INFORMATICA, 2007, Vol. 18, No. 1, 61–66
© 2007 *Institute of Mathematics and Informatics, Vilnius*

Security Flaw in Simple Generalized Group-Oriented Cryptosystem Using ElGamal Cryptosystem

Chuan-Ming LI, Tzonelih HWANG
Department of Computer Science and Information Engineering, National Cheng Kung University
Tainan, Taiwan 701, R.O.C.
e-mail: licm@ismail.csie.ncku.edu.tw, hwangtl@ismail.csie.ncku.edu.tw

Narn-Yih LEE
Department of Information Management, Southern Taiwan University of Technology
Tainan, Taiwan 710, R.O.C.
e-mail: nylee@mail.stut.edu.tw

Received: April 2005

Abstract. A generalized group-oriented cryptosystem (GGOC) based on ElGamal cryptosystem was proposed by Yang *et al.* in 2003. This study shows that if the authorized decryption sets of users are not properly predetermined in Yang *et al.'s* GGOC, an unauthorized decryption set of users can recover the encrypted message without difficulty. This study also presents an improved protocol to resist such an attack.

Key words: generalized group-oriented cryptosystem, access structure, security.

1. Introduction

In 1987, Desmedt (Desmedt, 1987) first proposed the concept of group-oriented cryptosystem (GOC) in which an encrypted message is sent to a group of users rather than an individual. Only the qualified subsets of users, called positive access instances, can cooperatively decrypt the message. In contrast, any unqualified subset of users, called negative access instance, is not able to correctly decrypt the ciphertext.

Many GOCs and the variants had been proposed in the literature (Chang and Lee, 1993; Frankel, 1990; Harn *et al.*, 2004; Hwang, 1991; Ingemarsson and Simmons, 1991; Ito *et al.*, 1987; Tsai *et al.*, 1999; Yang *et al.*, 2003; Yoon *et al.*, 2004). Recently Yang *et al.* (Yang *et al.*, 2003) utilized the ElGamal cryptosystem (ElGamal, 1985) to propose a generalized group-oriented cryptosystem (GGOC). In Yang *et al.'s* GGOC, the sender can freely determine the positive access instances of the receiving group and encrypts the message for each positive access instance by multiplying the users' public keys. The users in the predetermined positive access instances can cooperate to decrypt the message. Yang *et al.* claimed that, compared with Tsai *et al.'s* scheme (Tsai *et al.*, 1999), their

GGOC performs better in lowering the computational complexity for the sender and no symmetric cryptosystems are used to encrypt/decrypt the message.

This study will show that if the positive access instances are not properly defined in Yang *et al.'s* scheme, a negative access instance can decrypt the ciphertext without difficulty. This study also presents an improved scheme to avoid this security flaw.

The rest of this study is structured as follows. The next section deals with the preliminaries of the GGOC. Section 3 briefly reviews Yang *et al.'s* protocol. In Section 4, we demonstrate the security flaw in Yang *et al.'s* GGOC and then present an improved protocol to avoid this attack. Finally, a short conclusion is given in Section 5.

2. Preliminaries

Let U_0 denotes the sender of a message, and $U = \{U_1, U_2, \ldots, U_n\}$ denotes a receiving group of n users. In the GGOC, the set of all positive access instances is called the positive access structure which denoted as F, and the set of all negative access instances is called the negative access structure which denoted as W. F and W must satisfy following propositions.

PROPOSITION 1. $F \cup W = 2^U$ and $F \cap W = \phi$, where 2^U is the power set of U.

PROPOSITION 2. If f is a positive access instance, then any subset f', $f \subseteq f' \subseteq U$, is also a positive access instance. In other words, a positive access structure should be monotone.

PROPOSITION 3. If w is a negative access instance, then any subset w', $w' \subseteq w \subseteq U$, is also a negative access instance.

DEFINITION 1. Let $Min(F)$ be the minimal set in F, called the minimal access structure. $Min(F)$ is given as

$$Min(F) = \{f \in F | f' \nsubseteq f, \forall f' \in F - \{f\}\}.$$

For convenience, a positive access structure will always be given in the minimal set and simply be called an access structure in this paper. Take a group of four users $U = \{U_1, U_2, U_3, U_4\}$, for example. Suppose there exists an access structure $F = \{\{U_1, U_2, U_3\}, \{U_2, U_3, U_4\}, \{U_1, U_4\}\}$ which allows the ciphertext to be decrypted cooperatively either by U_1, U_2 and U_3 or by U_2, U_3 and U_4 or by U_1 and U_4. The access structure can also be represented in the disjunctive normal form (DNF) as follows

$$F = f_1 + f_2 + f_3 = U_1U_2U_3 + U_2U_3U_4 + U_1U_4,$$

where $f_1 = U_1U_2U_3$, $f_2 = U_2U_3U_4$, and $f_3 = U_1U_4$ are positive access instances.

3. Review of Yang *et al.'s* GGOC

This section briefly reviews Yang *et al.'s* protocol (Yang *et al.*, 2003) as follows. Assume that U_0 is the sender of a message M, and $U_1, U_2, \ldots, U_n$ are all the users in the receiving group. Let p be a large prime such that $p-1$ has a large prime factor q. Each user U_i, for $i = 1, 2, \ldots, n$, in the system has a private key x_i, $x_i \in GF(p)$, and the corresponding public key

$$y_i = g^{x_i} \pmod p,$$

where g is a generator of order q in $GF(p)$. To send the message M to the receiving group, U_0 firstly determines the access structure $F = f_1 + f_2 + \ldots + f_k$, and then performs the following steps.

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

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

Step 3. Send $\{F, R, C_1, C_2, \ldots, C_k\}$ to the receiving group.

After receiving $\{F, R, C_1, C_2, \ldots, C_k\}$ from the sender, the users in the access instance f_j ($f_j = U_{j_1} U_{j_2} \cdots U_{j_v}$) can cooperate to decrypt the message by using their secret keys as follows.

Step 1. Compute $t_i = R^{x_i} \pmod p$, for $i = j_1, j_2, \ldots, j_v$.

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

In Yang *et al.'s* protocol, the sender encrypts the message by multiplying the users' public keys y_i to be the public key in the original ElGamal cryptosystem. Then, the users U_i in the positive access instance f_j can cooperate to decrypt the message. According to the above descriptions, if each access instance has only one single user, Yang *et al.'s* GGOC is exactly the same as the ElGamal cryptosystem.

4. Attack on Yang *et al.'s* GGOC and the Improvement

4.1. *The Security Flaw in Yang et al.'s GGOC*

Yang *et al.* claimed that their GGOC is more efficient than Tsai et al.'s scheme (Tsai *et al.*, 1999) in terms of sender's computational complexity and no symmetric cryptosystems are used. However, we find that if the access structure is not properly defined, a negative access instance is able to decrypt the ciphertext. Now, we first use an example to demonstrate this security flaw.

Let the access structure F be predetermined by U_0 as

$$F = f_1 + f_2 + f_3 = U_1U_2U_3 + U_2U_3U_4 + U_1U_4.$$

U_0 chooses a random number $r \in GF(p)$, and then computes $R = g^r \pmod p$ and the ciphertext $\{C_1, C_2, C_3\}$ as

$$\begin{aligned}
C_1 &= M \cdot (y_1 \cdot y_2 \cdot y_3)^r \qquad (\mathrm{mod}\ p),\\
C_2 &= M \cdot (y_2 \cdot y_3 \cdot y_4)^r \qquad (\mathrm{mod}\ p),\\
C_3 &= M \cdot (y_1 \cdot y_4)^r \qquad (\mathrm{mod}\ p).
\end{aligned}$$

U_0 sends $\{F, R, C_1, C_2, C_3\}$ to the receiving group. Obviously, the ciphertext can be legally decrypted either by U_1, U_2 and U_3 or by U_2, U_3 and U_4 or by U_1 and U_4. However, although U_1 is not allowed to decrypt the ciphertext alone, he/she can calculate that

$$\begin{aligned}
(C_1/C_2) \cdot C_3 &= \left(\frac{M \cdot (y_1 \cdot y_2 \cdot y_3)^r}{M \cdot (y_2 \cdot y_3 \cdot y_4)^r}\right) \cdot (M \cdot (y_1 \cdot y_4)^r)\\
&= M \cdot y_1^{2r}\\
&= M \cdot R^{2x_1} \qquad (\mathrm{mod}\ p)\,.
\end{aligned}$$

Thus, U_1 can easily decrypt the ciphertext alone by computing

$$M = ((C_1/C_2) \cdot C_3) \cdot R^{-2x_1} \qquad (\mathrm{mod}\ p).$$

According to the above example, we generalize the security flaw in Yang *et al.'s* GGOC as follows. Let $F = f_1 + f_2 + \ldots + f_k$ be the access structure. Suppose f_a, f_b and f_c, where a, b, $c \in \{1, 2, \ldots, k\}$, are positive access instances in F and

$$f_a = (f_b \cup f_c) - (f_b \cap f_c).$$

Let the sender of a message M send the ciphertext $\{F, R, C_1, C_2, \ldots, C_k\}$ to the receiving group. A negative access instance f'_h, where $f'_h = f_a \cap f_b$, can recover the message M by computing

$$M = ((C_b/C_c) \cdot C_a) \cdot \left(\prod_{U_i \in f'_h} R^{-2x_i}\right) \qquad (\mathrm{mod}\ p).$$

4.2. *Improvement*

Since the ciphertext C_j, for $j = 1, 2, \ldots, k$, in Yang *et al.'s* GGOC is the product of the message M and $(\prod_{U_i \in f_j} y_i)^r$, a negative access instance f'_h can utilize the multiplication and division of ciphertexts to eliminate some unknown factors in C_j. Hence, any method which prevents the negative access instances from eliminating the unknown factors in the ciphertext C_j can overcome the security flaw. One possible solution is that, instead of computing the product of the message M and $(\prod_{U_i \in f_j} y_i)^r$, the sender calculates the ciphertexts C_j as

$$C_j = M \oplus \left(\prod_{U_i \in f_j} y_i \right)^r \pmod{p},$$

where $\oplus$ denotes the bit-wise exclusive OR operation. To decrypt the ciphertext, the users in the access instance f_j $(f_j = U_{j_1} U_{j_2} \cdots U_{j_v})$ compute $t_i = R^{x_i} \pmod{p}$, for $i = j_1, j_2, \ldots, j_v$, and recover the message $M = C_j \oplus (\prod_{U_i \in f_j} t_i) \pmod{p}$.

The only difference between the improvement and Yang *et al.'s* GGOC is the calculation of the ciphertext C_j, as the improvement uses XOR operation rather than the multiplication. Thus, the security of the improvement is also based on the ElGamel cryptosystem, which in turn is based on the difficulty of solving the discrete logarithm problem. It is difficult for a malicious user to compute the secret key x_i of user U_i from the public key $y_i = g^{x_i} \pmod{p}$. It is also difficult for an adversary to obtain the random number r from the equation $R = g^r \pmod{p}$. Besides, it is very difficult for the legal users U_i (for $i = j_1, j_2, \ldots, j_v$) in the access instance f_j to disclose the secret keys x_k of other users U_k from the equation $t_k = R^{x_k} \pmod{p}$ (for $k \neq i$ and $k = j_1, j_2, \ldots, j_v$). On the other hand, to recover M from the message $\{F, R, C_1, C_2, \ldots, C_k\}$ sent by U_0, the malicious user has to either break the Diffie-Hellman scheme (Diffie and Hellman, 1976) or find all the terms t_i, $i \in f_j$. Moreover, unlike Yang *et al.'s* GGOC, a negative access instance f'_h in the improvement cannot utilize the multiplication or division of ciphertexts to eliminate the unknown factors in the ciphertexts C_j. Thus, the improvement is secure against the security flaw proposed in this study.

5. Conclusions

This study demonstrates a security flaw in Yang *et al.'s* GGOC, and fixes the protocol to avoid such an attack.

Acknowledgments

The authors thank Mr. Sheng-Wei Liao for helpful discussions. The authors also thank the National Science Council of the Republic of China, Taiwan for financially supporting this research under Contract NO. NSC 95-2221-E-218-030.

References

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

Desmedt, Y. (1987). Society and group oriented cryptography: a new concept. In *Advances in Cryptology: Proceedings of Crypto'87, LNCS*. pp. 120–127.

Diffie, W., and M.E. Hellman (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, **22**(6), 644–654.

ElGamal, T. (1985). A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, **IT31**, 469–472.

Frankel, Y. (1990). A practical protocol for large group oriented networks. In *Advances in Cryptology: Proceedings of Eurocrypto'89, LNCS*. pp. 55–61.

Harn, L., C.-Y. Lin and T.-C. Wu (2004). Structured multisignature algorithms. In *IEE Proceedings – Computers and Digital Techniques*, **151**(3). pp. 231–234.

Hwang, T. (1991) Cryptosystem for group oriented cryptography. In *Advances in Cryptology: Proceedings of Eurocrypto'90, LNCS*. pp. 352–360.

Ingemarsson, I., and G.J. Simmons (1991). A protocol to set up shared secret schemes without the assistance of a mutually trusted party. In *Advances in Cryptology: Proceedings of Eurocrypto'90, LNCS*. pp. 266–282.

Ito, M., A. Saito and T. Nishizeki (1987). Secret sharing schemes realizing general access structure. In *Proc. IEEE Global Telecommunication Conf., Globecom'87*. IEEE Press, Piscat-away, New Jersey. pp. 99–102.

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.

Yang, C.-C., T.-T. Chang, J.-W. Li and M.-S. Hwang (2003). Simple generalized group-oriented cryptosystem using elgamal cryptosystem. *INFORMATICA*, **14**(1), 111–120.

Yoon, E.-J., E.-K. Ryu and K.-Y. Yoo (2004). Efficient remote user authentication scheme based on generalized ElGamal signature scheme. *IEEE Transactions on Consumer Electronics*, **50**(2), 568–570.

C.-M. Li was born in Tainan Taiwan, in 1964. He received the MS degree in computer science from National Cheng Kung University in 1994. He is currently a PhD student at Department of Computer and Information Engineering, Nation Cheng Kung University. His research interests include data security and cryptography.

T. Hwang was born in Tainan Taiwan, in 1958. He received his undergraduate degree in National Cheng Kung University in 1980, and the MS and PhD degrees in computer science from the University of Southwestern, Louisiana, USA, in 1988. He is presently a professor of Department of Computer and Information Engineering, Nation Cheng Kung University. His research interests include cryptology, network security and coding theory.

N.-Y. Lee was born in Chiayi, Taiwan, in 1967. He received the BS degree in information science from Tunghi University in 1990 and the MS degree in applied mathematics from Chung-Hsing University in 1992 and the PhD degree in information engineering from National Cheng-Kung University in 1996. He is currently a professor in the Information Management Department, Southern Taiwan University of Technology, Tainan, Taiwan. His research interests in information security, cryptography, and smart card system.

Nesudėtingos apibendrintosios grupinės kriptografinės sistemos, naudojančios ElGamalio kriptografinę sistemą, apsaugos trūkumas

Chuan-Ming LI, Tzonelih HWANG, Narn-Yih LEE

Yang ir kiti 2003 m. pasiūlė apibendrintąją grupinę kriptografinę sistemą (GGOC), kurios pagrindą sudaro ElGamalio algoritmas. Straipsnyje parodyta, kad jei įgaliojimų suteikimo vartotojams aprašai nėra tinkamai apibrėžti GGOC sistemoje, tuomet neįgaliotieji vartotojai gali užšifruotą pranešimą nesunkiai dešifruoti. Pasiūlytas geresnis protokolas, kuris apsaugo nuo tokios pranešimo dešifravimo atakos.