A $n^2 + n$ MQV Key Agreement Protocol

Li-Chin Hwang[1], Cheng-Chi Lee[2], and Min-Shiang Hwang[3]

[1]Department of Computer Science and Engineering, National Chung Hsing University, Taiwan, R.O.C

[2]Department of Library and Information Science, Fu Jen Catholic University, Taiwan, R.O.C

[3]Department of Computer Science and Information Engineering Asia University, Taiwan, R.O.C

Abstract: *In this paper, a novel scheme to generate (n^2 + n) common secret keys in one session is proposed, in which two parties can use them to encrypt and decrypt their communicated messages by using symmetric-key cryptosystem. The proposed scheme is based on the difficulty of calculating discrete logarithms problem. All the session keys can be used against the known key attacks, main-in-the middle attacks, replay attacks or forgery attacks. The security and efficiency of our proposed scheme are presented. Compare with other schemes, the proposed scheme can generate more session keys in one session. Therefore, the propose scheme is more efficient than the others.*

Keywords: *Authenticated key agreement, cryptography, multiple-key agreement, MQV.*

Received June 21, 2010; accepted March 1, 2011

1. Introduction

What is key agreement? The key agreement protocol allows two parties that have no prior knowledge of each other to jointly establish a shared common secret key over an insecure communications channel. This key can then be used to encrypt/decrypt subsequent communications using a symmetric-key cryptosystem such as [3, 11, 26, 27]. In 1976, Diffie and Hellman [2] introduced the first well-known key agreement to enable two parties to establish a common secret session key. However, the original Diffie-Hellman scheme does not support the authentication between the two parties as a result of the man-in-the-middle attack [13, 30]. Since then, several authenticated public key protocols [1, 4, 8, 14, 19] have been proposed to solve this problem. Here, we brief the Diffie-Hellman key agreement as follows. Assume that *A* and *B* want to establish a common session key to securely communicate with each other. Then, they execute the following steps.

1. *A* randomly chooses a large number *a* and computes K_A=g^a *mod p*, then sends it to *B*.
2. *B* also randomly chooses a large number *b* and sends K_B=g^b *mod p* to *A*.
3. After receiving K_A and K_B, they can compute their common session key $SK = K_B{}^a \bmod p = K_A{}^b \bmod p = g^{ab} \bmod p$,

where *g* is a generator and *p* is a large prime. Adversary cannot compute the session key without knowing *a* and *b* because of the discrete logarithm problem (DLP) [12, 18, 25].

1.1. Related Work

In 1995, Menezes et al. [17] proposed the first important key agreement protocol, which is also called the MQV protocol, to sign a signature for the Diffie-Hellman public keys without using a one-way hash function. And the MQV key agreement protocol has become a standard adopted by IEEE P1363 [10].

In 1998, Harn and Lin [6] presented an authenticated key agreement protocol based on the MQV protocol to efficiently establish n^2 common session keys between two parties. To avoid the known key attack [19], the Harn-Lin protocol adopted no more than (n^2 − *1*) common session keys while two parties send *n* Diffie-Hellman public keys. Yen and Joye [31] showed a forgery attack in the Harn-Lin protocol and proposed an improved protocol. However, the Yen-Joye protocol still cannot withstand a forgery attack proposed by Wu et al. [29]. Therefore, Hwang et al. proposed an improved Yen-Joye protocol to overcome its weakness [8]. In 2001, Harn and Lin [7] modified the signature signing equation in [6] to conquer the forgery attack, but their protocol still limits that only (n^2 − *1*) common session keys to be adopted between two parties.

In 2002, Tseng [28] firstly proposed a new authenticated multiple-key agreement protocol that can withstand the known-key attack if two parties use all n^2 common session keys. Tseng claimed that his protocol is robust against the forgery attack and the known-key attack if all the secret keys established are adopted. However, Shao showed that Tseng's protocol is insecure against signature forgery attacks and then proposed an improved authenticated multiple-key agreement protocol to resist the attacks [23]. Unfortunately, Shim showed that Shao's protocol is also insecure [24]. In 2008, Lee et al. proposed two new MQV protocols based on elliptic curves and bilinear pairings [16]. The first protocol based on elliptic curves is more efficient than [7, 9, 15] and it can achieve the same security with smaller key size. And the second protocol based on bilinear pairings keeps the same properties with previous schemes. The available number of shared session keys is more than that in [7, 9, 15]. In 2011, Ravala et al. proposed a novel key generation scheme based on the biometrics [21]. The common secret key is generated from finger prints of sender as well as receiver. However, the scheme only generated one secret key in one session. Key agreement or management is an important issue in any areas for the secure communications in the network. Recently, some key agreement schemes in wireless sensor networks are proposed for the secure communications [5, 20, 22]. However, these schemes only also generated one secret key in one session.

Until to now, all researches focus on how to establish n^2 common secret session keys. In this paper, the authors shall propose a novel protocol to generate $(n^2 + n)$ common session keys in one session.

1.2. Organization of This Paper

The organization of this paper is as follows: In Section 2, we propose our protocol. Then, we give a security analysis and efficiency analysis in Section 3. Finally, our brief conclusion will be in Section 4.

2. $n^2 + n$ MQV Key Agreement Protocol

In this section, an extension of key agreement protocol is proposed to establish $(n^2 + n)$ common session keys between two parties. The proposed protocol can be divided into two phases: the initiation phase and the multiple-key agreement phase which are described below. Now, we suppose that Bob and Alice want to establish 12 common session keys $(3^2 + 3)$ by 3 $(n = 3)$ short-term keys. The processes are described as follows.

2.1. The Initiation Phase:

The system, such as the Diffie-Hellman scheme, chooses a large prime number p. Then, Bob and Alice select their random numbers x_A and x_B. They compute the corresponding long-term public keys $y_A = g^{xA}$ mod p and $y_B = g^{xB}$ mod p, individually.

2.2. The Multiple-key Agreement Phase:

1. Alice selects 3 short-term secret keys k_{A_1}, k_{A_2}, and k_{A_3}, randomly and then computes $k_A = k_{A_1} + k_{A_2} + k_{A_3}$ mod q. Furthermore, the corresponding short-term public keys $r_A = g^{k_A}$ mod p, $r_{A_1} = y_B^{kA1}$ mod p, $r_{A_2} = y_B^{kA2}$ mod p, $r_{A_3} = y_B^{kA3}$ mod p, are computed. Alice is able to obtain the signature s_A based on the equation $s_A r_A = x_A - r_{A_1} k_A$ mod q. Finally, Alice sends $\{r_{A_1}, r_{A_2}, r_{A_3}, s_A, Cert(y_A)\}$ to Bob, where $Cert(y_A)$ is a certificate for the public key signed by a trustworthy party such as a certificated authority.
2. In the same way as Alice does, Bob also gets k_{B_1}, k_{B_2}, k_{B_3} and obtains r_{B_1}, r_{B_2}, r_{B_3} and s_B. Then Bob sends $\{r_{B_1}, r_{B_2}, r_{B_3}, s_B, Cert(y_B)\}$ to Alice.
3. Alice verifies the authenticated messages $\{r_{B_1}, r_{B_2}, r_{B_3}, s_B, Cert(y_B)\}$ from Bob, and then makes sure that the equation

$$y_B = (r_B)^{r_{B_1}} g^{s_B r_B} \bmod p \qquad (1)$$

is correct, where $r_B = r_{b1} r_{b2} r_{b3}$ mod p, $r_{b1} = (r_{B_1})^{x_A-1}$ mod p, $r_{b2} = (r_{B_2})^{x_A-1}$ mod p, $r_{b3} = (r_{B_3})^{x_A-1}$ mod p. We show that Equation (1) is correct as follows:

$$\begin{aligned} y_B &= g^{x_B} \bmod p \\ &= g^{s_B r_B + r_{B_1} k_B} \bmod p \\ &= g^{s_B r_B} (g^{k_B})^{r_{B_1}} \bmod p \\ &= g^{s_B r_B} (r_B)^{r_{B_1}} \bmod p \end{aligned}$$

If Equation (1) holds, Alice could obtain 12 common session keys as follows:

$$\begin{aligned} K_1 &= r_{b1}^{kA1} \bmod p, \\ K_2 &= r_{b1}^{kA2} \bmod p, \\ K_3 &= r_{b1}^{kA3} \bmod p, \\ K_4 &= r_{b2}^{kA1} \bmod p, \\ K_5 &= r_{b2}^{kA2} \bmod p, \\ K_6 &= r_{b2}^{kA3} \bmod p, \\ K_7 &= r_{b3}^{kA1} \bmod p, \\ K_8 &= r_{b3}^{kA2} \bmod p, \\ K_9 &= r_{b3}^{kA3} \bmod p, \\ K_{10} &= r_{b1} \oplus r_{b2}, \\ K_{11} &= r_{b1} \oplus r_{b3}, \end{aligned}$$

and

$$\begin{aligned} K_{12} &= g^{(k_A + k_B)} \bmod p \\ &= g^{k_A} \bullet g^{k_B} \bmod p \\ &= g^{k_A} \bullet r_B \bmod p. \end{aligned}$$

We show that Alice and Bob will share the common session key K_{10} as follows:

$$\begin{aligned} K_{10} &= r_{b1} \oplus r_{b2} \\ &= (r_{B_1})^{x_A-1} \oplus (r_{B2})^{x_A-1} \bmod p, \\ &= (y_A^{kB1})^{x_A-1} \oplus (y_A^{kB2})^{x_A-1} \bmod p \\ &= g^{k_{B1}} \oplus g^{k_{B2}} \bmod p. \end{aligned}$$

Alice can easily get K_{10} from $r_{b1} \oplus r_{b2}$. And Bob can also get the K_{10} from their short-term secret keys k_{B1} and k_{B2}. In the same way, Alice and Bob can obtain the common session key K_{11} successfully.

Even though Alice and Bob use all common secret keys from K_1 to K_{12}, an eavesdropper cannot derive any other shared secret keys. Therefore, the proposed scheme can withstand the known-key attack. We will explain it in next session.

4. Bob also verifies the authenticated messages $\{r_{A1}, r_{A2}, r_{A3}, s_A, Cert(y_A)\}$ from Alice. By using r_A, r_{A1}, r_{A2}, and r_{A3}, Bob checks the equation $y_A = (r_A)^{r_{A1}} g^{s_A r_A} \bmod p$. Bob can also generate 12 common secret keys when the following equations hold.

$$\begin{aligned}
K_1 &= r_{a1}^{kB1} \bmod p,\\
K_2 &= r_{a1}^{kB2} \bmod p,\\
K_3 &= r_{a1}^{kB3} \bmod p,\\
K_4 &= r_{a2}^{kB1} \bmod p,\\
K_5 &= r_{a2}^{kB2} \bmod p,\\
K_6 &= r_{a2}^{kB3} \bmod p,\\
K_7 &= r_{a3}^{kB1} \bmod p,\\
K_8 &= r_{a3}^{kB2} \bmod p,\\
K_9 &= r_{a3}^{kB3} \bmod p,\\
K_{10} &= r_{b1} \oplus r_{b2},\\
K_{11} &= r_{b1} \oplus r_{b3},
\end{aligned}$$

and

$$\begin{aligned}
K_{12} &= g^{(k_A + k_B)} \bmod p\\
&= g^{k_A} \bullet g^{k_B} \bmod p\\
&= g^{k_A} \bullet r_A \bmod p.
\end{aligned}$$

Hence, a generalized key agreement protocol without using a one-way hash function is proposed to enable two communicating parties to establish $(n^2 + n)$ common session keys in a single round of message exchange. Obviously, the proposed protocol generates more n session keys than other protocols do as shown in Table 1.

We take n public keys to combine, exclusive-or operation (XOR) and select all safe keys which will not have any attack as session keys that we called primitive keys. Now, we shall propose a lemma to prove that n public keys will generate $(n - 1)$ primitive keys.

Theorem 2.1. *The n keys generate $\sum^{n}_{s=2} C(n,s) = 2^n - n - 1$ combinations from $k_1, \ldots, k_n$. We define $k_1 \oplus k_i$, $i = 2, \ldots, n$ as the primitive keys from $\sum^{n}_{s=2} C(n,s)$. All $n - 1$ primitive keys can be adopted between two parties as their session keys for safe and sound communication.*

Proof. Let I be the number of keys which are selected by two parties, respectively.

Case 1. The property is true for $I = 3$:

The three keys generate $C(3, 2) + C(3, 3) = 4$ combinations from k_1, k_2, k_3. Obviously, the primitive key $k_1 \oplus k_2$ and $k_1 \oplus k_3$ can be adopted as session keys safely. The remainders may lead to the known key attack, which will be described as follows:

1. $k_2 \oplus k_3$ is produced by $(k_2 \oplus k_3) \oplus (k_1 \oplus k_3)$.
2. The primitive keys will be inferred if the exclusive-OR (XOR) apply to $k_1 \oplus k_2 \oplus k_3$ and primitive key. Therefore, k_1, k_2, k_3 will be inferred from the $((k_1 \oplus k_2 \oplus k_3) \oplus (k_i \oplus k_j))$ where $i, j = 1, 2, 3$; $i < j$. For instance, the k_1 infers from $(k_1 \oplus k_2 \oplus k_3) \oplus (k_2 \oplus k_3)$.

Case 2. Assume the property is true for $I = n - 1$:

The $n - 1$ keys generate $\sum^{n-1}_{s=2} C(n-1,s) = 2^{n-1} - n - 2$ combinations from $k_1, \cdots, k_{n-1}$. Clearly, the primitive key $k_1 \oplus k_2, \cdots, k_1 \oplus k_{n-1}$ can be adopted as a session key safely. The remainders will result in the know key attack.

Case 3. Prove the property is true for $I = n$:

The n keys generate $\sum^{n}_{s=2} C(n,s) = 2^n - n - 1$ combinations from $k_1, \cdots, k_{n}$. The $2^n - n - 1$ combination keys may be divided into primitive keys and non-primitive keys.

1. Show that the primitive keys is $k_1 \oplus k_i$, where $i = 2, \cdots, n$.
   a. $k_1 \oplus k_2, \cdots, k_1 \oplus k_{n-1}$ combination keys have been proved in Case 2 previously.
   b. $k_1 \oplus k_n$ is still a primitive key which can't be inferred from $k_1 \oplus k_2, \cdots, k_1 \oplus k_{n-1}$.
2. Show $2^n - 2n$ non-primitive keys.
   a. $2^{n-1} - 2n$ non-primitive keys have been proved in Case 2.
   b. The remainders of 2^{n-1} non-primitive keys are as follows:
      i. $k_n \oplus k_i$ where $i = 2, \cdots, n - 1$, $k_n \oplus k_i$ infer from $(k_n \oplus k_1) \oplus (k_1 \oplus k_i)$ where $i = 2, \cdots, n - 1$. Therefore, $k_n \oplus k_i$ are non-primitive keys.
      ii. $k_n \oplus k_{i1} \oplus \cdots \oplus k_{ij}$, $k_{ij} \in \{k_1, k_2, \cdots, k_{n-1}\}$ where $j = 2, \cdots, n-1$; $k_{ij} \neq k_{ip}$; $j \neq p$; $jp = 2, \cdots, n - 1$. In Case 2, $(k_{i1} \oplus \cdots \oplus k_{ij})$ have been proved. Now, the primitive key k_n will infer from $(k_n \oplus k_{i1} \oplus \cdots \oplus k_{ij}) \oplus (k_{i1} \oplus \cdots \oplus k_{ij}) = k_n$, where $ij = 2, \cdots, n-1$. For instance, k_1 will infer from $(k_n \oplus k_1 \oplus k_2) \oplus (k_1 \oplus k_2) = k_n$ and $k_n \oplus (k_n \oplus k_1) = k_1$. Therefore, $k_1, k_2, \cdots, k_n$ will be inferred.

Q.E.D.

3. Analysis

In this section, we shall show the security and efficiency analysis of our extended protocol as follows.

Security Analysis:

1. Known-key Attack:

Tseng [28] proved that his protocol could withstand the known-key attack. Similarly, our extended protocol can also withstand the known-key attack [19]. We suppose two parties use the 12 common session keys. Our extended protocol may withstand the known key attack. We derive g^{xAxB} as follows:

$$g^{xAxB} = g^{(sArA + rA1kA)(sBrB+rB1kB)} \bmod p$$

$$= g^{sAsBrArB} \cdot g^{sArArB1kB} \cdot g^{sBrBrA1kA} \cdot g^{kAkBrA1rB1} \bmod p$$

$$= g^{sAsBrArB} \cdot g^{sArArB1kB} \cdot g^{sBrBrA1kA}$$

$$\cdot (g^{(kA1+kA2+kA3)(kB1+kB2+kB3)})^{rA1rB1} \bmod p$$

$$= g^{sAsB\,rArB} \cdot g^{sA\,rA\,rB1kB} \cdot g^{sBrB\,rA1kA} \cdot (\Pi^{9}_{i=1}K_i)^{rA1\,rB1} \bmod p$$

Suppose two parties adopt and publish the common session keys $K_1, K_2, \cdots, K_{10} = g^{KB1} \oplus g^{KB2}$, and $K_{11} = g^{KB1} \oplus g^{KB3}$, an eavesdropper is still hard to derive the key $K_{12} = g^{kB}r_A \bmod p$ owing to unknowning secrets r_A and r_B. Furthermore, if an intruder can obtain all the common session keys from K_1 to K_{12}, where the transmitted message involves (r_{A1}, r_{A2}, r_{A3}, r_{B1}, r_{B2}, r_{B3}, s_A, s_B, $g^{KB1} \oplus g^{KB2}$, $g^{KB1} \oplus g^{KB3}$, and $g^{kB}r_A \bmod p$), it is still hard for the intruder to calculate g^{xAxB} by intercepting the transmitted message between the two parties. The intruder cannot derive r_A and r_B from any transmitted message. The security is based on the difficulty of calculating discrete logarithms. Consequently, the extended protocol can also withstand the known-key attack.

2. Replay Attack:

In order to resist the replay attack, our protocol uses short-term keys. The lifetime of the short-term keys k_{Ai} and k_{Bi} ($i \in 1, 2, . . .$) is only one session long, with a view of establishing ($n^2 + n$) keys. The two parties have to randomly choose new short-term keys again in the next session. If the intruder attempts to replay the previously intercepted message to Bob for masquerading as Alice, Bob will find out and reject this message.

3. Forgery Attack:

Assume that an intruder wants to impersonate Alice to establish the common session keys with Bob. The intruder forges the previously intercepted message (r_{A1}, r_{A2}, r_{A3}, s_A, $Cert(y_A)$) to (r'_{A1}, r'_{A2}, r'_{A3}, s'_A, $Cert(y_A)$) and send it to Bob, where (r'_{A1}, r'_{A2}, r'_{A3} and s'_A)

$$k'_A = k'_{A1} + k'_{A2} + k'_{A3} \bmod q$$

$$r_{A1} = g^{k'_{A1}} \bmod p,$$

$$r_{A2} = g^{k'_{A2}} \bmod p,$$

$$r_{A3} = g^{k'_{A3}} \bmod p,$$

$$s'_A\, r'_A = x'_{\mathrm{A}} - r'_{A1}k'_{A1} \bmod q.$$

Because the message cannot pass verification Equation (1), bob will reject the transmitted message sent from the intruder.

Efficiency Analysis:

In Table 1, we can see that our scheme is more efficient than Harn-Lin's protocol [7], Tseng's protocol [28], Shao's protocol [23], and Lee et al.'s protocol [16]. Harn-Lin's protocol establishes n^2 common secret session keys in one session within two parties, but only (n^2 − 1) can be used for withstanding the known-key attack. In Tseng's protocol, the n^2 common secret keys can be used without suffering from the attack. An improvement of Tseng's protocol proposed by Shao establishes n^2 common secret session keys and n^2 keys can be used. The first protocol of Lee et al.'s protocols establishes n^2 keys and only (n^2 − 1) keys can be used. The second protocol of Lee et al.'s protocols establishes n^2 keys and n^2 keys can be used. In our protocol, two parties can establish (n^2 + n) common secret session keys and all the keys can be used. It is seen that our protocol is superior to other protocols. Note that n denotes that two parties send n Diffie-Hellman public keys. In Table 2, we show an example to compare the efficiency of our scheme to the others.

Table 1. The comparison of efficiency.

	[7]	[28]	[23]	[16]	Our Scheme
Numbers of session key	n^2	n^2	n^2	n^2 / n^2	$n^2 + n$
Numbers of session key can be used	$n^2 - 1$	n^2	n^2	$n^2 - 1/ n^2$	$n^2 + n$

Table 2. An example $n=3$.

	[7]	[28]	[23]	[16]	Our Scheme
Numbers of session key	9	9	9	9 /9	12
Numbers of session key can be used	8	9	9	8/9	12

4. Conclusions

In this paper, we have constructed a more efficient MQV Key agreement protocol. (see Table 1). Other protocols establish n^2 common session keys between two parties in one session. Nevertheless, (n^2 + n) common session keys can be established in our extended protocol and what is more, attack is no longer a threat.

Acknowledgment

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC96-2219-E-009-013 and NSC99-2221-E-030-022.

References

[1] Alexandris N., Burmester M., Chrissikopoulos V., and Desmedt Y., "A proven secure public key distribution system," in *3rd Symp. on State and Progress of Research in Crytography*, pp. 30–34, Lecture Notes in Computer Science 330, 1993.

[2] Diffie W. and Hellman M., "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, 1976.

[3] Elminaam D., Kader H., and Hadhoud M., "Evaluating the performance of symmetric encryption algorithms," *International Journal of Network Security,* vol. 10, no. 3, pp. 213-219, 2010.

[4] Faraoun K., "Chaos-based key stream generator based on multiple maps combinations and its application to images encryption," *The International Arab Journal of Information Technology*, vol. 7, no. 3, pp. 231–240, 2010.

[5] Garcia M., Lloret J., Sendra S., and Lacuesta R., "Secure communications in group-based wireless sensor networks," *International Journal of Communication Networks and Information Security*, vol. 2, no. 1, pp. 8-14, 2010.

[6] Harn L. and Lin H., "An authenticated key agreement protocol without using one-way functions," in *Proceedings of the 8th National Conference on Information Security*, pp. 155–160, Kaohsiung, Taiwan, 1998.

[7] Harn L. and Lin H., "Authenticated key agreement without using one-way hash functions," *IEE Electronics Letters*, vol. 37, no. 10, pp. 629–630, 2001.

[8] Hwang M., Lin C., and Lee C., "Improved yen-joye's authenticated multiple-key agreement protocol," *IEE Electronics Letters*, vol. 38, no. 23, pp. 1429–1431, 2002.

[9] Hwang R., Shiau S., and Lai C., "An enhanced authentication key exchange protocol," in *Proceedings of the 17th international conference on Advanced Information Networking and Application*, pp. 202–205, 2003.

[10] IEEE 2000, "IEEE Standard 1363-2000: Standard specifications for public key cryptography," *IEEE*, 2002. Jr J., "Analysis of Venkaiah et al.'s AES design," *International Journal of Network Security,* vol. 9, no. 3, pp. 285-289, 2009.

[12] Kashyap S., Sharma B., and Banerjee A., "A cryptosystem based on DLP $\gamma \equiv \alpha^a \beta^b mod\ p$," *International Journal of Network Security,* vol. 3, no. 1, pp. 95-100, 2006.

[13] Kim M. and Koc C., "Improving the Novikov and Kiselev user authentication scheme," *International Journal of Network Security*, vol. 6, no. 3, pp. 241–245, 2008.

[14] Lee C., Hwang M., and Li L., "A new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343–349, 2003.

[15] Lee N. and Wu C., "Improved authentication key exchange protocol without using one-way hash function," *ACM Operation Systems Review*, vol. 38, no. 2, pp. 85–92, 2004.

[16] Lee N., Wu C., and Wang C., "Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings," *Computers and Electrical Engineering*, vol. 34, no. 1, pp. 12–20, 2008.

[17] Menezes A., Qu M., and Vanstone S., "Some key agreement protocols providing implicit authentication," in *Proceedings of 2nd Workshop Selected Areas in Cryptography*, pp. 22–32, 1995.

[18] Meshram C., "Enhancing the security of public key cryptosystem based on DLP $\gamma \equiv \alpha^a \beta^b$ *(mod p)*," *International Journal of Research and Reviews in Computer Science*, vol. 1, no. 4, pp. 67-70, 2010.

[19] Nyberg K. and Rueppel R., "Weakness in some recent key agreement protocol," *IEE Electronics Letters*, vol. 30, no. 1, pp. 26–27, 1994.

[20] Rasul K., Nuerie N., and Pathan A., "Securing wireless sensor networks with an efficient B+ tree-based key management scheme," *International Journal of Communication Networks and Information Security*, vol. 2, no. 3, pp. 162-168, 2010.

[21] Ravala S. and Tamirisa R., "High secured biometric key generation system for data transfer," *International Journal of Research and Reviews in Computer Science*, vol. 2, no. 1, pp. 152-155, 2011.

[22] Sen J., "A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security*, vol. 1, no. 2, pp. 55-78, 2009.

[23] Shao Z., "Security of robust generalized MQV key agreement protocol without using one-way hash functions," *Computer Standards and Interfaces*, vol. 25, no. 5, pp. 431–436, 2003.

[24] Shim K., "Vulnerabilities of generalized MQV key agreement protocol without using one-way

hash functions," *Computer Standards and Interfaces*, vol. 29, no. 4, pp. 467–470, 2007.

[25] Sramka M., "Cryptanalysis of the cryptosystem based on DLP $\gamma \equiv \alpha^a\beta^b$," *International Journal of Network Security,* vol. 6, no. 1, pp. 80–81, 2008.

[26] Singh S. and Singh M., "Encryption & decryption technique for a symmetric cryptosystem from an arithmetic group," *International Journal of Research and Reviews in Computer Science*, vol. 1, no. 4, pp. 86-89, 2010.

[27] Tripathy S. and Nandi S., "LCASE: lightweight cellular automata-based symmetric-key encryption," *International Journal of Network Security,* vol. 8, no. 3, pp. 243-252, 2009.

[28] Tseng Y., "Robust generalized MQV key agreement protocol without using one-way hash function," *Computer Standards and Interfaces*, vol. 24, no. 3, pp. 241–246, 2002.

[29] Wu T., He W., and Hsu C., "Security of authenticated multiple-key," *IEE Electronics Letters*, vol. 35, no. 5, pp. 391–392, 1999.

[30] Yang C., Lee C., and Hsiao S., "Man-in-the-middle attack on the authentication of the user from the remote autonomous object," *International Journal of Network Security*, vol. 1, no. 2, pp. 81–83, 2005.

[31] Yen S. and Joye M., "Improved authenticated multiple-key agreement protocol," *IEE Electronics Letters*, vol. 34, no. 18, pp. 1738–1739, 1998.

Li-Chin Hwang received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 2001 and in 2003. She is currently working toward the PhD degree in the Department of Computer Science and Engineering at the National Chung Hsing University (NCTU), Taiwan. Her current research interests include information security, cryptography, medical image, and mobile communications.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, 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 received the Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He was a Lecturer of Computer and Communication, Asia University, from 2004 to 2007. From 2007, he was an assistant professor of Photonics and Communication Engineering, Asia University. From 2009, he is an Editorial Board member of International Journal of Network Security and International Journal of Secure Digital Information Age. From 2010, he is now an assistant professor of Library and Information Science, Fu Jen Catholic University. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 60+ articles on the above research fields in international journals.

Min-Shiang Hwang 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. He was a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He obtained 1997, 1998, 1999, 2000, and 2001 Outstanding Research Awards of the National Science Council of the Republic of China. 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 140+ articles on the above research fields in international journals.