Cryptosystem for Group Oriented Cryptography

Tzonelih Hwang

National Cheng Kung University

Institute of Information Engineering

Tainan, Taiwan, R. O. C.

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 352-360, 1991.

Abstract *A practical non–interactive scheme is proposed to simultaneously solve several open problems in group oriented cryptography. The sender of the information is allowed to determine the encryption/decryption keys as well as the information destination without any coordination with the receiving group. The encrypted message is broadcasted to the receiving group and the receivers may authenticate themselves for legitimacy of the information directly from the ciphertext. The security of the scheme can be shown to be equivalent to the difficulty of solving the discrete logarithm problem.*

Key Words: Group Oriented Cryptography, Threshold Scheme, Chinese Remainder Theorem, Diffie–Hellman Key Distribution Scheme, Lagrange Interpolating Polynomial.

1. Introduction

When messages are intended for a group oriented society (or a company), there are several needs for the information sender/receiver depending on the nature of the information. The information maybe so important that it is readable only when a set of authorized receivers agree to decipher it. It may be so urgent that anyone of the authorized receivers could decipher it, whereas the unauthorized user is not allowed to do so. The message can also be transmitted in private to a particular user as usual. These problems and other related ones have been addressed in [Desmedt 88 , Frankel 89 , Desmedt 89 , Hwang 89].

Desmedt has proposed solutions to these problems [Desmedt 88] based on [

Goldreich 87] but are impractical and interactive [Desmedt 89]. Frankel has proposed a protocol to solve some of these problems [Frankel 89]. However, his protocol requires the use of trusted clerks or tamperfree modulars to distribute the encrypted message, thus may be impractical for use in large group oriented networks. In their recent paper, Desmedt and Frankel propose a non–interactive scheme based on the idea of threshold scheme discussing mainly the problem of deciphering the message by a group of people [Desmedt 89]. In their scheme, a trusted center has to distribute the shadows of the deciphering key in private to the authorized receivers. It is not very convenient if the deciphering key is renewed or if the number of the authorized receivers work together to decipher the message is changed.

In this paper, we propose a scheme based on the Diffie–Hellman key distribution scheme [Diffie 76] and Shamir's secret sharing scheme [Shamir 79] to solve these open problems simultaneously.

The sender, depending on the nature of the information, may broadcast the encrypted message to the destination company in such a way that either the ciphertext is decipherable only when a group of authorized receivers work together or it can be deciphered by anyone inside the authorized group, or it is decipherable only by a particular member. There are no assumptions of the existence of tamperfree modulars and trusted clerks or centers.

2. The Protocol

Assume that each member A_i inside the company A holds a secret $x_{A_i} \in \{ 1, \ldots , p-1 \}$ and publishes the value

$$Y_{A_i} = g^{x_{A_i}} \pmod{p}$$

where p is a large prime and g is a fixed primitive element in GF(p) [Diffie 76]. Each member A_i is also assigned a public prime number N_i ($N_i > p$). Note, $N_i \neq N_j$ if $i \neq j$.

2.1 Messages for a Group of Receivers

The sender may send a message M to a group G of n members inside A in such a way that M is readable only when any subset of t members ($t \leq n$) from G agree to decipher the message.

[The Sender]:

(1) Obtain the public values g, p, N_i and Y_{A_i} ($1 \leq i \leq n$, $A_i \in G$) from the public directory of **A** .

(2) Generate a secret random number $x_s \in \{ 1, \ldots , p-1 \}$.

Compute

$$Y_s = g^{x_s} \pmod{p}$$

$$K_{sA_i} = g^{x_{A_i} x_s} \pmod{p}, \quad 1 \leq i \leq n .$$

Repeat this step if $K_{sA_i} = K_{sA_j}$ for all $i \neq j$.

(3) Construct a polynomial h(x) of degree t–1 with random coefficients over GF(P),

$$h(x) = a_{t-1} x^{t-1} + \ldots + a_1 x + K \pmod{p}.$$

K will serve as the encryption key later.

(4) Encipher M into C_1 using the key K

$$C_1 = E_K (M),$$

where E denotes the predetermined encryption algorithm and D is the corresponding decryption algorithm.

(5) Compute n shadows $W_i = h(K_{sA_i})$ (mod p), $1 \leq i \leq n$.

(6) Compute a common solution C_2 using Chinese Remainder Theorem (CRT) from the following system of equations:

$$X = W_i \pmod{N_i}, \qquad 1 \leq i \leq n \ .$$

(7) Broadcast the ciphertext C

$$C = (C_1 , C_2 , N , Y_s)$$

where $N = N_1 N_2 \dots N_n$ is the product of all N_i's.

The purpose of introducing CRT here is to compute a common solution (C_2) of all shadows so that the ciphertext (C) can be broadcasted to the receiving group and every authorized receiver in the receiving group may compute his own part. Alternatively, the sender may send W_i directly to the member A_i. In this case, these N_i's and CRT are no more required.

[The Receiver]:

(1) The authorized user A_i can authenticate himself as a legal receiver by verifying

$$N_i \mid N \ .$$

(2) A_i computes his shadow W_i by

$$C_2 = W_i \pmod{N_i} \ .$$

Then he computes

$$K_{sA_i} = (Y_s)^{x_{A_i}} \pmod{p},$$

(3) When t authorized receivers (assume that, without loss of generality, they are A_1, A_2, ... , A_t) work together, the key K can be computed by using Shamir's (n,t) threshold scheme [Shamir 79].

(4) $M = D_K(C_1)$.

2.2 Message for Anyone in the Group

The sender may send M to G in the company A such that anyone in G can recover M. However, anyone outside the group G may not be able to recover M. Here, we extended the idea of the conference key distribution scheme in [Laih 88] to solve this problem.

[The Sender]:

(1) The sender first performs the steps (1), (2), (3), (4) and (5) as in section 2.1 .

(2) Compute t–1 extra shadows such that

$$W_i' = h(i) \quad (\text{mod } p), \qquad 1 \le i \le t-1 .$$

Assume that $K_{sA_i} > t$ for all i.

(3) Compute the common solution C_2 using CRT from the following equations

$$X = W_i' \quad \text{mod } p_i, \quad 1 \le i \le t-1$$

$$X = W_j \quad \text{mod } N_i, \quad 1 \le j \le n$$

where p_i's are distinct public primes ($p_i > p$) and $p_i \ne N_j$ for all i and j.

(4) Broadcast $C = (C_1, C_2, N, Y_s)$, where $N = p_1 p_2 \cdots p_{t-1} N_1 N_2 \cdots N_n$.

[The authorized Receiver A_j]

(1) Compute the t–1 extra shadows by

$$C_2 = W_i' \quad \text{mod } p_i, \quad 1 \le i \le t-1 .$$

(2) Compute $K_{sA_j} = (Y_s)^{x_{A_j}} \quad (\text{mod } p)$.

(3) Obtain K using Shamir's (n,t) threshold scheme.

(4) $M = D_k(C_1)$.

Notice that for the message intended to everyone in the group, it will be advantageous to use a polynomial h(x) of degree one (i.e., t=2). In this case, only one extra shadow is required.

It is clear that the sender can communicate with a particular member i inside the company A in private by using the common key K_{sA_i} to encipher/decipher the message.

3. Discussion & Security Analysis

Shamir's threshold scheme is applied to solving the group–oriented secret sharing problem. It is obvious that the encryption key K cannot be obtained easily even if t–1 authorized receivers are acting in collusion.

If the cryptanalyst tries to compute X_{A_i} from Y_{A_i}, he has to solve the discrete logarithm problem [Diffie 76].

To obtain K_{sA_i} from W_i (= C_2 mod N_i), the conspirators has to solve X from the polynomial [Purdy 74, Denning 82]

$$W_i = a_{t-1} X^{t-1} + ... + a_1 X + K \pmod{p},$$

with unknown coefficients. Therefore, this attack won't be successful.

4. Conclusion

We have proposed a scheme to simultaneously solve several open problems in group oriented cryptography. The new scheme is particularly useful in the case that the information sender has the authority to decide the destination of the information. It can also be modified to solve the case that the receiving group decides the destination of the information. In this scheme, since only one ciphertext is needed, the ciphertext can be broadcasted to the destination.

The scheme works without the use of trusted clerks, centers or tamperfree modulars. The encryption/decryption key and the number of receivers that have to work together to recover the plaintext can be renewed easily by the sender without any coordination with the destination. Furthermore, both the conventional or public–key cryptosystems are applicable to this scheme. The security of this scheme depends on the difficulty of computing the discrete logarithm problem.

[Acknowledgment]

The author would like to thank the referee of this paper for the comments and suggestions. This work was supported by the National Science Council of the Republic of China as research project NSC 80–0408–E–006–02.

[References]

<1> [Denning 82] D. E. R. Denning. *Cryptography and Data Security.* Addison – Wesley, Reading, Mass., 1982.

<2> [Diffie 76] W. Diffie and M. E. Hellman. "New directions in cryptography". *IEEE Trans. Inform. Theory*, IT–22(6):644–654, November 1976.

<3> [Desmedt 88] Y. Desmedt. "Society and group oriented cryptography : a new

concept". In C. Pomerance, editor, Advances in Cryptology, *proc. of Crypto'87* (Lecture Notes in Computer Science 293),pages 120–127. Springer–Verlag,1988. Santa Barbara, California, U.S.A., August 16–20.

<4> [Desmedt 89] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems". presented at *Crypto'89*. Santa Barbara, California, U.S.A. Aug. 20–24.

<5> [Frankel 89] Y. Frankel. "Practical Protocol for Large Group Oriented Networks". Presented at *Eurocrypt'89*, Houthalen, Belgium, to appear in Advances in Cryptology. Proc. of *Eurocrypt'89* (Lecture Notes in Computer Science), Springer–Verlag,April 1989.

<6> [Goldreich 87] O. Goldreich, S. Micali, and A. Wigderson. "How to play any mental game". In Proceedings of the *Nineteenth ACM symp.* Theory of Computing, STOC, pages 218–239, May 25–27, 1987.

<7> [Hwang 89] T. Hwang, "On the Secure Communications of Group Oriented Socienties", 1990 *IEEE International Symposium on Info. Theory.*

<8> [Laih 88] C. S. Laih, L. Harn, and J. Y. Lee, "A new threshold scheme and its application on designing the conference key distribution cryptosystem.", *Info. processing letters*, North–Holland Vol. 32, No. 3, 24 Aug. 1989.

<9> [Purdy 74] G. p. Purdy, " A High Security Log–in Procedure", *Commun. ACM* vol. 17(8), pp. 442–445 Aug. 1974.

<10> [Shamir 79] A. Shamir. How to share a secret. *Commun. ACM*, 22:612–613, November 1979.