A New Secure Broadcasting Method Based On ElGamal's Scheme

Chu-Hsing Lin* Ching-Te Wang**

*Department of Computer and Information Sciences, Tunghai University,
Taichung, Taiwan 407, R.O.C.
**National Chin-Yi Institute of Technology,
Taichung, Taiwan 411, R.O.C.

ABSTRACT

In this paper, we shall present a new scheme to solve the problem of secure broadcasting in a network. By the use of the proposed scheme, a sender can send secret messages to a group of users, but only the legitimate receivers can recover the plain messages. Our cryptosystem is based on the ElGamal's public-key scheme and the security is the same as that of the ElGamal's. Further, all of the computations in the scheme can be performed efficiently.

Keywords: Broadcasting, ElGamal's scheme, RSA, Security, Single key.

植基於葉伽瑪法之安全廣播策略

林祝興　　王清德

摘　要

在本文中，我們將提出一新策略以處理安全廣播網路系統中訊息傳送之問題。利用我們所提之方法，在網路中，傳送者送出一密文，對於系統中接收到密文的多個使用者，僅有合法的授權者才能夠解開此密文。我們的安全廣播系統植基於葉伽瑪公開金匙技術，而傳送中之資訊安全度建立在葉伽瑪法之安全度上。再者，於方法中皆能有效的處理各項計算式。

1. Introduction

The privacy and integrity of data transmission have become more and more important in the age of computers and communications. Secret data stored or transmitted in computer systems need to be well protected. In a large-scale telecommunication network, messages transmission among users have to be controlled and managed carefully. A broadcasting system has the property that a single transmisson from a user may be received simultaneously by several other users. There are several schemes for the problem of secure broadcasting. For instance, the secure broadcasting schemes in [2,3] are based on the RSA public-key scheme, and the scheme in [9] is based on the ElGamal's public-key scheme.

In 1993, Jan and Yu [9] proposed a broadcasting system based on the ElGamal's public-key scheme. They employ the ElGamal's scheme to devise the encryption, decryption methods, and the Chinese Remainder Theorem to compute an integer PB as the receivers location in the single key concept[8]. They also calculate the parameter B as a base of the single key. After receiving the broadcasting messages, a receiver can use the two parameters PB and B to recover the original messages if he is legitimate.

In this paper, we propose a new secure broadcasting cryptosystem based on the ElGamal's public-key scheme. In order to send secret messages to the other users, we design the cryptosystem in such a way that only the authorized receivers can decipher the ciphertext, while the illegal users can't get any plaintext. Our cryptosystem will employ the Elgamal's public-key scheme and two mathematical theorems. By the use of our method, we can find that the parameters PB and B will be combined and the length of the transmitted messages will be reduced. Moreover, the security of our cryptosystem is the same as that of the ElGamal's public-key scheme.

In next section, we will review the ElGamal's scheme and state the mathematical theorems, which are used in our proposed cryptosystem. In section 3, we will discuss in detail our proposed cryptosystem scheme and give an example to explain the scheme. The security analysis of the scheme will be appeared in section 4. Finally, we have some

conclusions about this paper in the last section.

2. Background of the scheme

In this section, let us review some techniques and mathematical background which will be used in the scheme. Firstly, we will discuss some properties of the ElGamal's public-key scheme. Let P be a large prime number and g be a primitive element in GF(P). Let $U = \{U_1, U_2, ..., U_n\}$ be a group of n users in the broadcasting network system. Each user U_i has an identification number id_i , a secret key x_i , and a public key y_i, where $x_i \in [1, P-2]$ and $y_i = g^{x_i}(modP)$.

If user U_a wants to send a message M to user U_b. User U_a selects a random number $r \in [1, P-2]$, and calculates $C_r = g^r(modP)$, then U_a uses the value r and the public key y_b of user U_b to encipher the message M ; i.e. , $C_M = M \cdot y_b^r(modP)$. The value r is kept secret and the two values C_r, C_M are transmitted to user U_b. Now , U_b can use C_r, C_M to decipher and get the plaintext M as following :

$$\begin{aligned} & C_M \cdot ((C_r)^{x_b})^{-1}(modP) \\ &= M \cdot y_b^r((g^r)^{x_b})^{-1}(modP) \\ &= M \cdot (g^{x_b})^r((g^r)^{x_b})^{-1}(modP) \\ &= M \cdot (g^{x_b r})(g^{r x_b})^{-1}(modP) \\ &= M(modP). \end{aligned}$$

Where $(\cdot)^{-1}$ indicates the multiplicative inverse of $(\cdot)$ with modulus P.

Secondly, let us discuss the following theorems for the encryption and decryption procedures such that only legal receivers can reveal the messages.

Theorem 2.1

Let $q_1, q_2, ..., q_n$ are pairwise relatively primes, and let $\{x_i\}_{i=1,2,...,n}$ be a set of nonnegative integers. If $Max\{x_i\}_{1 \le i \le n} < n < Min\{q_j\}_{1 \le j \le n}$, then there exists a constant $X = \sum_{i=1}^{n} Q_i p_i N_i \ mod\ n \times \prod_{i=1}^{n} q_i$ such that $\lfloor \frac{X}{q_i} \rfloor mod\ n = x_i$, where $Q_i = n \times \prod_{j \neq i}^{n} q_i, Q_i p_i \equiv n(mod\ n \times q_i)$ and $N_i = \lceil \frac{x_i \times q_i}{n} \rceil$.

For the proof of the theorem and how to find the values p_i, one can consult [1,2].

Example 2.1

Let $q_1 = 7, q_2 = 8, q_3 = 9, q_4 = 11, q_5 = 13, q_6 = 17$ and $x_1 = 3, x_2 = 4, x_3 = 1, x_4 = 4, x_5 = 0, x_6 = 2$, then

$$Q_i = n \times \prod_{j \neq i}^{n} q_j,$$

so $Q_1 = 1050192, Q_2 = 918918, Q_3 = 816816, Q_4 = 668304, Q_5 = 565488, Q_6 = 432432.$

$$N_i = \lceil \frac{x_i \times q_i}{n} \rceil,$$

we obatin $N_1 = 4, N_2 = 6, N_3 = 2, N_4 = 8, N_5 = 0, N_6 = 6.$

$$Q_i p_i \equiv n (mod\ n \times q_i),$$

we select $p_1 = 2, p_2 = 1, p_3 = -4, p_4 = 5, p_5 = 6, p_6 = 2$. So, $X = \sum_{i=1}^{n} Q_i p_i N_i mod\ n \times \prod_{i=1}^{n} q_i = (1050192 \times 2 \times 4 + 918918 \times 1 \times 6 + 816816 \times (-4) \times 2 + 668304 \times 5 \times 8 + 565488 \times 6 \times 0 + 432432 \times 2 \times 6) mod (7351344) = 39301860\ mod\ 7351344 = 2545140.$

$$\lfloor \frac{X}{q_1} \rfloor mod\ n = \lfloor \frac{2545140}{7} \rfloor mod\ 6 = 3 = x_1$$

$$\lfloor \frac{X}{q_2} \rfloor mod\ n = \lfloor \frac{2545140}{8} \rfloor mod\ 6 = 4 = x_2$$

$$\lfloor \frac{X}{q_3} \rfloor mod\ n = \lfloor \frac{2545140}{9} \rfloor mod\ 6 = 1 = x_3$$

$$\lfloor \frac{X}{q_4} \rfloor mod\ n = \lfloor \frac{2545140}{11} \rfloor mod\ 6 = 4 = x_4$$

$$\lfloor \frac{X}{q_5} \rfloor mod\ n = \lfloor \frac{2545140}{13} \rfloor mod\ 6 = 0 = x_5$$

$$\lfloor \frac{X}{q_6} \rfloor mod\ n = \lfloor \frac{2545140}{17} \rfloor mod\ 6 = 2 = x_6.$$

Theroem 2.2

Let $r_1, r_2, ...and\ r_n$ be n ($n \geq 2$) elements from GF(P), and P be a prime number. Then there exists an integer Q such that

$$r_i = (P+1) - \{\lceil \frac{Q}{(P+1)^{i-1}} \rceil mod(P+1)\},\ for\ i = 1,2,...,n$$

pf: Let

$$Q = (P+1)^n - \sum_{i=1}^{n} r_i(P+1)^{i-1}. \qquad Then,$$

$$\frac{Q}{(P+1)^{i-1}} = (P+1)^{n-i+1} - \left(\sum_{j=1}^{i-1} r_j(P+1)^{j-i} + r_i + \sum_{j=1}^{n-i} r_{i+j}(P+1)^j \right) = a - r_i - b,$$

where

$$a = (P+1)^{n-i+1} - \sum_{j=1}^{n-i} r_{i+j}(P+1)^j,\ and$$

$$b = \sum_{j=1}^{i-1} r_j(P+1)^{j-i},$$

we can see that

$$a\ mod(P+1) = 0$$

and

$$b = \sum_{j=1}^{i-1} r_j(P+1)^{j-i} < \sum_{j=1}^{i-1} P(P+1)^{j-i} = 1 - (P+1)^{1-i} \leq 1.$$

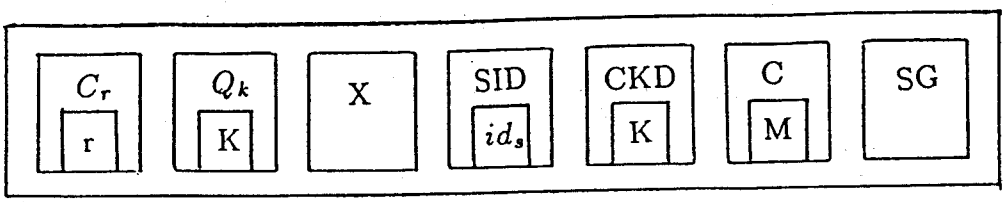
Therefore, we have

$$(P+1) - \{\lceil \frac{Q}{(P+1)^{i-1}} \rceil mod(P+1)\} = (P+1) - \{\lceil a - r_i - b \rceil\} = r_i.$$

3. Our proposed scheme

In this section, we shall present a cryptosystem to solve the problem of secure broadcasting. Based on the Elgamal's scheme, there are two public values P and g in the system. P is a large prime number and g is a primitive element in GF(P). Assuming $U = \{U_1, U_2, ..., U_n\}$ be a group of n users in the broadcasting network system. Let R is the receiver's group, $R \subseteq U$, U_s is the sender and U_r is the receiver, $U_s, U_r \in U, id_1, id_2, ..., id_n$ are user's id numbers which are pairwise relatively prime, and $n < id_i < P$, i=1,2,...,n. Each user U_i has his secret key x_i and public key y_i,

where $gcd(x_s, P-1) = 1$. Suppose K is the communication key , $K \in [1, P-2]$. The format of the broadcasting message is given as follows:



where

C_r : ciphertext of r;

Q_k : ciphertext of communication key K computed by Theroem 2.2;

X : the receiver's location by using Theorem 2.1;

SID : Ciphertext of sender's id number and is enciphered by the key K;

CKD : ciphertext of communication key K by using K;

C : ciphertext of the messages M by using K;

SG : ciphertext of the sender's signature.

Algorithm 3.1 [Message encryption for the sender U_s]

Input. The sending messages M, identification numbers id_i and the public keys y_i, i=1,2,...,n , the secret key x_s of U_s, the two public values P and g.

Output. C_r, Q_k, X, SID, CKD, C, SG

Step1. [Select a communication key K]

Select K value, $K \in [1, P-2]$.

Step2. [Compute C_r, Q_k, by using ElGamal's scheme, Theroem 2.2.]

(1) Select a random number r, $r \in [1, P-2]$.

(2) Compute

$$b_i = \begin{cases} K \cdot y_i^r (mod P) + 1, & \text{if } u_i \in R; \\ 0, & \text{otherwise,} \end{cases} \qquad \text{i=1,2,...,n.}$$

(3) Let

$$t_i = \begin{cases} i, & \text{if } U_i \in R; \\ 0, & \text{otherwise,} \end{cases} \qquad \text{i=1,2,...,n.}$$

(4) Compute

$$C_r = g^r (mod P),$$

$$Q_k = (P+1)^n - \sum_{i=1}^{n} b_i (P+1)^{i-1}.$$

Step3. [Compute X by using Theorem 2.1.]

Compute X such that

$$\lfloor \frac{X}{id_i} \rfloor mod\ n = t_i, \qquad i = 1, 2, ..., n.$$

Step4.[Encrypt the messages id_s, K, M using K by ElGamal's scheme.]

Compute the SID, CKD, C

$$SID = id_s (C_r)^K (mod P),$$
$$CKD = K \cdot (C_r)^K (mod P),$$
$$C = M \cdot (C_r)^K (mod P).$$

Step5. [Compute SG by using the Euclidean Algorithm[4] to solve the congruence.]

$$K = r \cdot y_s + x_s \cdot SG (mod P - 1).$$

Step6. [Send the broadcasting messages.]

The format is (C_r,Q_k, X, SID, CKD, C, SG).

Algorithm 3.2 [Message decryption for the receiver]

Input. The receiver id_r and secret key x_r,C_r,Q_k,X,SID,
CKD, C, SG, the two public values P and g.

Output. The plaintext M.

Step1. [Compute the t_r from X using Theorem 2.1.]

$$Compute\ t_r = \lfloor \frac{X}{id_r} \rfloor mod\ n.$$
$$If\ t_r = 0\ then\ STOP.$$

Step2. [Compute the b_r from Q_k by using Theroem 2.2.]

$$Compute\ b_r = (P+1) - \{\lceil \frac{Q_k}{(P+1)^{t_r-1}} \rceil mod(P+1)\}.$$

$$If\ b_r = 0\ then\ STOP.$$

Step3. [Compute the K using C_r and b_r by ElGamal's scheme.]

$$K\ mod\ P = (b_r - 1) \cdot ((C_r)^{x_r})^{-1} (modP).$$

Step4. [Compute the K' using CKD, and check with Step3.]

$$K' = CKD((C_r)^K)^{-1} (modP)$$

$$If\ K' \neq K\ then\ STOP.$$

Step5. [Decrypt the ciphertext C using K and C_r by ElGamal's scheme.]

$$M\ mod\ P = C \cdot ((C_r)^K)^{-1} (modP).$$

Step6. [Compute the sender's id_s number using SID,C_r,and K by ElGamal's scheme.]

$$id_s\ mod\ P = SID((C_r)^K)^{-1} (modP).$$

Step7. [Check the signature]

$$Compute\ \ S = (C_r)^{y_s} \cdot (y_s)^{SG} (modP).$$

If $S = g^K mod\ P$ then the message M is sent by U_s else the message M is invalid.

Example 3.1

Let $U = \{U_1, U_2, ..., U_6\}$ be six users in the cryptosystem and their keys are listed in the table 1. The public key values P = 31, g=3.

USER	Public key y_i	Secret key x_i	User id_i
1	29	9	7
2	26	5	8
3	20	8	9
4	19	4	11
5	9	2	13
6	16	6	17

Table 1. Public keys and Secret keys

Suppose user U_1 wants to send a messages M = "NORTH" to U_3 and U_4. To encipher the messages M, we use 2 digits to stand for each character, that is A=01, B=02,...,Z=26. Now, we present the encryption and decryption steps as follows.

The encryption steps

Step1. Let K =10.

Step2. (1) Let r =11.

(2) $b_1 = 0$, $b_2 = 0$,

$b_3 = Ky_3^r mod P + 1 = 10 \cdot 20^{11} mod 31 + 1 = 9$,

$b_4 = Ky_4^r mod P + 1 = 10 \cdot 19^{11} mod 31 + 1 = 8$,

$b_5 = 0$, $b_6 = 0$.

(3) Let $t_1 = 0, t_2 = 0, t_3 = 3, t_4 = 4, t_5 = 0, t_6 = 0$.

(4) Compute $C_r = g^r (mod P) = 3^{11} mod 31 = 13$,

$Q_k = (P+1)^n - \sum_{i=1}^{n} b_i (P+1)^{i-1}$

$= 32^6 - (0 + 0 + 9 \cdot 32^2 + 8 \cdot 32^3 + 0 + 0) = 1073470464.$

Step3. $\lfloor \frac{X}{7} \rfloor mod 6 = 0$, $\lfloor \frac{X}{8} \rfloor mod 6 = 0$, $\lfloor \frac{X}{9} \rfloor mod 6 = 3$,

$\lfloor \frac{X}{11} \rfloor mod 6 = 4$, $\lfloor \frac{X}{13} \rfloor mod 6 = 0$, $\lfloor \frac{X}{17} \rfloor mod 6 = 0$.

$X = \sum_{i=1}^{6} Q_i p_i N_i mod 6 \times \prod_{i=1}^{6} q_i$

$= (816816 \cdot (-4) \cdot 5 + 668304 \cdot 5 \cdot 8) mod (7351344) = 3044496.$

Step4. $SID = id_s (C_r)^K (mod P) = 7 \cdot 13^{10} mod 31 = 4.$

$CKD = K(C_r)^K (mod P) = 10 \cdot 13^{10} mod 31 = 19.$

M ="NORTH"=14 15 18 20 08.

$C = M \cdot (C_r)^K (mod P).$

$14(13)^{10} (mod 31) = 8.$

$15(13)^{10} (mod 31) = 13.$

$18(13)^{10} (mod 31) = 28.$

$20(13)^{10} (mod 31) = 7.$

$8(13)^{10} (mod 31) = 9.$

C =08 13 28 07 09.

Step5. $K = r \cdot y_s + x_s \cdot SG(mod P - 1)$,

$10 = 11 \cdot 29 + 9 \cdot SG(mod30)$, SG=9.

Step6. U_1 broadcasts these messages:

[13,1073470464,3044496,4,19,(08,13,28,07,09),9].

The decryption steps of the receiver U_3 are described as follows.

The decryption steps

Step1. $t_3 = \lfloor \frac{X}{id_3} \rfloor modn = \lfloor \frac{3044496}{9} \rfloor mod6 = 3.$

Step2. $b_3 = (P+1) - \{\lceil \frac{Q_k}{(P+1)^{t_3-1}} \rceil mod(P+1)\}$

$= 32 - \{\lceil \frac{1073470464}{(32)^2} \rceil mod(32)\} = 9.$

Step3. $K = (b_3 - 1)((C_r)^{x_3})^{-1}(modP) = 8(13^8)^{-1}(mod31)$

$= 8(13^{-1})^8(mod31) = 8 \cdot 12^8 mod31 = 10.$

Step4. $K' = CKD((C_r)^K)^{-1}(modP) = 19(13^{10})^{-1}(mod31)$

$= 19(13^{-1})^{10}(mod31) = 19 \cdot 12^{10} mod31 = 10.$

step5. $M = C \cdot ((C_r)^K)^{-1}(modP).$

$8((13)^{10})^{-1}(mod31) = 8 \cdot 12^{10} mod31 = 14.$

$13((13)^{10})^{-1}(mod31) = 13 \cdot 12^{10} mod31 = 15.$

$28((13)^{10})^{-1}(mod31) = 28 \cdot 12^{10} mod31 = 18.$

$7((13)^{10})^{-1}(mod31) = 7 \cdot 12^{10} mod31 = 20.$

$9((13)^{10})^{-1}(mod31) = 9 \cdot 12^{10} mod31 = 8.$

Therefore, M = 14 15 18 20 08 = "NORTH".

Step6. $id_s = SID((C_r)^K)^{-1}(modP) = 4(13^{10})^{-1} mod31 = 7.$

Step7. $S = (C_r)^{y_s} \cdot (y_s)^{SG}(modP) = 13^{29} \cdot 29^9(mod31) = 25.$

$g^K(modP) = 3^{10}(mod31) = 25.$

$S = g^K(modP)$,

which means that the message is sent by the user U_1.

4. Analysis of the presented Scheme.

In this section, we shall analyze the security of the presented scheme. From algorithm 3.2, we know that if someone wants to break our cryptosystem, he must know

the value of K. The value of K is computed by C_r, b_r, and x_r in step 3. The value of b_r can be computed by Q_k and t_r. The value of t_r can be computed by id_r and X. The values of C_r, Q_k, and X are mixed in the broadcasting messages. The value of x_r is the secret key of the receiver U_r. If an intruder wants to reveal the secret key x_i of U_i by knowing the associated public key y_i, he has to break the ElGamal's scheme. Therefore, the security of our cryptosystem is rest on the ElGamal's public-key scheme.

Further, We shall consider the computational and storage complexity of the proposed scheme. First, we analyze the computational complexity. The computational complexity relies on that of obtaining the integers X and Q_k in algorithm 3.1 and revealing b_r in algorithm 3.2. Before obtain the integer X, we must compute all of the integers Q_i,N_i,p_i, i=1,2,...,n. For the computation of all integers Q_i, i=1,2,...,n, it requires n multiplications and n divisions. For the computation of all integers N_i, i=1,2,...,n, it requires n multiplications and n divisions. For the computation of all integers p_i, i=1,2,...,n, it needs $n(0.843 \cdot \ln(n \cdot q) + 1.47)$ divisions operation on average[4]. For the computation of integer X, it requires n additions, 2n multiplications and one modular operation. Therefore, to obtain the integer X, it requires totally n additions, 4n multiplications, $2n + n(0.843 \cdot \ln(n \cdot q) + 1.47)$ divisions and one modular operation. Moreover, to obtain the integer Q_k, it requires n additions and $n + \log_2 n$ multiplications, if the Honer's rule is applied. To reveal one b_j, it requires $\log_2 j$ multiplications, one division, two additions and one modular operation.

Finally, the number of bits required to represent the public parameters Q_k, X, C_r, C are $n\lceil\log_2(P+1)\rceil$, $n\lceil\log_2(P+1)\rceil$, $\lceil\log_2(P+1)\rceil$, $\lceil\log_2(P+1)\rceil$, respectively, if there are n users in the broadcasting network system. Therefore, totally the storage needed is propertional to $2(n+1)\lceil\log_2(P+1)\rceil$.

5. Conclusions

We have proposed a new scheme to solve the problem of broadcasting in a network. In our cryptosystem, the encryption, decryption methods are based on ElGamal's scheme. The sender can arbitrarily select some users who are authorized to reveal the messages. After the legitimate receivers accepted the messages, he can decrypt the ciphertext and check the sender's signature. In the system, the parameters of transmit-

ted messages are reduced and the security of the cryptosystem is also the same as the ElGamal's scheme. Further, all of the computations in the scheme can be performed efficiently.

References

[1] Chang, C. C. and Chen, C. P., "A Key-Lock-Pair mechanism based upon Generalized Chinese Remainder Theorem," Journal of the Chinese Institute of Engineers, Vol. 9, No. 4, 1986, pp. 383-390.

[2] Chang, C. C. and Lin, C. H., "A Cryptosystem for Secure Broadcasting,", Proceedings of National Science Council, Vol. 12, No. 4, July 1988, pp. 233-239.

[3] Chen, W. T. and Chiou, G. H., "Secure Broadcasting Using the Secure Lock.", IEEE Trans. on Software Engineering, Vol. 15, No. 8, Aug. 1989, pp. 929-934.

[4] Denning, D. E. R., Cryptography and Data Security, Addision-Wesley, Reading, Mass., 1982.

[5] Diffie, W. and Hellman, M., "New Directions in Cryptography," IEEE Trans. Inform. Theory, Vol.IT-22, 6 (Nov. 1976), pp. 644-654.

[6] ElGamal, T., "A Public-key Cryptosystem and A Signature Scheme Based on Discrete Logarithms," IEEE Trans. on Information Theory, Vol.IT-31, 1985, pp. 469-472.

[7] Gifford, D. K., "Cryptographic Sealing for Information Secrecy and Authentications," CACM, Vol. 25, No. 4, 1982, pp. 274-286.

[8] Jan, J.K., "A Single-Key Access Control Scheme in Information Protection System," Information Science, 51, 1990, pp. 1-11.

[9] Jan, J.K. and Yu, C.D., "Secure Broadcasting in the ElGamal Public-Key Scheme," The Third Conference On Information Security, May, 1993.

[10] Lin, C.H., "On the Design of a Conference Key Distribution Scheme," Tunghai Journal, Vol. 34, June, 1993, pp. 729-742.

[11] Rivest, R.L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystem," CACM, Vol. 21, No. 2, Feb. 1978, pp. 120-126.