Regular Paper

Yet Another Approach for Secure Broadcasting Based Upon Single Key Concept

JINN-KE JAN* and CHOUNG-DONG YU*

In this paper, we propose a cryptosystem to solve the problem of broadcasting in the network. The cryptosystem has the following advantages:

(1) Only one ciphertext is sent out.
(2) The operation of enciphering is performed only once.
(3) The key which is held by each user is the same as the one in the public key cryptosystem.
(4) The length of ciphertext is shorter than the ones proposed so far.
(5) The sender can arbitrarily select the receivers who are requested to know the message.
(6) Digital signature can easily be implemented.
(7) The security of the cryptosystem is the same as the one of *RSA*.

1. Introduction

To send secret messages by using cryptography is very important in the area of data transmission. A broadcasting system is characterized by the property that a single transmission from a user may be received simultaneously by several other users. This kind of application exists in the medium of satellite, radio, etc. The cryptosystems in the past were all devised with point-to-point type communication. Point-to-multipoint data communication will be studied as well in the near future.

In this paper, we propose a cryptosystem to solve the problem of broadcasting in the network. We can send any secret message to several authorized users simultaneously. Our cryptosystem is based on the *RSA* public key scheme [10] and single key concept [7].

Let $U=\{U_1, U_2, \cdots, U_n\}$ be a group of n users in a broadcasting network system. All users can directly communicate with each other. Now, we suppose that a sender in U wants to send a secret message M to all users in set A, a subset of U. By using our proposed cryptosystem, the sender enciphers the message M into ciphertext C and then broadcasts it to all other users in the broadcasting network system; although all other users in U can receive the ciphertext, only the users of set A can decipher it. Moreover, since the keys which are held by all users in A are the same as the ones of *RSA*. The security of our cryptosystem is the same as the one of *RSA*.

*Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan 40227, Republic of China.

2. Cryptographic Techniques

In this section, we will review the essence of some knowledge and techniques which will be used in our proposed cryptosystem. First, we will give some properties of the *RSA* public key scheme [10]. Each user U_i has his public enciphering key (e_i, N_i) and secret deciphering key (d_i, N_i). The encryption and decryption functions of *RSA* are as following:

$$C=(M)^{e_i} \bmod N_i.$$
$$M=(C)^{d_i} \bmod N_i.$$

Since the enciphering and deciphering functions are mutually inverse, we can use *RSA* public key scheme to implement the digital signature. For example, if user S wants to send a signed, secret message to user R, then he should encipher the message as follows:

$$C=((M)^{d_s} \bmod N_s)^{e_r} \bmod N_r.$$

where

(e_s, N_s) is the sender's public key.

(d_s, N_s) is the sender's secret key.

(e_r, N_r) is the receiver's public key.

(d_r, N_r) is the receiver's secret key.

Because only the sender knows his secret key (d_s, N_s), the ciphertext C can not be forged by any others.

Secondly, we recall the *Chinese Remainder Theorem* (*CRT*). Let $N_1, N_2, \cdots, N_n$ denote n positive integers that are relatively prime in pair, and let $R_1, \cdots, R_n$ denote any n positive integers. Then the congruences

$X \equiv R_i \ (mod\ N_i)$, $i=1, \cdots, n$ have a common solution X which is in the range of $[1, m-1]$ and

$$X=\left(\sum_{i=1}^{n}(m/N_i)*R_i*b_i\right) mod\ m,$$

where

$$m=N_1*N_2*\cdots*N_n,$$
$$b_i*(m/N_i)\ mod\ N_i \equiv 1.$$

The proof of *CRT* and the algorithm can consult [1] and [9]. For example:

Let $N_1=5$, $N_2=7$, $N_3=8$,
$R_1=2$, $R_2=4$, $R_3=3$.
Then $m=N_1*N_2*N_3=5*7*8=280$,
$b_1=6$, $b_2=3$, $b_3=3$.
Thus

$$\begin{aligned}X&=(((m/N_1)*b_1*R_1)\\&\quad+((m/N_2)*b_2*R_2)\\&\quad+((m/N_3)*b*R_3))\ mod\ m\\&=(672+480+315)\ mod\ 280\\&=67.\end{aligned}$$

Since

$$X\ mod\ N_1=67\ mod\ 5=2=R_1,$$
$$X\ mod\ N_2=67\ mod\ 7=4=R_2,$$
$$X\ mod\ N_3=67\ mod\ 8=3=R_3.$$

Now we state the single key concept [7]. An access control matrix establishes the relationship of each user subject and every resource object; conventionally the accessible objects are arranged in columns and various user subjects are arranged in rows. Each elements a_{ij} in the access control matrix A stands for the corresponding access privilege of user i to resource j. We identify every access privilege as a positive integer, and assign zero to every matrix element which represents no access priviledge. Let $A_{m\times n}$ be an access control matrix, t be the total number of access control privileges, and a_{ij} be the (i,j)th element of the access control matrix $A_{m\times n}$. Then there exists an integer K_i, called the key of the user i, such that

$$a_{ij}=\left\lfloor\frac{K_i}{(t+1)^{j-1}}\right\rfloor mod\ (t+1),$$
$$where\ 1\le i\le m\ and\ 1\le j\le n,$$

if

$$K_i=\sum_{q=1}^{n}a_{iq}(t+1)^{q-1}. \tag{1}$$

For example, let us consider the simple access control matrix with 4 users and 5 files as depicted in Table 1.

Since the total number t of access control privileges is 4 and the number of files is 5, by (1) each key can be computed as

Table 1 An access control matrix.

User i	File $j=1$	2	3	4	5
1	2	0	1	1	3
2	1	3	1	2	0
3	3	0	2	0	1
4	1	1	0	2	0

0: No access
1: Execute
2: Read
3: Write
4: Own

$$\begin{aligned}K_i&=\sum_{q=1}^{5}a_{iq}(4+1)^{q-1}\\&=\sum_{q=1}^{5}a_{iq}5^{q-1}.\end{aligned}$$

Thus

$$K_1=2027,$$
$$K_2=291,$$
$$K_3=653,$$
$$K_4=256.$$

Now, let us compute a_{ij} for the (i,j)th element. For instance, if $i=3$ and $j=4$, then the corresponding access control privilege is computed as

$$\begin{aligned}a_{34}&=\left\lfloor\frac{K_3}{(4+1)^{4-1}}\right\rfloor mod\ (4+1)\\&=\left\lfloor\frac{653}{5^3}\right\rfloor mod\ 5\\&=5\ mod\ 5\\&=0,\end{aligned}$$

which is correct.

3. Our Proposed Solution

In our cryptosystem, we employ *RSA*, single key concept, and *CRT*. In the *RSA* public key scheme, each user U_i has his public enciphering key (e_i, N_i) and secret deciphering key (d_i, N_i). Meanwhile, there are some assumptions listed below:

(1) Let $U=\{U_1, U_2, \cdots, U_n\}$ be a group of n users in a broadcasting network system.
(2) A is the receiver's group, $A \subseteq U$.
(3) U_s is the sender and U_r is the receiver, U_s, $U_r \in U$.
(4) (e, d, N) is the communication key.
(5) $id_1, \cdots, id_n$ are user's *id* numbers, which are pairwise relatively prime, and $id_i > |A|$, $i=1, \cdots, n$.
(6) $N_1, \cdots, N_n$ are pairwise relatively prime.

The format of the message is given as follows:

K	B	PB	N	SID	CKD	C	SG

K: the ciphertext of the deciphering key d, computed by single key concept.
B: the base of single key concept.

PB: the receiver's location in the single key concept, by using *CRT*.
SID: sender's *id* number and is enciphered by the key (e, N).
CKD: ciphertext of deciphering key d by using (e, N).
C: ciphertext of the message M by using (e, N).
SG: ciphertext of the sender's signature.

The Encryption Method

Step 1: Use the *RSA* algorithm to compute the communication key (e, d, N) of system.

Step 2: Compute K and B by the single key concept.

(1) $a_i=(d^{e_i} \bmod N_i)+1$ for all $U_i \in A$ or $U_i=U_s$, $i=1, \cdots, n$.
$a_i=0$ for all $U_i \notin A$ and $U_i \neq U_s$, $i=1, \cdots, n$.

(2) $B=Max(a_i)+1$, $i=1, \cdots, n$.

(3) Select
$R_i \neq 0$ for all $U_i \in A$, and
$R_i=0$ for all $U_i \notin A$.
Here $1 \leq R_i$, $R_j \leq |A|$, and $R_i \neq R_j$ for all U_i, $U_j \in A$.

(4) $K=\sum_{i=1}^{n} a_i B^{R_i}$.

Setp 3: Compute *PB* by *CRT*.
$PB \equiv R_i (mod\ id_i)$ for all $U_i \in U$, $i=1, \cdots, n$.

Step 4: Compute the *SID*, *CKD*, *C*, and *SG* using (e, N) by *RSA* scheme.
$SID=(id_s)^e \bmod N$,
$CKD=d^e \bmod N$,
$C=M^e \bmod N$,
$SG=(d^{d_s} \bmod N_s)^e \bmod N$.

The Decryption Method

Step 1: Compute the R_r from *PB* using *CRT*.
$R_r=PB \bmod id_r$.
If $R_r=0$ then **STOP**.

Step 2: Compute the a_r from K using B, and R_r by single key concept.

$$a_r=\left\lfloor \frac{K}{B^{R_r}} \right\rfloor \bmod B.$$

If $a_r=0$ then **STOP**.

Step 3: Compute the (d, N) using (d_r, N_r) by *RSA* scheme.
$d=(a_r-1)^{d_r} \bmod N_r$.
If d is not equal to $((CKD)^d \bmod N)$ then **STOP**.

Step 4: Decipher the ciphertext using (d, N) by *RSA* scheme.
$M=C^d \bmod N$.

Step 5: Check the signature.
$SG'=((SG)^d \bmod N)^{e_s} \bmod N_s$.
If $SG'=d$ then the message M is sent by U_s,
else the message M is invalid.

It is clear to see that the keys held by all users are the same as the ones of *RSA*.

Example

Let $U_1, U_2, \cdots, U_r$ be seven users in the cryptosystem and their keys are given in Table 2.

Table 2 Public keys and secret keys.

User	Public key		Secret key	User *id*
	e	N	d	*ID*
1	125	141	53	8
2	107	215	11	9
3	179	287	59	11
4	139	253	19	13
5	211	377	43	17
6	37	527	13	19
7	85	703	61	23

Suppose user U_1 wants to send a message $M=$"*HELLO*" to U_3 and U_6. To encipher the message M, we use 2 digits, for instance, for each character, where $A=01$, $B=02, \cdots, Z=26$.

In the following, we present the encryption and decryption steps of our proposed solution.

The encryption steps:

Step 1: Let $e=275$, $d=11$, $N=817$.

Step 2:

(1) $a_1=(11^{125} \bmod 141)+1=6$.
$a_2=0$.
$a_3=(11^{179} \bmod 287)+1=150$.
$a_4=0$.
$a_5=0$.
$a_6=(11^{37} \bmod 527)+1=45$.
$a_7=0$.

(2) $B=Max(a_i)+1=150+1=151$.

(3) Select
$R_1=0$, $R_2=0$, $R_3=1$, $R_4=0$,
$R_5=0$, $R_6=2$, $R_7=0$.

(4) $K=\sum_{i=1}^{7} a_i B^{R_i}$
$=6*151^0+0*151^0+150*151^1+0*151^0+$
$0*151^0+45*151^2+0*151^0$
$=6+22650+1026045$
$=1048701$.

Step 3: $PB \equiv 0\ (mod\ 8)$,
$PB \equiv 0\ (mod\ 9)$,
$PB \equiv 1\ (mod\ 11)$,
$PB \equiv 0\ (mod\ 13)$,
$PB \equiv 0\ (mod\ 17)$,
$PB \equiv 2\ (mod\ 19)$,
$PB \equiv 0\ (mod\ 23)$,
therefore,
$PB=(3*6953544*1+6*4025736*2)\ mod\ (\prod_{i=1}^{7} id_i)=69169464$.

Step 4: $M=$"*HELLO*"$=08\ 05\ 12\ 12\ 15$.
$8^{275} \bmod 817=753$.
$5^{275} \bmod 817=104$.
$12^{275} \bmod 817=673$.
$12^{275} \bmod 817=673$.
$15^{275} \bmod 817=268$.
$C=753\ 104\ 673\ 673\ 268$.
$SID=8^{275} \bmod 817=753$.
$CKD=11^{275} \bmod 817=121$.

$SG=(11^{53} \bmod 141)^{275} \bmod 817=125^{275} \bmod 817=672.$

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

The decryption steps:

Step 1: $R_3=69169464 \bmod 11=1.$

Step 2: $a_3=\left\lfloor \frac{1048701}{151^1} \right\rfloor \bmod 151=6945 \bmod 151=150.$

Step 3: $d=149^{59} \bmod 287=11.$
$CKD^d \bmod N=121^{11} \bmod 817=11=d.$

Step 4: $M=C^d \bmod N.$
$753^{11} \bmod 817=8.$
$104^{11} \bmod 817=5.$
$673^{11} \bmod 817=12.$
$673^{11} \bmod 817=12.$
$268^{11} \bmod 817=15.$
Therefore, $M=$"*HELLO*".

Step 5: $SG'=(672^{11} \bmod 817)^{125} \bmod 141$
$=125^{125} \bmod 141=11=d,$
which verifies that the message is sent by the user U_1.

4. Security of Our Cryptosystem

We claim that the security of our cryptosystem is the same as the one of *RSA*. If some one wants to break our cryptosystem, he must know the value of d. The value of d is computed from a_r and R_r. The value of R_r can be computed from id_r. The value of a_r must be computed from d_r. The value of d_r, which is the secret key of U_r is known by the receiver U_r himself only. The intruder must first break the *RSA* scheme and then can find d_r. Therefore, the security of our cryptosystem is the same as the one of *RSA*, no matter how large the number of receivers will be.

5. Space Required of Our Cryptosystem

In our cryptosystem, the involved operations are the same as the ones of *RSA*. The total length of the additional messages (K, B, PB) is smaller than the ones of any scheme proposed so far [2, 3]. The value of PB is computed from id_i by *CRT*. The value of id_i is smaller than N_i, therefore PB is smaller than K. The value of B is computed from a_i by *RSA* scheme. In worst case, B is equal to the maximum of N_i. The value of K is computed from a_i, R_i, and B by single key concept. R_i is less than the number of users. From the step 2 of the encryption method, we can see that only the authorized user's a_i is greater than zero, so the value of K is less than $\prod_{i=1}^{n} N_i$.

The length of B is less than $len(Max(N_i))$, here $len(N)$ denotes the length of N in bit. Suppose $2^{m-1} \le N_i < 2^m$, $m>0$. Then $len(N_i)=m$. We can see that $len(\prod_{i=1}^{n} N_i)=OLDL \le mn$. If $|A|=k$, then $B^k<K \le B^{k+1}$. In worst case, $len(B)=len(Max(N_i))=m$. So $len(K)=m(k+1)=mk+m$. If $2^{p-1} \le id_i < 2^p$, $p>0$, then $len(id_i)=p$. In worst case, $len(PB)<pn$. The total length of additional message is:

$$\begin{aligned} NEWL &= len(PB)+len(B)+len(K) \\ &\le pn+m+(mk+m) \\ &\le mk+pn+2m. \end{aligned}$$

If $p \ll m$ and $k \ll n$, then $NEWL < OLDL$. In general, m, n are two large numbers, and p, k are smaller than m, n. It is clear to see that the total length of additional messages is shorter than the ones of ever before [2, 3]. It means that our method can reduce the communication cost. On the other hand, the computational cost for computing the communication keys is a little bit higher than the ones of [2, 3]. Since we employ $\left\lfloor \frac{K}{B^{R_r}} \right\rfloor \bmod B$ to compute the value a_r, while [2, 3] use $K \bmod N_r$ to compute the value a_r instead.

6. Conclusions

In our proposed method, the security is the same as the one of *RSA*. The sender can arbitrarily select the users who are authorized to know the message, so the multi-level security can be successfully implemented, as well. The length of additional message of our scheme is less than the ones before, and the steps of encryption and decryption of our scheme are simple and clear too.

References

1. AHO, A. V., HOPCROFT, J. E. and ULLMAN, J. D. *The Design and Analysis of Computer Algorithms*, Addision-Wesley, Reading, Mass., 1974.
2. CHANG, C. C. and LIN, C. H. A Cryptosystem for Secure Broadcasting, *Proceedings of National Science Council*, **12**, 4 (July 1988), 233-239.
3. CHEN, W. T. and CHIOU, G. H. Secure Broadcasting Using Chinese Remainder Theorem, *Proceedings of National Computer Symposium* (1985), 787-797.
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*, IT-**22**, 6 (Nov. 1976), 644-654.
6. GIFFORD, D. K. Cryptographic Sealing for Information Secrecy and Authentications, *CACM*, **25**, 4 (1982), 274-286.
7. JAN, J. K. A Single-Key Access Control Scheme in Information Protection System, *Information Sciences*, **51** (1990), 1-11.
8. KENT, S. T. Security Requirements and Protocols for a Broadcast Scenario, *IEEE Trans. Comm.*, Com-**29**, 6 (1981), 778-786.
9. NIVEN, I. and ZUCKERMAN, H. A. *An Introduction to the Theory of Numbers*, John Wiley and Sons, New York, 1972.
10. RIVEST, R. L., SHAMIR, A. and ADLEMAN, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystem, *CACM*, **21**, 2 (Feb. 1978), 33-39.

(Received March 18, 1991; revised June 24, 1991)