A Publicly Verifiable Authenticated Encryption Scheme Based on Factoring and Discrete Logarithms

Cheng-Yi Tsai[1], Chi-Yu Liu[1], Shyh-Chang Tsaur[2,3], and Min-Shiang Hwang[1,4]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung 41354, Taiwan
Department of Electronic Engineering, National Chin-Yi University of Technology[2]
No.57, Sec. 2, Zhongshan Rd., Taiping Dist., Taichung 41170, Taiwan
Department of Business Administration, Tunhai University[3]
No.1727, Sec.4, Taiwan Boulevard, Xitun District, Taichung 40704, Taiwan
Department of Medical Research, China Medical University Hospital, China Medical University[4]
No.91, Hsueh-Shih Road, Taichung 40402, Taiwan
(Email: mshwang@asia.edu.tw)
(Received May 12, 2016; revised and accepted July 21 & Aug. 4, 2016)

Abstract

In this article, we propose a publicly verifiable authenticated encryption scheme based on factoring and discrete logarithms. We point out that even if either factoring or discrete logarithms is broken, this scheme still could keep the authentication, integration, and confidentiality of the message.

Keywords: Authenticated encryption scheme, discrete logarithm problem, factoring problem

1 Introduction

Traditionally, we use a hand-written signature to manifest the validity of a document and the identity of a signer. In the wake of development network, the information could be easily transmitted through the network in the form of electronic types. According to the requirements of secure data, senders must provide a secure protocol in the environment. The signer could use his/her secret key to generate a signature for the given message, and the verifier then uses the signer's public key to verify the authentication function of a paper [10, 26, 31]. Most previously proposed digital signature schemes were based on the well-known public key systems such as RSA [1, 5, 12, 32, 34] system or ElGamal system [7, 9, 21, 30, 38]. According to those public key systems, the sender not only encrypts the documents which are taken in electronic form but protects the content security of the documents as well.

Although the original digital signature could verify the creator identity of a document, it is not enough in some special applications [20, 29, 36]. When a sender wants to securely transmit data to a particular receiver, he/she must ensure that nobody but the particular receiver could authenticate the signature [2, 25, 28]. For example, in the movie "mission impossible", when the government assigns a task to Tom Cruise, only he could know the message of the task. Since the third party is unable to know the content of the message, the third party could not authenticate the task sent from government. According to the requirements of the special application, we could get the criterion of the authenticated encryption scheme, so signing signature and protecting the security of a document could be made at the same time [16, 18]. We can infer that an authenticated encryption scheme corresponds with the following properties [3, 17, 37]:

Confidentiality. It must ensure that the secret information can only be obtained, by the sender and the receiver, but not anyone else.

Authentication. It must ensure the sender and the receivers' identities, and avoid the adversary to send a malicious message.

Non-repudiation. It must confirm the sender's identity, and the sender could not repudiate his signature and message.

All of the above are the basic requirements of the authenticated encryption scheme (AES for short). If the proposed scheme satisfies those characteristics, it will be called an authenticated encryption scheme.

Nyberg and Rueppel [27] proposed a signature with message recovery based on the discrete logarithm problem. In this scheme, there are some advantages with which the application without a hash function is possible to be achieved, such as a smaller bandwith for signatures of small messages, and direct use in other schemes like identity-based public key systems or key agreement protocols. Recently, Horster, Michels, and Petersen [14] (HMPs for short) proposed an authenticated encryption scheme based on a message recovery method which is the modification of Nyberg-Rupple's scheme [27]. In their scheme, a sender does not have to transmit a message to the receiver. Then, the receiver not only could verify the message authentication and the message integrity, but he/she could also get the original message from the information that he/she has received. Although HMPs provided the confidentiality, this scheme was not secure in use because it suffered from "known ciphertext-plaintext attack". Li and Chang proposed an improved scheme [24]. Then Wu and Hsu [15] pointed out Li and Chang's scheme [24] was not perfect when a dispute occurred, so they proposed a scheme to make up for the disadvantage. Next, Ma and Chen [4] proposed a new application in AES. Their scheme could provide the third party to verify the signature without knowing a plaintext, except the sender and the receiver. Many schemes have been proposed to achieve the properties of authenticated encryption schemes [8, 22, 35].

We have described that if someone wants to sign or encrypt a message, he/she will often use public key systems. The security of RSA system is constructed in factorization, and ElGamal system is built on solving the discrete logarithm problem. In general, to verify a signature or to decrypt an encrypted message which is based on factoring or discrete logarithms is not easy to achieve. However, it is optimistic to improve the computation capability of a computer. Nobody could ensure the perpetual security of a cryptography algorithm which is based on either the factoring or the discrete logarithm problem in the future. Therefore, He first proposed a signature scheme which is based on both factoring and discrete logarithm problems. The proposed scheme could improve the degree of the security and ensure the feasibility of the algorithm.

In 1976, Diffie-Hellman [6] presented a concept of public-key cryptography. Since then, the security of each public-key cryptosystem has been based on just one cryptographic assumption, either factoring or discrete logarithms. However, it is possible that efficient algorithms will be developed in the future to break one or more of these assumptions.

Harn [11] first proposed a new public-key cryptosystem based on factoring and discrete logarithms. Unfortunately, Shao [33] showed that Harn's scheme would be subject to substitution attacks without using any hash function. Then Shao proposed an improved scheme to resist such a substitution attack on the condition that the factoring problem would not be broken. However, Lee [23] showed that Shaos' [33] improved scheme is still insecure. When the factoring problem is broken, the adversary will obtain signer's secret key from a known signature. He [13] pointed out a common disadvantage of those schemes that have been proposed. Every user has his or her key pair and arithmetic module, so there exists the key management problem for those schemes. Then his scheme aimed at this disadvantage. Lastly, Hwang et al. [19] proposed an improved scheme for his scheme.

We base on the proposed scheme of Hwang et al., and propose a new authenticated encryption scheme based on FAC and DL. In this article, we present a scheme that could satisfy properties of authenticated encryption schemes based on factoring and discrete logarithms. In addition, the third party could verify the signature without divulging the receiver's private key.

Thus, the proposed authenticated encryption schemes are either based on factoring difficulty or discrete logarithm difficulty. According to the essence of He's scheme, we propose a new AES based on FAC and DL, which correspond to the characteristics of the traditional AES based on FAC or DL, and is securer than others. In this article, the third party could verify the signature without divulging the receiver's private key. In Section one, a brief development of AES and signature based on FA and DL is discussed. In Section two, we describe the main scheme. Then we point out in Section three some possible attacks and show that this scheme could avoid these attacks. Finally, we make a conclusion for this article.

2 The Proposed Scheme

In this section, we propose a new scheme could not only achieve authentication and encryption functions, but could increase security by solving two difficulties of factoring and discrete logarithms as well. This scheme could be divided into three phases. In the initialization phase, related system parameters should be defined. In the encryption and signature generation phase, the signer could create a signature with message recovery to a special recipient. In signature verification and message recovery phase, the special recipient will verify the correctness and integrity of the message, and recover the message. To prevent certain dispute later, the designated recipient may convert the encryption into an ordinary signature.

Initialization Phase.

In this phase, the trusted center of the system selects the following parameters:

- p_1, p_2, q_1, q_2: Four large primes where $p_1 = 2p_2 + 1$ and $q_1 = 2q_2 + 1$;
- P: A large prime where $P = 4p_1q_1 + 1$;
- R: $R = p_1q_1$;
- g: A generator of order p_1p_2 over $GF(P)$.

P, R, and g are published, and p_1, p_2, q_1, q_2 are all discarded. Then each user selects his/her private

key X_i in Z_R where $gcd(X_i^2, R) = 1$, and computes his/her public key y_i where $y_i = g^{X_i^2} \bmod P$.

Encryption and Signature Generation Phase.

If a sender wants to transmit a secure message, he/her should perform the following protocol to generate a ciphertext and a signature for a message m.

Step 1. He/she should randomly select an integer K in Z_R such that $\gcd(K^2, R) = 1$, and compute

$$\begin{aligned} r_1 &= g^{K^2} \bmod P \\ r_2 &= g^{K^{-2}} \bmod P. \end{aligned}$$

Step 2. And he/she could encrypt the message m to find a ciphertext C such that

$$C = mH(y_B^{K^2} \bmod P)^{-1} \bmod P,$$

where H is a one-way function.

Step 3. He/she signs the message m in order to convince the verifier of the validity of the original message. And then he/she performs the following equations:

$$X_A = SK + H(r_1, r_2, m)K^{-1} \bmod R.$$

The pairs (r_1, r_2, S) is a signature of the message m. Then the sender delivers (r_1, r_2, S, C) to the receiver.

Signature Verification and Message Recovery Phase.

When the receiver obtains those four messages, he could perform the following equation to recover the message m from the ciphertext C, $m' = CH(r_1^{X_B^2} \bmod P) \bmod P$. The receiver will check the format of the message m', and then he could decide whether to accept it or not. After recovering the message, he must check the validity and the correctness of the signature. He could use the following equation to verify the signature:

$$y_A = r_1^{S^2} r_2^{H^2(r_1, r_2, m)} g^{2SH(r_1, r_2, m)} \bmod P.$$

If the signature are valid, then the receiver could make the conclusion that the information is correct.

In case of dispute, the special recipient must reveal the content of the message m with (r_1, r_2, S, m) and send it to the third party. When the third party receives those information, he/she will verify the legality and the correctness with the following equation:

$$y_A = r_1^{S^2} r_2^{H^2(r_1, r_2, m)} g^{2SH(r_1, r_2, m)} \bmod P.$$

If the equation equals, the sender is not able to disclaim that he has sent the message m to the special recipient.

All the explanation above introduces our scheme that is based on factoring and discrete logarithms. We can easily find that our scheme is more secure and could achieve the purpose of authenticated encryption.

3 Security Analysis and Performance Analysis

In this section, we will present some securities of the proposed scheme. Then we will present the performance analysis of our proposed scheme.

3.1 Security Analysis

The following attack analysis methods are all general attack assumptions, and we will present other possible problems that may occur in the future. First, we assume that the well-known public key system based on discrete logarithm problems has been broken and shows whether our proposed scheme could resist those crunches or not. Next, we will assume that the cryptosystem security is based on factoring problems, and prove that our scheme could still resist the crisis.

Attack 1. The receiver wants to forge the sender's signature (r_1, r_2, S, C).

If a receiver wants to forge the sender's identity to sign a message m' which is chosen by him, he must know the sender's private key X_A. He could randomly chose a number K', and compute the ciphertext C' and the signature (r_1', r_2, S') of the message m'. However, he could not find the signature S', because he does not know the sender's private key X_A. And thus, he could not forge the sender's identity to generate a signature.

Attack 2. An intruder tries to obtain the private key X_i from a user $U_i's$ signature.

In our scheme, if the intruder wants to obtain user A's secret key X_i from the user's signature, he must solve the equation $X_A = SK + H(r_1, r_2, m)K^{-1} \bmod R$, even though he could know the public hash functions $H(.), R$, and the four values (r_1, r_2, S, C) which is transmitted through the network. He should know the secret random number K which is the same as each signature process and message m.

First, the intruder should find a message m' and compute the hash value which is equal to the original hash value such as $H(r_1, r_2, m') = H(r_1, r_2, m')$. Nerveless, he will face the difficulty of finding a hash value; a hash function is computationally infeasible to find any second input which has the same output as any specified input, i.e., given x, to find a $x' \neq x$ such that $h(x) \equiv h(x')$. At the same time, he could infer that the random number K' is same as K, and he could only obtain the sender's private key X_i.

Attack 3. An opponent tries to impersonate the signer to generate a valid signature of a message m'.

If an opponent wants to forge a valid signer's signature for a random message m', he could fix r_1, r_2 and computes a fake S' to pass the verification process. If he wants to find a legal S', he will confront

discrete logarithm problems. Because he must know the correct value K, he should compute the K from the $r_1 = g^{K^2} \bmod P$. Second, he could fix S which is obtained from the transmitted process and finds the corresponded r_1, and r_2. However, he must know the correct message m. Otherwise, he could find a hash value $H(r_1, r_2, m')$ which is same as $H(r_1, r_2, m)$.

Attack 4. An adversary without the special receiver B's private key X_B tries to decrypt the ciphertext C.

If an adversary wants to know the message m, he should get the receiver's private key X_B to decrypt the ciphertext C. Also, he could solve the discrete logarithm problems, and obtain the value K^2. However, the difficulty is not easy to be solved. The reason is just as those described above.

Attack 5. Suppose that either the difficulty of computing discrete logarithm problem or the factoring problem has been broken.

Given the ciphertext C, the adversary attempts to find the solution of three variables r_1, r_2, and S that satisfies the equation $y_A = r_1^{S^2} r_2^{H^2(r_1,r_2,m)} g^{2SH(r_1,r_2,m)} \bmod P$. He first fixes two variables and finds the solution of the other variable from the verification equation. Besides, given y_A, g, C, r_1, and r_2, finding S to satisfy verification equation is under the factoring and discrete logarithm assumptions. In another similar approach, those are under the factoring, the discrete logarithm, and hash function assumptions.

3.2 Performance Analysis

In this subsection, we will focus on the performance of our scheme and to analyze the efficiency. For convenience, we first define some notations to denote the performance time: T_{mul} is the time for multiplication; T_h is the time for executing hash function; T_{exp} is the time for exponentiation with modulo P; and T_{inv} is the time for inversion modulo P. We only consider those heavy computational cost of T_h, T_{exp}, T_{mul}, and T_{inv}.

And then we could dispute the computational cost over two phases, signature and ciphertext generation phase, and message recovery and verification phase. In the signature and ciphertext generation phase, the sender will perform $3T_{exp}, 2T_{inv}, 2T_h, 2T_{mul}$ to achieve the processes of this phase. In the message recovery and verification phase, the verifier should perform $4T_{exp}, 1T_h, 4T_{mul}$ to complete the processes of this phase. In the dispute phase, we will not take into consideration the computational cost.

4 Conclusions

Our proposed scheme is based on Nyberg and Rueppel's scheme [27] and Hwang et al. [19] proposed scheme. Nyberg and Rueppel's method could be applied to small message transmissions such as ID-based systems or key agreement systems. The other one, Hwang et al.'s scheme, could provide good security based on factoring and discrete logarithm assumptions. We extend both schemes to construct our algorithm. The proposed scheme is a publicly verifiable authenticated encryption scheme based on factoring and discrete logarithms. This scheme could ensure the security and authentication of the message by solving two difficult problems.

In the future, some subjects, especially the mobile environment, are worth considering in applications. In a mobile environment, short response time and efficient computation are very important. When a user requests a service to a provider with a payment way, he will considerably care about the transmitted time and cost. Since it costs quite much for the computation of authentication encryption schemes, more efforts should be made to improve the efficiency.

References

[1] C. C. Chang and M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365–1366, 1996.

[2] C. C. Chang, C. Y. Sun, and S. C. Chang, "A strong RSA-based and certificateless-based signature scheme," *International Journal of Network Security*, vol. 18, no. 2, pp. 201–208, 2016.

[3] T. Y. Chang, C. C. Yang, and M. S. Hwang, "Cryptanalysis of publicly verifiable authenticated encryption," *IEICE Transactions on Foundations*, vol. E87-A, no. 6, pp. 1645–1646, 2004.

[4] M. Changshe and C. Kefei, "Publicly verifiable authenticated encryption," *Electronics Letters*, vol. 39, no. 3, pp. 281–282, 2003.

[5] L. Deng, H. Huang, and Y. Qu, "Identity based proxy signature from RSA without pairings," *International Journal of Network Security*, vol. 19, no. 2, pp. 229–235, 2017.

[6] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[7] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 220–222, July 1985.

[8] L. H. Encinas, A. M. del Rey, and J. M. Masqué, "A weakness in authenticated encryption schemes based on tseng et al.'s schemes," *International Journal of Network Security*, vol. 7, no. 2, pp. 157–159, 2008.

[9] O. B. Fredj, "An automatic alert unification method for heterogeneous alert signatures," *International Journal of Network Security*, vol. 18, no. 6, pp. 1180–1191, 2016.

[10] Y. Gao, P. Zeng, K. K. R. Choo, F. Song, "An improved online/offline identity-based signature scheme

for WSNs," *International Journal of Network Security*, vol. 18, no. 6, pp. 1143–1151, 2016.

[11] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms," *IEE Proceedings - Computers and Digital Techniques*, vol. 141, no. 3, pp. 193–195, 1994.

[12] D. He, M. K. Khan, and S. Wu, "On the security of a RSA-based certificateless signature scheme," *International Journal of Network Security*, vol. 16, no. 1, pp. 78–80, 2014.

[13] W. H. He, "Digital signature scheme based on factoring and discrete logarithms," *Electronics Letters*, vol. 37, no. 4, pp. 220–222, 2001.

[14] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," *Electronics Letters*, vol. 30, no. 15, pp. 1212–1213, 1994.

[15] C. L. Hsu and T. C. Wu, "Authenticated encryption scheme with *(t, n)* shared verification," *IEE Proceedings - Computers and Digital Techniques*, vol. 145, no. 2, pp. 117–120, 1998.

[16] H. F. Huang, P. H. Lin, and M. H. Tsai, "Convertible Multi-authenticated Encryption Scheme for Data Communication," *International Journal of Network Security*, vol. 17, no. 1, pp. 40–48, 2015.

[17] M. S. Hwang and C. Y. Liu, "Authenticated encryption schemes: Current status and key issues," *International Journal of Network Security*, vol. 1, no. 2, pp. 61–73, 2005.

[18] M. S. Hwang, J. W. Lo, and S. Y. Hsiao, "Improvement of authenticated encryption schemes with message linkages for message flows," *IEICE Transactions on Information and Systems*, vol. E89-D, no. 4, pp. 1575–1577, 2006.

[19] M. S. Hwang, C. C. Yang, and S. F. Tzeng, "Improved digital signature scheme based on factoring and discrete logarithms," *Discrete Mathematical Sciences & Cryptography*, vol. 5, no. 2, pp. 151–155, 2002.

[20] J. Kar, "Provably secure online/off-line identity-based signature scheme for wireless sensor network," *International Journal of Network Security*, vol. 16, no. 1, pp. 29–39, 2014.

[21] A. V. N. Krishna, A. H. Narayana, K. M. Vani, "Window method based cubic spline curve public key cryptography," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 94–102, 2016.

[22] C. C. Lee, M. S. Hwang, and S. F. Tzeng, "A new convertible authenticated encryption scheme based on the elgamal cryptosystem," *International Journal of Foundations of Computer Science*, vol. 20, no. 2, pp. 351–359, 2009.

[23] N. Y. Lee, "Security of shao's signature schemes based on factoring and discrete logarithms," *IEE Proceedings - Computers and Digital Techniques*, vol. 146, no. 2, pp. 119–121, 1999.

[24] W. B. Lee and C. C. Chang, "Authenticated encryption scheme without using a one way function," *Electronics Letters*, vol. 31, no. 19, pp. 1656–1657, 1995.

[25] C. Y. Liu, C. C. Lee, and T. C. Lin, "Cryptanalysis of an efficient deniable authentication protocol based on generalized elgamal signature scheme," *International Journal of Network Security*, vol. 12, no. 1, pp. 58–60, 2011.

[26] D. Liu, S. Zhang, H. Zhong, R. Shi, and Y. Wang, "An efficient ID-based online/offline signature scheme without key escrow ," *International Journal of Network Security*, vol. 19, no. 1, pp. 127–137, 2017.

[27] K. Nyberg and R. A.Rueppel, "A new signature scheme based on the dsa giving message recovery," In *ACM Computer & Communications Security*, vol. 1, pp. 58–61, 1993.

[28] N. Ojha and S. Padhye, "Weak keys in rsa over the work of blomer & may," *International Journal of Network Security*, vol. 14, no. 2, pp. 80–85, 2012.

[29] C. Pan, S. Li, Q. Zhu, C. Wang, and M. Zhang, "Notes on Proxy Signcryption and Multi-proxy Signature Schemes," *International Journal of Network Security*, vol. 17, no. 1, pp. 29–33, 2015.

[30] S. Qadir, M. U. Siddiqi, W. F. M. Al-Khateeb, "An investigation of the Merkle signature scheme for cryptographically generated address signatures in mobile IPv6," *International Journal of Network Security*, vol. 17, no. 3, pp. 311–321, 2015.

[31] Y. Ren, S. Wang, X. Zhang, M. S. Hwang, "An efficient batch verifying scheme for detecting illegal signatures," *International Journal of Network Security*, vol. 17, no. 4, pp. 463–470, 2015.

[32] K. R. Santosh, C. Narasimham, and P. Shetty, "Cryptanalysis of multi-prime RSA with two decryption exponents," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 40–44, 2016.

[33] Z. Shao, "Signature schemes based on factoring and discrete logarithms," *IEE Proceedings - Computers and Digital Techniques*, vol. 145, no. 1, pp. 33–36, 1998.

[34] G. Sharma, S. Bala, A. K. Verma, "An improved RSA-based certificateless signature scheme for wireless sensor networks," *International Journal of Network Security*, vol. 18, no. 1, pp. 82–89, 2016.

[35] S. F. Tzeng, Y. L. Tang, and M. S. Hwang, "A new convertible authenticated encryption scheme with message linkages," *Computers and Electrical Engineering*, vol. 33, no. 2, pp. 133–138, 2007.

[36] F. Wang, C. C. Chang, C. Lin, S. C. Chang, "Secure and Efficient Identity-based Proxy Multi-signature Using Cubic Residues," *International Journal of Network Security*, vol. 18, no. 1, pp. 90–98, 2016.

[37] Z. Yang, C. Liu, W. Liu, S. Luo, H. Long and S. Li, "A lightweight generic compiler for authenticated key exchange from non-interactive key exchange with auxiliary input," *International Journal of Network Security*, vol. 18, no. 6, pp. 1109–1121, 2016.

[38] Y. Zhang, H. Li, X. Li, and H. Zhu, "Subliminal-free Variant of Schnorr Signature with Provable Security," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 19–30, 2015.

Biography

Cheng-Yi Tsai received the B.S. degree in Department of Business Administration from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 2001; the M.S. degree in Computer Science & Information Engineering from Asia University, Taichung, Taiwan, in 2005. He is currently pursuing his PHD degree in Graduate Institute of Computer Science & Information Engineering from Asia University. His current research interests include applied cryptography and mobile communications.

Chi-Yu Liu received the B.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2003. She is currently pursuing her M.S. degree in Graduate Institute of Networking and Communication Engineering from CYUT. Her current research interests include applied cryptography and mobile communications.

Shyh-Chang Tsaur received the B.S. in Electronic Engineering from National Taiwan University, Taiwan, in 1967; the M.A. in Physics from State University of New York at Stony Brook, USA, in1969; the Ph.D. in Electronic Engineering from Carnegie Mellon University, USA, in 1973. Dr. Tsaur with Dr. C Kuo jointly have received more than 10 US patents in Semiconductor Memories during his work in Texas Instruments, USA from 1973 to 1981. From 1981 to 1996, Dr. Tsaur has been in computer industries for 15 years including owning a PC store, employed as CIO in CMS, CA, USA, Information consultants, etc. Since 1996, Dr Tsaur has been employed as the Special Assistant to HCG Chairman for 5 years successfully to reengineer MIS department; hired as an information consultant of TSANN KUEN 3C Group to accomplish a real time EIS system of 150 chain stores in one year; a professor in CSIE department of Asia University until he retired. In last ten years, in addition to teaching in Universities, Dr. Tsaur has co-authored 3 books: RFID principle, Application and Implementation; Database System Theory and Applications; Cloud Computing Introduction: Entering APP Software World.

Min-Shiang Hwang Min-Shiang Hwang received the B.S. in Electronic Engineering from the National Taipei Institute of Technology, Taipei, Taiwan, in 1980; the M.S. in Industrial Engineering from the National Tsing Hua University, Taiwan, in 1988; and a Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at the 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. He was also the 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 was a professor and chairman of the Department of Management Information Systems, National Chung Hsing University (NCHU), during 2003-2009. He was also a visiting professor of UC. Riverside and UC. Davis (USA) during 2009-2010. He was a distinguished professor of the department of Management Information Systems, NCHU, during 2007-2011. He obtained the 1997, 1998, 1999, 2000, and 2001 Excellent Research Award of National Science Council (Taiwan). He was a dean of College of Computer Science, Asia University (AU). He is currently a Chair Professor of the department of Computer Science & Information Engineering, AU. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include information security, electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 200+ articles on the above research fields in international journals.