Control and Computers, Vol. 20, No. 2, 1992

A SECURE BROADCASTING SCHEME BASED ON DISCRETE LOGARITHMS

Chin-Chen Chang and Shin-Jia Hwang
Institute of Computer Science and Information Engineering
National Chung Cheng University, Chiayi, Taiwan 62107 ROC

Abstract

In this article, a new broadcasting scheme based on El-gamal's public key cryptosystem and signature scheme is proposed. Without any truster's help, the user who uses the new scheme can send one copy to many recipients at the same time, but only dedicated recipients are able to recover the broadcasting message.

Key Words:
Secure broadcasting, cryptosystem, public key, digital signature, Chinese remainder theorem

1. Introduction

What is a secure broadcasting? Generally, secure broadcasting can be seen as a point-to-multipoint secure communication; that is, a sender broadcasts a message to many recipients at the same time. For reasons of security, the broadcasting messages should be known only by the recipients who "need to know." Therefore, a broadcasting message should be encrypted by the sender and can be decrypted by the recipients who have the right to the information.

However, in most current systems when data are transmitted over such a broadcast channel, the channel is always treated as a point-to-point link and no use is made of the valuable point-to-multipoint feature [1]. If a point-to-point cryptosystem is used in broadcasting networks, the sender encrypts the same message into many different ciphertexts for each recipient who needs to know and then broadcasts the ciphertexts through the broadcast channel separately. This is rather inefficient. Hence, it is important to have a secure broadcasting scheme for point-to-multipoint communication. By the scheme, the sender can encrypt a message into only one copy of ciphertext and then broadcast this ciphertext once. The recipients will get this ciphertext at the same time, but only those who need to know are able to decrypt this ciphertext and obtain the desired messages.

Recently, Chiou and Chen [2] proposed a scheme using "secure lock." Their problem can be stated as follows: We are given a group G of N users in a broadcast network, where each user can communicate directly with every other user through the broadcast channel, but on a need-to-know basis. Suppose that a sender wants to send a message M just to a group U of users, where $U \subseteq G$. The ciphertext of M should be decipherable by the users in U but not every other user in G. Chiou and Chen's scheme has the following properties: (1) the scheme broadcasts only one copy of ciphertext, that is, the sender can encrypt the broadcasting message into one secret message; (2) an encryption/decryption key used to encrypt the broadcasting message is randomly selected by the senders and that key is sent to the recipients safely, so the recipients in the broadcast network need not store any extra keys, and (3) the sender does not need any help from the truster to broadcast or encrypt/decrypt the messages. However, Chiou and Chen's scheme does not take the authentication of sender into consideration. That is, they do not consider the sender's signature in the broadcasting system.

To enhance this, we propose a broadcasting scheme based on El-gamal's public key cryptosystem and signature scheme [3]. Our scheme not only has the above three properties, but also can authenticate the sender itself. Because our scheme is based on the Chinese remainder theorem and El-gamal's public key cryptosystem, we shall review these two in the next section. We present our scheme in the Section 3 and give an example to illustrate the scheme in Section 4. The security analysis and discussions appear in Section 5. Section 6 provides conclusions.

2. A Review of El-gamal's Public Key Cryptosystem and the Chinese Remainder Theorem

We first review El-gamal's public key cryptosystem. Let there be two users, say, user A and user B, in the cryptosystem. Here user B has a secret key D_B and a public key (α, E_B, P), where α, E_B, and P satisfy the following three conditions: (1) P is a large prime number and P - 1 has at least one large prime factor in order to guarantee that computing discrete logarithms is difficult [3] (we call this "discrete logarithm's condition"); (2) α is a primitive element mod P; and (3) $E_B \equiv \alpha^{D_B} \pmod P$. Suppose that user A wants to send a message M to user B, where $0 \leq M \leq P - 1$. User A should select a random integer k between 0 and P-1. The corresponding ciphertext is the pair (C_1,C_2), where $C_1 \equiv \alpha^k \pmod P$ and $C_2 \equiv (E_B)^k M \pmod P$. After receiving this ciphertext, user B uses the decryption equation, $M \equiv ((C_1)^{D_B})^{-1} C_2 \pmod P$, to decrypt the ciphertext (C_1, C_2).

The signature scheme of El-gamal is described as follows. Suppose that user B wants to sign the message M that will be sent to A, where $0 \le M \le P-1$. First, B selects a random integer k' such that $\gcd(k', P-1) = 1$, where $0 \le k' \le P-1$, and $\gcd(x, y)$ means the greatest common divisor of x and y. The signature is the pair (R, S), where $R \equiv \alpha^{k'} \pmod{P}$ and $M \equiv D_B R + S k' \pmod{(P-1)}$. User A uses the authentication equation, $\alpha^M \equiv E_B{}^R R^S \pmod{P}$, to verify whether or not the message is sent from B.

However, there is an important restriction to El-gamal's public key cryptosystem. That is, the same random number k cannot be repeatedly used to encrypt any two different messages [3]. For example, user A encrypts two different messages M_1 and M_2, by using the same k as their encryption keys. The corresponding ciphertexts, $(C_{1,1}, C_{1,2})$ and $(C_{2,1}, C_{2,2})$, are computed as follows:

$C_{1,1} \equiv \alpha^k \pmod{P}$, $C_{1,2} \equiv D_B{}^k M_1 \pmod{P}$,

and $C_{2,1} \equiv \alpha^k \pmod{P}$, $C_{2,2} \equiv D_B{}^k M_2 \pmod{P}$.

Then M_2 can be computed from $M_1/M_2 \equiv C_{1,2}/C_{2,2} \pmod{P}$ easily if M_1 is known. El-gamal's signature scheme has the same restriction. If the random number k' is used more than once then the secret key can be recovered. In this article, we call this feature the "random number restriction."

From El-gamal's public key cryptosystem, we see that El-gamal's has an excellent property: there is no obvious relation between the enciphering of M_3, M_4, and $(M_3)(M_4)$, or any other simple function of M_3 and M_4 [3]. For example, two different messages, M_3 and M_4, are encrypted by user A, the corresponding ciphertexts, $(C_{3,1}, C_{3,2})$ and $(C_{4,1}, C_{4,2})$, are computed as follows:

$C_{3,1} \equiv \alpha^k \pmod{P}$, $C_{3,2} \equiv D_B{}^k M_3 \pmod{P}$,

and $C_{4,1} \equiv \alpha^{k'} \pmod{P}$, $C_{4,2} \equiv D_B{}^{k'} M_4 \pmod{P}$,

where k and k' are two different random integers.

Obviously, we could not find any relations between $(C_{3,1}, C_{3,2})$ and $(C_{4,1}, C_{4,2})$. This is an excellent property that is not provided by the other known cryptosystems.

Now we introduce the Chinese remainder theorem (CRT). The interested reader should consult [4] for more information.

Let $N_1, N_2, \ldots, N_m$ be m positive integers that are pairwise coprimes, and let $R_1, R_2, \ldots, R_m$ be m positive integers, and let $L = N_1 * N_2 * N_3 * \ldots * N_m$. Then the set of congruence equations

$X \equiv R_1 \pmod{N_1}$

$\vdots$

$X \equiv R_j \pmod{N_j}$, where "$\equiv$" denotes the congruence sign,

$\vdots$

and $X \equiv R_m \pmod{N_m}$

have a common solution X that is in the range of $[1, L-1]$ and $X \equiv \left(\sum_{j=1}^{m} \left(\frac{L}{N_j}\right) * R_j * F_j\right) \bmod L$, where $F_j * \left(\frac{L}{N_j}\right) \equiv 1 \pmod{N_j}$. □

Our broadcasting scheme will use the CRT, El-gamal's public key cryptosystem, and El-gamal's signature scheme. In the next section we present our scheme.

3. The Scheme

In this section, a new broadcasting scheme based on El-gamal's public key cryptosystem and El-gamal's signature scheme is presented. Let $G = \{U_1, U_2, \ldots, U_n\}$ be a set of n users in a broadcasting network. Let the user U_j have a secret key D_j, a public key (α_j, E_j, P_j), and a user identification number ID_j, where D_j and (α_j, E_j, P_j) satisfy the conditions of El-gamal's secret key and public key and $0 < ID_j < P_j$, for $j = 1, 2, \ldots, n$. Note that all P_j's satisfy the discrete logarithm's condition stated in Section 2, and $P_i \ne P_j$, for $i \ne j$ and $1 \le i, j \le n$. A public directory containing all users' IDs and their public keys is published in the broadcasting network. The following depicts the format of a public directory.

Table 1
A public directory

User	U_1	U_2	U_3	...	U_n
ID number	ID_1	ID_2	ID_3	...	ID_n
Pubic key	(a_1, E_1, P_1)	(a_2, E_2, P_2)	(a_3, E_3, P_3)	...	(a_n, E_n, P_n)

Our scheme adopts a format of sealed objects similar to Gifford's [5]. That format of sealed objects is depicted in Figure 1.

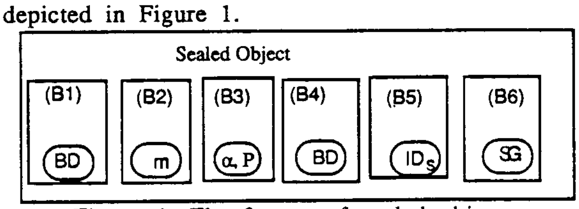

Figure 1. The format of sealed objects.

Our format of sealed objects has six blocks, B1, B2, B3, B4, B5, and B6. The first block, B1, provides the information to recover the broadcasting secret key BD. B2 is the exact ciphertext of the broadcasting message M. B3 is the part of a public key. B4 is used to make the validation of BD. B5 is the ciphertext of the sender's identification number, ID_s, which is used to help the legal recipient know who the sender is. B6 is the ciphertext of the signature, SG, which is used to authenticate the sender. In our scheme, the sender broadcasts the sealed objects instead of the original message.

Suppose that U_s wants to broadcast a message to h recipients, $U_{j_1}, U_{j_2}, \ldots$, and U_{j_h}, where $U_{j_i} \in G - \{U_s\}$, for $i = 1, 2, \ldots, h$. Our scheme is divided into two parts: the sender's part and the recipient's part. They are described in the following sections.

3.1 The Sender's Part

Step1 (Constructing Broadcasting Keys)

First, the sender U_s chooses a large prime number P that satisfies the discrete logarithm's condition, where $P > P_s$, a large prime number as a part of the sender's public key, and $P \neq P_i$ for $i = 1,2, \ldots, n$. Then U_s chooses a secret key BD satisfying that $0 < BD < P$ and $0 < BD < P_{j_i}-1$, for $i=1,2, \ldots, h$. Then the corresponding public key is the triple (α, BE, P), where $\alpha \in \{1,2,\ldots,P-1\}$, $BE \equiv \alpha^{BD} \pmod{P}$, and $(\alpha, BE, P) \neq (\alpha_i, E_i, P_i)$, for $i = 1,2, \ldots, n$. Therefore, B3 is the pair (α, P).

Step 2 (Encrypting Broadcasting Message)

The sender chooses a random number k_1 from the set $\{0,1,\ldots,P-1\}$, U_s encrypts the broadcasting message M into the ciphertext $(C_{2,1}, C_{2,2})$, where $C_{2,1} \equiv \alpha^{k_1} \pmod{P}$, and $C_{2,2} \equiv m(BE^{k_1}) \pmod{P}$, and $0 \leq M \leq P-1$. So B2 is the pair $(C_{2,1}, C_{2,2})$.

Step 3 (Computing B1)

The sender selects a random number k_2 from the set $\{0,1,\ldots, P-1\}$. Then the following ciphertexts are computed: $(C_{j_1,1}, C_{j_1,2})$, $(C_{j_2,1}, C_{j_2,2})$, ... ,$(C_{j_h,1}, C_{j_h,2})$ by $C_{j_x,1} \equiv \alpha_{j_x}^{k_2} \pmod{P_{j_x}}$ and $C_{j_x,2} \equiv BD(E_{j_x})^{k_2} \pmod{P_{j_x}}$, for $x=1,2,\ldots, h$. Using CRT, a common solution $C_{1,1}$ can be obtained from the following congruence equations:

$$C_{j_1,1} \equiv C_{1,1} \pmod{P_{j_1}},$$
$$C_{j_2,1} \equiv C_{1,1} \pmod{P_{j_2}},$$
$$\vdots$$
$$C_{j_h,1} \equiv C_{1,1} \pmod{P_{j_h}},$$
$$0 \equiv C_{1,1} \pmod{P_{j_{h+1}}},$$
$$\vdots$$
and $0 \equiv C_{1,1} \pmod{P_{j_n}}$,

where $P_{j_{h+1}}, P_{j_{h+1}}, \ldots$,and P_{j_n} correspond to $U_{j_{h+1}}, U_{j_{h+1}}, \ldots, U_{j_n}$, which are in the set $G - \{U_{j_1}, U_{j_2}, \ldots, U_{j_h}\}$.

Similarly, he can compute $C_{1,2}$ satisfying the following congruence equations:

$$C_{j_1,2} \equiv C_{1,2} \pmod{P_{j_1}},$$
$$C_{j_2,2} \equiv C_{1,2} \pmod{P_{j_2}},$$
$$\vdots$$
$$C_{j_h,2} \equiv C_{1,2} \pmod{P_{j_h}},$$
$$0 \equiv C_{1,2} \pmod{P_{j_{h+1}}},$$
$$\vdots$$
and $0 \equiv C_{1,2} \pmod{P_{j_n}}$,

where $P_{j_{h+1}}, P_{j_{h+1}}, \ldots$,and P_{j_n} correspond to $U_{j_{h+1}}, U_{j_{h+1}}, \ldots, U_{j_n}$, which are in the set $G - \{U_{j_1}, U_{j_2}, \ldots, U_{j_h}\}$.

So B1 is the pair $(C_{1,1}, C_{1,2})$.

Step 4 (Encrypting BD)

The sender chooses a random number k_3 from the set $\{0,1,\ldots, P-1\}-\{k_1\}$. Then $C_{4,1} \equiv \alpha^{k_3} \pmod{P}$ and $C_{4,2} \equiv BD(BE)^{k_3} \pmod{P}$ are computed. So B2 is the pair $(C_{4,1}, C_{4,2})$.

Step 5 (Encrypting the Sender's ID)

The sender chooses a random number k_4 from the set $\{0,1,\ldots, P-1\}-\{k_1, k_3\}$. Then $C_{5,1} \equiv \alpha^{k_4} \pmod{P}$ and $C_{5,2} \equiv ID_s(BE)^{k_4} \pmod{P}$ are computed. That is, B5 is the pair $(C_{5,1}, C_{5,2})$.

Step 6 (Broadcasting Signature)

SG is computed by the following procedures:

1. Choose a random number k' from the set $\{0,1,\ldots, P_s-1\}$ where k' satisfies that $\gcd(k', P_s-1) = 1$.
2. Compute $R=(\alpha_s)^{k'} \pmod{P_s}$.
3. Finding an S satisfying the equation $M = D_sR + Sk' \pmod{P_s-1}$.

Step 7 (Encrypting an SG)

The sender chooses two different random numbers k_5 and k_6 from the set $\{0,1,\ldots, P-1\} - \{k_1, k_3, k_4\}$. The ciphertext of R is the pair (RC_1, RC_2), where $RC_1 \equiv (\alpha)^{k_5} \pmod{P}$ and $RC_2 \equiv R(BE)^{k_5} \pmod{P}$. The ciphertext of S is the pair (SC_1, SC_2), where $SC_1 \equiv (\alpha)^{k_6} \pmod{P}$ and $SC_2 \equiv S(BE)^{k_6} \pmod{P}$. So B6 is $((RC_1, RC_2),(SC_1, SC_2))$.

Step 8 (Broadcasting)

The sender broadcasts a set of sealed objects {B1, B2, B3, B4, B5, B6} in the broadcast network. Noted that in order to follow the random number restriction presented in Section 2, the random numbers k_1, k_3, k_4, k_5, and k_6 selected by the senders are different.

3.2 The Receiver's Part

Suppose that a legal recipient U_{jx} gets the set of sealed objects sent by U_s, where $1 \leq X \leq h$.

Step 1 (Recovering BD)

The recipient U_{jx} computes the pair $(C_{jx,1}, C_{jx,2})$,where $C_{jx,1} \equiv C_{1,1} \pmod{P_{jx}}$ and $C_{jx,2} \equiv C_{1,2} \pmod{P_{jx}}$. Then U_{jx} uses the decryption equation $BD \equiv C_{jx,2}((C_{jx,1})^{D_{jx}})^{-1} \pmod{P_{jx}}$ to recover BD.

Step 2 (Checking BD)

U_{jx} can recover another BD' from B4 by using the equation $BD' \equiv C_{4,2}((C_{4,1})^{BD})^{-1} \pmod{P}$. If BD = BD', then BD is the correct broadcasting secret key; otherwise BD is incorrect.

Step 3 (Recovering M)

U_{jx} recovers M by using $M \equiv C_{2,2}((C_{2,1})^{BD})^{-1} \pmod{P}$.

Step 4 (Recovering ID_s)

U_{jx} recovers the sender identification number ID_s by using the decryption equation $ID_s \equiv C_{5,2}((C_{5,1})^{BD})^{-1} \pmod{P}$. Thus U_{jx} knows who the sender is.

Step 5 (Authenticating)

U_{jx} recovers SG=(R, S) by using equations $R \equiv RC_2((RC_1)^{BD})^{-1} \pmod{P}$ and $S \equiv SC_2((SC_1)^{BD})^{-1} \pmod{P}$. U_{jx} finds (α_s, D_s, P_s) in the public directory according to the entry number ID_s. From the authentication equation $\alpha_s^M \equiv (E_s)^R R^S \pmod{P_s}$, U_{jx} can verify whether or not message M is sent from U_s.

4. An Example

In this section, we give an example to illustrate our scheme. The public key, secret key, and identification number of each user of the broadcasting network are listed in the following.

	U_1	U_2	U_3	U_4	U_5
ID number	1	2	3	4	5
Public key	(8,11,61)	(3,52,67)	(6,24,53)	(9,2,79)	(11,85,89)
Secret key	5	9	4	2	3

Suppose that U_1 wants to broadcast the message M = 39 and only the recipients, U_2 and U_3, have the ability to decrypt the broadcasting ciphertext. Now we follow the procedures described in Section 3 to compute each sealed object.

4.1 The Sender's Part

Again, suppose that U_1 is the sender and U_2, U_3 are two legal recipients in the broadcasting network.

Step 1 (Constructing Broadcasting Keys)

The sender computes a secret key BD = 4 and a public key (5, 41, 73), where P = 73, α = 5, and BE = 41 = 5^4 mod 73. Then B3 is the pair (5, 73).

Step 2 (Encrypting Broadcasting Message)

The sender chooses k_1=3. Then the pair ($C_{2,1}$, $C_{2,2}$) is computed, where $C_{2,1} = 52 = 5^3$ mod 73 and $C_{2,2} = 59 = 39(41^3)$ mod 73. So B2 is the pair (52, 59).

Step 3 (Computing B1)

The sender selects $k_2 = 2$. First, U_1 encrypts BD into ($C'_{2,1}$, $C'_{2,2}$) for U_2 and ($C'_{3,1}$, $C'_{3,2}$) for U_3 b y computing $C'_{i,1} \equiv \alpha_i^{k_2}$ (mod P_i) and $C'_{i,2} \equiv BD(E_i^{k_2})$ (mod P_i), for i = 1,2. So $C'_{2,1} = 9 = 3^2$ mod 67, $C'_{2,2} = 29 = 4(52^2)$ mod 67, $C'_{3,1} = 36 = 6^2$ mod 53, and $C'_{3,1} = 25 = 4(24^2)$ mod 53. By CRT, a common solution $C_{1,1}$ can be computed by evaluating the following congruence equations: $C'_{2,1} \equiv C_{1,1}$ (mod P_2), $C'_{3,1} \equiv C_{1,1}$ (mod P_3), $0 \equiv C_{1,1}$ (mod P_1), $0 \equiv C_{1,1}$ (mod P_4), and $0 \equiv C_{1,1}$ (mod P_5).

So $C_{1,1} = (\frac{L}{67})*9*(\frac{L}{67})^{-1} + (\frac{L}{53})*36*(\frac{L}{53})^{-1}$ mod L
= (22731223*9*66 + 28735697*36*26) mod 1522991941
= 801168388.

Similarly, we have another common solution $C_{1,2}$ by evaluating the following congruence equations: $C'_{2,2} \equiv C_{1,2}$ (mod P_2), $C'_{3,2} \equiv C_{1,2}$ (mod P_3), $0 \equiv C_{1,2}$ (mod P_1), $0 \equiv C_{1,2}$ (mod P_4), and $0 \equiv C_{1,2}$ (mod P_5).

Therefore, $C_{1,2} = (\frac{L}{67})*29*(\frac{L}{67})^{-1} + (\frac{L}{53})*25*(\frac{L}{53})^{-1}$ mod L = (22731223*29*66+ 28735697*25*26) mod 1522991941 = 1266086232.

Thus, B1 = (801168388, 1266086232).

Step 4 (Encrypting BD)

The sender chooses $k_3 = 4$. U_1 computes $C_{1,1} = 5^4$ mod 73 =41 and $C_{1,1} = 4(41)^3$ mod 73 =16. Thus B4 = (41, 16).

Step 5 (Encrypting the Sender's ID)

The sender chooses $k_4 = 5$. U_1 computes $C_{5,1} = 5^5$ mod 73 =59 and $C_{5,2} = 1(41)^5$ mod 73=18. Then B5=(59, 18).

Step 6 (Broadcasting signature)

The sender chooses k'=7. The sender's signature, SG, of M is the pair (R, S). Here R = $(\alpha_1)^{k'}$ mod $P_1 = 8^7$ mod 61 = 33. And because S has to satisfy the equation 39 $\equiv$ 5*33+ 7*S (mod 60), we have S = 42.

Step 7 (Encrypting an SG)

The sender chooses k_5=2 and k_6=6. U_1 computes $RC_1 = 5^2$ mod 73 =25, $RC_2 = 33(41)^2$ mod 73 =66, $SC_1 = 5^6$ mod 73 =3, and $SC_2 = 42(41)^6$ mod 73 =44. Then B6 = ((25, 66), (3, 44)).

Step 8 (Broadcasting)

Finally, U_1 broadcasts the set of sealed objects {B1, B2, B3, B4, B5, B6} in the broadcast network.

4.2 The Receiver's Part

Suppose that U_2 receives the set of sealed objects sent by U_1. Now U_2 wants to decrypt it. The following is the decryption procedure.

Step 1 (Recovering BD)

Using the decryption equation proposed by El-gamal, U_2 can recover the broadcasting secret key, BD, as follows:

$C_{1,1}$ = 801168388 mod 67=9,
$C_{1,2}$ = 1266086232 mod 67= 29,

and BD = $((C_{1,1})^{D_2})^{-1} C_{1,2}$ mod P_2 = $29((9)^{52})^{-1}$ mod 67 = 4.

Step 2 (Checking BD)

Using the decryption function, U_2 computes BD' = $((C_{4,1})^{BD})^{-1} C_{4,2}$ mod P= $16((41)^4)^{-1}$ mod 73 = 4. Because BD = BD' = 4, BD is correct.

Step 3 (Recovering M)

Using the decryption function again, U_2 recovers the message M = $((C_{2,1})^{BD})^{-1} C_{2,2}$ mod P = $59((52)^4)^{-1}$ mod 73 = 39.

Step 4 (Recovering ID_s)

By computing $ID_s = ((C_{5,1})^{BD})^{-1} C_{5,2}$ mod P = $18((59)^4)^{-1}$ mod 73 = 1, U_2 knows the sender should be U_1.

Step 5 (Authenticating)

By computing $R = RC_2((RC_1)^{BD})^{-1}$ mod P = $66((25)^4)^{-1}$ mod 73= 33 and $S = SC_2((SC_1)^{BD})^{-1}$ mod P = $44((3)^4)^{-1}$ mod 73 = 42, U_2 recovers SG = (R, S) = (33, 42). According to the authentication equation $\alpha_s^M \equiv (E_s)^R R^S$ (mod P_s), U_2 validates $8^{39} \equiv 23 \equiv (11^{33})(33^{42})$ (mod 61). Thus, U_2 believes that M is indeed sent by U_1.

5. The Security Analysis and Discussions

Because our scheme follows the random number estriction and is based on El-gamal's public key ryptosystem and signature scheme, it is as secure as l-gamal's. In our broadcasting network, each ecipient is able to get the broadcasting sealed objects. Iowever, illegal recipients cannot have the roadcasting secret key. Trying to recover the roadcasting secret key, BD, from B1 and B2 is quivalent to computing the discrete logarithm roblem. Thus, it is very difficult for illegal recipients o compute the BD. Further, since our scheme is based n El-gamal's public key cryptosystem, there is no way or illegal recipients to find any relation among B2, B4, nd B5.

If an illegal recipient wants to recover the ender's secret key from B6, he or she should have BD n advance. However, this is difficult. El-gamal's ignature scheme allows an intruder, who knows ne legitimate signature for one message, to generate ther legitimate signatures and messages [3]. The ignature of our scheme is more secure than that of El-amal's.

El-gamal's ciphertext is double the size of the orresponding RSA ciphertext, and El-gamal's ignature is the same size as for the RSA scheme [3]. Because our signature is encrypted by BD, the signature is double the size of that needed for the RSA scheme. From the above discussion, our sealed objects are double the size of those needed for a similar scheme based on RSA. This is one drawback to our proposal.

6. Conclusions

In this article, we have proposed a scheme based on El-gamal's public key cryptosystem and signature scheme. From the discussions of Section 5, we conclude that our scheme is as secure as El-gamal's. In addition, it not only satisfies Chiou and Chen's three properties described previously but also can authenticate the sender.

References

[1] J. S. Gopal & J. M. Jaffe "Point-to-multipoint Communication over Broadcast Links," IEEE Trans. on Communications, COM-32(9), 1034-1044.

[2] G. H. Chiou & W. T. Chen "Secure Broadcasting Using the Secure Lock," IEEE Trans. on Software Engineering, 15(8), 929-934.

[3] T El-gamal "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. on Information Theory, IT-31(4), 469-472.

[4] D. E. R. Denning Cryptography and Data Security (Reading, MA. 1982), Addison-Wesley, 47-48.

[5] D. K. Gifford "Cryptographic Sealing for Information Secrecy and Authentications," Comm. of the Association for Computing Machinery, 25(4) 274-286.