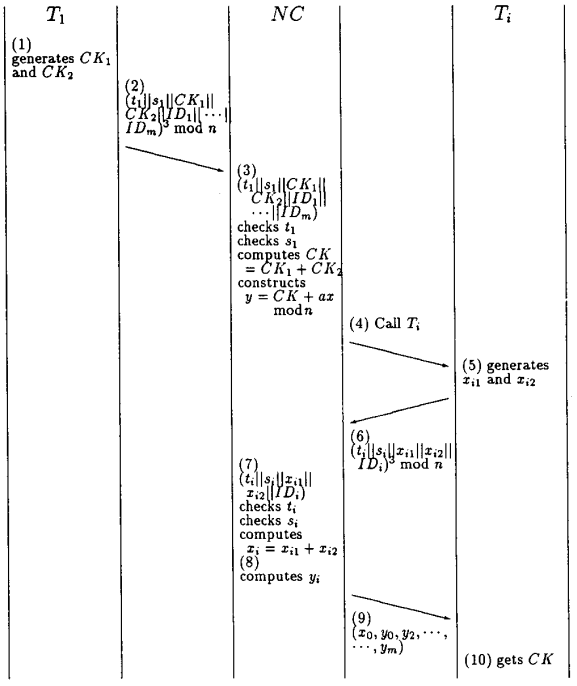

Fig. 1. Conference key distribution protocol (CKDP1).

CK_2 the random numbers generated by T_i; and t_i the date and time at which message is sent. The symbol $\|$ denotes a concatenation of two numbers. NC generates each user U_i's secret information s_i from ID_i and $s_i = f(\mathrm{ID}_i)$, where f is a secret one-way function which only the network center knows.

Protocol 1: This protocol for conference key distribution is based on asymmetric key cryptography. We use the RSA cryptographic method as the asymmetric cryptosystem. In the following protocol, the modulus n is a product of p and q, where p and q are large prime numbers. The encryption exponent e is chosen to be 3. The decryption exponent d is a number satisfying $ed \bmod \phi(n) = 1$, where $\phi(n)$ denotes the Euler's totient function of n. This key distribution protocol, which is illustrated in Fig. 1, can be summarized as follows.

1) Conference Key Distribution Protocol 1 (CKDP1):

Step 1: Initial terminal T_1 chooses random numbers CK_1 and CK_2, and the key $\mathrm{CK} = \mathrm{CK}_1 + \mathrm{CK}_2$ is chosen as the common secret session key.

Step 2: T_1 sends $(t_1\|s_1\|\mathrm{CK}_1\|\mathrm{CK}_2\|\mathrm{ID}_i,\ i = 1, \cdots, m)^3 \bmod n$ to the network center (NC).

Step 3: NC decrypts the encrypted data signal and obtains $(t_1\|s_1\|\mathrm{CK}_1\|\mathrm{CK}_2\|\mathrm{ID}_i,\ i = 1, \cdots, m)$. NC extracts t_1, s_1, CK_1, CK_2, and ID_i, $i = 1, \cdots, m$ from the decrypted data. NC checks the validity of the timestamp t_1. NC verifies T_1 and computes $\mathrm{CK} = \mathrm{CK}_1 + \mathrm{CK}_2$.

Step 4: NC calls the terminals of the other conferees. NC randomly chooses a coefficient a which is securely known only by NC and then constructs a polynomial of one degree $y = \mathrm{CK} + ax \bmod n$. NC also randomly chooses x_0 and obtains y_0 from $y = \mathrm{CK} + ax \bmod n$.

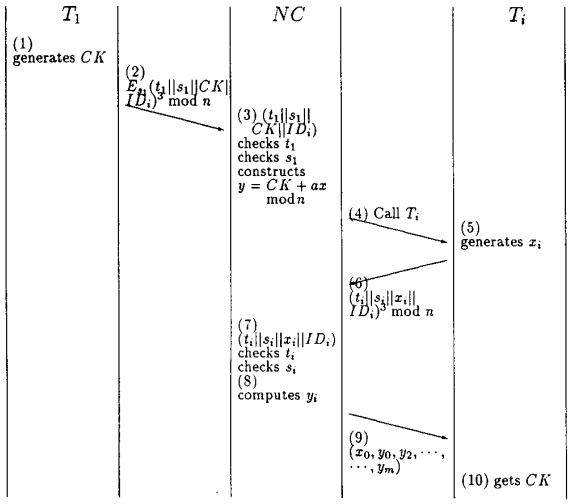

Fig. 2. Conference key distribution protocol (CKDP2).

Step 5: Each terminal, T_i, $i = 2, \cdots, m$, chooses random numbers x_{i1} and x_{i2} as a key-encryption key.
Step 6: Each T_i, $i = 2, \cdots, m$ sends $(t_i\|s_i\|x_{i1} \parallel x_{i2}\|\mathrm{ID}_i)^3 \bmod n$ to NC.
Step 7: NC decrypts the encrypted data signal and obtains $(t_i\|s_i\|x_{i1}\|x_{i2}\|\mathrm{ID}_i)$. NC extracts t_i, s_i, x_{i1}, x_{i2}, and ID_i from the decrypted data. NC checks the validity of the timestamp t_i. NC verifies T_i and computes $x_i = x_{i1} + x_{i2}$.
Step 8: NC obtains y_i, $i = 2, \cdots, m$ by substituting x_i into the equation $y_i = \mathrm{CK} + ax_i \bmod n$.
Step 9: NC broadcasts $(x_0, y_0, y_2, y_3, \cdots, y_m)$ to T_i, $i = 2, \cdots, m$.
Step 10: T_i computes the common secret session key of T_is, $\mathrm{CK} = y_i - \left(\frac{y_i - y_0}{x_i - x_0}\right) x_i \bmod n$.

Protocol 2: This protocol for conference key distribution is based on symmetric key cryptography. We use secure private-key encryption and decryption algorithms as the symmetric cryptosystem. In the following protocol, we assume that all terminals in the system are capable of secret private-key encryption and decryption. Let E and D denote secure private-key encryption and decryption algorithms, respectively. For the plaintext M, the following equation holds

$$M = D_s(E_s(M)) \tag{1}$$

where s is the private key used in the symmetric cryptosystem. The key distribution protocol, illustrated in Fig. 2, can be summarized as follows.

2) Conference Key Distribution Protocol 2 (CKDP2):

Step 1: Initial terminal, T_1, generates CK as a common secret session key.
Step 2: T_1 sends $E_{s_1}(t_1\|\mathrm{ID}_1\|\mathrm{ID}_2\|\cdots\|\mathrm{ID}_m\|\mathrm{CK})$ to NC.
Step 3: NC decrypts the encrypted data signal and obtains $(t_1\|\mathrm{ID}_1\|\mathrm{ID}_2\|\cdots\|\mathrm{ID}_m\|\mathrm{CK})$. NC extracts t_1, $\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_m$ and CK from the decrypted data. NC checks the validity of the timestamp t_1 and verifies T_1.
Step 4: NC calls the terminals of the other conferees. NC randomly chooses a coefficient a which is securely known only by NC and then constructs a polynomial of one degree $y = \mathrm{CK} + ax \bmod n$. NC also randomly chooses x_0 and obtains y_0 from $y = \mathrm{CK} + ax \bmod n$.
Step 5: Each terminal T_i, $i = 2, \cdots, m$, generates x_i as a key-encryption key.
Step 6: Each T_i, $i = 2, \cdots, m$ sends $E_{s_i}(t_i\|\mathrm{ID}_i\|x_i)$ to NC.
Step 7: NC decrypts the encrypted data signal and obtains $(t_i\|\mathrm{ID}_i\|x_i)$. NC extracts t_i, ID_i and x_i from the decrypted data. NC checks the validity of the timestamp t_i and verifies T_i.
Step 8: NC obtains y_i, $i = 2, \cdots, m$ by substituting x_i into equation $y_i = \mathrm{CK} + ax_i \bmod n$.
Step 9: NC broadcasts $(x_0, y_0, y_2, y_3, \cdots, y_m)$ to T_i, $i = 2, \cdots, m$.
Step 10: T_i computes the common secret session key with T_is, $\mathrm{CK} = y_i - \left(\frac{y_i - y_0}{x_i - x_0}\right) x_i \bmod n$.

If a user is one of the legal conferees, he can obtain the secret session key $\mathrm{CK}(= y_i - (\frac{y_i - y_0}{x_i - x_0}) x_i \bmod n)$ by solving the following simultaneous equations

$$\begin{cases} y_i = \mathrm{CK} + ax_i \bmod n \\ y_0 = \mathrm{CK} + ax_0 \bmod n. \end{cases} \tag{2}$$

IV. Security Analysis

In this section, we shall show that user authentication and session key distribution are both addressed in our schemes.

The network center will authenticate the chairperson's identification ID_1 by checking the correctness of ID_1 at step 3 of the proposed protocols. Similarly, the network center can authenticate the identification ID_i of other users invited by the chairperson to participate in the conference by checking the correctness of ID_i at Step 7 of the proposed protocols. Therefore, the above protocols ensure that a portable unit cannot access the network using a false identity in order to avoid charges for usage.

Since the common secret session key CK is sent to the network center by an encryption function, an intruder cannot decipher CK unless he knows the secret key of the network center in the CKDP1 protocol or the private key of conferees in the CKDP2 protocol. Therefore, the conferees can hold a secure conversation.

Similarly, the location of conferees is protected by the above-mentioned encryption function. It is difficult for an intruder to obtain the location of ID_i from the equation $(t_1\|s_1\|\mathrm{CK}_1\|\mathrm{CK}_2\|\mathrm{ID}_i, i = 1, \cdots, m)^3 \bmod n$ of Step 2 in the CKDP1 protocol or from the equation $E_{s_1}(t_1\|\mathrm{ID}_1\|\mathrm{ID}_2\|\cdots\|\mathrm{ID}_m\|\mathrm{CK})$ of step 2 in the CKDP2 protocol.

Basically, Steps 8, 9, and 10 in the proposed protocols are implementations of Shamir's $(2, m)$ threshold scheme [19]. Therefore, revealing the secret conference key of our schemes is equivalent to nullifying the Shamir threshold scheme.

In order to pass the verification of Step 3 and Step 7 in our protocols, an intruder must change t_i into a new time t^* such that $(T'' - t^*) \leq \Delta T$, where T'' is the time when the system receives the illegal login message and ΔT is the expected legal time interval for transmission delay. Once t_i is changed, an intruder will fail the verification of Step 3 and Step 7 in the

proposed protocols. Therefore, the proposed scheme is secure against replaying attacks.

V. Computational Analysis

The computational complexity of our schemes in the portable is dominated by the computation of Steps 6 and 10 in the CKDP1 and CKDP2 protocols. This computation requires only 3 modular multiplications (2 for Step 6, 1 for step 10), 1 modular division, and 3 subtractions for Step 10 in CKDP1.

The computation of Step 6 in CKDP2 is based on that of the private-key encryption algorithms. If DES is used as the symmetric cryptosystem, it partitions the data text into blocks of 64 b each. This requires

$$T_{\mathrm{DES}} = \lceil L/64 \rceil \mathrm{DES}(64),$$

where DES(64) is the time required to encipher 64 b of text using the DES device and is the length of the encrypted data. Assume that each t_i, ID_i, and x_i of Step 6 in CKDP2 is an integer 256 b in length. Thus

$$T_{\mathrm{DES}} = 12 * \mathrm{DES}(64).$$

DES has been implemented both in software and in hardware. Hardware implementations achieve encryption rates of 1 Gbs [5]. A software implementation of DES on an Intel 80486/33 MHz microprocessor can perform 2.6 million bps; one on a Motorola 68020/16 MHz microprocessor can perform 0.22 million bps [18]. Therefore, T_{DES} is equal to 0.8 μs using hardware implementation and 4.6 μs using software implementation. The computation requires only one modular multiplication, one modular division, and three subtractions for Step 10 in CKDP2.

This is achievable in real time by a portable unit. Thus, our schemes are practical for implementation in a low-cost, low-power secure mobile communication system.

VI. Discussion and Conclusion

Mobile communication systems consist of mobile switching centers, base stations, and portable units. Since the mobile switching centers and base stations generally reside at a fixed location, the switching centers and base stations can be installed using high-power, high-cost mechanisms. However, the portables are movable and are carried by persons or on vehicles. Since the portables must operate over long periods of time on small low-power batteries, low complexity implementation is critical.

One mobile switching center can service many base stations, and one base station can service many portables. Thus, mobile communication systems can be geographically regarded as a star-type network. The role of the network center in our schemes can be taken over by the base station or the mobile switching center, both of which can perform complex computations in a reasonable time. In comparison, the portables are required to perform only relatively simple computations, as showed in Section V. Thus, our schemes are suitable for low-cost, low-power mobile communication systems.

Since the fundamental arithmetic of conventional conference key distribution schemes is extremely complex, these schemes are not suitable for use in low-cost, low-power mobile communication systems. The two simple but effective schemes proposed here for holding secure electronic conferences in digital mobile communication systems enable hardware-limited user terminals to obtain a common secret conference key in a reasonable time.

The CKDP2 protocol is implemented using a private-key encryption algorithm, and thus requires less hardware complexity than the CKDP1 protocol, which is implemented with a public-key encryption algorithm. However, the CKDP2 protocol requires key management at the network center. Both user authentication and key distribution are considered in the proposed schemes. Another feature of our schemes is that the chairperson can freely choose a common key CK shared among all legitimately intended principals and himself.

Acknowledgment

We would like to thank the nonymous referees for their many helpful comments and suggessions.

References

[1] M. J. Beller, L. F. Chang and Y. Yacobi, "Privacy and authentication on a portable communications system," in *Proc. IEEE GLOBECOM '91*, Phoenix, AZ, Dec. 1991, pp. 1922–1927.
[2] ——, "Privacy and authentication on a portable communications system," *IEEE J. Select. Areas Commun.*, vol. 11, pp. 821–829, Aug. 1993.
[3] D. E. R. Denning, *Cryptography and Data Security*. Reading, MA: Addison-Wesley, 1982.
[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. 22, pp. 644–654, 1976.
[5] H. Eberle, "A high-speed DES implementation for network applications," in *Proc. CRYPTO '92, Lecture Notes in Computer Science*, 1993, pp. 527–545.
[6] ETSI, "Digital European cordless telecommunications common interface part 7: Security features," European Telecommun. Standards Inst., ETSI, Tech. Rep. Version 5.03, May 1991.
[7] S. R. Hall and D. P. Maher, "Closing in on wireless privacy," *AT&T Technol.*, vol. 8, no. 3, pp. 22–25, 1993.
[8] T. Hwang, "Scheme for secure digital mobile communications based on symmetric key cryptography," *Inform. Processing Lett.*, vol. 48, pp. 35–37, 1993.
[9] I. Ingemarsson, D. T. Tang, and C. K. Wong, "A conference key distribution system," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 714–720, Sep. 1982.
[10] K. Koyama, "Identity-based conference key distribution system," *IEE Electron. Lett.*, vol. 23, no. 10, pp. 495–496, May 1987.
[11] K. Koyama and K. Ohta, "Identity-based conference key distribution system," in *Proc. CRYPTO '87, Lecture Notes in Computer Science*, pp. 194–202, 1987.
[12] ——, "Identity-based conference key distribution systems in broadcast networks," *IEE Electron. Lett.*, vol. 23, no. 12, pp. 647–649, June 1987.
[13] S. Miyaguchi, "The FEAL cipher family," in *Proc. CRYPTO '90, Lecture Notes in Computer Science*, vol. 435, pp. 727–638, Aug. 1990.
[14] National Bureau of Standard, "Data encryption standard," *FIPS*, NBS, 1977.
[15] C. Park, K. Kurosawa, T. Okamoto, and S. Tsujii, "On key distribution and authentication in mobile radio networks," in *Proc. Eurocrypt '93*, 1993, pp. 131–138.
[16] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Lab. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, Tech. Rep. MIT/LCS/TR-212, Jan. 1979.
[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[18] B. Schneier, *Applied Cryptography*. New York: Wiley, 1994.
[19] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, 1979.

[20] M. E. Smid and D. K. Branstad, "The data encryption standard: past and future," *Proc. IEEE*, vol. 76, no. 5, pp. 550–559, May 1988.
[21] M. Tatebayashi, N. Matsuzaki and J. D. B. Newman, "Key distribution protocol for digital mobile communication systems," in *Proc. Crypto '89*, pp. 324–334, 1989.

Min-Shiang Hwang received the B.S. degree in electronic engineering from National Taipei Institute of Technology, Taipei, Taiwan, China, in 1980, and the M.S. degree in industrial engineering from National Tsing Hua University, Taiwan, in 1988. He is currently pursuing the doctoral degree in computer and information science at National Chiao Tung University. He also studied applied mathematics at National Cheng Kung University, Tainan, from 1984–1986.

From to 1991, he was the leader of the computer center at Directorate General of Telecommunication Laboratories (TL), Ministry of Transportation and Communications. He was also a project leader for research in computer security at TL in July 1990. He research interests include cryptography, data security, mobile Communications, and network management.

Wei-Pang Yang (M'87–SM'90) was born on May 17, 1950, in Hualien, Taiwan, China. He received the B.S. degree in mathematics from National Taiwan Normal University, 1974, and the M.S. and Ph.D. degrees from the National Chaio Tung University, in 1979 and 1984, respectively, both in computer science.

Since August 1979, he has been on the faculty of the Department of Computer 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. From 1986 to 1987, he was the Director of the Computer Center of National Chiao Tung University. In August 1988, 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 Almaden Research Center, San Jose, CA, 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 systems.

Dr. Yang is a member of the ACM and Phi Tau Phi . He was the winner of the 1988 and 1992 Acer Long Term Award for Outstanding M.S. Thesis Supervision, and the winner of the 1990 Outstanding Paper Award of the Computer Society of China. In 1991–1993, he also obtained the Outstanding Research Award of National Science Council of China.