INFORMATICA, 2003, Vol. 14, No. 1, 111–120

Simple Generalized Group-Oriented Cryptosystems Using ElGamal Cryptosystem

Chou-Chen YANG, Ting-Yi CHANG, Jian-Wei LI,
Department and Graduate Institute of Computer Science and Information Engineering
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.
e-mail: ccyang@mail.cyut.edu.tw

Min-Shiang HWANG
Department of Information Management
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.
e-mail: mshwang@mail.cyut.edu.tw

Received: December 2002

Abstract. In the generalized group-oriented cryptosystem, the sender can send a conditional message to a group of users such that only the specified sets of users in this group can cooperate to decrypt this message. In this paper, we will use an ElGamal cryptosystem and an elliptic curve ElGamal cryptosystem to achieve the purposes of generalization and group-orientation, respectively. Both of our schemes are more efficient than Tsai *et al.*'s scheme in terms of sender's computational complexity.

Key words: Diffie–Hellman scheme, ElGamal cryptosystem, elliptic curve cryptosystem, group-oriented cryptosystem.

1. Introduction

The concept of group-oriented cryptosystem was first introduced by Desmedt (1987). In the generalized group-oriented cryptosystem (GGOC), a sender sends an encrypted message to a group such that the received message can only be decrypted by the authorized subsets of users in the receiver group. An authorized subset of the receiver group is called an access instance denoted as f. The collection of the access instances for a particular type of message is called the access structure denoted as F. An access structure can be denoted in the disjunctive normal form (DNF), i.e., $F = f_1 + f_2 + \cdots + f_k$. Let $U_1, U_2, \cdots, U_N$ be all of the users in the group, and the access instances $f_1 = U_1U_2U_4$, $f_2 = U_3U_5$, $f_3 = U_7$. The access structure can be represented as $F = U_1U_2U_4 + U_3U_5 + U_7$. The ciphertext sent by a sender can only be decrypted by the cooperation of either U_1, U_2 and U_4 or U_3 and U_5 or U_7 alone. If $F = U_1 + U_2 + \cdots + U_N$, it means the urgent message can be decrypted by any user in the group.

Lin and Chang (1994) proposed a GGOC based on the Diffie–Hellman key distribution scheme (Diffie and Hellman, 1976). Later, Tsai *et al.* (1999) proposed a more efficient GGOC than Lin and Chang's scheme that was also based on the Diffie–Hellman key distribution scheme. However, Lin and Chang's scheme and Tsai *et al.*'s scheme employed none of the existing asymmetric cryptosystems (ElGamal, 1985; Hwang *et al.*, 2002). They proposed new schemes to live up to the requirements of GGOC and used additional asymmetric cryptosystems to encrypt/decrypt the message. The computational complexity on the sender's side increases, causing both the number of users in the access structure and that of the access instances to grow in (Lin and Chang, 1994) and making the number of users in the access structure in (Tsai *et al.*, 1999) go up.

In this paper, we will propose a new GGOC to further reduce the computational complexity on the sender's side, and there will be no symmetric cryptosystem to encrypt/decrypt the message. Our scheme only uses the ElGamal cryptosystem (ElGamal, 1985) to achieve the purpose of generalization and group-orientation. Compared with Tsai *et al.*'s scheme, our scheme performs better in lowering the computational complexity of the sender. On the other hand, many researchers have explored the concept of elliptic curve cryptosystem, which was firstly proposed by Miller (1986) and Koblitz (1987). The elliptic curve cryptosystem provides smaller key sizes, more bandwidth savings and faster implementations, features which are especially attractive to applications of security demands (Koblitz *et al.*, 2000). Taking advantage of such features, we will also propose the elliptic curve version of our proposed GGOC.

This article is organized as follows: In Section 2, we will briefly review Tsai *et al.*'s GGOC. In Section 3, our new GGOC scheme based on ElGamal cryptosystem will be proposed, and the security will be analyzed. Moreover, the elliptic curve version of our proposed GGOC will also be presented. In Section 4, the performance of our schemes and Tsai *et al.*'s scheme will be compared. In Section 5, there will be some discussions. Finally, Section 6 will present our conclusion.

2. Review of Tsai *et al.*'s GGOC

In this section, we shall briefly review Tsai *et al.*'s scheme. Assume that U_0 is the sender, and $U_1, U_2, \cdots, U_N$ are all the users in the receiver group. Let p be a large prime such that $p-1$ has a large prime factor with order q in the Galosis field $GF(p)$. Each user U_i in the group has a secret key x_i in $GF(p)$ and the corresponding public key $y_i = g^{x_i} \bmod p$, for $i = 1, 2, \cdots, N$. Anyone can get the public keys via some authentication service (e.g., the X.509 directory authentication service (Stallings, 1999)). To send the message M to the group, the sender U_0 firstly determines the access structure $F = f_1 + f_2 + \cdots + f_k$ for M. Assume that $U_1, U_2, \cdots, U_n$ $(n <= N)$ are all the users in the access structure. Then U_0 performs the following steps.

Step 1. Choose a random number r in $GF(p)$ and compute $b = g^r \bmod p$.

Step 2. Compute $t_i = (y_i)^r \bmod p$, for $i = 1, 2, \cdots, n$.

Step 3. Choose a random encrypting key Key in $GF(p)$ and compute the ciphertext $C = E_{Key}(M)$, where E is the encryption algorithm in the symmetric cryptosystem such as DES (Smid and Branstad, 1988) and Rijndael (Daemen and Rijem, 1999; Daemen and Rijem, 2001).

Step 4. Compute $r_j = Key \oplus (\prod_{U_i \in f_j} t_i \bmod p)$, for $j = 1, 2, \cdots, k$.

Step 5. Send $\{F, b, r_1, r_2, \cdots, r_k, C\}$ to the receiver group.

After receiving $\{F, b, r_1, r_2, \cdots, r_k, C\}$, the users U_is (for $i = j_1, j_2, \cdots, j_v$) in the access instance f_j can cooperate to decrypt the message by using their secret keys as follows:

Step 1. Compute $t_i = b^{x_i} \bmod p$, for $i = j_1, j_2, \cdots, j_v$.

Step 2. Compute $Key = r_j \oplus (\prod_{U_i \in f_j} t_i \bmod p)$.

Step 3. Recover $M = D_{Key}(C)$, where D is the encryption algorithm in the symmetric cryptosystem.

In Tsai *et al.*'s scheme, each user U_i in the receiver group has the secret key x_i and the corresponding public key y_i in the system. However, to live up to the requirements of GGOC, their scheme requires an additional symmetric cryptosystem to encrypt/decrypt the message.

3. Our Proposed GGOC Schemes

In this section, we will first propose our GGOC scheme with the ElGamal cryptosystem and then present the elliptic curve version of our proposed scheme.

3.1. *GGOC with the ElGamal Cryptosystem*

The parameters (p, q, g, x_i, y_i) are the same as those in Tsai *et al.*'s scheme. Suppose U_0 wants to send the message M to the access structure $F = f_1 + f_2 + \cdots + f_k$, and $U_1, U_2, \cdots, U_n$ are all the users in the access structure. Then U_0 performs the following steps.

Step 1. Choose a random number r in $GF(p)$ and compute $b = g^r \bmod p$.

Step 2. Compute $C_j = M \cdot (\prod_{U_i \in f_j} y_i)^r \bmod p$, for $j = 1, 2, \cdots, k$.

Step 3. Send $\{F, b, C_1, C_2, \cdots, C_k\}$ to the receiver group.

After receiving $\{F, b, C_1, C_2, \cdots, C_k\}$, the users U_is (for $i = j_1, j_2, \cdots, j_v$) in the access instance f_j can cooperate to decrypt the message by using their secret keys as follows:

Step 1. Compute $t_i = b^{x_i} \bmod p$, for $i = j_1, j_2, \cdots, j_v$.

Step 2. Recover $M = C_j \cdot (\prod_{U_i \in f_j} t_i)^{-1} \bmod p$.

In our scheme, the sender encrypts the message by multiplying the users' public keys y_is to be the public key in the original ElGamal cryptosystem. Then, the users U_is in the access instance f_j can cooperate to recover the message M.

Theorem 1. *The users U_is (for $i = j_1, j_2, \cdots, j_v$) in the access instance f_j can cooperate to recover the message M.*

Proof. Because

$$\begin{aligned} C_j &= M \cdot (\prod_{U_i \in f_j} y_i)^r \bmod p \\ &= M \cdot (\prod_{U_i \in f_j} g^{x_i})^r \bmod p \\ &= M \cdot (g^{\sum_{U_i \in f_j} x_i})^r \bmod p, \end{aligned}$$

thus

$$\begin{aligned} M &= C_j \cdot (g^{\sum_{U_i \in f_j} x_i})^{-r} \bmod p \\ &= C_j \cdot (g^{\sum_{U_i \in f_j} x_i \cdot r})^{-1} \bmod p \\ &= C_j \cdot (\prod_{U_i \in f_j} t_i)^{-1} \bmod p. \end{aligned}$$

According to the descriptions above, in our scheme, if the access structure has only one single user and the sender encrypts the message for each user in this access structure, then the function of our scheme is exactly the same as that of the ElGamal cryptosystem.

It is clear that the security of the proposed GGOC is based on the ElGamal cryptosystem, which in turn is based on the intractability of the discrete logarithm problem (DLP). It is very difficult for an adversary to compute the secret key x_i of user U_i from the equation $y_i = g^{x_i} \bmod p$. For the same reason, to obtain the random number r generated by U_0 from the equation $b = g^r \bmod p$ is also difficult. In addition, it is also very difficult for the legal users U_is (for $i = j_1, j_2, \cdots, j_v$) in the access instance f_j to reveal secret keys x_ks of other users U_ks from the equation $t_k = b^{x_k} \bmod p$ ($i \neq k$, $k = j_1, j_2, \cdots, j_v$). On the other hand, to recover M from the message $\{F, b, C_1, C_2, \cdots, C_k\}$ sent by U_0, the adversary has to break the Diffie–Hellman scheme and find all the terms t_is without knowing x_is, $i \in f_j$.

3.2. *GGOC with the Elliptic Curve ElGamal Cryptosystem*

Let E be the elliptic curve defined over a finite field F_{2^m}, and let G be a publicly known base point with order p on E, preferably a generator of E (Koblitz *et al.*, 2000). Each user U_i in the group has a secret key $x_i \in [1, p-1]$ and the corresponding public key $Y_i = x_i \cdot G$, for $i = 1, 2, \cdots, N$. Similarly, suppose U_0 wants to send the message M to

the access structure $F = f_1 + f_2 + \cdots + f_k$, and $U_1, U_2, \cdots, U_n$ are all the users in the access structure. Then U_0 performs the following steps.

Step 1. Choose a random number $r \in [1, p-1]$ and compute the point $B = r \cdot G$.

Step 2. Express M as the x-coordinate of a point P_M on E (Koblitz, 1998). Then, compute $C_j = P_M + (\sum_{U_i \in f_j} Y_i) \cdot r$, for $j = 1, 2, \cdots, k$.

Step 3. Send $\{F, B, C_1, C_2, \cdots, C_k\}$ to the receiver group.

After receiving $\{F, B, C_1, C_2, \cdots, C_k\}$, the users U_is (for $i = j_1, j_2, \cdots, j_v$) in the access instance f_j can cooperate to decrypt the message by using their secret keys as follows:

Step 1. Compute the point $T_i = x_i \cdot B$, for $i = j_1, j_2, \cdots, j_v$.

Step 2. Compute $P_M = C_j - (\sum_{U_i \in f_j} T_i)$ and recover M from the x-coordinate of P_M.

The correctness of the elliptic curve version of our proposed GGOC is described as follows:

Theorem 2. *The users U_is (for $i = j_1, j_2, \cdots, j_v$) in the access instance f_j can cooperate to compute P_M and then recover the message M.*

Proof. Because

$$\begin{aligned} C_j &= P_M + (\sum_{U_i \in f_j} Y_i) \cdot r \\ &= P_M + (\sum_{U_i \in f_j} x_i \cdot G) \cdot r, \end{aligned}$$

thus

$$\begin{aligned} P_M &= C_j - (\sum_{U_i \in f_j} x_i \cdot G) \cdot r \\ &= C_j - (\sum_{U_i \in f_j} x_i \cdot B), \\ &= C_j - (\sum_{U_i \in f_j} T_i). \end{aligned}$$

For the same reason, if the access structure has only one single user, the function of this scheme is exactly the same as that of the elliptic curve ElGamal cryptosystem. The security of the elliptic curve version of GGOC, which is the same as that of the elliptic curve ElGamal cryptosystem, is based on the elliptic curve discrete logarithm problem (ECDLP).

4. Performances and Comparisons

In this section, we shall compare the computational complexity performance of our schemes with that of Tsai *et al.*'s scheme. To analyze the computational complexity, we first define the following notations.

T_{EXP}: the time for computing modular exponentiation.

T_{MUL}: the time for computing modular multiplication.

T_{INV}: the time for computing modular inverse.

T_{XOR}: the time for computing eXclusive-OR operation.

T_{EC_MUL}: the time for computing the multiplication of a number and a point on the elliptic curve.

T_{EC_ADD}/T_{EC_SUB}: the time for computing the addition/subtraction of two points on the elliptic curve.

$T_{E_{Key}(M)}/T_{D_{Key}(C)}$: the time for encrypting/decrypting the message M/C by using the symmetric cryptosystem.

n: the number of different users in the access structure.

m: $m = \sum_{i=1}^{n}(\#(U_i) - 1)$, where $\#(U_i)$ denotes the number of access instances containing U_i.

k: the number of access instances.

v: the number of users in the access instance f_j.

In our GGOC with the ElGamal cryptosystem, to encrypt the message M, the sender U_0 computes b in Step 1, which requires $1 \times T_{EXP}$. Then, in Step 2, the ciphertexts C_is (for $i = 1, 2, \cdots, k$) are computed, which requires $k \times T_{EXP} + (m+1) \times T_{MUL}$. The total computational complexity for encrypting the message is therefore $(k+1) \times T_{EXP} + (m+1) \times T_{MUL}$.

After receiving $\{F, b, C_1, C_2, \cdots, C_k\}$ sent by U_0, U_is (for $i = j_1, j_2, \cdots, j_v$) in the access instance f_j as a whole computes t_is in Step 1, which requires $v \times T_{EXP}$. Then, in Step 2, they can cooperate to recover the message M, which requires $v \times T_{MUL} + 1 \times T_{INV}$. The total computational complexity for decrypting the message is $v \times T_{EXP} + v \times T_{MUL} + 1 \times T_{INV}$.

Like we have just seen in the performance analysis of the GGOC with the ElGamal cryptosystem, the sender's total computations and f_j's computations in the elliptic curve version of our proposed GGOC are $(k+1) \times T_{EC\_MUL} + (m+1) \times T_{EC\_ADD}$ and $v \times T_{EC\_MUL} + v \times T_{EC\_ADD} + 1 \times T_{EC\_SUB}$, respectively.

The computational complexity of Tsai *et al.*'s scheme has been shown in (Tsai *et al.*, 1999). Since T_{EXP} is much larger than T_{MUL}, T_{XOR} and T_{INV}, we only compare the number of T_{EXP} in the following descriptions. According to Table 1, the numbers of T_{EXP} in f_j's computations of both Tsai *et al.*'s scheme and our scheme with the ElGamal cryptosystem increase by v. Due to the sender's computations, the numbers of T_{EXP} in Tsai *et al.*'s scheme and our scheme with the ElGamal cryptosystem are increased by n and k, respectively. Because n and k are different variables, we will have to discuss what scheme is suitable for real-world applications.

On the other hand, the authors of (Koblitz *et al.*, 2000; Schroeppel *et al.*, 1995; Win *et al.*, 1996) have pointed out that the base point G with order p is a 160-bit prime in the

Table 1

Computational complexities of Tsai *et al.*'s scheme and our schemes

	Sender's computations	f_j's computations
Tsai *et al.*'s scheme	$(n+1) \times T_{EXP} + m \times T_{MUL} + k \times T_{XOR} + 1 \times T_{E_{Key}(M)}$	$v \times T_{EXP} + (v-1) \times T_{MUL} + k \times T_{XOR} + 1 \times T_{D_{Key}(C)}$
Our scheme using the ElGamal cryptosystem	$(k+1) \times T_{EXP} + (m+1) \times T_{MUL}$	$v \times T_{EXP} + v \times T_{MUL} + 1 \times T_{INV}$
The elliptic curve version our proposed scheme	$(k+1) \times T_{EC\_MUL} + (m+1) \times T_{EC\_ADD}$	$v \times T_{EC\_MUL} + v \times T_{EC\_ADD} + 1 \times T_{EC\_SUB}$

elliptic curve ElGamal cryptosystem that offers approximately the same level of security as modulus a 1024-bit prime in the ElGamal cryptosystem. T_{EC_MUL} can be expected to be about 8 times faster than T_{EXP} ($8 \times T_{EC\_MUL} = T_{EXP}$). Hence, the sender's computations and f_j's computations in the elliptic curve version are much more efficient.

5. Discussions

In this section, we shall consider a practical application of the GGOC and discuss the three scenarios ($n > k$, $n = k$ and $n < k$). For example, suppose company has N employees and k departments. Here, we can take the company as the receiver group, the departments as the access instances $f_1, f_2, \cdots, f_k$, and the employees as the users $U_1, U_2, \cdots, U_N$.

Case 1: $n > k$
Assume that each department has more than one director. A managing director wants to send the message M to the directors of all the departments such as the personnel department, administrative department etc., and only the directors in the same department can cooperate to decrypt this message. Here, n is the number of directors whom the managing director sends the message to. In this case, no matter how many employees in the same department can cooperate to decrypt the message, n is always greater than k.

Case 2: $n = k$
A managing director wants to send the urgent message M to some specific employees in the company. Each of these employees can decrypt the message independently. The access structure can be presented as $F = U_1 + U_2 + \cdots + U_n$. For the same reason, if a managing director wants to send the urgent message M to all the employees in the company, the access structure can be presented as $F = U_1 + U_2 + \cdots + U_N$. Here, n is equal to k.

Case 3: $n < k$
If the same employee belongs to more than one department at the same time, n is less than k. Obviously, this rarely occurs. However, this situation occurs when GGOC extends to the threshold cryptosystem. In threshold cryptosystems such as (Desmedt and Frankel, 1989; Frankel, 1989; Hwang, 1990), the authorized subsets are all subsets of t or more members of this group. The access structure with the threshold value t can be represented as $F = U_1U_2 \cdots U_t + U_1U_2 \cdots U_{t-1}U_{t+1} + \cdots + U_{N-t+1}U_{N-t+2} \cdots U_N$. The number of access instances is $k = N!/t!(N-t)! = n!/t!(n-t)!$. However, when the GGOC schemes extend to be threshold cryptosystems, they become inefficient. The sender only encrypts the message by using the group's public key in the threshold cryptosystem.

The sender's computations in our scheme using ElGamal cryptosystem are more efficient than that in Tsai *et al.*'s scheme. The elliptic curve version of GGOC can further reduce the computations the sender and f_j have to do. Furthermore, Tsai *et al.*'s scheme requires an additional symmetric cryptosystem to encrypt/decrypt the message, but ours do not.

6. Conclusions

Several GGOCs have been proposed previously (Chang and Lee, 1992; Chang and Lee, 1993; Lin and Chang, 1994). Among those GGOC-related schemes, Tsai *et al.*'s scheme (Tsai *et al.*, 1999), reviewed in this paper, is one of the most efficient. In this article, we have shown that the computational complexity of our scheme using the ElGamal cryptosystem is lower than that of Tsai *et al.*'s scheme. Besides, our elliptic curve version of GGOC is much more efficient in the sender's computations and f_j's computations. Furthermore, Tsai *et al.*'s scheme requires an additional symmetric cryptosystem to encrypt/decrypt the message, while ours do not.

Acknowledgements

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-004.

References

Chang, C.C., and H.C. Lee (1992). A solution to generalized group oriented cryptography. In *IFIP/Sec'92-Singapore Day2/Track2-Cryptography*. pp. 289–299.

Chang, C.C., and H.C. Lee (1993). A new generalized group-oriented cryptoscheme without trusted centers. *IEEE Journal on Selected Area in Communication*, **11**(5), 725–729.

Daemen, J., and V. Rijmen (1999). AES Proposal: Rijndael. *Tech. Rep., Document Version 2*.

Daemen, J., and V. Rijmen (2001). Rijndael, the advanced encryption standard. *Dr. Dobb's Journal*, **26**(3), 137–139.

Desmedt, Y. (1987). Society and group oriented cryptography: A new concept. In *Advances in Cryptology, CRYPTO'87*. pp. 120–127.

Desmedt, Y., and Y. Frankel (1989). Threshold cryptosystem. In *Advances in Cryptology, CRYPTO'89*. pp. 307–315.

Diffie, W., and M. Hellman (1976). New direction in cryptography. *IEEE Transactions on Information Theory*, **22**(6), 472–492.

ElGamal, T. (1985). A public-key cryptosystem and a signature scheme based on discrete logarithms. In *IEEE Transactions on Information Theory*, **IT-31**. pp. 469–472.

Frankel, Y. (1989). A practical protocol for large group oriented networks. In *Advances in Cryptology, CRYPTO'89*. pp. 56–61.

Hwang, M.-Sh., Ch.-Ch. Chang and K.-F. Hwang (2002). An ElGamal-like cryptosystem for enciphering large messages. In *IEEE Transactions on Knowledge and Data Engineering*, **14**(2). pp. 445–446.

Hwang, T. (1990). Cryptosystem for group oriented cryptography. In *Advances in Cryptology, EUROCRYPT'90*. pp. 317–324.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, **48**, 203–209.

Koblitz, N. (1998). Algebraic aspects of cryptography. *Algorithms and Computation in Mathematics*, **3**.

Koblitz, N., A. Menezes and Scott A. Vanstone (2000). The state of elliptic curve cryptography. *Designs, Codes and Cryptography*, **9**(2/3), 173–193.

Lin, C.H., and C.C. Chang (1994). Method for constructing a group-oriented cipher system. *Computer Communications*, **17**(11), 805–808.

Miller, V. (1986). Use of elliptic curves in cryptography. In *Advances in Cryptology, CRYPTO'85*. pp. 417–426.

Schroeppel, R., H. Orman, S. O'Malley and O. Spatscheck (1995). Fast key exchang with elliptic curve systems. In *Advances in Cryptology, CRYPTO'95*. pp. 43–56.

Smid, M.E., and D. K. Branstad (1988). The data encryption standard: Past and future. In *Proc. of the IEEE*, **76**. pp. 550–559.

Stallings, W. (1999).it Cryptography and Network Security: Principles and Practice. Prentice Hall, second edition.

Tsai, J.J., T. Hwang and C.H. Wang (1999). New generalized group-oriented cryptosystem based on Diffie–Hellman scheme. *Computer Communications*, **22**(8), 727–729.

Win, E. De, A. Bosselaers, S. Vandenberghe, P. De Gersem and J. Vandewalle (1996). A fast software implementation for arithmetic operations in $GF(2^n)$. In *Advances in Cryptology, Asiacrypt'96*. pp. 65–76.

C.-C. Yang received his B.S. in Industrial Education from the National Kaohsiung Normal University, in 1980, and his M.S. in Electronic Technology from the Pittsburg State University, in 1986, and his Ph.D. in Computer Science from the University of North Texas, in 1994. He has been an associate professor in the Dept. of Computer Science and Information Engineering since 1994. His current research interests include network security, mobile computing, and distributed system.

T.-Y. Chang received the B.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 1999 and 2001. He is currently pursuing his master degree in Computer Science and Information Engineering from CYUT. His current research interests include information security, cryptography, and mobile communications.

J.-W. Li received the B.S. in Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan, Republic of China, from 1997–2001. He is currently pursuing his M.S. in Computer Science and Information Engineering from CYUT. His current research interests include information security, cryptography, and mobile communications.

M.-S. Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, 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 project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

Nesudėtingas, grupei skirtas, apibendrintas šifravimas, naudojant ElGamal šifravimo sistemą

Chou-Chen YANG, Ting-Yi CHANG, Jian-Wei LI, Min-Shiang HWANG

Apibendrintoje, grupei skirtoje šifravimo sistemoje vartotojas gali siųsti sąlyginį pranešimą vartotojų grupei taip, kad tik išskirtiniai vartotojų pogrupiai, iššifruodami tą žinutę, gali bendrauti grupėje. Tam, kad būtų galima pasiekti apibendrinimo ir grupinio bendravimo tikslus, šiame straipsnyje naudojamos dvi šifravimo sistemos: ElGamal šifravimas ir ElGamal elipsinės kreivės šifravimas. Abi pasiūlytos sistemos yra efektyvesnės už Tsai *et al.* schemą skaičiavimo sudėtingumo siuntėjo pusėje atžvilgiu.