Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **4**, October **2014**

A Secure Broadcasting Method Based on the Generalized Aryabhata Remainder Theorem

Yanjun Liu

Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education
School of Computer Science and Technology
Anhui University
No.111 Jiulong Rd., Hefei, 230601, China
Department of Computer Science and Information Engineering
Asia University
No.500, Lioufeng Rd., Wufeng, Taichung, 413, Taiwan
yjliu104@gmail.com

Chin-Chen Chang

Department of Information Engineering and Computer Science
Feng Chia University
No.100 Wenhwa Rd., Seatwen, Taichung, 407, Taiwan
Department of Computer Science and Information Engineering
Asia University
No.500, Lioufeng Rd., Wufeng, Taichung, 413, Taiwan
alan3c@gmail.com

Received May 2014; revised April 2014

Abstract. *With the prevalence of group communications, how to implement secure broadcasting among group members has become one of the most important issues. Broadcasting is a point-to-multipoint communication, and secure broadcasting should ensure that only authorized group members can obtain the correct content of the message that is broadcast by a sender. In this paper, we propose a secure broadcasting method based on the generalized Aryabhata remainder theorem (GART). By the use of the RSA public-key scheme, the proposed scheme allows the sender to send one copy of an encrypted message to all group members, but only the authorized members can recover the plaintext. Analysis showed that our scheme is secure and efficient.*

Keywords: Secure broadcasting, Generalized aryabhata remainder theorem (GART), Security, Public-key scheme, Encryption, Decryption

1. **Introduction.** Since group communications [11-14, 23] have been studied extensively by scholars and experts, transmitting messages secretly among group members is the main topic for group communication. There are two communication modes in group communication, i.e., point-to-point and point-to-multipoint communication. Point-to-point communication means that a sender transmits a message to only one receiver, while, in point-to-multipoint communication, which also is called broadcasting communication, a sender can transmit a message to several receivers simultaneously. In recent years, broadcasting communication has been addressed in many scientific publications, and it has been applied extensively in many areas, such as electronic conferences, video information systems, and satellite systems [1, 3, 4, 6, 8-10, 15, 16, 18, 21, 22, 24, 25].

Broadcasting for group communication should satisfy the security requirement that only authorized group members can obtain the correct content of the message that is broadcast by a sender, whereas any unauthorized users should not be able to decipher any part of the message. Generally, various cryptographic techniques are used to implement secure broadcasting, including the NBS data encryption standard (DES) [7] and the RSA public-key scheme [20]. These cryptographic techniques encrypt the message to be transmitted into ciphertext, and, then, the sender broadcasts the ciphertext to all group members. However, only the receivers who are authorized to know the message can decrypt the ciphertext.

In 1982, Gifford [10] proposed an approach for secure broadcasting in which the communication key was hidden in the transmitted message, and only legitimate receivers were able to recover the communication key. In 1988, Chang and Lin [3] proposed a secure broadcasting cryptosystem that was similar to Gifford's approach. Their cryptosystem was based on the generalized Chinese remainder theorem (GCRT), and its security relied on the RSA public-key scheme. There have been many extensions of Chang and Lin's cryptosystem. In 1991, Jan and Yu [16] presented a design for secure broadcasting based on the single-key concept for which security was the same as that of the RSA public-key scheme. In 1993, Jan and Chen [15] proposed a design for secure broadcasting to reduce the size of the communication key. Chang and Buehrer [1] presented a generalized, secure, broadcasting cryptosystem, in which many messages could be encrypted into a single ciphertext. Recently, Wu and Chang [21] presented five message authorization strategies in a group-oriented, secure broadcasting system.

Inspired by Chang and Lin's method, in this paper, we propose a new method for secure broadcasting based on the generalized Aryabhata remainder theorem (GART) and the RSA public-key scheme. The main contributions of our proposed method are listed below:

(1) In our proposed method, the sender can send one copy of encrypted messages to all group members, but only the authorized members can use the deciphering key to decrypt the ciphertext.
(2) The GART is used to conceal the information related to the deciphering key in a message. The GART is flexible in such a way that, if we want to conceal the deciphering key in another message, only a parameter k must be reconfigured.
(3) The security of our proposed method is the same as that of the RSA public-key scheme.
(4) Our proposed method is more efficient than Chang and Lin's method in terms of computational cost.

The rest of this paper is organized as follows. In Section 2, we briefly introduce some fundamental knowledge that is useful in our proposed method. In Section 3, we propose our new method for secure broadcasting. Section 4 gives security and efficiency analyses of the proposed method, and our conclusions are presented in Section 5.

2. Preliminaries.

In this section, we briefly review some fundamental knowledge that is useful in our proposed method. First, we review the RSA public-key scheme and its basic properties, and, then, we introduce the Chinese remainder theorem (CRT) and the generalized Chinese remainder theorem (GCRT). Finally, we describe Chang and Lin's method [3] for secure broadcasting, which is based on the RSA public-key scheme and the GCRT.

2.1. RSA public-key scheme.

Let us review how the RSA public-key scheme [20] performs. Let $U = \{u_1, u_2, ..., u_t\}$ denote a group of t users who wish to communicate with each other. Assume that user u_i $(i = 1, 2, ..., t)$ has one public enciphering key (e_i, N_i) and one private deciphering key d_i. If M and C represent the plaintext and ciphertext of the transmitted message, respectively, the encryption and decryption processes of the RSA public-key scheme can be described as $C = M^{e_i}(\text{mod}N_i)$ and $M = C^{d_i}(\text{mod}N_i)$, respectively.

From the principle of encryption and decryption, the RSA public-key scheme can be used for digital signature. Next, we give an example to illustrate the implementation of a digital signature that is based on the RSA public-key scheme. Let us consider the situation below. If user u_i attempts to transmit a signed, secret message M to user u_j, u_i should first encipher M with his/her private deciphering key and then with u_j's public enciphering key by $C = (M^{d_i}\text{mod}N_i)^{e_j}\text{mod}N_j$, where d_i is the sender's (u_i's) private deciphering key, (e_i, N_i) is the sender's (u_i's) public enciphering key, d_j is the receiver's (u_j's) private deciphering key, and (e_j, N_j) is the receiver's (u_j's) public enciphering key. Upon receiving the ciphertext C, u_j can recover the message M by deciphering C as $M = (C^{d_j}\text{mod}N_j)^{e_i}\text{mod}N_i$. Because only the sender u_i knows the private deciphering key d_i, no one else can forge ciphertext C. Therefore, receiver u_j can conclude that message M was, indeed, sent by u_i.

2.2. **Chinese remainder theorem.** The Chinese remainder theorem (CRT) is a very important tool in many applications, such as cryptology, signal processing, and access control. Let p_1, p_2, ..., p_t be positive, pairwise, relative prime integers and x_1, x_2, ..., x_t be positive integers. Thus, a system of equations can be established as follows:

$$\begin{aligned} x_1 &= X(\text{mod}p_1),\\ x_2 &= X(\text{mod}p_2),\\ &\vdots\\ x_t &= X(\text{mod}p_t). \end{aligned}$$

According to the CRT, there is a unique solution X in Z_P and X can be computed as: $X = \sum_{i=1}^{t} M_i \cdot M_i^{'} \cdot x_i(\text{mod}P)$, where $P = \prod_{i=1}^{t} p_i$, $M_i = \frac{P}{p_i}$, and $M_i \cdot M_i^{'} \equiv 1(\text{mod}p_i)$.

2.3. **Generalized Chinese remainder theorem.** The generalized Chinese remainder theorem (GCRT) [2, 17] is a significant extension of the CRT in which an integer k is added in the computational process. Let p_1, p_2, ..., p_t denote positive integers that are pairwise relatively prime to each other, and x_1, x_2, ..., x_t denote positive integers. Select an integer k that satisfies $\text{Max}\{x_i\}_{1\le i\le t} < k < \text{Min}\{p_i\}_{1\le i\le t}$. Then, a system of equations can be constructed as follows:

$$\begin{aligned} x_1 &= \lfloor X/p_1 \rfloor(\text{mod}k),\\ x_2 &= \lfloor X/p_2 \rfloor(\text{mod}k),\\ &\vdots\\ x_t &= \lfloor X/p_t \rfloor(\text{mod}k). \end{aligned}$$

From the GCRT, the solution X in Z_{kP} can be computed as $X = \sum_{i=1}^{t} A_i \cdot A_i^{'} \cdot B_i(\text{mod}k \cdot P)$, where $P = \prod_{i=1}^{t} p_i$, $A_i = k \cdot \frac{P}{p_i}$, $A_i \cdot A_i^{'} \equiv k(\text{mod}k \cdot p_i)$, and $B_i = \lceil \frac{x_i \cdot p_i}{k} \rceil$.

Although the GCRT requires slightly more computational cost than the CRT, the GCRT has an advantage over the CRT in that it is more flexible due to the additional integer k. In the CRT, it is necessary to modify the entire system of equations that has been constructed to change the integer X, whereas, in GCRT, only the integer k must be modified to alter the value of X.

2.4. **Chang and Lin's method for secure broadcasting.** Chang and Lin's method [3] for secure broadcasting is based on the RSA public-key scheme and the GCRT. Let $U = \{u_1, u_2, ..., u_t\}$ denote a group of t users in a group communication. Assume that the sender u_i wants to transmit a secret message M to the authorized users in group U. Chang and Lin's method for secure broadcasting consists of two phases, i.e., the encryption phase and the decryption phase. In the encryption phase, the sender u_i encrypts message M into ciphertext C and then broadcasts C to all of the other users in group U simultaneously. First, u_i generates a public enciphering key and a private deciphering key. Second, u_i conceals the private deciphering key into the message X by using the GCRT. Third, u_i uses the public enciphering key to create the ciphertext C of message M and broadcasts C and X to all of the other users in group U simultaneously. In the decryption phase, although all of the other users in group U can receive the ciphertext C, only the authorized users who are requested to obtain the message M can decrypt it. Each authorized user can calculate the private deciphering key from the message X by using the GCRT and then uses the recovered private deciphering key to decrypt C to obtain M.

According to Chang and Lin's method for secure broadcasting, the sender can select an arbitrary number of users who are authorized to know the secret message M. The security of their method depends on the RSA public-key scheme. However, the efficiency can still be improved. In the next section, we will propose a method for secure broadcasting that is more efficient than Chang and Lin's method in terms of computational cost.

3. **Our proposed method.** In this section, we propose a new method for secure broadcasting based on the generalized Aryabhata remainder theorem (GART) and the RSA public-key scheme. Let $U = \{u_1, u_2, ..., u_t\}$ denote a group of t users such that each user is able to transmit a secret message to any other users in group U. Assume that H is a subset of U. Then, the objective of our proposed method is to allow the sender u_s to broadcast a message M securely to all of the users in H. In order to achieve this goal, the RSA public-key scheme is used for ciphering the message M into ciphertext C, and the GART is used for ciphering the private deciphering key into a message L. All authorized receivers can decipher the message L to obtain the private deciphering key to recover the message M that is sent by u_s.

3.1. **Definitions.** Let us define the terms that are used in our proposed method. Each user u_i $(i = 1, 2, ..., t)$ is associated with one public enciphering key (e_i, N_i) and one private deciphering key d_i. Each user u_i also has a unique identification number p_i, which satisfies two conditions, i.e., 1) p_1, p_2, ..., p_t are positive integers that are pairwise relatively prime to each other and 2) $p_i > N_i$ for $i = 1, 2, ..., t$. In addition, the sender u_s must generate a public enciphering key (e, N) or encrypting the message M he/she wants to broadcast and a private deciphering key d for decrypting the ciphertext C of message M. To ensure that only the authorized receivers can obtain the private deciphering key d to decrypt the ciphertext C, the broadcast message sent by the sender u_s must be in the format shown in Figure 1.

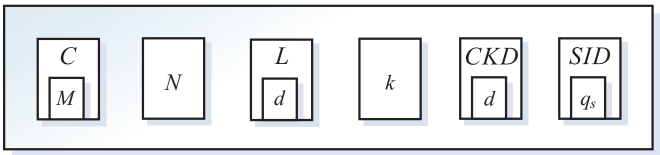

Figure 1. Format of the broadcast message

Now, we explain the components of the broadcast message.
C: the ciphertext of message M;
L: the ciphertext of the private deciphering key d by using the GART;
k: a parameter selected in the GART to compute L;
CKD: the ciphertext of the private deciphering key d obtained by using the public enciphering key (e, N);
SID: the ciphertext of the sender's identification number p_s.

Since using the GART to conceal the information of private deciphering key d in the message L is a critical step in our secure broadcasting method, we will first review the GART and then provide details of our proposed method in the following two subsections.

3.2. **Generalized Aryabhata remainder theorem.** As mentioned in Sections 2.2 and 2.3, both CRT and GCRT are required to compute an integer X by a large number, which is the product of all pairwise, relative prime integers. This process can increase the computational cost. To overcome this weakness, Rao and Yang [19] proposed the Aryabhata remainder theorem (ART) in 2006. The ART is conducted with only two relative prime integers and described as follows. Let p_1 and p_2 be two relative prime integers and x_1 and x_2 be two positive integers. Thus, two equations $x_1 = X(\text{mod} p_1)$ and $x_2 = X(\text{mod} p_2)$ can be established. According to the ART, there is a unique solution X in $Z_{p_1 \cdot p_2}$ and X can be computed as $X = p_1 \cdot (((x_2 - x_1) \cdot p_1^{-1})\text{mod} p_2) + x_1$, where $p_1 \cdot p_1^{-1} = 1 \text{mod} p_2$. The proof of ART is shown in [19].

Later in 2010, Chang et al. [5] proposed a valuable extension of the ART, which they called the generalized Aryabhata remainder theorem (GART). They presented the GART with two and t relative prime integers, respectively. The GART with two relative prime integers can be described as follows. Let p_1 and p_2 be two relative prime integers and x_1 and x_2 be two positive integers. Select an integer k that satisfies $\text{Max}\{x_1, x_2\} < k < \text{Min}\{p_1, p_2\}$. Then, two equations $x_1 = \lfloor X/p_1 \rfloor (\text{mod} k)$ and $x_2 = \lfloor X/p_2 \rfloor (\text{mod} k)$ can be constructed and the solution X in $Z_{k \cdot p_1 \cdot p_2}$ can be computed by $X = k \cdot p_1 \cdot ((\lceil (x_2 \cdot p_2 - x_1 \cdot p_1)/k \rceil \cdot p_1^{-1})\text{mod} p_2) + x_1 \cdot p_1$. Chang et al. also extended the proposed GART to t relative prime integers for the general case. Let p_1, p_2, ..., p_t denote positive integers that are pairwise relatively prime to each other and x_1, x_2, ..., x_t denote positive integers. Select an integer k that satisfies $\text{Max}\{x_i\}_{1 \le i \le t} < k < \text{Min}\{p_i\}_{1 \le i \le t}$. Then, a system of equations can be constructed as follows:

$$\begin{aligned} x_1 &= \lfloor X/p_1 \rfloor (\text{mod} k), \\ x_2 &= \lfloor X/p_2 \rfloor (\text{mod} k), \\ &\vdots \\ x_t &= \lfloor X/p_t \rfloor (\text{mod} k). \end{aligned}$$

From the GART, the solution X in Z_{kP} can be computed by the iterative algorithm shown below, where $P = \prod_{i=1}^{t} p_i$.

```
GART Algorithm
Input: $(k, \{x_1, x_2, ..., x_t\}, \{p_1, p_2, ..., p_t\})$
Output:integer $X$
1. $P_1 = p_1, X_1 = x_1 \cdot p_1$
2. for $i = 2$ to $t$ do
3. $P_i = P_{i-1} \cdot p_i$
4. $X_i = k \cdot P_{i-1} \cdot ((\lceil (x_i \cdot p_i - X_{i-1})/k \rceil \cdot (P_{i-1})^{-1})\text{mod} p_i) + X_{i-1}$, where $(P_{i-1})^{-1}\text{mod} p_i$
   is the multiplicative inverse of $P_{i-1}$ modulo $p_i$.
5. end for
```

6. Return X_t

Next, an example is given to demonstrate the computational process of the GART.

Example 3.1. Given $\{x_1, x_2, x_3\}$=$\{11, 2, 11\}$, $\{p_1, p_2, p_3\}$=$\{23, 37, 43\}$, $k = 15$, and $x_i = \lfloor X/p_i \rfloor (\text{mod} k)$, where $1 \le i \le 3$, compute the integer X using the GART.

The three steps of the computational process are shown below:

Step 1:

$$P_1 = p_1 = 23, X_1 = x_1 \cdot p_1 = 11 \cdot 23 = 253.$$

Step 2:

$$P_2 = P_1 \cdot p_2 = 23 \cdot 37 = 851,$$

$$\begin{aligned} X_2 &= k \cdot P_1 \cdot ((\lceil (x_2 \cdot p_2 - X_1)/k \rceil \cdot (P_1)^{-1}) \text{mod} p_2) + X_1 \\ &= 15 \cdot 23 \cdot ((\lceil (2 \cdot 37 - 253)/15 \rceil \cdot 23^{-1}) \text{mod} 37) + 253 \\ &= 15 \cdot 23 \cdot 14 + 253 = 5083. \end{aligned}$$

Step 3:

$$P_3 = P_2 \cdot p_3 = 851 \cdot 43 = 36593,$$

$$\begin{aligned} X_3 &= k \cdot P_2 \cdot ((\lceil (x_3 \cdot p_3 - X_2)/k \rceil \cdot (P_2)^{-1}) \text{mod} p_3) + X_2 \\ &= 15 \cdot 851 \cdot ((\lceil (11 \cdot 43 - 5083)/15 \rceil \cdot 851^{-1}) \text{mod} 43) + 5083 \\ &= 15 \cdot 851 \cdot 15 + 5083 = 196558. \end{aligned}$$

The unique solution X_3 in Z_{548895} can be verified as follows:
$x_1 = \lfloor X_3/p_1 \rfloor \text{mod} k = \lfloor 196558/23 \rfloor \text{mod} 15 = 11$,
$x_2 = \lfloor X_3/p_2 \rfloor \text{mod} k = \lfloor 196558/37 \rfloor \text{mod} 15 = 2$,
and $x_3 = \lfloor X_3/p_3 \rfloor \text{mod} k = \lfloor 196558/43 \rfloor \text{mod} 15 = 11$.

The difference between the GCRT and the GART comes from the GCRT use of a modular operation with a large integer, say kP, as its last operation, whereas the GART uses a modular operation with a relatively smaller integer, say p_i, in each iteration. Thus, the use of the GART can reduce the computational cost.

3.3. **Description of the proposed method.** Our proposed method for secure broadcasting consists of two phases, i.e., the encryption phase and the decryption phase. The sender u_s enciphers the message M that he/she wants to broadcast by the encryption phase and, then, each authorized receiver can decipher the ciphertext of M by the decryption phase. The encryption phase is shown as follows:

Encryption phase (performed by the sender u_s)

Step 1. Compute the public enciphering key (e, N) and the private deciphering key d for message M by using the RSA scheme.

Step 2. Conceal the private deciphering key d in the integer L by using the GART.

(1) Encipher d by each authorized user's public enciphering key.

```
For $i = 2$ to $t$ do
    If $u_i \in H$
        Then compute $l_i = d^{e_i} \text{mod} N_i$
    Else $l_i = 0$;
End for.
```

(2) Select an integer k that satisfies $\text{Max}\{l_i\}_{1 \le i \le t} < k < \text{Min}\{p_i\}_{1 \le i \le t}$, where p_i is u_i's identification number.

(3) Compute the integer L by using the GART algorithm introduced in Subsection 3.2 with the inputs of k, $\{l_1, l_2, ..., l_t\}$, and $\{p_1, p_2, ..., p_t\}$.

Step 3. Compute C and CKD as $C = M^e \text{mod} N$ and $CKD = d^e \text{mod} N$.
Step 4. Compute SID as $SID = {p_s}^e \text{mod} N$.
Step 5. Broadcast the message (C, N, L, k, CKD, SID) as shown in Figure 1 to all users in group U.

From the encryption phase, we can infer that Step 2 is the most important step and that the GART used in Step 2 is very flexible. If we want to encrypt the private deciphering key d into another integer, it is only necessary to modify the integer k that was selected for the GART.

The decryption phase is demonstrated below:

Decryption phase (performed by each authorized receiver u_i in H)
Step 1. Compute the private deciphering key d.

(1) Use the GART to compute l_i as $l_i = \lfloor L/p_i \rfloor \text{mod} k$.
(2) Use u_i's private deciphering key d_i to recover d by $d = {l_i}^{d_i} \text{mod} N_i$.

Step 2. Authenticate that the message M was sent by u_s.

(1) Compute $d' = (CKD)^d \text{mod} N$.
(2) If $d' = d$,
    Then go to Step 3
    Else dispose of the message M;

Step 3. Decipher the ciphertext C by computing $M = C^d \text{mod} N$.
Step 4. Check the sender's identification number p_s as $p_s = (SID)^d \text{mod} N$.

3.4. **Example.** This subsection provides an example to illustrate our proposed method for secure broadcasting.

Example 3.2. Assume that $U = \{u_1, u_2, u_3, u_4, u_5\}$ is a group of five users. Table 1 gives each user u_i's public enciphering key (e_i, N_i), private deciphering key d_i, and identification number p_i. Now, user u_2 wants to broadcast a message $M = KEY$ to users u_1, u_3, and u_4 ($H = \{u_1, u_3, u_4\} \subset U$). Each character of message M is represented by two digits, such that $A = 01$, $B = 02$, ..., $Z = 26$. In the following, we discuss the encryption phase and the decryption phase in this example.

Table 1. Information of users in group U

User	Enciphering key (e_i, N_i)	Deciphering key d_i	Identification number p_i
u_1	(7, 22)	3	23
u_2	(5, 10)	9	31
u_3	(17, 21)	5	37
u_4	(3, 15)	3	41
u_5	(11, 14)	17	43

Encryption phase
Step 1. Select $(e, N) = (35, 65)$ and compute $d = 11$.
Step 2.

(1) Compute $l_1 = d^{e_1} \text{mod} N_1 = 11^7 \text{mod} 22 = 11$, $l_3 = d^{e_3} \text{mod} N_3 = 11^{17} \text{mod} 21 = 2$, and $l_4 = d^{e_4} \text{mod} N_4 = 11^3 \text{mod} 15 = 11$. Set $l_5 = 0$.
(2) Select $k = 15$.
(3) Assume that as $l_i = \lfloor L/p_i \rfloor \text{mod} k$ if $l_i \neq 0$, we use $k = 15$, $\{l_1, l_3, l_4\}$=$\{11, 2, 11\}$, and $\{p_1, p_3, p_4\}$=$\{23, 37, 43\}$ to compute $L = 196558$ by the GART as in Example 3.1.

Step 3. $M = HELP = 08\ 05\ 12\ 16$. Compute $8^{35}\text{mod}65 = 57$, $5^{35}\text{mod}65 = 60$, $12^{35}\text{mod}65 = 38$, and $16^{35}\text{mod}65 = 61$. $C = 57\ 60\ 38\ 61$. Compute $CKD = d^e\text{mod}N = 11^{35}\text{mod}65 = 6$.
Step 4. Compute $SID = {p_2}^e\text{mod}N = 31^{35}\text{mod}65 = 21$.
Step 5. Broadcast the message (C, N, L, k, CKD, SID) as shown in Figure 1 to all users in group U.

The decryption phase for user u_3 is demonstrated below. Other authorized users can perform the decryption phase similarly.

Decryption phase (performed by u_3)
Step 1.

(1) Compute $l_3 = \lfloor L/p_3 \rfloor \text{mod}k = \lfloor 196558/37 \rfloor \text{mod}15 = 2$.
(2) Compute $d = {l_3}^{d_3}\text{mod}N_3 = 2^5\text{mod}21 = 11$.

Step 2. Compute $d' = (CKD)^d\text{mod}N = 6^{11}\text{mod}65 = 11 = d$.
Step 3. Compute $57^{11}\text{mod}65 = 8$, $60^{11}\text{mod}65 = 5$, $38^{11}\text{mod}65 = 12$, and $61^{11}\text{mod}65 = 16$. $M = 08\ 05\ 12\ 16 = HELP$.
Step 4. Compute $p_2 = (SID)^d\text{mod}N = 21^{11}\text{mod}65 = 31$.

4. **Analysis.** In this section, we present our analysis of the security and efficiency of our proposed method for secure broadcasting. The security analysis is presented first. The approach for verifying the security of our method was to analyze whether an attacker could thwart or bypass the security measures that we implemented. In the encryption phase, the private deciphering key d is concealed in the integer L by using the GART [24]. If the attacker wants to break our method, he/she must know the private deciphering key d, which is computed by $d = {l_i}^{d_i}\text{mod}N_i$, indicating that the attacker must obtain both l_i and d_i. However, since each authorized user keeps his/her private deciphering key d_i secretly, the attacker cannot obtain d_i from each authorized user's public enciphering key (e_i, N_i) due to the RSA public-key scheme. Therefore, our method is secure and the security is the same as that of RSA public-key scheme.

Next, we analyze the efficiency of our proposed method and compare the computational cost of our method with that of Chang and Lin's method [3]. Because the difference between the two methods lies mainly in Step 2 of the encryption phase, we only need to analyze the computational cost in Step 2 of each of the methods.

In our method, Step 2 of the encryption phase uses the GART to conceal the private deciphering key d in the integer L. From the GART, L is computed by the integer k, {l_1, l_2, ..., l_t} (where l_i is the ciphertext of d) and the identification numbers {p_1, p_2, ..., p_t} via t-1 rounds. In each round:

$$L_i = k \cdot P_{i-1} \cdot ((\lceil (l_i \cdot p_i - L_{i-1})/k \rceil \cdot (P_{i-1})^{-1})\text{mod}p_i) + L_{i-1} \tag{1}$$

Assume that k, l_i, and p_i are allocated b digits. Because $k \cdot P_{i-1} \cdot ((P_{i-1})^{-1}\text{mod}p_i)$ can be computed earlier, Equation (1) requires two multiplications, one subtraction, one division, one addition, and one modular operation. Consequently, when (t-1) rounds have been conducted, the computational cost is about $(t-1) \times (2b^2 + b + b^2 + b + b^2)$ bit operations. Hence, the time complexity of computing an integer by the GART is $O(tb^2)$.

Chang and Lin's method uses the GCRT to achieve the same goal as in our proposed method. From the GCRT, L can be computed as:

$$L = \sum_{i=1}^{t} A_i \cdot A_i' \cdot B_i(\text{mod}k \cdot P), \tag{2}$$

where $P = \prod_{i=1}^{t} p_i$, $A_i = k \cdot \frac{P}{p_i}$, $A_i \cdot A_i^{'} \equiv k(\bmod k \cdot p_i)$, and $B_i = \lceil \frac{l_i \cdot p_i}{k} \rceil$. Similarly, assume that k, l_i, and p_i are allocated b digits. Because $A_i \cdot A_i^{'}$ can be computed earlier, Equation (2) requires $2t$ multiplications, t divisions, (t-1) additions, and one modular operation. Therefore, the computational cost is about $2t \times b^2 + t \times b^2 + (t-1) \times b + ((t+1) \times b)^2$ bit operations, which implies that the time complexity of computing an integer by the GCRT is $O(t^2 b^2)$. Since the time complexity of the GART is less than that of the GCRT, our method is more efficient than Chang and Lin's method. Table 2 compares our proposed scheme with Chang and Lin's scheme.

Table 2. Comparison of our proposed scheme and Chang and Lin's scheme

Scheme	Method	Time complexity of encryption	Time complexity of decryption
Chang and Lin [3]	GCRT	$O(t^2b^2)$	$O(b^2)$
Ours	GART	$O(tb^2)$	$O(b^2)$

5. **Conclusions.** In this paper, we proposed an efficient method for secure broadcasting based on the GART and the RSA public-key scheme. In our proposed method, the sender can broadcast an encrypted message to all group members, but only authorized members can obtain the deciphering key d to decrypt the ciphertext. In order to ensure security, the deciphering key d is concealed in an integer L, and the security is the same as that of the RSA public-key scheme. In addition, our proposed method is more efficient than Chang and Lin's method in terms of computational cost.

Acknowledgment. This research was supported in part by the National Nature Science Foundation of China (grant number: 61202228) and the College Natural Science Key Project of Anhui Province of China (grant number: KJ2012A008).

REFERENCES

[1] C. C. Chang, and D. J. Buehrer, Transmitting multiple secrets securely in broadcasting networks, *Proc. of International Carnahan Conference on Security Technology*, pp. 19-21, 1993.

[2] C. C. Chang, and Y. P. Lai, A fast modular square computing method based on the generalized chinese remainder theorem for prime module, *Applied Mathematics and Computation*, vol. 161, no. 1, pp. 181-194, 2005.

[3] C. C. Chang, and C. H. Lin, A cryptosystem for secure broadcasting, *Proc. of National Science Council*, vol. 12, no. 4, pp. 233-239, 1988.

[4] C. C. Chang, and T. C. Wu, Broadcasting cryptosystem in computer networks using interpolating polynomials, *Computer Systems Science and Engineering*, vol. 6, no. 3, pp. 185-188, 1991.

[5] C. C. Chang, J. S. Yeh, and J. H. Yang, Generalized aryabhata remainder theorem, *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 4, pp. 1865-1871, 2010.

[6] C. H. Chiou, and W. T. Chen, Secure broadcasting using the secure lock, *IEEE Trans. Software Engineering*, vol. 15, no. 8, pp. 929-934, 1989.

[7] Data Encryption Standard, Federal Information Processing Standard Publication 46, National Technical Information Service, Springfield, VA. 1977.

[8] E. Ekrem, and S. Ulukus, Secure broadcasting using multiple antennas, *Journal of Communications and Networks*, vol. 12, no. 5, pp. 411-432, 2010.

[9] A. Fiat, and M. Naor, *Broadcast encryption*, LNCS 773, Springer, pp. 480-491, 1994.

[10] D. K. Gifford, Cryptographic sealing for information secrecy and authentications, *Communications of Association for Computing Machinery*, vol. 25, no. 4, pp. 274-286, 1982.

[11] C. Guo, and C. C. Chang, An authenticated group key distribution protocol based on the generalized chinese remainder theorem, *International Journal of Communication Systems*, vol. 27, no. 1, pp. 126-134, 2014.

[12] L. Harn, Group authentication, *IEEE Trans. on Computers*, vol. 62, no. 9, pp. 1893-1898, 2013.

[13] L. Harn, and C. L. Lin, Authenticated group key transfer protocol based on secret sharing, *IEEE Trans. on Computers*, vol. 59, no. 6, pp. 842-846, 2010.

[14] D. B. He, J. H. Chen, and J. Hu, A pairing-free certificateless authenticated key agreement protocol, *International Journal of Communication Systems*, vol. 25, no. 2, pp. 221-230, 2012.

[15] J. K. Jan, and Y. Y. Chern, A practical design for secure broadcasting using PKD concept, *Proc. of International Carnahan Conference on Security Technology*, pp. 22-27, 1993.

[16] J. K. Jan, and C. D. Yu, Yet another approach for secure broadcasting based upon single key concept, *Proc. of 25th IEEE International Carnahan Conference on Security Technology*, pp. 47-54, 1991.

[17] Y. P. Lai, and C. C. Chang, Parallel computational algorithms for generalized chinese remainder theorem, *Computers and Electrical Engineering*, vol. 29, no. 8, pp. 801-811, 2003.

[18] D. Qiao, M. C. Gursoy, and S. Velipasalar, Secure broadcasting over fading channels with statistical QoS constraints, *Global Telecommunications Conference (GLOBECOM 2010)*, Miami, USA, pp. 1-5, 2010.

[19] T. R. N. Rao, and C. H. Yang, Aryabhata remainder theorem: relevance to public-key crypto-algorithms, *Circuits, Systems, and Signal Processing*, vol. 25, no. 1, pp. 1-15, 2006.

[20] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signature and public-key cryptosystem, *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[21] T. C. Wu, and Y. S. Chang, Authorization-based group-oriented secure broadcasting system, *Journal of Information Science and Engineering*, vol. 15, no. 5, pp. 653-667, 1999.

[22] T. C. Wu, and Y. S. Yen, Cryptosystem for selectively broadcasting separate secrets, *Computer Systems Science and Engineering*, vol. 8, no. 2, pp. 121-124, 1993.

[23] Q. Xie, A new authenticated key agreement for session initiation protocol, *International Journal of Communication Systems*, vol. 25, no. 1, pp. 47-54, 2012.

[24] E. J. Yoon, and K. Y. Yoo, A secure broadcasting cryptosystem and its application to grid computing, *Future Generation Computer Systems*, vol. 27, no. 5, pp. 620-626, 2011.

[25] J. Zhang, and M. C. Gursoy, Collaborative relay beamforming for secure broadcasting, *Proc. of Wireless Communications and Networking Conference (WCNC)*, Sydney, Australia, pp. 1-6, 2010.