An Anonymous Multi-Receiver Encryption Based on RSA

Lein Harn[1], Chin-Chen Chang[2,3], and Hsiao-Ling Wu[2]
(Corresponding author: Chin-Chen Chang)

Department of Computer Science Electrical Engineering & University of Missouri- Kansas City[1]
No. 5100 Rockhill Rd.,Kansas City, MO 64110, USA
Department of Information Engineering and Computer Science & Feng Chia University[2]
No. 100, Wenhwa Rd., Seatwen, Taichung, 40724, Taiwan
Department of Computer Science and Information Engineering & Asia University[3]
No. 500, Lioufeng Rd., Wufeng, Taichung, 41354, Taiwan
(Email: alan3c@gmail.com)

(Received Mar. 22, 2013; revised and accepted May 26, 2013)

Abstract

With the rapid development of information and network technologies, communication security has become an important issue in many applications. There are many public-key based encryption schemes proposed in the literature. Network applications are no longer just one-to-one type of communication; but it involves multiple receivers (>1) (e.g., multicast transmission). One-to-one type encryption is no longer satisfying this type of applications. Ghodosi et al. proposed a threshold RSA cryptosystem in 1996. Their scheme is also called a multi-receiver encryption. In Ghodosi et al.'s scheme, each receiver's decryption key depends on all public keys of receivers. When the number of receivers is large, Ghodosi et al.'s scheme becomes impractical. We proposed a novel anonymous multi-receiver encryption. In our scheme, each receiver's decryption key is fixed. In addition, the scheme provides anonymity of receivers. We include performance analysis and comparisons with other schemes.

Keywords: RSA cryptosystems, Chinese Remainder Theorem, Anonymity, Multi-receiver encryption

1 Introduction

Public-key encryptions [4, 17, 18] allow a sender to send an encrypted message to a receiver (i.e., one-to-one type of encryption). However, network applications are no longer just one-to-one type of communication; but it involves multiple receivers (>1), (e.g., multicast transmission). One-to-one type encryption is no longer satisfying this type of applications.

In 1989, Chiou and Chen have proposed a secure broadcasting [7] using the CRT for protecting the messages. In their scheme, receivers need to have their public and private key pairs initially. The sender selects a random session key to encrypt the message. Then, the sender uses any public-key encryption and the CRT to securely transmit the decryption key corresponding to the random session key to all legitimate receivers. In summary, the scheme uses the key-encrypt-key technique to protect the messages. If the key-encrypt-key algorithm is a public-key algorithm, the parameters of the public-key algorithm can be used for only one time transmission; otherwise, if the key-encrypt-key algorithm is a private-key algorithm, their scheme is a mixed scheme since it uses both the public-key and private-key cryptosystems.

The notion of broadcast encryption was first introduced by Berkovits in [3] and was given a formal definition by Fiat and Naor in [13]. The goal of the broadcast encryption is to securely transmit a message to all legitimate receivers via insecure broadcast channels. In Fiat and Naor scheme, each user joining the system needs to obtain multiple prearranged keys during registration and then use these keys in real-time operation. There are several papers [2, 10, 19] related to Fiat and Naor scheme to discuss the number of private keys, the size of ciphertext and computational cost.

In 2005, Du et al. [11] first proposed an ID-based broadcast encryption based on Boneh and Franklin scheme [4] using matrix. In that scheme, receivers do not need to register with a center initially. However, in 2007, Chien [6] pointed out that their scheme is insecure. In 2005, Wang and Wu [24] proposed an ID-based multicast scheme using bilinear pairing. There are a key generation center to register all receivers initially and a group center to send messages to receivers. Only the group center can be the sender. Later, Sakai and Furukawa proposed another ID-based broadcast encryption [22] that the sender can be any user.

Most existing multi-receiver encryption schemes in the literature [2, 3, 4, 6, 10, 11, 13, 19, 24] cannot provide the anonymity of receivers. Fan et al. [12] proposed an anonymous multi-receiver ID-based encryption scheme in 2010. Wang et al. [25] pointed out that their scheme cannot provide the anonymity of receivers and is insecure in 2012. They also proposed a modified scheme. Unfortunately, Zhang et al. [27] pointed out that Wang et al.'s scheme cannot provide the anonymity and is insecure.

There are many papers on the pairing-based multi-receiver encryption scheme [1, 5, 6, 11, 12, 24, 25, 27]; but only a few papers are focused on the RSA-based multi-receiver encryptions [14, 23]. RSA [21] is one of the most commonly used public-key encryptions. However, there exists a well-known attack on the RSA-based broadcast encryption when all receivers use the same public key. The detail of this attack can be found in [16]. When each receiver uses different public key, this attack can be avoided. The public keys of receivers are all distinct in our proposed scheme.

In [14], Ghodosi et al. proposed a dynamic threshold cryptosystems based on the RSA. In their paper, a threshold RSA cryptosystem is the same as a multi-receiver encryption scheme. In their scheme, a sender can arbitrarily select a set of legitimate receivers without needing any key distribution. Each receiver's decryption key depends on all public keys of receivers. Unfortunately, when the number of receivers is large, Ghodosi et al.'s scheme becomes impractical. In addition, their scheme cannot provide the anonymity of receivers.

In this paper, we propose a RSA-based multi-receiver encryption scheme based on the Chinese Remainder Theorem (CRT). In the decryption, each receiver can use his/her fixed privet key which does not depend on other receivers to decrypt the ciphertext.

The rest of this paper is organized as follows. In Section 2, we review CRT, RSA and Ghodosi's threshold RSA scheme. In Section 3, we propose an anonymous multi-receiver encryption scheme. Then, Sections 4 and 5 are the discussion and analyses. Conclusion is given in Section 6.

2 Preliminaries

In this section, we briefly review basic fundamentals used in our scheme including the CRT [8], RSA encryption [21], and Ghodosi et al.'s scheme [14] based on the RSA encryption.

2.1 Chinese Remainder Theorem (CRT)

Assume that there are positive integers which are pairwise coprimes, and arbitrary integers where Then, there exists a unique integer satisfying following system of simultaneous congruence:

$$\begin{aligned} X &= a_1 \bmod N_1; \\ X &= a_2 \bmod N_2; \\ &\vdots \\ X &= a_n \bmod N_n, \end{aligned} \quad (1)$$

where $X = (\sum_{i=1}^{n} (\frac{N}{N_i}) \times y_i a_i) \bmod N$,

$N = N_1 \times N_2 \times \cdots \times N_n$, $(\frac{N}{N_i}) \times y_i \equiv 1 (\bmod N_i)$,

$(\frac{N}{N_i}) \times y_i \equiv 0 (\bmod N_j)$ and $0 < X < N$ for $i \neq j$.

2.2 RSA Encryption

In 1978, Rivest, Shamir and Adleman proposed a public-key cryptosystem [21]. Here, we only review the RSA encryption and assume that Alice performs the following steps to generate her public and private keys.

1) First, Alice chooses two strong primes, p and q, such that $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are two large primes. The detail about strong prime can be found in [24, 25]. Then, she computes the product, $N = p \times q$.

2) Second, she chooses the public key e, such that e and N are relatively prime, namely $\gcd(e, N) = 1$.

3) After choosing the public key and getting the product N, Alice can compute $\phi(N)$ and private key d as $ed \equiv 1(\bmod N)$, where $\phi(N) = (p-1) \times (q-1)$. In addition, the Euler's totient function $\phi(N)$ means the number of positive integers which are less than and relatively prime to N.

4) Finally, Alice keeps the private key (d, p, q) secretly and publishes the public key (e, N).

We also assume that Bob wants to send the message M to Alice secretly, where $0<M<N$. Bob must employ Alice's public key e to compute the ciphertext as $C = M^e \bmod N$ and sends it to Alice. Once Alice receives the ciphertext C, she can use her private key d to decrypt the ciphertext C as $C^d \bmod N = M$.

2.3 Ghodosi et al.'s Multi-receiver Encryption Scheme

In this subsection, we briefly review Ghodosi et al.'s multi-receiver encryption scheme [14]. There is a group G consisting of n users and one trusted public registry. Each user U_i has his/her RSA key pair (i.e., the public key is (e_i, N_i) and the private key is d_i). Furthermore, the trusted public registry stores and manages all public keys of users. Their scheme consists of two phases: 1) encryption phase and 2) decryption phase. A sender S can encrypt one message M and broadcast the ciphertext to all receivers in encryption phase. In decryption phase, the receiver U_i needs to compute a decryption key first and then uses the decryption key to decrypt the ciphertext to obtain the message M.

Encryption Phase

Assume that the sender S wants to send one message M to the group G. S has to get all receivers' public-key digital certificates and validate their public keys [26]. If the verification is passed, S computes the encryption key as $E = \prod_{i=1}^{n} e_i$ and the modulus as $N = N_1 \times N_2 \times \cdots \times N_n$ of the group. Then, the sender S computes the ciphertext:

$$C = M^E \bmod N.$$

The sender S broadcasts E, N and C to all receivers.

Decryption Phase

When each receiver U_i receives the broadcasted message, (E, N, C), he/she needs to validate public keys N_j and e_j of other receivers, for $j = 1, 2, \ldots, n$ and $i \neq j$. If N and E are valid, each receiver U_i can check $N_i \mid N$ to determine whether he/she is one of the intended receivers. If he/she is, each receiver U_i computes the decryption key D_i as $E \times D_i \equiv 1 \bmod \phi(N_i)$. Then, each receiver U_i uses D_i to decrypt the ciphertext C as $C^{D_i} \bmod N_i = M^{E \times D_i} \bmod N_i = M \bmod N_i$.

3 The Proposed Scheme

In this section, we propose a multi-receiver encryption scheme based on the RSA and CRT. Our scheme consists of two phases: 1) encryption phase and 2) decryption phase. A sender uses all receivers' public keys to encrypt the secret message and then broadcasts the ciphertext to the receivers in the encryption phase. When a legitimate receiver receives the ciphertext, he/she can decrypt the encrypted message by using a fixed decryption key in the decryption phase.

Encryption Phase

First, we assume that there are n receivers and one sender. Each receiver U_i has one RSA key pair, $(d_i, (e_i, N_i))$, for $i = 1, 2, \cdots, n$. The public key and private key of each receiver are generated according to the procedures described in Section 2.1. When a sender wants to send the message M to n receivers, he/she has to validate public-key digital certificates of all receivers at the beginning. The message M must be smaller than N', where N' is the minimal modulus in the set of $\{N_1, N_2, \ldots, N_n\}$. Then the sender S computes $N = N_1 \times N_2 \times \cdots \times N_n$ and

$$\begin{aligned} c_1 &= M^{e_1} \bmod N_1; \\ c_2 &= M^{e_2} \bmod N_2; \\ &\vdots \\ c_n &= M^{e_n} \bmod N_n. \end{aligned} \tag{2}$$

According to the CRT, when $N_1, N_2, \ldots, N_n$ are pairwise coprimes and $0 < c_1 < N_1$, $0 < c_2 < N_2$, $\ldots$, $0 < c_n < N_n$, there exists a unique solution C in (3) satisfying following system of simultaneous congruence:

$$\begin{aligned} C &= c_1 \bmod N_1; \\ C &= c_2 \bmod N_2; \\ &\vdots \\ C &= c_n \bmod N_n. \end{aligned} \tag{3}$$

The sender broadcasts C to all receivers.

Decryption Phase

Once receiver U_i obtaining the ciphertext C, he/she can perform the following steps to retract the secret message M.

1) First, he/she uses the public key N_i to execute the modulo reduction, that is, $C \bmod N_i = c_i$.

2) After getting c_i, receiver U_i can use the private key d_i to decrypt c_i as $c_i^{d_i} = (M^{e_i})^{d_i} \bmod N_i = M$. Since $0 < M < N'$, each receiver can retrieve the same message M.

In decryption phase, each receiver uses his/her fixed key pair to retract the message M.

4 Discussion

In this section, we discuss the similarities and differences between Ghodosi *et al.*'s scheme and our scheme. There are two similarities. First, both Ghodosi *et al.* and our scheme use RSA encryption to provide multi-receiver encryption. Second, the sender can select any set of legitimate receivers. On the other hand, there are three differences between Ghodosi *et al.*'s scheme and our scheme. The details are given below.

4.1 Computational Complexity

In Ghodosi *et al.*'s scheme, each receiver U_i obtains the ciphertext (N, C, E). U_i needs to validate public keys N_j and e_j of other receivers, for $i, j = 1, 2, \ldots, n$, and $i \neq j$, i.e., verifying $n-1$ times. The time complexity is $O(n)$, where n is the total number of receivers. When there are a large number of receivers, their scheme is impractical. In our scheme, each receiver does not need to validate public keys of other receivers. Furthermore, in the next section, we will show that in Ghodosi *et al.*'s scheme, the sender spends more computational time to encrypt the message than the time needed in our scheme.

4.2 Anonymity of Receivers

In Ghodosi et *al.*'s scheme, when receiver U_i gets the N, he/she needs to determine whether he/she is one of legitimate receivers by computing $N_i \mid N$. Since N_i and N are public information, their scheme cannot provide the anonymity of receivers. In our scheme, sender broadcasts

C only. Hence, nobody, except the sender, knows who legitimate receivers are. Detail analysis will be included in Section 5.

4.3 Decryption Key

In Ghodosi *et al.*'s scheme, receiver U_i needs to compute a decryption key D_i as $E \times D_i \equiv 1 (\bmod N_i)$. However, E is the product of public keys of all receivers. Hence, each receiver's decryption key is dynamic for each session. But, in our scheme, each receiver U_i can uses his/her private key d_i to recover the original message M as $C^{d_i} \bmod N_i = M$. So the decryption key is fixed for all sessions.

5 Analysis

In this section, we discuss the properties of correctness, performance, security and anonymity. Correctness means that each legitimate receiver can retrieve the message and the anonymity means that the identities of receivers can be protected. We compare the computational cost and the size of ciphertext among our scheme and other schemes.

5.1 Correctness

When sender wants to send the message the range of message M is restricted to be between zero and N' which is the minimal modulus in the set of $\{N_i \mid \text{for } 1 \le i \le n\}$. Accordingly, each legitimate receiver having valid values, d_i and N_i, can retrieve the message.

5.2 Performance

In this subsection, we compare the performance among unicast RSA, Ghodosi *et al.* scheme and our scheme. In unicast RSA, the sender needs to perform RSA encryption for *n* times and sends each ciphertext to one of receivers separately. We assume to use the 1024-bits RSA encryption, i.e., modulus $N_i \approx 2^{1024}$ for $1 \le i \le n$. Since modulo exponentiation takes more computational time than other operations, we only consider the time needed for RSA encryption and decryption in the following discussion. We let T_{E_1024}, $T_{E\_n\times1024}$ and T_D denote the 1024-bit RSA encryption operation, the $(n \times 1024)$-bit RSA encryption operation and the RSA decryption operation, separately. Table 1 shows the comparison results.

The computational cost and ciphertext size of unicast RSA is the same as our scheme; but it needs *n* times transmission. In addition, there has other traffic information needed in unicast transmission. In the following analysis, we adopt results published in [9] that include complexities of standard hardware implementation of modulo operations. For $(n \times 1024)$-bit operation, the hardware complexity of modular exponentiation, is 4^{n-1} times the hardware complexity of 1024-bit modular exponentiation. Hence, we can get $T_{E\_n\times1024} = 4^{n-1} \times T_{E\_1024}$. In summary, the computational cost of the sender is $4^{n-1} \times T_{E\_1024}$ in Ghodosi *et al.*'s scheme and is $n \times T_{E\_1024}$ in our scheme. Furthermore, in our scheme, the sender needs one CRT computation. Although the sender does not need to compute CRT in Ghodosi *et al.*' scheme, the decryption key of each receiver is dynamic. On the receiver side, both Ghodosi *et al.* scheme and our scheme need one RSA decryption. The different is that their scheme needs to compute one multiplicative inverse; but ours needs to compute one modulo reduction. Obviously, the computational complexity of multiplicative inverse is much larger than the computational complexity of modulo reduction. Therefore, our scheme is more computationally efficient than Ghodosi *et al.*'s scheme and the ciphertext size of ours is $\frac{1}{3}$ of the ciphertext size of their scheme.

Table 1: Comparison results among different schemes

	Unicast RSA	**Ghodosi *et al.* scheme**	**Our scheme**
Sender	$n \times T_{E\_1024}$	$4^{n-1} \times T_{E\_1024}$ (i.e., $T_{E\_n\times1024}$)	$n \times T_{E\_1024}$
Receiver	T_D	T_D	T_D
Size of ciphertext	$n \times 1024$ bites	$3 \times n \times 1024$ bites	$n \times 1024$ bites
Rounds of transmission	n	1	1
Anonymity of receivers	No	No	Yes

* n : the number of receivers

5.3 Security

Since our scheme uses RSA encryption, the security of our scheme is the same as RSA. Namely, the security of ours is based on the integer factoring problem. If an illegitimate receiver wants to decrypt the encrypted message, he/she needs to break the RSA assumption.

5.4 Anonymity

We assume that sender S wants to send the ciphertext C to t legitimate receivers in a group G consisting of n users, where $t \le n$. The attacker Eve has intercepted the ciphertext C and knows n users' public keys, N_i for $1 \le i \le n$. Even Eve can use C and N_i to compute $M^{e_i} \bmod N_i$, where N_i is the public key of one of the legitimate receivers, Eve cannot recover the message and to identify identities of legitimate receivers. Hence, our scheme can provide the anonymity of receivers.

6 Conclusions

In this paper, we propose a novel multi-receiver encryption scheme which can provide the anonymity of receivers. Our scheme is a simple integration of both the RSA and CRT. The proposed scheme is more efficient than existing schemes in terms of computational cost and ciphertext size. Each receiver only needs to keep one private key and uses this private key to decrypt the ciphertext.

References

[1] J. Baek, R. Safavi-Naini, and W. Susilo, "Efficient multi-receiver identity-based encryption and its application to broadcast encryption," in *Proceeding of Public Key Cryptography – PKC '05*, LNCS 3386, pp. 380-397, Springer-Verlag, Les Diablerets, Switzerland, Jan. 2005.

[2] M. Bellare, A. Boldyreva, and S. Micali, "Public-key encryption in a multi-user setting: security proofs and improvements," in *Proceeding of Advances Cryptology – Eurocrypt 2000*, LNCS 1807, pp.259-274, Springer-Verlag, Bruges, Belgium, May 2000.

[3] S. Berkovits, "How to broadcast a secret," in *Proceeding of Advances Cryptology – Eurocrypt'91*, LNCS 547, pp. 535-541, Springer-Verlag, Brighton, UK, Apr.1991.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proceeding of Advances Cryptology – Crypto '01*, LNCS 2139, pp. 213-229, Springer-Verlag, California, USA, Aug. 2001.

[5] Z. H., Chen, S. D., Li, C. Z., Wang and Y. P. Shen, "Two constructions of multireceiver encryption supporting constant keys, short ciphertexts, and identity privacy," *International Journal of Network Security*, vol. 14, no. 5, pp. 270-279, Sep. 2012

[6] H. Y. Chien, "Comments on an efficient ID-based broadcast encryption scheme," *IEEE Transations Broadcast*, vol. 53, no. 4, pp. 809-810, Dec. 2007.

[7] G. H. Chiou and W. T. Chen, "Secure broadcasting using the secure lock" *IEEE Transations on Software Engineering*, vol. 15, no. 8, pp. 929-934, Aug. 1989.

[8] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 4th ed. , pp. 19-20, New York, 2000.

[9] J. P., David, K. Kalach, and N. Tittley, "Hardware complexity of modular multiplication and exponentiation," *IEEE Transations on Computers*, vol. 56, no. 10, pp. 1308-1319, Oct. 2007.

[10] Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers," in *Proceeding of Digital Rights Management 2002*, LNCS 2696, pp. 61-80, Springer-Verlag, Washington, DC, USA, 2002.

[11] X. Du, Y. Wang, J. Ge, and Y. M. Wang, "An ID-based broadcast encryption scheme for key distribution," *IEEE Transations Broadcast*, vol. 51, no. 2, pp. 264-266, June 2005.

[12] C. I. Fan, L. Huang, and P. Ho, "Anonymous multi-receiver identity-based encryption," *IEEE Transations on Computers*, vol. 59, no. 9, pp. 1239-1249, Sep. 2010.

[13] A. Fiat and M. Naor, "Broadcast encryption," in *Proceeding of Advances Cryptology – Crypto*, LNCS 839, pp. 480-491, Springer-Verlag, California, USA, Aug. 1994.

[14] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini, "Dynamic threshold cryptosystems: a new scheme in group oriented cryptography," in *Proceeding of Pragocrypt'96: the 1st International Confernce on thw Theory and Applications of Crytology*, pp. 370-379, Prague, Czech Republic, Sep. 1996.

[15] J. Gordon, "Strong RSA key," *IET Electronics Letters*, vol. 20, no. 12, pp. 514-516, June 1984.

[16] J. Hastad, "Solving simultaneous modular equations of low degree," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 336-341, Apr. 1988.

[17] IEEE Standard Specifications for Public-Key Cryptography, IEEE Standard 1363–2000, 2000.

[18] IEEE Draft Standard for Identity-Based Cryptographic Techniques using Pairings, IEEE P1363/D6, 2011.

[19] K. Kurosawa, "Multi-recipient public-key encryption with shortened ciphertext," in *Proceeding of Public Key Cryptography*, LNCS 2274, Springer-Verlag, pp. 48-63, Pairs, France, February 2002.

[20] J. H. Moore, "Protocol failures in cryptosystems," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 594-602, May 1988.

[21] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[22] R. Sakai and J. Furukawa, "Identity-based broadcast encryption," *Cryptology ePrint Archive*, Report 2007/217, 2007.

[23] E. Sigurd, "A multi-receiver public key cryptosystem," in *Proceedings of Norwegian Symposium Information Security (NISK)*, pp. 110-121, Trondheim, Norway, Nov. 2009.

[24] L. Wang and C. K. Wu, "Efficient identity-based multicast scheme from bilinear pairing," *IEE Proceedings – Communications*, vol. 152, no. 6, pp. 877-882, Dec. 2005.

[25] H. Wang, Y. Zhang, H. Xiong, and B. Qin, "Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme," *IET Information Security*, vol. 6, no. 1, pp. 20-27, Mar. 2012.

[26] R. W. Younglove, "Public key infrastructure. How it works," *Computing & Control Engineering Journal*, vol. 12, no. 2, pp. 99-102, Apr. 2001.

[27] J. Zhang and Y. Cui, "Comment an anonymous multi-receiver identity-based encryption scheme," in *Proceeding* of *4th International conference on Intelligent Networking and Collaborative Systems (INCoS)*, pp. 473-476, Bucharest, Romania, Sep. 2012.

Lein Harn received his BS degree in Electrical Engineering from the National Taiwan University in 1977. In 1980, he received his MS degree in Electrical Engineering from the State University of New York-Stony Brook and in 1984 he received his Ph. D. degree in Electrical Engineering from the University of Minnesota. Currently, he is a Full Professor at the Department of Computer Science Electrical Engineering, University of Missouri- Kansas City, USA. His research interests are cryptography, network security and wireless communication security. He has published number of papers on digital signature design and applications, wireless and network security.

Chin-Chen Chang received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Taiwan. He was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the College of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office of the Ministry of Education of the R.O.C. Since February 2005, he has been a Chair Professor of Feng Chia University. He is currently a Fellow of IEEE and a Fellow of IEE, UK. He also published several hundred papers in Information Sciences. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures.

Hsiao-Ling Wu was born in Kaohsiung, Taiwan, in 1986. She received the BS degree in Applied Mathematics from Feng Chia University, Taichung, Taiwan in 2007. She is currently pursuing her Ph.D. degree in information engineering and computer science from Feng Chia University, Taichung, Taiwan. Her current research interests include electronic commerce, information security, cryptography, and mobile communications.