Security Enhancement on a New Authentication Scheme With Anonymity For Wireless Environments*

Cheng-Chi Lee[†§], *Non-member, IEEE*, Min-Shiang Hwang[‡], *Member, IEEE,* I-En Liao[†], *Member, IEEE*

Department of Management Information System[‡]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw

Department of Computer Science[†]
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.

Department of Computer & Communication Engineering[§]
Taichung Healthcare and Management University
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.

April 26, 2005

*Responsible for correspondence: Prof. Min-Shiang Hwang (Department of Management Information System, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C., Email: mshwang@nchu.edu.tw)

Security Enhancement on a New Authentication Scheme With Anonymity For Wireless Environments

Abstract

In a paper recently published in the IEEE Transaction on Consumer Electronics, Zhu and Ma proposed a new authentication scheme with anonymity for wireless environments. However, this paper shows that Zhu and Ma's scheme has some security weaknesses. Therefore, we propose a slight modification to their scheme to improve their shortcomings. As a result, our scheme can enhance the security of Zhu and Ma's scheme. Finally, the performance of our scheme is analyzed. Compare with the Zhu-Ma scheme, our scheme is also simple and efficient.

Keywords: Anonymity, authentication, security, wireless network.

1 Introduction

Wireless communications technologies have undergone rapid development. Small mobile devices within range of a wireless network can transfer data at any place and any time. 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 [5, 6, 9, 12, 13].

In recent years, many literatures had been written on privacy and authentication for wireless communications [1, 2, 3, 4, 5, 6, 7, 8]. A good security protocol for wireless communications must not only provide high security but also low computation. Recently, Zhu and Ma proposed a new authentication scheme with anonymity for wireless environments [14]. The scheme has some advantages as follows. The first is that it is based on the hash function and smart cards, and mobile users only do symmetric encryption and decryption.

The second is that it takes only one round of message exchange between the mobile user and the visited network, and one round of messages exchange between the visited network and the corresponding home network. The third is that one-time use of key between mobile user and visited network is used. However, the Zhu-Ma scheme has three security weaknesses as follows:

1. It cannot achieve perfect backward secrecy.
2. It cannot achieve mutual authentication.
3. It cannot protect against a forgery attack.

We shall point out these shortcomings more clearly later.

In next section, we shall point out that the Zhu-Ma scheme is not strong enough against the above security weaknesses. Hence, we propose a slight modification of the Zhu-Ma scheme. The proposed scheme does not only achieve their advantages but also enhances their security by withstanding the security weaknesses. In addition, the efficiency of our scheme is even higher than that of the original Zhu-Ma scheme. Compare with Zhu-Ma scheme, our scheme is also simple and efficient.

This paper is organized as follows. In Section 2, we shall analyze Zhu-Ma scheme to show its weaknesses. Then, we shall propose a slightly modified version of their scheme to enhance the security in Section 3. Next, we shall analyze the improved scheme in Section 4. Finally, the conclusion will be in Section 5.

2 The Weaknesses of Zhu-Ma Scheme

Zhu and Ma proposed a simple and efficient authentication scheme with anonymity for wireless environment [14]. In Table 1, we list the abbreviations and notations used in their scheme. Their scheme can be divided into three phases: initial phase, first phase, and second phase. In the initial phase, HA delivers a password and a smart card for the mobile user through a secure channel. In the first phase, FA authenticates to MN and establishes a session key. In the second phase, MN visits FA and FA serves for MN. The detailed phases are shown in the following.

Table 1: Notations

HA	Home Agent of a mobile user
FA	Foreign Agent of the network
MN	Mobile User
PW_{MN}	A password of MN
ID_A	Identity of en entity A
T_A	Timestamp generated by an entity A
$Cert_A$	Certificate of an entity A
$(X)_K$	Encryption of a message X using a symmetric key K
$E_K(X)$	Encryption of a message X using an asymmetric key K
$h(X)$	A one-way hash function
p	A large prime
q	A large prime such $q \vert p-1$
$g \in Z_p^*$	An element of Z_p^* of order q
$\Vert$	Concatenation
$\oplus$	XOR operation

2.1 The Initial Phase

When a new mobile user MN wants to register at his/her HA, he/she submits his/her identity ID_{MN} to the HA. Then, HA delivers PW_{MN} and a smart card, which contains ID_{HA}, r, and $h(\cdot)$, for the user through a secure channel. The PW_{MN} and r are calculated as follows:

$$\begin{aligned} PW_{MN} &= h(N||ID_{MN}), \quad \text{and} \\ r &= h(N||ID_{HA}) \oplus h(N||ID_{MN}) \oplus ID_{HA} \oplus ID_{MN}, \end{aligned}$$

where N is a long random number kept secretly by the HA.

2.2 The First Phase

In this phase, FA authenticates MN and issues a temporary certificate to MN, which will be used in the second phase when MN always communicates this FA within this area. The statement $\{A \rightarrow B : messages\}$ denotes that the messages are transmitted from A to B. The steps of this phase are shown as follows:

Step 1: $MN \rightarrow FA : n, (x_0)_L, ID_{HA}, T_{MN}$

MN computes $n = r \oplus PW_{MN}$ and his/her temporary key $L = h(T_{MN} \oplus PW_{MN})$, and then encrypts x_0 with L using symmetric encrypt algorithm, where x_0 is a secret random number.

Step 2: $FA \rightarrow HA : b, n, (x_0)_L, T_{MN}, E_{KR_{FA}}(h(b, n, (x_0)_L, T_{MN}, Cert_{FA}))$, $Cert_{FA}$, T_{FA}

Upon receiving messages from MN, FA checks if the timestamp T_{MN} is valid. If it is valid, FA generates a secret random number b, and then computes its signature using his/her private key KR_{FA}.

Step 3: $HA \rightarrow FA : c, E_{KU_{FA}}(h(ID_{MN})||x_0)$, $E_{KR_{HA}}(h(b, c, E_{KU_{FA}}(h(ID_{MN})$ $||x_0)$, $Cert_{HA}))$, $Cert_{HA}$, T_{HA}

Upon receiving messages from FA, HA checks if the certificate $Cert_{FA}$ and timestamp T_{FA} are valid. If they are valid, HA computes the MN's real identity, $h(N||ID_{HA}) \oplus n \oplus ID_{HA} = ID_{MN}$. Then, verify if the MN is a legal user. If it is, HA computes $L = h(T_{MN} \oplus h(N||ID_{MN}))$ and decrypts x_0. Then, HA generates a secret random number c. Next, HA encrypts $(h(ID_{MN})||x_0)$ with the public key of FA KU_{FA} and computes its signature using his/her private key KR_{HA}.

Step 4: $FA \rightarrow MN : (TCert_{MN})_k$

Upon receiving messages from HA, FA checks if the certificate $Cert_{HA}$ and timestamp T_{HA} are valid. If they are valid, FA issues to MN the temporary certificate $TCert_{MN}$, which includes lifetime and other information. Then, FA encrypts it with the session key k using a symmetric encryption algorithm, where $k = h(ID_{MN}) \oplus x_0$.

Afterward, MN can compute k and derive $TCert_{MN}$.

2.3 The Second Phase

In this phase, MN visits FA at ith session when he/she is always within this FA. The process is as follows.

$MN \rightarrow FA$**:** $TCert_{MN}, (x_i||TCert_{MN}||OtherInformation)_{k_i}$

MN encrypts $(x_i||TCert_{MN}||OtherInformation)$ with ith session key k_i, where $k_i = h(ID_{MN}) \oplus x_{i-1}$, for $i = 1, 2, \cdots, n$. Upon receiving messages from MN, FA checks if the certificate $TCert_{MN}$ is valid. If it is, FA decrypts $(x_i||TCert_{MN}||OtherInformation)$ with k_i. Then, compare the two $TCert_{MN}$ and verify the integrity of the messages. If it holds, FA saves x_i for the next communication.

2.4 The Security Weaknesses

Zhu and Ma proposed a simple and efficient authentication scheme which is based on the public key cryptosystems, but mobile users only do symmetric encryption and decryption. The most significant feature is one-time use of key between mobile user and visited network. However, there still remain three weaknesses in their scheme as explained in the following:

1. *It cannot achieve perfect backward secrecy.*

   The backward secrecy is defined as the assurance that session keys will not be compromised if one of the future session keys known to an attacker [10, 11]. In Zhu-Ma scheme, we can see that if the session key k_i is known to an attacker, he/she can derive x_i in the second phase. Because the attacker can intercept $(x_i||TCert_{MN}||OtherInformation)_{k_i}$, he/she can decrypt x_i using the knowing session key k_i. Then, the attacker can compute the future session keys from $k_i = h(ID_{MN}) \oplus x_{i-1}, i = 1, 2, \cdots, n$. Therefore, it cannot achieve perfect backward secrecy.

2. *It cannot achieve mutual authentication.*

   In the first phase of Zhu-Ma scheme, FA can authenticate MN and issues a temporary certificate to MN. However, MN cannot authenticate FA in this phase. It cannot provide the security requirement mutual authentication. An attacker can intercept $(TCert_{MN})_k$ in the first phase. Then, he/she can modify it to $(TCert'_{MN})_{k'}$, where k' and $(TCert'_{MN})$ are random numbers chosen by the attacker. Therefore, MN will receive a wrong temporary certificate because MN does not authenticate FA.

3. *It cannot protect against a forgery attack.*

   In the first phase of Zhu-Ma scheme, an attacker can intercept (n, $(x_0)_L$, ID_{HA}, T_{MN}). He/she modifies it to $(n, (x'_0)_{L'}, ID_{HA}, T'_{MN})$, where x'_0 and L' are random numbers chosen by the attacker, and T'_{MN} is a new timestamp generated by the attacker. The attacker can forge the MN to cheat the HA, because HA can derive the ID_{MN} and then pass authentication. Therefore, it cannot protect against a forgery attack.

In concluding the above three weaknesses of Zhu and Ma's scheme, we improve their scheme to suit mobile devices. Based on their scheme, our improved scheme is also a simple and efficient authentication scheme with anonymity for wireless environment. In the following section, we will explain our improved scheme.

3 The Improved Scheme

In this phase, we improve the Zhu and Ma's scheme to remedy their security weaknesses. Our improved scheme not only inherits the advantages of their scheme but also enhances the security of their scheme. The improved scheme can achieve perfect backward secrecy, achieve mutual authentication, and protect against a forgery attack. It is also divided into three phases: initial phase, first phase, and second phase. In the initial phase, HA delivers a password and a smart card for the mobile user through a secure channel. In the first phase, FA authenticates to MN and establishes a session key. In the second phase, MN visits FA and FA serves for MN. The initial phase is the same as the Zhu and Ma's scheme. Here, we also use the same abbreviations and notations in Table 1 and the statement $\{A \rightarrow B : messages\}$ denotes that the messages are transmitted from A to B. The improved first phase and second phase are shown in the following.

3.1 The Improved First Phase

In this phase, FA authenticates MN and issues a temporary certificate to MN, which will be used in the second phase when MN always communicates this FA within this area. The steps of this phase are shown in Figure 1 and as follows:

Step 1: $MN \rightarrow FA : n, (h(ID_{MN})||x_0||x)_L, ID_{HA}, T_{MN}$

MN computes $n = r \oplus PW_{MN}$ and his/her temporary key $L = h(T_{MN} \oplus PW_{MN})$, and then encrypts $(h(ID_{MN})||x_0||x)$ with L using symmetric encrypt algorithm, where x_0 and x are secret random numbers.

Step 2: $FA \rightarrow HA : b, n, (h(ID_{MN})||x_0||x)_L, T_{MN}, E_{KR_{FA}}(h(b, n, (h(ID_{MN}) ||x_0 ||x)_L, T_{MN}, Cert_{FA})), Cert_{FA}, T_{FA}$

Upon receiving messages from MN, FA checks if the timestamp T_{MN} is valid. If it is valid, FA generates a secret random number b, and then computes its signature using his/her private key KR_{FA}.

Step 3: $HA \rightarrow FA : c, E_{KU_{FA}}(h(ID_{MN})||x_0||x), E_{KR_{HA}}(h(b, c, E_{KU_{FA}}(h(ID_{MN}) ||x_0 ||x), Cert_{HA})), Cert_{HA}, T_{HA}$

Upon receiving messages from FA, HA checks if the certificate $Cert_{FA}$ and timestamp T_{FA} are valid. If they are valid, HA computes the MN's real identity, $h(N||ID_{HA}) \oplus n \oplus ID_{HA} = ID_{MN}$ and $h(ID_{MN})$. Then, HA computes $L = h(T_{MN} \oplus h(N||ID_{MN}))$ and decrypts $(h(ID_{MN})||x_0||x)$. Then, verify if the MN's identity is a legal user and compare if the two $h(ID_{MN})$ are equal to verify the integrity of ID_{MN}. If they hold, HA generates a secret random number c. Next, HA encrypts $(h(ID_{MN})||x_0||x)$ with the public key of FA KU_{FA} and computes its signature using his/her private key KR_{HA}.

Step 4: $FA \rightarrow MN : (TCert_{MN}||h(x_0||x))_k$

Upon receiving messages from HA, FA checks if the certificate $Cert_{HA}$ and timestamp T_{HA} are valid. If they are valid, FA issues to MN the temporary certificate $TCert_{MN}$, which includes lifetime and other information. FA decrypts $(h(ID_{MN})||x_0||x)$ with the private key of FA KR_{FA} and computes $h(x_0||x)$. Then, FA encrypts $(TCert_{MN}||h(x_0||x))$ with the session key k using a symmetric encryption algorithm, where $k = h(ID_{MN}||x) \oplus x_0$.

Afterward, MN can compute k and derive $TCert_{MN}$. Additionally, MN can authenticate to FA. He/she can compute $h(x_0||x)$ and compare it with the received $h(x_0||x)$. If it holds, it confirms that FA is authenticated by HA. Therefore, MN can make sure that it is communicating with a legitimate FA.

3.2 The Improved Second Phase

In this phase, MN visits FA at ith session when he/she is always within this FA. The process is as follows.

$MN \rightarrow FA : TCert_{MN}, (x_i||TCert_{MN}||OtherInformation)_{k_i}$

MN encrypts $(x_i||TCert_{MN}||OtherInformation)$ with ith session key

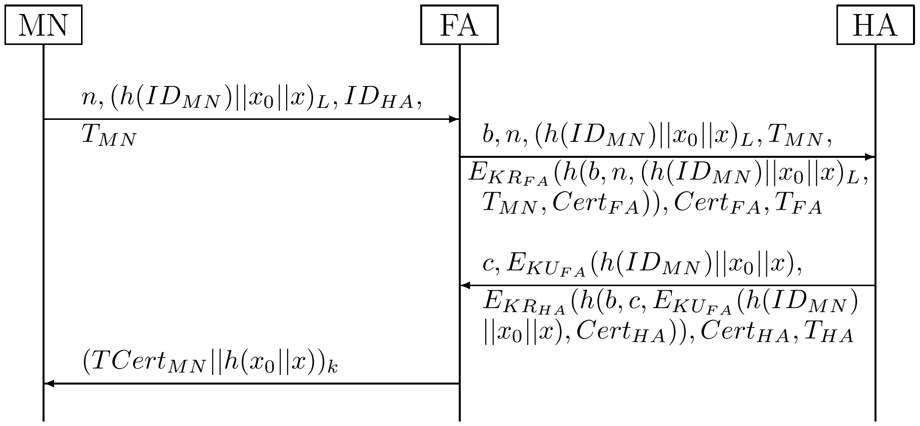

Figure 1: The protocol of the improved first phase

k_i, where $k_i = h(ID_{MN}||x) \oplus x_{i-1}$, for $i = 1, 2, \cdots, n$. Upon receiving messages from MN, FA checks if the certificate $TCert_{MN}$ is valid. If it is, FA decrypts $(x_i||TCert_{MN}||OtherInformation)$ with k_i. Then, compare the two $TCert_{MN}$ and verify the integrity of the messages. If it holds, FA saves x_i for the next communication.

4 Analysis

Our scheme is a slight modification of the Zhu-Ma scheme. The security and efficiency of the Zhu-Ma scheme have already been discussed and demonstrated in [14]. In this section, we shall only discuss the difference between their scheme and ours.

4.1 Security Analysis

The proposed scheme can overcome the security weaknesses that the Zhu-Ma scheme falls for. The advantages of the proposed scheme are explained as follows:

- *It can achieve perfect backward secrecy.*

  In our scheme, we can see that if the session key k_i is known to an attacker, he/she can derive x_i in the second phase. Because the attacker can intercept $(x_i||TCert_{MN}||OtherInformation)_{k_i}$, he/she can decrypt x_i using the knowing session key k_i. However, the attacker cannot compute the future session keys from $k_i = h(ID_{MN}||x) \oplus x_{i-1}, i = 1, 2, \cdots, n$, because the attacker does not know x. Therefore, it can achieve perfect backward secrecy.

- *It can achieve mutual authentication.*

  In improved first phase of our scheme, FA can authenticate MN and issues a temporary certificate to MN. Additionally, MN can authenticate to FA. He/she can compute $h(x_0||x)$ and compare it with the received $h(x_0||x)$. If it holds, it confirms that FA is authenticated by HA. Therefore, it can achieve mutual authentication.

- *It can protect against a forgery attack.*

  In improved first phase of our scheme, an attacker can intercept (n, $(h(ID_{MN})||x_0||x)_L$, ID_{HA}, T_{MN}). He/she modifies it to (n, $(h(ID_{MN})' ||x_0' ||x')_{L'}$, ID_{HA}, T'_{MN}), where $h(ID_{MN})'$, x_0', x', and L' are random numbers chosen by the attacker, and T'_{MN} is a new timestamp generated by the attacker. The attacker cannot forge the MN to cheat the HA, because HA can compare if the two $h(ID_{MN})$ are equal to verify the integrity of ID_{MN}. Therefore, it can protect against a forgery attack.

4.2 Efficiency Analysis

We compare our scheme with the Zhu-Ma scheme in terms of communication and computation cost. In communication cost, our scheme is the same as their scheme. It takes only one round of message exchange between the mobile user and the visited network, and one round of messages exchange between the visited network and the corresponding home network.

In computation cost, we consider a computational load on user part of the proposed scheme and Zhu-Ma scheme. Table 2 shows our scheme and Zhu-Ma scheme in computation cost. We can see that the number of hash operation is just increased one in our scheme. Our scheme is not only simple and efficient but also enhances their security.

Table 2: The computational costs at user

	Zhu-Ma Scheme	Our Scheme
Hash Operations	2	3
Symmetric Encryptions/Decryptions	3	3
XOR Operations	3	3

5 Conclusions

In this paper, we have pointed out that the Zhu-Ma scheme is not strong enough against some security weaknesses. Therefore, we have proposed a slight modification of the Zhu-Ma scheme. The proposed scheme does not only achieve their advantages but also enhances their security by withstanding the security weaknesses. In addition, the efficiency of our scheme is even higher than that of the original Zhu-Ma scheme.

References

[1] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," *IEEE Personal Communications*, vol. 1, no. 1, pp. 24–31, 1994.

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

[3] Chin-Chen Chang, Kuo-Lun Chen, and Min-Shiang Hwang, "End-to-end security protocol for mobile communications with end-user identification/authentication," *Wireless Personal Communications*, vol. 28, no. 2, pp. 95–106, 2004.

[4] Min-Shiang Hwang, Cheng-Chi Lee, and Wei-Pang Yang, "An improvement of mobile users authentication in the integration environments," *International Journal of Electronics and Communications*, vol. 56, no. 5, pp. 293–297, 2002.

[5] Min-Shiang Hwang and Chii-Hwa Lee, "Authenticated key-exchange in a mobile radio network," *European Transactions on Telecommunications*, vol. 8, no. 3, pp. 265–269, 1997.

[6] Min-Shiang Hwang and Wei-Pang Yang, "Conference key distribution protocols for digital mobile communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 2, pp. 416–420, 1995.

[7] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang, "Extension of authentication protocol for GSM," *IEE Proceedings - Communications*, vol. 150, no. 2, pp. 91–95, 2003.

[8] Cheng-Chi Lee, Chou-Chen Yang, and Min-Shiang Hwang, "A new privacy and authentication protocol for end-to-end mobile users," *International Journal of Communication Systems*, vol. 16, no. 9, pp. 799–808, 2003.

[9] Chii-Hwa Lee, Min-Shiang Hwang, and Wei-Pang Yang, "Enhanced privacy and authentication for the global system of mobile communications," *Wireless Networks*, vol. 5, pp. 231–243, July 1999.

[10] M. Peyravian, A. Roginsky, and N. Zunic, "Hash-based encryption system," *Computers & Security*, vol. 18, no. 4, pp. 345–350, 1999.

[11] Roberto D. Pietro, Luigi V. Mancini, and Sushil Jajodia, "Providing secrecy in key management protocols for large wireless sensors networks," *Ad Hoc Networks*, vol. 1, no. 4, pp. 455–468, 2003.

[12] Ching-Wen Chen, and Ming-Chin Chuang, Chwei-Shyong Tsai, "An Efficient Authentication Scheme Between MANET and WLAN Based on Mobile IPv6," *International Journal of Network Security*, vol. 1, no. 1, pp. 12–19, 2005.

[13] Cheng-Ying Yang, Cheng-Chi Lee, and Shu-Yin Hsiao, "Man-in-the-middle attack on the authentication of the user from the remote autonomous object," *International Journal of Network Security*, vol. 1, no. 1, pp. 22–24, 2005.

[14] Jianming Zhu and Jianfeng Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 50, Feb. 2004.

BIOGRAPHY

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 researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He is currently pursuing his Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, Republic of China. He is a Lecturer of Computer and Communication, Taichung Healthcare and Management University (THMU), from 2004. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 25 articles on the above research fields in international journals.

Min-Shiang Hwang was born on August 27, 1960 in Tainan, Taiwan, Republic of China (ROC.). He received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, 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 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 Outstanding Research Award of National Science Council of the Republic of China. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. 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 had published over 100 articles on the above research fields in international journals.

I-En Liao received the BS degree in Applied Mathematics from National Cheng-Chi University, Taiwan, in 1978, and both the MS degree in Mathematics and the PhD degree in Computer and Information Science from the Ohio State University in 1983 and 1990, respectively. He is currently an associate professor in the Department of Computer Science of National Chung-Hsing University, Taiwan. His research interests are in database tuning, data mining, XML database, and bioinformatics. He is a member of the ACM and the IEEE Computer Society.