

METHOD AND SYSTEM FOR DISTRIBUTING ENCRYPTION AND  
DECRYPTION KEYS IN  
SECURE BROADCAST COMMUNICATION

5 Background of the Invention

1. Field of the Invention

The present invention relates to a technique of distributing a key for decryption in secure broadcast communication to restricted receivers.

2. Description of Related Art

10 Conventionally, as techniques of secure broadcast communication, some systems have been proposed.

For example, there is known a copied key method described in an article, S.J. Kent: "Security Requirements and Protocols for a Broadcast Scenario", IEEE Trans. Commun., COM-29, 6, pp. 778 - 786 (1981).

15 This copied key method is a fundamental system for secure broadcast communication, and is simple extension of the conventional one-to-one individual cipher communication. Namely, in this method, copies of one kind of key are distributed to a sender and a plurality of regular receivers. The sender encrypts information by use of the distributed copy key and sends  
20 the encrypted information. Each of the regular receivers uses the distributed copy key to decrypt the encrypted information.

Further, there is known a technique of distributing a common key using an individual key assigned for every receiver. For example, a system of key distribution by multiplexing-demultiplexing of an information  
25 sequence using the Chinese remainder theorem is described in an article, Lee, Tokiwa, et al: "A Multi-Address Communication Using a Method of



Multiplexing and Demultiplexing, 1986 Symposium on encryption and information security". Also, Mambo et al: "A Secure Broadcast Communication Method with Short Messages", IEICE TRNS. FUNDAMENTALS, VOL. E77-A, No. 8 AUGUST 1994 describes such a  
5 technique.

The system of multiplexing-demultiplexing an information sequence by use of the Chinese remainder theorem performs the following processes.

(1) Key generation process:

10 For receivers  $i$  ( $1 \leq i \leq s$ ),  $s$  integers  $g_1, g_2, \dots, g_s$  ( $r \leq s$ ) which are relatively prime to one another are generated, and  $g_i$  is distributed in advance to  $i$ -th receiver as secret key of that receiver  $i$ .

(2) Encryption process:

An information sequence of  $s$  items to be multiplexed is expressed  
15 as  $M_1, M_2, \dots, M_s$ . The sender calculates a multiplexed sentence  $F$  to be sent by:

$$F = \sum_{i=1}^k A_i G_i M_i \text{ mod } G$$

and broadcasts it. Here,  $G$ ,  $G_i$ , and  $A_i$  are defined as follows:

$$G = \prod_{i=1}^k g_i$$

$$G_i = G / g_i$$

$$A_i G_i \equiv 1(\text{mod } g_i)$$

20 and  $A_i$  is the smallest integer which satisfies the above equations.

(3) Decryption process:

Using  $g_i$ , the receiver  $i$  demultiplexes  $M_i$  from  $F$  by the following equation,



$$M_i = F \bmod g_i$$

Here,  $M_i$  is a common key to be distributed to the receiver  $i$ . Thus, according to this system, the copy key can be distributed in secret to the restricted receivers only.

5           Next, the system described in the literature, Mambo et al: "A Secure Broadcast Communication Method with Short Messages", IEICE TRNS. FUNDAMENTALS, VOL. E77-A, No. 8 AUGUST 1994 performs following processes.

(1) Key generation process:

10           A trusted center produces following information.

Secret key:

$$P = 2p + 1, Q = 2q + 1: \text{prime number } (p, q: \text{prime number})$$

$$e_i \in Z, 0 < e_i < L (1 \leq i \leq m)$$

Public key:

$$g \in Z, 0 < g < N$$

$$N = PQ$$

$$v_i = g^{e_i} \bmod N (1 \leq i \leq m)$$

15           For  $\sigma \in S$ , the center calculates  $s_\sigma$  that satisfies:

$$s_\sigma \sum_{i=1}^k e_{\sigma(i)} \equiv 1 \pmod{L}$$

and distributes it as secret key of a receiver  $U_\sigma$ . Here, the set  $S$  is defined as  $S = \{f | \text{one to one map } f: A\{1, 2, \dots, k\} \rightarrow B\{1, 2, \dots, m\}, m > k\}$ .

(2) Key distribution process:

20           A sender selects an integer  $r$  at random, and, in order to have a common key  $K$  defined as:

$$K = g^r \bmod N$$



in common with restricted receivers, calculates  $z_i$  that satisfies:

$$z_i = v_i' \bmod N \quad (1 \leq i \leq m)$$

and broadcasts  $z_i$  ( $1 \leq i \leq m$ ).

The receiver  $U\sigma$  uses the following equation:

5

$$K = \left( \prod_{i=1}^k z_{\sigma(i)} \right)^{s\sigma} \bmod N$$

to calculate the common key  $K$ .

### Summary of the Invention

In the above-described conventional method of key distribution by  
10 multiplexing using the Chinese remainder theorem, common key data for  
respective receivers are arranged serially and transmitted. Thus, broadcast  
data length becomes longer in proportion to the number of the receivers.  
Accordingly, it is not suitable for communication for millions of receivers or  
more, such as satellite broadcasting.

15 On the other hand, according to the system described in the above-  
referred literature, Mambo et al: "A Secure Broadcast Communication  
Method with Short Messages", IEICE TRNS. FUNDAMENTALS, VOL. E77-  
A, No. 8 AUGUST 1994, data for distributing the common key can be  
shortened. In this system, however, it is not possible to have the key  
20 commonly used among restricted receivers belonging to any set of receivers.

Further, in all systems, when there are a plurality of senders,  
receivers must obtain the above-described user secret key for respective  
senders, and manage them.

Thus, an object of the present invention is to provide a key  
25 distribution system in which a receiver can receive delivery of respective



common keys from a plurality of senders by means of only one secret key. A further object is to make it possible that, in such a key distribution system, a common key for data decryption can be commonly owned only among any sender and any set of receivers, and to shorten broadcast data for distributing  
5 a common key even when the number of receivers are large.

To attain the above objects, the present invention provides a method of key distribution having an encryption-decryption key of secure broadcast communication commonly used among a plurality of senders and a plurality of receivers in a communication system comprising apparatuses of  
10 said plurality of senders and apparatuses of said plurality of receivers, wherein:

in an apparatus of a trusted center provided separately from said senders and said receivers, first key information, which is common to said plurality of senders and is used for a key commonly used among said senders  
15 and said receivers, is produced and distributed to prescribed receivers, while second key information which is used for a key commonly used among said senders and said receivers is produced and distributed to said senders;

in apparatuses of said senders, third key information, which is used by said receivers together with said first key information to calculate an  
20 encryption-decryption key used by the sender in question in broadcast communication, is produced using the second key information distributed from said trusted center and is sent to said receivers who have a key in common with said sender; and

in an apparatus of a receiver, the encryption-decryption key which  
25 is used for broadcast communication by the sender who distributed said third key information is obtained using the first key information distributed from



said trusted center and the third key information distributed from said sender.

According to the present method of key distribution, it is sufficient for each receiver to have only the first key information distributed from the trusted center as a user secret key. When an encryption-decryption key of a new sender is to be obtained, it is not necessary to receive distribution of new user secret key.

In detail, the present invention provides a method of key distribution, in which an encryption-decryption key for secure broadcast communication performed by said sender is distributed to receivers, in a communication system comprising apparatuses of a plurality of senders and apparatuses of a plurality of receivers, and an apparatus of a trusted center, comprising:

a step, in which, in the apparatus of the trusted center,

$$e_i \in Z \quad (1 \leq i \leq m)$$

are produced as trusted center secret key,

$$t_A \in Z$$

is produced as sender registration key of a sender A, and, as receiver secret key,  $\sigma_x \in S_{km}$  and

$$s_x(\sigma_x) \in Z$$

are produced (here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$  defined as:

$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m \}$$

it is expressed as:

$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A),$$



with " $\sim$ " becoming an equivalence relation on  $S_{km}$ , leading to an expression:

$$\tilde{S}_{km} = S_{km} / \sim$$

), and the receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  are distributed to the receiver x;

a step, in which, in the apparatus of the sender A,

5 sender secret key  $g_A$ ,  $L_A$ , and a finite Abelian group  $G_A$  satisfying:

$$\begin{aligned} g_A &\in G_A \\ L_A &= \text{ord}_{G_A}(g_A) \end{aligned}$$

are produced (here,

$$\text{ord}_{G_A}(g)$$

means the least positive integer a satisfying:

10 
$$g^a = 1 (\in G_A)$$

), and the sender secret key  $g_A$  is sent to said trusted center;

a step, in which, in the apparatus of the trusted center, receiver registration data:

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

15 is calculated from the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and the receiver secret key  $s_x(\sigma_x)$ ,  $\sigma_x$ , and the receiver registration data  $s_x(\sigma_x, A)$  is sent to the sender A, and key distribution data:

$$y_{Ai} = g_A^{t_A e_i} (\in G_A) \quad (1 \leq i \leq m)$$

is calculated from  $g_A$  received from the sender A, the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and this key distribution data  $y_{Ai}$  is sent to  
20 the sender A;

a step, in which, in the apparatus of the sender A, random integers  $r$ ,  $r'$  are produced, receiver registration key  $r_x(\sigma_x, A)$  satisfying:

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$



is calculated from the receiver registration data  $s_x(\sigma_x, A)$  received from said trusted center, the sender secret key  $L_A$ , and the random integer  $r'$ ; the receiver registration key  $r_x(\sigma_x, A)$  is sent to the receiver  $x$ ; and key distribution data defined as:

$$5 \quad z_{Ai} = y_{Ai}^{r'} \quad (\in G_A) \quad (1 \leq i \leq m)$$

is calculated from the key distribution data  $y_{Ai}$  received from said trusted center, and the random integer  $r$ , and the key distribution data  $z_{Ai}$  is broadcasted to each receiver; and

a step, in which, in the apparatus of the receiver  $x$ , an encryption-  
10 decryption key  $K_A$  used for broadcast communication is calculated using:

$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A)s_x(\sigma_x)} \quad (\in G_A)$$

from the receiver registration key  $r_x(\sigma_x, A)$  received from the sender, the key distribution data  $z_{Ai}$ , and the receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$ , with the encryption-decryption key  $K_A$  being produced by the sender  $A$ , using:

$$15 \quad K_A = g_A^{r'} \quad (\in G_A).$$

According to this method of key distribution, it is not necessary for the receivers to own private keys which are different for respective senders. Further, in secure broadcast communication, even when the number of receivers is large, the length of the key distribution data can be made short.  
20 Further, in the present method of key distribution, the receiver secret key is made secret from the senders and the sender secret key is more reliably made secret from the receivers since the sender registration key is owned only by the trusted center in secret. Accordingly, security against impropriety is improved.

25

This Sheet Has Been Replaced



## Brief Description of the Drawings

Fig. 1 is a block diagram showing a configuration of a key distribution system according to an embodiment of the present invention;

Fig. 2 is a block diagram showing a configuration of a trusted center side apparatus according to a first embodiment of the present invention;

Fig. 3 is a block diagram showing a configuration of a sender side apparatus according to the first embodiment of the present invention;

Fig. 4 is a block diagram showing a configuration a receiver side apparatus according to the first embodiment of the present invention;

Fig. 5 is a view showing information flow caused by key distribution process in the first embodiment of the present invention;

Fig. 6 is a block diagram showing a configuration of a receiver side apparatus according to a second embodiment of the present invention;

Fig. 7 is a block diagram showing a configuration of a trusted center side apparatus according to a fifth embodiment of the present invention;

Fig. 8 is a block diagram showing a configuration of a sender side apparatus according to the fifth embodiment of the present invention; and

Fig. 9 is a block diagram showing a configuration of a receiver side apparatus according to the fifth embodiment of the present invention.

## Detailed Description

In the following, there will be described a key distribution system according to an embodiment of the present invention.

Firstly, the first embodiment will be described.

Fig. 1 shows a configuration of a key distribution system according to the present embodiment of the invention.

This Sheet Has Been Replaced



As shown in the figure, the present system comprises a trusted center side apparatus 100, sender side apparatuses 200, and receiver side apparatuses 300. These apparatuses are connected to one another via communication lines 400. The trusted center side apparatus 100 is the one  
5 and only apparatus used by the trusted center organization in the system, while the system has a plurality of sender side apparatuses 200 and a plurality of receiver side apparatuses 300.

Fig. 2 shows a configuration of the trusted center side apparatus 100.

10 As shown in the figure, the trusted center side apparatus 100 comprises a random number generator 101, a prime number generator 102, a power multiplier 103, a remainder computing unit 104, an arithmetic unit 105, a memory 106, and a communication unit 107. The trusted center side apparatus 100 is connected to receiver side portable apparatuses 306 which  
15 are delivered to receivers off line.

Fig. 3 shows a configuration of the sender side apparatus 200.

As shown in the figure, the sender side apparatus 200 comprises a random number generator 201, a prime number generator 202, a power multiplier 203, a remainder computing unit 204, an arithmetic unit 205, a  
20 memory 206, a communication unit 207, an encryption-decryption unit 208, an authentication unit 209, and an accounting unit 210.

Fig. 4 shows a configuration of the receiver side apparatus 300.

As shown in the figure, the receiver side apparatus 300 comprises a power multiplier 301, a remainder computing unit 302, an arithmetic unit  
25 303, a memory 304, a communication unit 305, a receiver side portable apparatus 306 which has been delivered off line from the trusted center, an



encryption-decryption unit 307, and an authentication unit 308.

In the following, three processes will be described, i.e., a preparation process, a key distribution process, and an encryption-decryption process.

5 First, the preparation process will be described.

(1) Preparation process

(i) A sender A uses the random number generator 201, the prime number generator 202, the power multiplier 203, the remainder computing unit 204 and the arithmetic unit 205 within the sender side apparatus 200, to  
10 produce the following keys, and makes only public key open to the public.

Secret key:

$P_A, Q_A$ : prime numbers

$L_A = \text{lcm}(\text{ord}_{P_A}(g_A), \text{ord}_{Q_A}(g_A))$

$g_A \in Z, 0 < g_A < N_A$

$r, r' \in Z, 0 < r, r' < L_A$

Public key:

$N_A (= P_A Q_A)$

15 The secret key is stored in the memory 206. Further, pieces of the secret key  $g_A, L_A$  are sent to the trusted center by means of the communication unit 207.

(ii) The reliable trusted center uses the arithmetic unit 105 within the trusted center side apparatus 100 to generate the following information.

20 Trusted center secret key:

$e_i \in Z (1 \leq i \leq m)$

Sender registration key for the sender A:

$t_A \in Z, 0 < t_A < L_A$

Receiver secret key for a receiver x:



$$s_x(\sigma_x) \in Z, \quad 0 < t_A < L_A$$

All these are stored in the memory 106 together with  $\sigma_x$ .

Here, for a set:

$$S_{km} = \{\sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \\ \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m\}$$

5 when  $\sigma, \sigma' \in S_{km}$ , it is assumed that:

$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$$

Here, " $\sim$ " becomes an equivalence relation on  $S_{km}$ , and

$$\tilde{S}_{km} = S_{km} / \sim$$

Further, the trusted center takes the receiver secret key  $s_x(\sigma_x)$  from  
10 the memory 106, stores it in the receiver side portable apparatus 306  
together with  $\sigma_x$ , and delivers that apparatus to the receiver x off line. Of  
course, it may be delivered to the receiver in another way.

Next, the key distribution process will be described.

(2) Key distribution process

15 Fig. 5 shows information flow among the trusted center, senders  
and receivers in the present key distribution process.

(i) The trusted center uses the remainder computing unit 104 and the  
arithmetic unit 105 within the trusted center side apparatus 100 to calculate  
receiver registration key  $s_x(\sigma_x, A)$  defined as:

$$20 \quad s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \bmod L_A$$

from  $L_A$  received from the sender A, trusted center secret key  $e_i$ ,  $\sigma_x$ , receiver  
secret key  $s_x(\sigma_x)$  and the sender registration key  $t_A$ , and sends it to the sender  
A using the communication unit 107.



Further, the trusted center uses the power multiplier 103, the remainder computing unit 104 and the arithmetic unit 105 to calculate sender key distribution data  $y_{Ai}$  of the sender A:

$$y_{Ai} = g_A^{t_i} \bmod N_A \quad (1 \leq i \leq m)$$

5 from  $g_A$  received from the sender A, sender public key  $N_A$  of the sender A, and trusted center public key  $e_i$ , and sends it to the sender A by means of the communication unit 107.

(ii) The sender A generates random integers  $r, r'$  by means of the random number generator 201 within the sender side apparatus 200, and  
10 stores them in the memory 206. Further, the sender A uses the power multiplier 203, the remainder computing unit 204 and the arithmetic unit 205 to calculate data encryption key  $K_A$  defined by:

$$K_A = g_A^{r'} \bmod N_A$$

from these random integers  $r, r'$ , his own secret key  $g_A$  and his own public key  
15  $N_A$ , and stores it in the memory 206. Then, for the purpose of having the key  $K_A$  in common with the receiver  $x$ , the sender A uses the remainder computing unit 204 and the arithmetic unit 205 to calculate receiver registration key  $r_x(\sigma_x, A)$  of the receiver  $x$ , satisfying:

$$r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

20 from his own secret key  $L_A$ , the random number  $r'$  and the receiver registration key  $s_x(\sigma_x, A)$ , and sends it to the receiver by means of the communication unit 207.

Further, the sender A uses the power multiplier 203, the remainder computing unit 204 and the arithmetic unit 205 within the sender side  
25 apparatus 200 to calculate receiver key distribution data  $z_{Ai}$  defined by:

$$z_{Ai} = y_{Ai}^{r'} \bmod N_A \quad (1 \leq i \leq m)$$



from his own public key  $N_A$ , the random number  $r$  and  $y_{Ai}$  received from the trusted center, and broadcasts it to the receivers by means of the communication unit 207.

In the above process, the trusted center performs a part of the processes for producing  $r_x(\sigma_x, A)$  and  $z_{Ai}$ , for one thing, to keep  $\sigma_x$  of the receiver  $x$ , the receiver secret key  $s_x(\sigma_x)$  and the sender registration number  $t_A$  secret from the sender  $A$  so as to prevent improprieties by the sender  $A$ .

(iii) The receiver  $x$  uses the power multiplier 301, the remainder computing unit 302 and the arithmetic unit 303 within the receiver side apparatus 300 to calculate the data encryption key  $K_A$  by the expression:

$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \mod N_A$$

from the key distribution data  $z_{Ai}$  received from the sender  $A$ , the receiver registration key  $r_x(\sigma_x, A)$ ,  $\sigma_x$  and the receiver secret key  $s_x(\sigma_x)$  delivered from the trusted center and the sender public key  $N_A$  opened to the public, and stores it in the memory 304.

By the above-described process, the sender  $A$  and the receiver  $x$  can have the key  $K_A$  in common. Similarly, for any other sender and any other receiver, it is possible to have a key in common. In that case, receiver key distribution data  $z_{Ai}$  broadcasted by each sender is the same for each receiver.

Further, in the above-described process, the receiver  $x$  receives the key distribution data  $z_{Ai}$  and the receiver registration key  $r_x(\sigma_x, A)$  from the sender  $A$ . These  $z_{Ai}$  and  $r_x(\sigma_x, A)$  have been produced under the effect of the sender registration number  $t_A$  of the sender  $A$ , and  $t_A$  is kept secret from the receiver. Thus, owing to the use of the above-described sender registration number  $t_A$ , it becomes very difficult for the receiver  $x$  to deduce a data



encryption key  $K_B$  of another sender B from the key distribution data  $z_{Ai}$  and the receiver registration key  $r_x(\sigma_x, A)$  received from the sender A and key distribution data  $z_{Bi}$  broadcasted by the sender B.

5 In the following, the encryption-decryption process will be described.

### (3) Encryption-decryption process

(i) The sender A uses the encryption-decryption unit 208 within the sender side apparatus 200 to encrypt data P with the common key  $K_A$  produced in the key distribution process. Then, the sender A sends a cipher  
10 text  $C=E(K_A: P)$  to a receiver by means of the communication unit 207.

(ii) The receiver uses the communication unit 305 within the receiver side apparatus 300 to receive the public key C, and uses the encryption-decryption unit 307 to decrypt the public key C with the common key  $K_A$  stored in the memory 304, so as to obtain the original data.

15 The above is the first embodiment of the present invention.

In the conventional technique, when a sender newly enters a key distribution system, it is necessary for the sender to produce  $\sigma_x$  and receiver secret key  $s_x(\sigma_x)$  by himself and to deliver them to a receiver off line. On the other hand, according to the key distribution system of the first embodiment,  
20 it suffices for a sender who newly enters the system to produce the sender secret key  $P_A, Q_A, L_A, g_A$  and the sender public key  $N_A$ . Further, receiver secret key owned by a receiver is same for all the senders. Thus, when a receiver wishes to receive data from a new sender, it is not necessary to obtain new receiver secret key.

25 Further, the receiver registration key  $r_x(\sigma_x, A)$  makes it possible to have a common key in common with receivers belonging to any set of



receivers, for data encryption and decryption concerning them only. Even when the number of receivers is large, it is not necessary to correspondingly lengthen the key distribution data  $z_{Ai}$  broadcasted for distribution of a common keys.

5 In the above processes, it is possible alternatively that the sender sends the sender secret key  $L_A$  to the trusted center in advance, and in the step of the preparation process, the trusted center generates the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and the receiver secret key  $s_x(\sigma_x)$  satisfying:

$$\begin{aligned} e_i &\in Z, \quad 0 < e_i < L_A, \quad (1 \leq i \leq m) \\ t_A &\in Z, \quad 0 < t_A < L_A \\ 10 \quad s_x(\sigma_x) &\in Z, \quad 0 < s_x(\sigma_x) < L_A, \end{aligned}$$

and, in the step of the key distribution process, the trusted center calculates the receiver registration key  $s_x(\sigma_x, A)$  by:

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \mod L_A$$

from the sender secret key  $L_A$ , the trusted center secret key  $e_i$ , the sender  
15 registration key  $t_A$  and the receiver secret key  $s_x(\sigma_x)$ .

Next, a second embodiment of the present invention will be described.

In the second embodiment of the present invention, the receiver side portable apparatus 300 of the above first embodiment is provided with a  
20 power multiplier 3064, a remainder computing unit 3063, an arithmetic unit 3061 and a memory 3062 as shown in Fig. 6. Further, the process of calculating the data encryption key  $K_A$  in the receiver side apparatus 300 of the above first embodiment is partly performed in the receiver side portable



apparatus 306.

Namely, in the second embodiment, (1) in the step of the preparation process, the trusted center stores  $\sigma_x$  and the receiver secret key  $s_x(\sigma_x)$  in the receiver side portable apparatus 306 (such as an IC card (a smart card)), and delivers them to the receiver x.

Then, (2) in the key distribution process, the receiver x outputs the key distribution data  $z_{Ai}$  stored in the memory within the receiver side apparatus 300 to the receiver side portable apparatus 306. Next, within the receiver side portable apparatus 306, the receiver x uses the power multiplier 3064 and the remainder computing unit 3063 to calculate:

$$\xi_x(\sigma_x, A) = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \bmod N_A$$

from  $\sigma_x$ , the receiver secret key  $s_x(\sigma_x)$ , the key distribution data  $z_{Ai}$  and the sender public key  $N_A$ , and outputs the calculated result  $\xi_x(\sigma_x, A)$  to the receiver side apparatus 300.

Next, the receiver x uses the power multiplier 301, the remainder computing unit 302 and the arithmetic unit 303 within the receiver side apparatus 300 to calculate the data encryption key  $K_A$  by:

$$K_A = \xi_x(\sigma_x, A)^{r_x(\sigma_x, A)} \bmod N_A$$

from  $\xi_x(\sigma_x, A)$  outputted to the receiver side apparatus 300, the receiver registration key  $r_x(\sigma_x, A)$  stored in the memory 304, and the sender public key  $N_A$ , and stores it in the memory 304.

Thus,  $\sigma_x$  and the receiver secret key  $s_x(\sigma_x)$  are prevented from being outputted outside the receiver side portable apparatus 306, so that these are prevented from being stolen by electronic duplicating or the like.

The above is the second embodiment of the present invention.



Next, a third embodiment of the present invention will be described.

The third embodiment of the present invention is different from the above-described first embodiment in that the value of  $r$  in the equation:

$$K_A = g_A^{rr'} \bmod N_A$$

5 is changed periodically every short time period, and  $z_{Ai}$  obtained by using the changed  $r$  is broadcasted periodically for update of the data encryption-decryption key  $K_A$  calculated in the sender side apparatus 200 and in the receiver side apparatus 300.

Further, in the present embodiment, the value of  $r'$  is made to be  
10 characteristic to sending data so as to identify data broadcasted by a sender. Namely, a registration key  $r_x(\sigma_x, A)$  which the receiver  $x$  received from a sender to decrypt certain broadcast data or a set of broadcast data is characteristic to that broadcast data. To obtain another broadcast data or another set of broadcast data, the receiver  $x$  must receive another  $r_x(\sigma_x, A)$  for  
15 that broadcast data or that set of broadcast data.

The above is the third embodiment of the present invention.

Next, a fourth embodiment of the present invention will be described.

The fourth embodiment is different from the above-described first  
20 embodiment in that authentication of receivers is performed so as to charge receivers who have a common key  $K_A$  in common for fee-charging data  $P$  encrypted with the key  $K_A$  and sent by a sender.

Namely, in the fourth embodiment of the present invention, following processes are further performed.

25 (1) Preparation process

(i) The trusted center uses the arithmetic unit 105 within the trusted



center side apparatus 100 to produce a number  $UID_x$  for the receiver  $x$  in advance, and stores it in the receiver side portable apparatus 306 together with the receiver secret key  $s_x(\sigma_x)$ , and delivers that apparatus. Further  $UID_x$  is stored in the memory 106, so as to correspond to  $s_x(\sigma_x)$ .

5 (ii) The sender  $A$  uses the arithmetic unit 205 within the sender side apparatus 200 to produce his own number  $BIDA$ , and stores it in the memory 206. The sender  $A$  sends  $BIDA$  to the trusted center by means of the communication unit 207.

(iii) The trusted center receives  $BIDA$ , the number of the sender  $A$ ,  
10 using the communication unit 107 within the trusted center side apparatus 100, and stores it in the memory 106 so as to correspond to the sender registration key  $t_A$ .

(iv) The receiver  $x$  uses the authentication unit 308 within the receiver side apparatus 300 to produce information for authentication from the  
15 receiver secret key  $s_x(\sigma_x)$ , and sends it to the sender  $A$ .

(v) The sender  $A$  confirms the information for authentication by means of the authentication unit 209 within the sender side apparatus 200.

As the method of authentication, any conventionally-known authentication method may be employed in which authentication is not  
20 effected as long as the receiver does not know  $s_x(\sigma_x)$ . However, it is necessary for the sender to be prevented from knowing the receiver private key  $s_x(\sigma_x)$  itself.

For example, authentication of the receiver  $x$  may be performed as in the following processes according to a method employing a signature using  
25 the RSA algorithm (described in an article by, R. L. Rivest, A. Shamir, L. Adelman: "A Method for Obtaining Digital Signatures and Public Key

This Sheet Has Been Replaced



Cryptosystems", Commun. of the ACM, Vol. 21, No. 2, pp. 120-126, 1978).

(1) The trusted center uses the arithmetic unit 105 within the trusted center side apparatus 100 to produce  $(y_x, n_x)$  satisfying:

$$\begin{aligned} s'_x y_x &\equiv 1 \pmod{\text{lcm}(p_x - 1, q_x - 1)} \\ n_x &= p_x q_x \quad (p_x, q_x : \text{prime numbers}) \end{aligned}$$

5 for the receiver x, and deliver them to the sender in advance. Here, for a function  $\pi$  which has been opened,  $s'_x$  is defined as  $s'_x = \pi(s_x(\sigma_x))$ .

(2) The receiver x uses the authentication unit 308 within the receiver side apparatus 300 to calculate a hash value  $(h(w); 0 < h(W) < n_x)$  of broadcast data W using a unidirectional hash function h as public key, and produces a  
10 signature for h(W) by the following expression:

$$\text{sgn}_x(h(W)) = h(W)^{s'_x} \pmod{n_x}$$

using the private key  $s'_x$ , and sends it to the sender by means of the communication unit 305 together with a data sending request.

(3) The sender uses the authentication unit 209 within the sender side  
15 apparatus 200 to confirm that:

$$\text{sgn}_x(h(W))^{y_x} = h(W) \pmod{n_x}$$

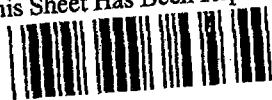
is satisfied.

After the authentication, the sender A uses the communication unit 207 within the sender side apparatus 200 to send his own number BIDA and  
20 UIDx, the number of the receiver x, to the trusted center.

The trusted center uses the arithmetic unit 105 within the trusted center side apparatus 100 to calculate the receiver registration data  $s_x(\sigma_x, A)$  expressed by:

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \pmod{LA}$$

This Sheet Has Been Replaced



from the sender registration key  $t_A$  and the receiver secret key  $s_x(\sigma_x)$  corresponding to the sender number BIDA and the receiver number UIDx received respectively, and sends it to the sender A.

The sender uses the remainder computing unit 204 and the arithmetic unit 205 within the sender side apparatus 200 to calculate the receiver registration key  $r_x(\sigma_x, A)$  satisfying:

$$r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

from the receiver registration key  $s_x(\sigma_x, A)$  received from the trusted center, and sends it to the receiver by means of the communication unit 207. At that time, in the case that data to be delivered being encrypted with the common key  $K_A$  (namely, the data which the receiver requested to the sender) is chargeable, the sender A charges the receiver x by means of the accounting unit 210.

The above is the fourth embodiment of the present invention.

Next, a fifth embodiment of the present invention will be described.

The fifth embodiment of the present invention is an extension of the copy key system described in the Description of Related Art to the system shown in Fig. 1 which includes a plurality of senders, a plurality of receivers and a trusted center.

Fig. 7 shows a configuration of a trusted center side apparatus 100 according to the fifth embodiment of the present invention. As shown in the figure, the trusted center side apparatus 100 comprises a random number generator 111, an arithmetic unit 112, a memory 113, and a communication unit 114. Further, Fig. 8 shows a configuration of a sender side apparatus 200 according to the fifth embodiment of the present invention. As shown in the figure, the sender side apparatus 200 comprises a random number



generator 211, an arithmetic unit 212, an encryption-decryption unit 213, a memory 214, and a communication unit 215. Further, Fig. 9 shows a configuration of a receiver side apparatus 300 according to the fifth embodiment of the present invention. As shown in the figure, the receiver side apparatus 300 comprises an arithmetic unit 311, an encryption-decryption unit 312, a memory 313, and a communication unit 314.

In the present embodiment, firstly, the following process is performed as a preparation process.

(1) Preparation process

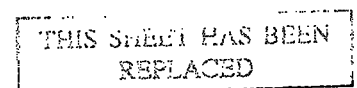
- 10 (i) The trusted center uses the random number generator 111 within the trusted center side apparatus 100 to generate a secret key  $K_0$  and stores it in the memory 113. Also, the trusted center distributes it to senders and receivers.
- (ii) The sender A uses the random number generator 211 within the sender side apparatus 200 to generate sender registration key BIDA, and sends it to the receivers by means of the communication unit 215.

Thereafter, the following process is performed as a key distribution process.

(2) Key distribution process

- 20 (i) The sender A uses the arithmetic unit 212 within the sender side apparatus 200 to calculate a common key  $KA' = F(K_0, BIDA)$  from the secret key  $K_0$  and the sender registration key BIDA, using a suitable one-way function  $F$ .
- (ii) The receiver uses the arithmetic unit 312 within the receiver side apparatus 300 to calculate the common key  $KA' = F(K_0, BIDA)$  from the secret key  $K_0$  distributed from the trusted center and the sender registration key

This Sheet Has Been Replaced



BIDA received from the sender, using the one-way function  $F$ .

(iii) The sender A uses the random number generator 211 within the sender side apparatus 200 to produce a suitable integer  $r$  and sends it to the receiver by means of the communication unit 215. Further, the sender A  
5 calculates a data encryption-decryption key  $DK=F'(r, KA)$  from the integer  $r$  and the common key  $KA$  using a suitable function  $F'$ , and stores it in the memory 214.

(iv) The receiver uses the arithmetic unit 312 within the receiver side apparatus 300 to calculate the data encryption-decryption key  $DK=F'(r, KA)$   
10 from the integer  $r$  received from the sender A and the common key  $KA$ , and stores it in the memory 314.

After the distribution of the data encryption-decryption key  $DK$  by the key distribution process, an encryption-decryption process is performed as described in the following.

15 (3) Encryption-decryption process

(i) The sender A encrypts data  $P$  to be delivered with the data encryption-decryption key  $DK$  using the encryption-decryption unit 213 within the sender side apparatus 200, and sends it to the receiver  $x$  by means of the communication unit 215.

20 (ii) The receiver receives the encrypted delivered data  $P$  by the communication unit 314 within the receiver side apparatus 300, and decrypts it with the data encryption-decryption key  $DK$  using the encryption-decryption unit 312.

In the above-described fifth embodiment of the present invention  
25 also, a single piece of secret key suffices for a receiver to have respective common keys of a plurality of senders in common with them.



Next, a sixth embodiment of the present invention will be described.

In the sixth embodiment of the present invention, senders and receivers have a common key in common among them, through cipher communication using respective keys of the receivers.

5           Configurations of the whole system, a trusted center side apparatus 100, a sender side apparatus 200, and a receiver side apparatus 300 according to the present embodiment are similar to those in the above-described fifth embodiment of the present invention.

          In the present embodiment, the following process is performed as a  
10   preparation process.

(1) Preparation process

(i)       The trusted center uses the random number generator 111 within the trusted center side apparatus 100 to produce secret key  $s_x$  of the receiver  $x$ , and delivers it to the receiver. Further, the trusted center uses the  
15   random number generator 111 to produce BIDA, the number of the sender  $A$ , and distributes it to the sender  $A$  and the receiver  $x$ .

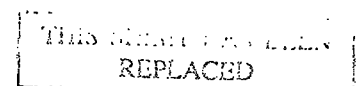
(ii)      The sender  $A$  uses the random number generator 211 within the sender side apparatus 200 to produce the common key  $K_A$ .

          Thereafter, the following process is performed as a key distribution  
20   process.

(2) Key distribution process

(i)       The trusted center uses the arithmetic unit 112 within the trusted center side apparatus 100 to calculate a session key  $K_{Ax}$ , which is to be used in a session between the receiver  $x$  and the sender  $A$  and defined as  $K_{Ax}=F(s_x,$   
25    $K_A)$  using a suitable one-way function  $F$ . The trusted center calculates  $K_{Ax}$  from BIDA, the number of the sender  $A$ , and the receiver secret key  $s_x$ , and

This Sheet Has Been Replaced



stores it in the memory 113.

(ii) The receiver x uses the arithmetic unit 312 within the receiver side apparatus 300 to calculate  $K_{Ax}=F(s_x, BIDA)$  from the number of the sender A BIDA and his own secret key  $s_x$  using the one-way function  $F$ , and stores it in the memory 313.

(iii) The sender A uses the encryption-decryption unit 213 within the sender side apparatus 200 to encrypt the common key  $K_A$  with the session key  $K_{Ax}$  to obtain key distribution data  $K_{Cx}$ , and sends the key distribution data  $K_{Cx}$  to the receiver by means of the communication unit 215. Further, the sender A uses the random number generator 211 to produce a suitable integer  $r$ , and sends it to the receiver by means of the communication unit 215. In addition, the sender A uses the arithmetic unit 212 to calculate a data encryption-decryption key  $DK=F'(r, K_A)$  from the integer  $r$  and the common key  $K_A$  using a suitable function  $F'$ , and stores it in the memory 214.

(iv) The receiver x receives the key distribution data  $K_{Cx}$  from the sender A, and uses the encryption-decryption apparatus 303 within the receiver side apparatus 300 to decrypt the key distribution data  $K_{Cx}$  with the session key  $K_{Ax}$ . Then, the receiver x uses the arithmetic unit 302 to calculate the data encryption-decryption key  $DK=F'(r, K_A)$  from the decrypted common key  $K_A$  and the received integer  $r$ , using the function  $F'$ , and stores it in the memory 303.

After the distribution of the data encryption-decryption key  $DK$  by the key distribution process, an encryption-decryption process is performed as described in the following.

### (3) Encryption-decryption process

(i) The sender A uses the encryption-decryption unit 203 within the

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED

sender side apparatus 200 to encrypt data P to be delivered with the data encryption-decryption key DK, and sends it to the receiver x by means of the communication unit 205.

(ii) The receiver x receives the encrypted delivered data P through the communication unit 305 within the receiver side apparatus 300. Then, the receiver x uses the encryption-decryption unit 303 to decrypt the received data P with the data encryption-decryption key DK.

The sender A may change the value of the common key  $K_A$  periodically so as to change the value of the data encryption-decryption key DK periodically.

According to the above-described sixth embodiment of the present invention also, the receiver can have respective common keys of a plurality of senders in common with them, by means of single piece of secret key.

Next, a seventh embodiment of the present invention will be described.

Similarly to the above-described sixth embodiment, in the seventh embodiment of the present invention, senders and receivers have a common key in common among them by cipher communication using respective keys of the receivers.

Configurations of the whole system, a trusted center side apparatus 100, a sender side apparatus 200, and a receiver side apparatus 300 according to the present embodiment are similar to those in the above-described fifth embodiment of the present invention.

In the present seventh embodiment, the following process is performed as a preparation process.

(1) Preparation process

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED

- (i) The trusted center uses the random number generator 111 and the arithmetic unit 112 within the trusted center side apparatus 100 to produce a private key  $s_x$  and public key  $p_x$  of the receiver  $x$  according to a suitable open key cryptographic system  $E$  and sends  $s_x$  to the receiver. Further, the
- 5 trusted center produces BIDA, a number of the sender  $A$ , using the random number generator 111, and delivers or sends it to the sender  $A$  and the receiver  $x$ .
- (ii) The sender  $A$  uses the random number generator 211 within the sender side apparatus 200 to produce a common key  $K_A$ , and stores it in the
- 10 memory 114.
- Thereafter, the following process is performed as a key distribution process.
- (2) Key distribution process
- (i) The sender  $A$  uses the encryption-decryption unit 213 within the sender side apparatus 200 to calculate a key distribution data  $K_{Cx}=E(p_x, K_A)$
- 15 from the receiver public key  $p_x$  and the common key  $K_A$  employing a suitable above-described public key cipher system  $E$ . Then, the sender  $A$  sends  $K_{Cx}$  to the receiver  $x$  by means of the communication unit 215.
- (ii) The receiver  $x$  uses the encryption-decryption unit 313 within the receiver side apparatus 300 to encrypt, with his own private key  $s_x$ , the key
- 20 distribution data  $K_{Cx}$  received from the sender  $A$ , and stores the encrypted common key  $K_A$  in the memory 314.
- (iii) The sender  $A$  uses the random number generator 211 within the sender side apparatus 200 to generate a suitable integer  $r$ , and sends it to the receiver  $x$  by means of the communication unit 215. Further, the sender  $A$
- 25 uses the arithmetic unit 212 to calculate the data encryption-decryption key  $DK=F(r, K_A)$  from the integer  $r$  and the common key  $K_A$  using a suitable



function  $F$ , and stores it in the memory 214.

- (iv) The receiver  $x$  uses the arithmetic unit 312 within the receiver side apparatus 300 to calculate the data encryption-decryption key  $DK=F(r, K_A)$  from the common key  $K_A$  and the integer  $r$  received from the sender, using the function  $F$ , and stores it in the memory 314.

After the distribution of the data encryption-decryption key  $DK$  by the key distribution process, an encryption-decryption process is performed as described in the following.

(3) Encryption-decryption process

- (i) The sender  $A$  uses the encryption-decryption unit 213 within the sender side apparatus 200 to encrypt data to be delivered  $P$  with the data encryption-decryption key  $DK$ , and sends it to the receiver  $x$  by means of the communication unit 213.
- (ii) The receiver  $x$  receives the encrypted delivered data  $P$  through the communication unit 314 within the receiver side apparatus 300. Then, the receiver  $x$  decrypts the data  $P$  with the data encryption-decryption key  $DK$  using the encryption-decryption unit 312.
- (iii) The sender  $A$  changes the value of the common key  $K_A$  periodically so as to change the data encryption-decryption key  $DK$ .

According to the above-described seventh embodiment of the present invention also, the receiver can have respective common keys of a plurality of senders in common with them, using a single piece of secret key.

Next, an eighth embodiment of the present invention will be described.

The eighth embodiment of the present invention is similar to the above-described sixth and seventh embodiments except that sending of the

This Sheet Has Been Replaced



key distribution data  $K_{Cx}$  from the sender to the receiver is modified as described in the following.

Namely, in the present eighth embodiment, the sender A separates the set of all of the receivers into some subsets. Next, in sending key distribution data  $K_{Ci}$  ( $1 \leq i \leq n$ ,  $n$ : the number of the receivers) to the receivers, the sender assigns communication channels to the above-described subsets of the receivers respectively, and sends the key distribution data  $K_{Ci}$  to the receivers through the communication unit 215 within the sender side apparatus 200.

On the other hand, any receiver  $x$  receives the key distribution data  $K_{Cx}$  by the communication unit 314 within the receiver side apparatus 300 through the communication channel assigned to the subset to which he belongs.

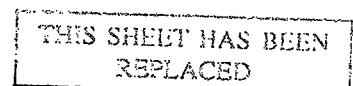
The embodiments of the present invention have been described above.

Each of the above-described processes performed by the trusted center side apparatus 100, the sender side apparatus 200, and the receiver side apparatus 300 may be performed by a computer which executes programs describing procedures for performing respective processes. In that case, each program describing a procedure for performing a process may be stored in a storing medium to be supplied to each computer.

As described above, according to the present invention, a receiver can receive distribution of respective common keys of a plurality of senders, using only one receiver secret key.

Further, in some inventions disclosed herein, it is possible to have a common key for data encryption and decryption in common among any

This Sheet Has Been Replaced



sender and receivers belonging to any set of receivers. Further, even if the number of the receivers is large, it is possible to realize common key distribution using short broadcast communication data for distribution of a common key.

---

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED

What is claimed is:

- 1 1. A method of key distribution having an encryption-decryption  
2 key of secure broadcast communication in common among a plurality of  
3 senders and a plurality of receivers in a communication system  
4 comprising apparatuses of said plurality of senders and apparatuses of  
5 said plurality of receivers, wherein:
  - 6 in an apparatus of a trusted center provided separately from  
7 said senders and said receivers, first key information which is common  
8 to said plurality of senders and is used for having a key in common  
9 among said senders and said receivers, is produced and distributed to  
10 prescribed receivers, while second key information which is used for a  
11 key in common among said senders and said receivers is produced and  
12 distributed to said senders;
  - 13 in an apparatus of a sender, third key information, which is  
14 used by said receivers together with said first key information to  
15 calculate an encryption-decryption key used by the sender in question  
16 in broadcast communication, is produced using the second key  
17 information distributed from said trusted center and is sent to said  
18 receivers who have the encryption-decryption key in common with said  
19 sender; and
  - 20 in an apparatus of a receiver, the encryption-decryption key  
21 which is used for broadcast communication by the sender who  
22 distributed said third key information is obtained using the first key  
23 information distributed from said trusted center and the third key  
24 information distributed from said sender.

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED

1     2.        A method of key distribution having an encryption-decryption  
2     key of secure broadcast communication in common among a plurality of  
3     senders and a plurality of receivers in a communication system  
4     comprising an apparatus of a trusted center, apparatuses of said  
5     plurality of senders and apparatuses of said plurality of receivers,  
6     comprising:  
7                a first step, in the apparatus of the trusted center, of producing  
8     receiver secret key  $s_x$  of receiver  $x$  so as to correspond to a subset  $S'$  of a  
9     finite set  $S$ , and distributing the receiver secret key  $s_x$  to said receiver  $x$ ,  
10    while producing sender registration key  $t_A$  of a sender  $A$ ;  
11                a second step, in the apparatus of the sender  $A$ , of producing  
12    sender secret key  $g_A$  of the sender  $A$  and calculating an encryption-  
13    decryption key  $K_A$  from the sender secret key  $g_A$ ;  
14                a third step, in cooperation between the apparatus of the  
15    trusted center and the apparatus of the sender  $A$ , of producing key  
16    distribution data  $W$  by a function of at least the sender secret key  $g_A$  and  
17    the sender registration key  $t_A$ , while producing receiver registration key  
18     $r_x$  of the receiver  $x$  for the sender  $A$  by a function of at least the receiver  
19    private key information  $s_x$  and the sender registration key  $t_A$ ;  
20                a fourth step, in the apparatus of the sender  $A$ , of sending the  
21    receiver registration key  $r_x$  to the receiver  $x$  and broadcasting the key  
22    distribution data  $W$  to each receiver; and  
23                a fifth step, in the apparatus of the receiver  $x$ , of calculating  
24    the encryption-decryption key  $K_A$  from the receiver private key  
25    information  $s_x$  distributed from the trusted center and the key  
26    distribution data  $W$  and the receiver registration key  $r_x$  received from  
27    the sender  $A$ , the encryption-decryption key  $K_A$  being to be used for  
28    secure broadcast communication performed by the sender  $A$ ;

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED



29                wherein said receiver secret key  $s_x$ , the key distribution data  $W$ ,  
30    and the receiver registration key  $r_x$  are produced in such a relation that  
31    the encryption-decryption key  $K_A$  can be derived from said receiver  
32    secret key  $s_x$ , the key distribution data  $W$ , and the receiver registration  
33    key  $r_x$ , and other information opened to each receiver.

1    3.            The method of key distribution according to Claim 2, wherein:  
2                said second step is one in which, in the apparatus of the sender  
3    A, variable information  $r_A$  and  $r_A'$  for changing the encryption-  
4    decryption key are produced, and the encryption-decryption key  $K_A$  is  
5    calculated by a function of the variable information  $r_A$  and  $r_A'$  acting on  
6    the secret key  $g_A$ , the variable information  $r_A$  being for changing the  
7    encryption-decryption key periodically, and the variable information  $r_A'$   
8    being for changing the encryption-decryption key for every broadcast  
9    content; and

10              said third step is one in which:  
11              in the apparatus of the trusted center, data  $W'$  is produced by a  
12    function of the sender secret key  $g_A$  and the sender registration key  $t_A$ ,  
13    and sent to the sender A, while data  $r_x'$  is produced by a function of the  
14    receiver secret key  $s_x$  of the receiver  $x$  and the sender registration key  $t_A$ ,  
15    and sent to the sender A; and

16              in the apparatus of the sender A, the key distribution data  $W$  is  
17    produced by a function of the variable information  $r_A$  acting on the data  
18     $W'$ , and the receiver registration key  $r_x$  of the receiver  $x$  for the sender A  
19    is produced by a function of the variable information  $r_A'$  acting on the  
20    data  $r_x'$ .

1    4.            A method of key distribution for having an encryption-

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED

2 decryption key of secure broadcast communication in common among a  
 3 plurality of senders and a plurality of receivers in a communication  
 4 system comprising an apparatus of a trusted center, apparatuses of said  
 5 plurality of senders and apparatuses of said plurality of receivers,  
 6 comprising:

7 a first step for distributing receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  to the  
 8 receiver  $x$ , in which, in the apparatus of the trusted center,

9 
$$e_i \in Z \quad (1 \leq i \leq m)$$

10 are produced as a trusted center secret key;

11 
$$t_A \in Z$$

12 is produced as a sender registration key of a sender  $A$ ;  $\sigma_x \in S_{km}$  and

13 
$$s_x(\sigma_x) \in Z$$

14 are produced (here, when  $\sigma, \sigma' \in S_{km}$  for  $S_{km}$ :

15 
$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \rightarrow B = \{1, 2, \Lambda, m\}, 0 < k < m \}$$
,

16 it is expressed by the following expression:

17 
$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$$

18 “ $\sim$ ” being an equivalence relation on  $S_{km}$ , to lead to the following  
 19 expression:

20 
$$\tilde{S}_{km} = S_{km} / \sim$$

21 ), a second step, in which, in an apparatus of the sender  $A$ , are  
 22 produced sender secret keys  $g_A$ ,  $L_A$ , and a finite Abelian group  $G_A$   
 23 satisfying:

24 
$$g_A \in G_A$$
  

$$L_A = \text{ord}_{G_A}(g_A)$$

25 (here,

26 
$$\text{ord}_{G_A}(g)$$

27 means a least positive integer  $a$  which satisfies:



This Sheet Has Been Replaced





28  $g^a = 1 (\in G_A)$

29 ), and the sender secret key  $g_A$  is sent to the trusted center;

30 a third step, in which, in the apparatus of the trusted center,  
31 receiver registration data defined by the following expression:

32 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

33 is calculated from the trusted center secret key  $e_i$ , the sender  
34 registration key  $t_A$ , and the receiver secret key  $s_x(\sigma_x)$ ,  $\sigma_x$ ; and the  
35 receiver registration data  $s_x(\sigma_x, A)$  is sent to the sender A, while key  
36 distribution data defined as:

37 
$$y_{Ai} = g_A^{u_i} (\in G_A) \quad (1 \leq i \leq m)$$

38 is calculated from the  $g_A$  received from the sender A, the trusted center  
39 secret key  $e_i$ , and the sender registration key  $t_A$ ; and the key  
40 distribution data  $y_{Ai}$  is sent to the sender A;

41 a fourth step, in which, in the apparatus of the sender A,  
42 integers  $r, r'$  are produced; a receiver registration key  $r_x(\sigma_x, A)$   
43 satisfying:

44 
$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

45 is calculated from the receiver registration data  $s_x(\sigma_x, A)$  received from  
46 the trusted center, the sender secret key  $L_A$ , and the integer  $r'$ ; and the  
47 receiver registration key  $r_x(\sigma_x, A)$  is sent to the receiver x; while key  
48 distribution data defined as:

49 
$$z_{Ai} = y_{Ai}^r (\in G_A) \quad (1 \leq i \leq m)$$

50 is calculated from the key distribution data  $y_{Ai}$  received from the  
51 trusted center and the integer  $r$ ; and the key distribution data  $z_{Ai}$  is  
52 broadcasted to each receiver; and

53 a fifth step, in which, in an apparatus of the receiver x, an  
54 encryption-decryption key  $K_A$  is calculated by:





55 
$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} (\in G_A)$$

56 from the receiver registration key  $r_x(\sigma_x, A)$  received from the sender, the  
 57 key distribution data  $z_{Ai}$ , the receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  distributed  
 58 from the trusted center; the encryption-decryption key  $K_A$  being  
 59 generated by the sender A employing:

60 
$$K_A = g_A^{r' r'} (\in G_A)$$

61 to be used for broadcast communication.

1 5. A method of key distribution having an encryption-decryption  
 2 key of secure broadcast communication in common among a plurality of  
 3 senders and a plurality of receivers in a communication system  
 4 comprising an apparatus of a trusted center, apparatuses of said  
 5 plurality of senders and apparatuses of said plurality of receivers,  
 6 comprising:

7 a first step, in which, in the apparatus of the trusted center,

8 
$$e_i \in Z \quad (1 \leq i \leq m)$$

9 is produced as a trusted center secret key;

10 
$$t_A \in Z$$

11 is produced as a sender registration key of a sender A;  $\sigma_x \in S_{km}$  and

12 
$$s_x(\sigma_x) \in Z$$

13 are produced as receiver secret keys of a receiver x;

14 (here, when  $\sigma, \sigma' \in S_{km}$  for a set defined as:

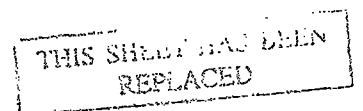
15 
$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \rightarrow B = \{1, 2, \Lambda, m\}, 0 < k < m \}$$
,

16 it is expressed by the following expression:

17 
$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$$

18 and, in that case, " $\sim$ " becomes an equivalence relation on  $S_{km}$ , which

This Sheet Has Been Replaced





19 leads to the following expression:

20 
$$\tilde{S}_{km} = S_{km} / \sim$$

21 ); and the receiver secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$  are sent to the receiver x;

22 a second step, in which, in an apparatus of the sender A,

23 
$$\begin{aligned} P_A, Q_A: & \text{ prime numbers} \\ L_A &= \text{lcm}(\text{ord}_{P_A}(g_A), \text{ord}_{Q_A}(g_A)) \\ g_A &\in \mathbb{Z}, \quad 0 < g_A < N_A \\ r, r' &\in \mathbb{Z}, \quad 0 < r, r' < L_A \end{aligned}$$

24 are produced as sender secret keys;

25 
$$N_A (= P_A Q_A)$$

26 is produced as a sender public key; and the sender secret key  $g_A$  is sent  
27 to the trusted center;

28 a fourth step, in which, in the apparatus of the trusted center,  
29 receiver registration data defined as:

30 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

31 is calculated from the trusted center secret key  $e_i$ , the sender  
32 registration key  $t_A$ , and the receiver secret keys  $s_x(\sigma_x)$ ,  $\sigma_x$ ; and the  
33 receiver registration data  $s_x(\sigma_x, A)$  is sent to the sender A; while key  
34 distribution data defined as:

35 
$$y_{Ai} = g_A^{u_i} \bmod N_A \quad (1 \leq i \leq m)$$

36 is calculated from  $g_A$  received from the sender A, the trusted center  
37 secret key  $e_i$ , and the sender registration key  $t_A$ ; and the key  
38 distribution data  $y_{Ai}$  is sent to the sender A;

39 a fifth step, in which, in the apparatus of the sender A, integers  
40  $r, r'$  are produced; and a receiver registration key  $r_x(\sigma_x, A)$  satisfying:

41 
$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

42 is calculated from the receiver registration data  $s_x(\sigma_x, A)$  received from  
43 the trusted center, the sender secret key  $L_A$ , and the integer  $r'$ ; and the





44 receiver registration key  $r_x(\sigma_x, A)$  is sent to the receiver  $x$ ; while key  
45 distribution data defined as:

46 
$$z_{Ai} = y_{Ai}^r \bmod N_A \quad (1 \leq i \leq m)$$

47 is calculated from the key distribution data  $y_{Ai}$  received from the  
48 trusted center and the integer  $r$ ; and the key distribution data  $z_{Ai}$  is  
49 broadcasted to each receiver; and

50 a sixth step, in which, in an apparatus of the receiver  $x$ , an  
51 encryption-decryption key  $K_A$  is calculated by:

52 
$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A)s_x(\sigma_x)} \bmod N_A$$

53 from the receiver registration key  $r_x(\sigma_x, A)$  received from the sender, the  
54 key distribution data  $z_{Ai}$ , and the receiver secret keys  $\sigma_x, s_x(\sigma_x)$   
55 distributed from the trusted center; the encryption-decryption key  
56 being generated by the sender  $A$  using:

57 
$$K_A = g_A^{rr'} \bmod N_A$$

58 to be used for broadcast communication.

1 6. The method of key distribution according to Claim 5, further  
2 comprising:

3 a seventh step, in which, in said apparatus of the sender  $A$ ,  
4 said secret key  $L_A$  is generated and sent to the trusted center before the  
5 apparatus of the trusted center performs the first step of generating the  
6 trusted center secret key  $e_i$ , the sender identification  $t_A$ , and the  
7 receiver secret key  $s_x(\sigma_x)$ ;

8 wherein:

9 in said first step, in the apparatus of the trusted center, the  
10 trusted center information  $e_i$ , the sender identification  $t_A$ , and the  
11 receiver secret key  $s_x(\sigma_x)$  are produced from the sender secret key  $L_A$

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED



12 received from the sender so as to satisfy:

$$\begin{aligned}
 &e_i \in \mathbb{Z}, \quad 0 < e_i < L_A, \quad (1 \leq i \leq m) \\
 &t_A \in \mathbb{Z}, \quad 0 < t_A < L_A \\
 &s_x(\sigma_x) \in \mathbb{Z}, \quad 0 < s_x(\sigma_x) < L_A,
 \end{aligned}$$

14 and,

15 in said fourth step, in the apparatus of the trusted center, the  
 16 receiver registration data  $s_x(\sigma_x, A)$  is calculated from the sender secret  
 17 key  $L_A$ , the trusted center secret key  $e_i$ , the sender registration key  $t_A$ ,  
 18 and the receiver secret key  $s_x(\sigma_x)$  so as to satisfy:

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^t e_{\sigma_x(i)} \pmod{L_A}.$$

1 7. The method of key distribution according to Claim 5, further  
 2 comprising:

3 an eighth step, in which, in the apparatus of the sender A, a  
 4 value of the integer  $r$  is changed; and a value of the encryption-  
 5 decryption key  $K_A$  is recalculated in accordance with the changed  
 6 integer  $r$ ; while the key distribution data  $z_{Ai}$  is recalculated in  
 7 accordance with the changed integer  $r$  and broadcasted to each receiver  
 8 again; and

9 a ninth step, in which, in the apparatus of the receiver  $x$ , the  
 10 encryption-decryption key  $K_A$  is recalculated in accordance with the key  
 11 distribution data  $z_{Ai}$  broadcasted again.

1 8. The method of key distribution according to Claim 5, wherein:  
 2 in said fifth step, in the apparatus of the sender A, a value of  
 3 the integer  $r'$  is generated in accordance with each piece of information  
 4 or each kind of information to be encrypted and broadcasted; and





5 encryption-decryption keys  $K_A$  are calculated for respective information  
6 or respective kinds of information in accordance with respective values  
7 of the integer  $r'$  generated in accordance with the information or kinds  
8 of information; while pieces of receiver registration key  $r_x(\sigma_x, A)$  are  
9 calculated in accordance with respective integers  $r'$  generated in  
10 accordance with respective said information or kinds of information on  
11 which the receiver  $x$  is allowed to perform decryption, and the said  
12 pieces of receiver registration key  $r_x(\sigma_x, A)$  are sent to the receiver  $x$ ; and  
13 in said sixth step, in the apparatus of the receiver  $x$ ,  
14 encryption-decryption key  $K_A$  for said information or kinds of  
15 information on which said receiver  $x$  is allowed to perform decryption  
16 are calculated in accordance with respective pieces of receiver  
17 registration key  $r_x(s_x, A)$  received.

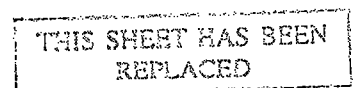
1 9. The method of key distribution according to Claim 5, further  
2 comprising:

3 a tenth step in which, in the apparatuses of the sender  $A$  and  
4 the receiver  $x$ , possession of the receiver secret key  $s_x(\sigma_x)$  by said  
5 receiver  $x$  is authenticated according to a system by which the receiver  
6 secret key  $s_x(\sigma_x)$  is made secret from the sender  $A$ , before the fifth step  
7 for sending the receiver registration key  $r_x(\sigma_x, A)$  from the sender  $A$  to  
8 the receiver  $x$ .

1 10. The method of key distribution according to Claim 5, further  
2 comprising:

3 an eleventh step in which, in the apparatus of the sender  $A$ , a  
4 fee for information or a kind of information, which is encrypted with the  
5 encryption-decryption key  $K_A$  corresponding to the receiver registration

This Sheet Has Been Replaced





6 key  $r_x(\sigma_x, A)$  and broadcasted, is calculated as accounting information  
7 for the receiver A, said eleventh step being performed when the fifth  
8 step is performed for sending the receiver registration key  $r_x(\sigma_x, A)$  from  
9 the sender A to the receiver x.

1 11. A method of key distribution having an encryption-decryption  
2 key of secure broadcast communication in common among a plurality of  
3 senders and a plurality of receivers in a communication system  
4 comprising apparatuses of said plurality of senders and apparatuses of  
5 said plurality of receivers, comprising:

6 a first step, in which, in an apparatus of a trusted center  
7 provided separately from said apparatuses of senders and said receivers,  
8 a secret key K0 is generated and distributed to each sender and each  
9 receiver;

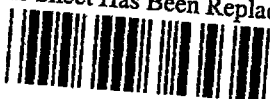
10 a second step, in which, in an apparatus of a sender A, a sender  
11 registration key BIDA is generated and sent to the receivers, while a  
12 common key  $K_A' = F(K0, BIDA)$  is calculated from the secret key K0  
13 distributed from the trusted center and the sender registration key  
14 BIDA using a given one-way function F;

15 a third step, in which, in the apparatuses of the receivers, the  
16 common key  $K_A'$  is calculated from the secret key K0 distributed from  
17 the trusted center and the sender registration key BIDA received from  
18 the sender A using said one-way function F;

19 a fourth step, in which, in the apparatus of the sender A, an  
20 integer r is produced and sent to the receivers; and

21 a fifth step, in which, in the apparatuses of the receivers, an  
22 encryption-decryption key  $K_A$  is calculated by  $K_A = F'(r, K_A')$  from the  
23 integer r received from the sender A and the common key  $K_A'$  using a

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED



24 given function  $F'$ , the encryption-decryption key  $K_A$  being calculated by  
25 the sender A using  $K_A = F'(r, K_A')$ .

1 12. A method of key distribution having an encryption-decryption  
2 key of secure broadcast communication in common among a plurality of  
3 senders and a plurality of receivers in a communication system  
4 comprising apparatuses of said plurality of senders and apparatuses of  
5 said plurality of receivers, comprising:

6 a first step, in which, in an apparatus of a trusted center  
7 provided separately from said apparatuses of senders and said receivers,  
8 a personal key  $s_x$  for a receiver  $x$  is produced, and distributed to the  
9 sender A and the receiver  $x$ ;

10 a second step, in which, in an apparatus of the sender A, a  
11 common key  $K_A$  is produced, and said common key  $K_A$  is owned in  
12 common with the receiver  $x$  by cipher communication using the personal  
13 key  $s_x$  for the receiver  $x$ , which has been distributed from the trusted  
14 center;

15 a third step, in which, in the apparatus of the sender A,  
16 information  $r$  is produced and sent to the receiver  $x$ ; and

17 a fourth step, in which, in each of the apparatuses of the  
18 receiver  $x$  and the sender A, an encryption-decryption key  $DK$  is  
19 calculated in accordance with an expression,  $DK = F(r, K_A)$ .

1 13. The method of key distribution according to Claim 12, further  
2 comprising:

3 a fifth step, in which, in the apparatus of the sender A, the  
4 common key  $K_A$  is changed, and the changed common key  $K_A$  is owned in  
5 common with the receiver  $x$  by cipher communication using the personal

This Sheet Has Been Replaced





6 key  $s_x$  for the receiver  $x$ ; and  
7 a sixth step, in which, in each of the apparatuses of the sender  
8 A and the receiver  $x$ , the encryption-decryption key  $DK$  is recalculated  
9 by  $DK=F(r, K_A)$  in accordance with the changed common key  $K_A$ .

1 14. The method of key distribution according to Claim 12, further  
2 comprising:

3 a seventh step, in which, in the apparatus of the sender A, the  
4 information  $r$  is changed, and the changed information  $r$  is informed to  
5 the receivers; and

6 an eighth step, in which, in each of the apparatuses of the  
7 sender A and the receivers, the encryption-decryption key  $DK$  is  
8 recalculated by  $DK=F(r, K_A)$  in accordance with the changed  
9 information  $r$ .

1 15. The method of key distribution according to Claim 12, further  
2 comprising:

3 a ninth step, in which, in the apparatus of the sender A, key  
4 information for the receiver  $x$  to calculate said encryption-decryption  
5 key  $DK$  is sent through a given communication channel which is  
6 different from a communication channel for broadcasting information  
7 encrypted with the encryption-decryption key  $DK$ .

1 16. A key distribution system for having an encryption-decryption  
2 key used for secure broadcast communication in common among senders  
3 and receivers, wherein:

4 said system comprises a trusted center apparatus, a plurality  
5 of sender apparatuses, and a plurality of receiver apparatuses;

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED



6 said trusted center apparatus comprises:

7 means for producing:

8 
$$e_i \in Z \quad (1 \leq i \leq m)$$

9 as a trusted center secret key;

10 
$$t_A \in Z$$

11 as a sender registration key of a sender A; and  $\sigma_x \in S_{km}$  and

12 
$$s_x(\sigma_x) \in Z$$

13 (here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$  defined as:

14 
$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \\ \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m \}$$

15 it is expressed by the following expression:

16 
$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$$

17 and, in that case, " $\sim$ " becomes an equivalence relation on  $S_{km}$ , leading

18 to the following definition:

19 
$$\tilde{S}_{km} = S_{km} / \sim$$

20 ); and for distributing the receiver secret keys  $\sigma_x, s_x(\sigma_x)$  to said receiver

21 apparatus used by the receiver x;

22 means for calculating receiver registration data defined by:

23 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

24 from the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and

25 the receiver secret keys  $s_x(\sigma_x), \sigma_x$ , and for sending the receiver

26 registration data  $s_x(\sigma_x, A)$  to said sender apparatus used by the sender

27 A; and

28 means for calculating key distribution data defined by:

29 
$$y_{Ai} = g_A^{u_i} \quad (\in G_A) \quad (1 \leq i \leq m)$$

30 from  $g_A$  received from said sender apparatus used by the sender A, the

31 trusted center secret key  $e_i$ , and the sender registration key  $t_A$ , and for





32 sending the key distribution data  $y_{Ai}$  to said sender apparatus used by  
33 the sender A;

34 said sender apparatus used by the sender A comprises:

35 means for producing sender secret keys  $g_A$ ,  $L_A$ , and a finite

36 Abelian group  $G_A$ , satisfying:

$$\begin{aligned} 37 \quad & g_A \in G_A \\ & L_A = \text{ord}_{G_A}(g_A) \end{aligned}$$

38 (here,

$$39 \quad \text{ord}_{G_A}(g) )$$

40 means a least positive integer  $a$  satisfying:

$$41 \quad g^a = 1 (\in G_A)$$

42 ), and for sending the sender secret key  $g_A$  to said trusted center

43 apparatus;

44 means for producing integers  $r$ ,  $r'$ , calculating receiver

45 registration key  $r_x(\sigma_x, A)$  satisfying:

$$46 \quad r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

47 from the receiver registration data  $s_x(\sigma_x, A)$  received from said trusted

48 center apparatus, the sender secret key  $L_A$ , and the integer  $r'$ ; and for

49 sending the receiver registration key  $r_x(\sigma_x, A)$  to said receiver apparatus

50 of the receiver  $x$ ; and

51 means for calculating key distribution data defined as:

$$52 \quad z_{Ai} = y_{Ai}^r (\in G_A) \quad (1 \leq i \leq m)$$

53 from the key distribution data  $y_{Ai}$  received from said trusted center

54 apparatus, and the integer  $r$ ; and for broadcasting the key distribution

55 data  $z_{Ai}$  to said plurality of receiver apparatuses; and

56 said receiver apparatus of the receiver  $x$  comprises:

57 means for calculating encryption-decryption key  $K_A$  by the

58 following expression:

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED



59 
$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} (\in G_A),$$

60 said encryption-decryption key  $K_A$  being generated by said sender  
61 apparatus of the sender A by the following expression:

62 
$$K_A = g_A^{r'} (\in G_A).$$

1 17. A trusted center apparatus which supports distribution of an  
2 encryption-decryption key from a sender apparatus to a receiver  
3 apparatus, having said encryption-decryption key used in secure  
4 broadcast communication in common among senders and receivers,  
5 comprising:

6 means for producing:

7 
$$e_i \in Z \quad (1 \leq i \leq m)$$

8 as a trusted center secret key;

9 
$$t_A \in Z$$

10 as a sender registration key of a sender A; and, as receiver secret keys of  
11 a receiver x,  $\sigma_x \in S_{km}$  and:

12 
$$s_x(\sigma_x) \in Z$$

13 (here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$ :

14

15 
$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \rightarrow B = \{1, 2, \Lambda, m\}, 0 < k < m \},$$

16 it is expressed by the following expression:

17 
$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A),$$

18 with " $\sim$ " being an equivalence relation on  $S_{km}$ , which lead to an  
19 expression:

20

21 
$$\tilde{S}_{km} = S_{km} / \sim,$$





22 and for distributing the receiver secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$  to said receiver  
 23 apparatus used by the receiver x;

24 means for calculating receiver registration data defined by:

$$25 \quad s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

26 from the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and  
 27 the receiver secret keys  $s_x(\sigma_x)$ ,  $\sigma_x$ ; and for sending the receiver  
 28 registration data  $s_x(\sigma_x, A)$  to said sender apparatus used by the sender  
 29 A; and

30 means for calculating key distribution data defined as:

$$31 \quad y_{Ai} = g_A^{u_i} (\in G_A) \quad (1 \leq i \leq m)$$

32 from  $g_A$  received from said sender apparatus of the sender A, the trusted  
 33 center secret key  $e_i$ , and the sender registration key  $t_A$ ; and for sending  
 34 the key distribution data  $y_{Ai}$  to said sender apparatus of the sender A.

1 18. A sender apparatus which distributes an encryption-decryption  
 2 key to a receiver apparatus being supported by a trusted center  
 3 apparatus, having said encryption-decryption key used in secure  
 4 broadcast communication in common among senders and receivers,  
 5 comprising:

6 means for producing sender secret key  $g_A$ ,  $L_A$ , and a finite  
 7 Abelian group  $G_A$  satisfying:

$$8 \quad \begin{aligned} g_A &\in G_A \\ L_A &= \text{ord}_{G_A}(g_A) \end{aligned}$$

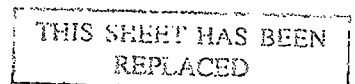
9 (here,

$$10 \quad \text{ord}_{G_A}(g) )$$

11 means a least positive integer a satisfying:

$$12 \quad g^a = 1 (\in G_A)$$

This Sheet Has Been Replaced





13 ); and for sending the sender secret key  $g_A$  to said trusted center  
14 apparatus;

15 means for producing integers  $r, r'$ ; calculating a receiver  
16 registration key  $r_x(\sigma_x, A)$  satisfying:

$$17 \quad r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

18 from the receiver registration data  $s_x(\sigma_x, A)$ , the sender secret key  $L_A$ ,  
19 and the integer  $r$ , and for sending the receiver registration key  $r_x(\sigma_x, A)$   
20 to said receiver apparatus used by the receiver  $x$ ;

21 means for calculating key distribution data defined as:

$$22 \quad z_{Ai} = y_{Ai}^r \quad (\in G_A) \quad (1 \leq i \leq m)$$

23 from key distribution data  $y_{Ai}$  received from said trusted center  
24 apparatus, and the integer  $r$ ; and for broadcasting the key distribution  
25 data  $z_{Ai}$  to a plurality of said receiver apparatuses as objects of  
26 broadcast communication; and

27 means for calculating an encryption-decryption key  $K_A$  used for  
28 broadcast communication, in accordance with:

$$29 \quad K_A = g_A^{r'} \quad (\in G_A).$$

1 19. A receiver apparatus which receives an encryption-decryption  
2 key from a sender apparatus being supported by a trusted center  
3 apparatus, having said encryption-decryption key used in secure  
4 broadcast communication in common among senders and receivers,  
5 comprising:

6 means for calculating the encryption-decryption key  $K_A$  used  
7 for the broadcast communication by an expression:

$$8 \quad K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A)s_x(\sigma_x)} \quad (\in G_A)$$

9 from a receiver registration data  $r_x(\sigma_x, A)$  and a key distribution data  $z_{Ai}$

This Sheet Has Been Replaced





10 received from the sender apparatus used by a sender A, and receiver  
 11 secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$  received from the trusted center apparatus, the  
 12 encryption-decryption key  $K_A$  being generated by said sender apparatus  
 13 of the sender A using an expression:

$$14 \quad K_A = g_A^{r'} (\in G_A).$$

1 20. A receiver apparatus which receives an encryption-decryption  
 2 key from a sender apparatus being supported by a trusted center  
 3 apparatus, having said encryption-decryption key used in secure  
 4 broadcast communication in common among senders and receivers,  
 5 comprising:

6 a main apparatus and an auxiliary apparatus;

7 wherein:

8 said auxiliary apparatus comprises:

9 means for connection with said trusted center apparatus;

10 storing means for taking in and storing receiver secret keys

11  $s_x(\sigma_x)$ ,  $\sigma_x$  produced by said trusted center apparatus;

12 means for connection with said main apparatus, and

13 means for taking in key distribution data  $z_{Ai}$  received by said

14 main apparatus from said sender apparatus used by a sender A;

15 calculating:

$$16 \quad \xi_x(\sigma_x, A) = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \bmod N_A$$

17 from the key distribution data  $z_{Ai}$  and the receiver secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$   
 18 stored in said storing means; and for outputting a result  $\xi_x(\sigma_x, A)$  of the  
 19 calculation to said main apparatus; and

20 said main apparatus comprises:

21 means for outputting the key distribution data  $z_{Ai}$  received





22 from said sender apparatus of the sender A to said auxiliary apparatus;  
23 and

24 means for calculating encryption-decryption key  $K_A$  used in  
25 broadcast communication, using an expression:

$$26 \quad K_A = \xi_x(\sigma_x, A)^{r_x(\sigma_x, A)} \bmod N_A$$

27 from a receiver registration key  $r_x(\sigma_x, A)$  received from the sender  
28 apparatus of the sender A, and  $\xi_x(\sigma_x, A)$  output from the auxiliary  
29 apparatus, the encryption-decryption key  $K_A$  being generated by said  
30 sender apparatus of the sender A, using an expression:

$$31 \quad K_A = g_A^{m'} (\in G_A).$$

1 21. An auxiliary apparatus used being connected with a trusted  
2 center apparatus and a plurality of receiver apparatuses, in a  
3 communication system comprising a plurality of sender apparatuses  
4 which perform broadcast communication, said plurality of receiver  
5 apparatuses, and said trusted center apparatus which supports  
6 distribution of an encryption-decryption key of a sender apparatus used  
7 in secure broadcast communication to a receiver apparatus; said  
8 auxiliary apparatus comprising:

9 means for connection with said trusted center apparatus;

10 storing means for taking in and storing receiver secret keys  
11  $s_x(\sigma_x)$ ,  $\sigma_x$  for a receiver x, produced by said trusted center apparatus;

12 means for connection with said receiver apparatus used by the  
13 receiver x; and

14 means for taking in key distribution data  $z_{Ai}$  received by said  
15 receiver apparatus used by the receiver x from said sender apparatus  
16 used by the sender A; for calculating:

This Sheet Has Been Replaced





17 
$$\xi_x(\sigma_x, A) = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \bmod N_A$$

18 from the key distribution data  $z_{Ai}$  and the receiver secret keys  $\sigma_x, s_x(\sigma_x)$   
 19 stored in said storing means; and for outputting a calculation result  
 20  $\xi_x(\sigma_x, A)$  to said receiver apparatus of the receiver x.

1 22. A storing medium which stores a program for making an  
 2 information processing apparatus execute a process for supporting  
 3 distribution of an encryption-decryption key from sender apparatuses to  
 4 receiver apparatuses, having said encryption-decryption key used in  
 5 secure broadcast communication in common among senders and  
 6 receivers, wherein:

7 said program makes the information processing apparatus  
 8 execute:

9 a step of producing:

10 
$$e_i \in Z \quad (1 \leq i \leq m)$$

11 as a trusted center secret key,

12 
$$t_A \in Z$$

13 as a sender registration key of a sender A, and, as receiver secret keys of  
 14 a receiver x,  $\sigma_x \in S_{km}$  and:

15 
$$s_x(\sigma_x) \in Z$$

16 (here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$  defined as:

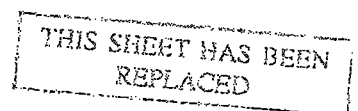
17 
$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \\ \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m \}$$

18 it is expressed by the following expression:

19 
$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A),$$

20 with " $\sim$ " becoming an equivalence relation on  $S_{km}$ , leading to an  
 21 expression:

This Sheet Has Been Replaced





22  $\tilde{S}_{km} = S_{km} / \sim$

23 ); and of distributing the receiver secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$  to said receiver  
24 apparatus used by the receiver x;

25 a step of calculating receiver registration data defined as:

26 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

27 from the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and  
28 the receiver secret keys  $s_x(\sigma_x)$ ,  $\sigma_x$ ; and of sending the receiver  
29 registration data  $s_x(\sigma_x, A)$  to said sender apparatus used by the sender  
30 A; and

31 a step of calculating key distribution data  $y_{Ai}$  defined as:

32 
$$y_{Ai} = g_A^{u_i} (\in G_A) \quad (1 \leq i \leq m)$$

33 from  $g_A$  received from said sender apparatus used by the sender A, the  
34 trusted center secret key  $e_i$ , and the sender registration key  $t_A$ ; and of  
35 sending the key distribution data  $y_{Ai}$  to said sender apparatus used by  
36 the sender A.

1 23. A storing medium which stores a program for making an  
2 information processing apparatus execute a process in sender  
3 apparatuses which distribute an encryption-decryption key to receiver  
4 apparatuses, being supported by a trusted center apparatus, having  
5 said encryption-decryption key used in secure broadcast communication  
6 in common among senders and receivers, wherein:  
7 said program makes the information processing apparatus  
8 execute:  
9 a step of producing sender secret keys  $g_A$ ,  $L_A$ , and a finite  
10 Abelian group  $G_A$  satisfying:

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED

11  $g_A \in G_A$   
 $L_A = \text{ord}_{G_A}(g_A)$

12 (here,

13  $\text{ord}_{G_A}(g)$

14 means a least positive integer a satisfying:

15  $g^a = 1 (\in G_A)$

16 ), and of sending the sender secret key  $g_A$  to said trusted center  
 17 apparatus;

18 a step of producing integers  $r, r'$ ; calculating receiver  
 19 registration key  $r_x(\sigma_x, A)$  satisfying:

20  $r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$

21 and sending the receiver registration key  $r_x(\sigma_x, A)$  to said receiver  
 22 apparatus used by the receiver  $x$ ;

23 a step of calculating key distribution data defined as:

24  $z_{Ai} = y_{Ai}^{r'} (\in G_A) \quad (1 \leq i \leq m)$

25 from key distribution data  $y_{Ai}$  received from said key administration  
 26 apparatus, and the integer  $r$ ; and broadcasting the key distribution data  
 27  $z_{Ai}$  to said plurality of receiver apparatuses as objects of broadcast  
 28 communication; and

29 a step of calculating an encryption-decryption key  $K_A$  used in  
 30 broadcast communication, using:

31  $K_A = g_A^{rr'} (\in G_A).$

1 24. A storing medium which stores a program for making an  
 2 information processing apparatus execute a process in receiver  
 3 apparatuses which receive an encryption-decryption key distributed  
 4 from sender apparatuses, being supported by a trusted center apparatus,  
 5 having said encryption-decryption key used in secure broadcast



This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED



6 communication in common among senders and receivers, wherein:  
 7 said program makes the information processing apparatus  
 8 execute:  
 9 a step of calculating an encryption-decryption key  $K_A$  used for  
 10 broadcast communication, using an expression:

$$11 \quad K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} (\in G_A)$$

12 from a receiver registration key  $r_x(\sigma_x, A)$  received from said sender  
 13 apparatus used by a sender A, key distribution data  $z_{Ai}$ , and a receiver  
 14 secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  distributed from the trusted center, the  
 15 encryption-decryption key  $K_A$  being generated by said sender apparatus  
 16 used by the sender A, using:

$$17 \quad K_A = g_A^{r'} (\in G_A).$$

1 25. A key distribution system for having an encryption-decryption  
 2 key used for secure broadcast communication in common among senders  
 3 and receivers, wherein:

4 said system comprises a trusted center apparatus, a plurality  
 5 of sender apparatuses, and a plurality of receiver apparatuses;

6 said trusted center apparatus comprises:

7 means for producing:

$$8 \quad e_i \in Z \quad (1 \leq i \leq m)$$

9 as a trusted center secret key,

$$10 \quad t_A \in Z$$

11 as a sender registration key of a sender A, and, as receiver secret keys of  
 12 a receiver x,  $\sigma_x \in S_{km}$  and

$$13 \quad s_x(\sigma_x) \in Z$$

14 (here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$  defined as:

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED



15 
$$S_{km} = \{\sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \\ \rightarrow B = \{1, 2, \Lambda, m\}, 0 < k < m\}$$
,

16 it is expressed by:

17 
$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$$

18 with “ $\sim$ ” becoming an equivalence relation on  $S_{km}$ , leading to the  
19 following expression:

20 
$$\tilde{S}_{km} = S_{km} / \sim$$

21 ), and of distributing the receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  to said receiver  
22 apparatus used by a receiver x;

23 means for calculating:

24 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

25 from the key distributor secret key  $e_i$ , the sender registration key  $t_A$ ,  
26 and the receiver secret keys  $s_x(\sigma_x)$ ,  $\sigma_x$ , and sending the receiver  
27 registration data  $s_x(\sigma_x, A)$  to said sender apparatus used by the sender  
28 A; and

29 means for calculating key distribution data  $y_{Ai}$ :

30 
$$y_{Ai} = g_A^{e_i} \bmod N_A \quad (1 \leq i \leq m)$$

31 from  $g_A$  received from the sender A, the trusted center secret key  $e_i$ , and  
32 the sender registration key  $t_A$ , and sending the key distribution data  $y_{Ai}$   
33 to said sender apparatus used by the sender A;

34 said sender apparatus used by the sender A comprises:

35 means for producing:

36 
$$P_A, Q_A : \text{prime numbers} \\ L_A = \text{lcm}(\text{ord}_{P_A}(g_A), \text{ord}_{Q_A}(g_A)) \\ g_A \in \mathbb{Z}, 0 < g_A < N_A \\ r, r' \in \mathbb{Z}, 0 < r, r' < L_A$$

37 as sender secret keys of the sender A,





38  $N_A (= P_A Q_A)$   
 39 as a sender public key of the sender A, and sending the sender secret  
 40 key  $g_A$  to said trusted center apparatus;  
 41 means for generating  $r, r'$ , calculating receiver registration key  
 42  $r_x(\sigma_x, A)$  satisfying:

43 
$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

44 from receiver registration data  $s_x(\sigma_x, A)$  received from the trusted center,  
 45 the sender secret key  $L_A$ , and the integer  $r'$ , and sending the receiver  
 46 registration key  $r_x(\sigma_x, A)$  to said receiver apparatus used by the receiver  
 47 x; and

48 means for calculating key distribution data defined as:

49 
$$z_{Ai} = y_{Ai}^r \pmod{N_A} \quad (1 \leq i \leq m)$$

50 from key distribution data  $y_{Ai}$  received from the trusted center, and the  
 51 integer  $r$ , and broadcasting the key distribution data  $z_{Ai}$  to said  
 52 plurality of receiver apparatuses as objects of broadcast  
 53 communication;

54 and,

55 said receiver apparatus used by the receiver x comprise:

56 means for calculating an encryption-decryption key  $K_A$  for  
 57 broadcast communication, using:

58 
$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \pmod{N_A}$$

59 from the receiver registration key  $r_x(\sigma_x, A)$  received from said sender  
 60 apparatus used by the sender A, the key distribution data  $z_{Ai}$ , and the  
 61 receiver secret keys  $\sigma_x, s_x(\sigma_x)$  distributed from the trusted center, said  
 62 encryption-decryption key  $K_A$  being generated by said sender apparatus  
 63 used by the sender A, using:

64 
$$K_A = g_A^{r'} \pmod{N_A}.$$

This Sheet Has Been Replaced



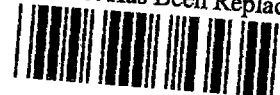
THIS SHEET HAS BEEN  
REPLACED

65

### Abstract of the Disclosure

It is made possible to obtain a common key owned in common with a plurality of senders, using only one receiver secret key. A trusted center produces the receiver secret key of a receiver, so as to correspond to a subset consisting of two or more elements from a  
70 suitable finite set  $Z$ , and distributes it the receiver. Further, the trusted center produces identification information  $t_A$  for a sender. The sender produces an encryption-decryption key  $K_A$  from his own sender secret key. Keeping the receiver secret key and the identification information  $t_A$  secret from the sender, the trusted center cooperates  
75 with the sender to produce data related to each element of the finite set  $Z$  and the sender secret key, and data related to a subset corresponding to the receiver secret key and related to the sender secret key, and broadcasts these data. The receiver  $x$  calculates the encryption-decryption key  $K_A$  from the received data and his own receiver secret  
80 key.

This Sheet Has Been Replaced



THIS SHEET HAS BEEN  
REPLACED

FIG. 1

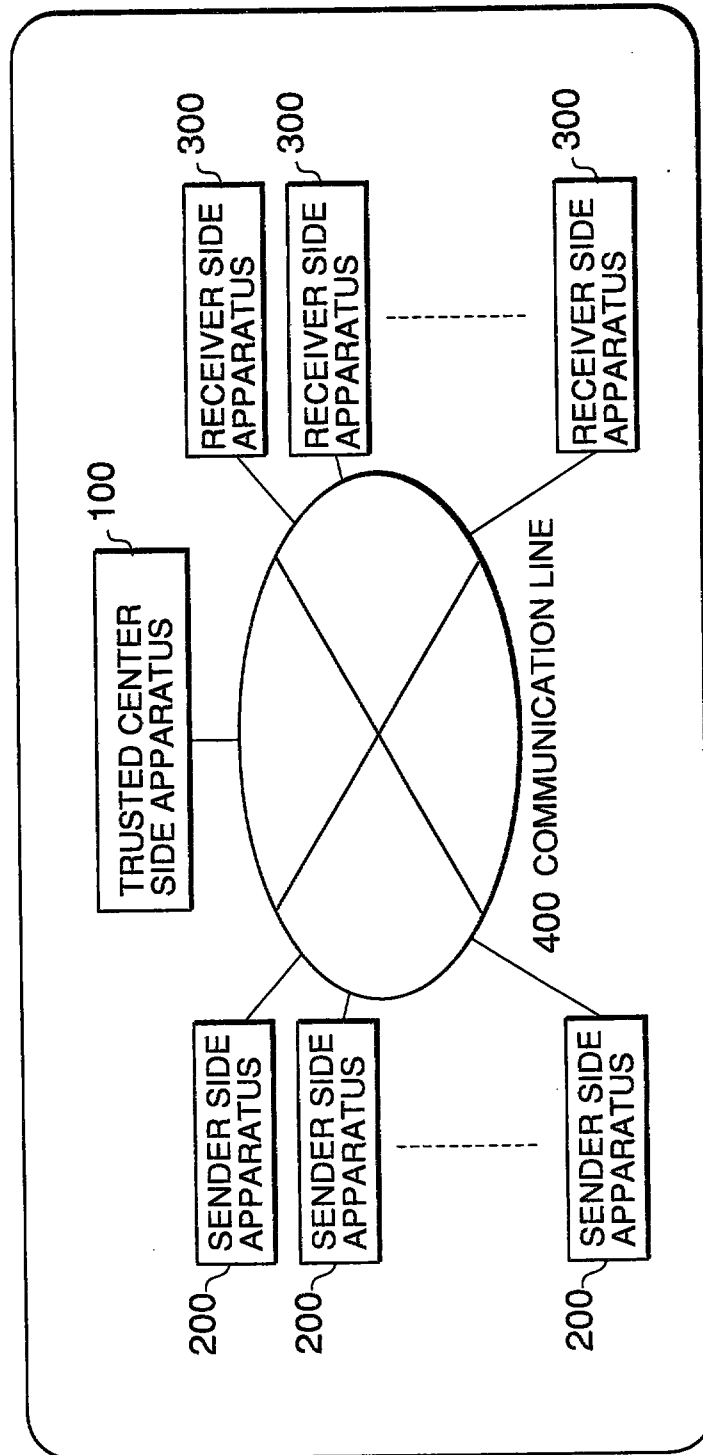


FIG. 2

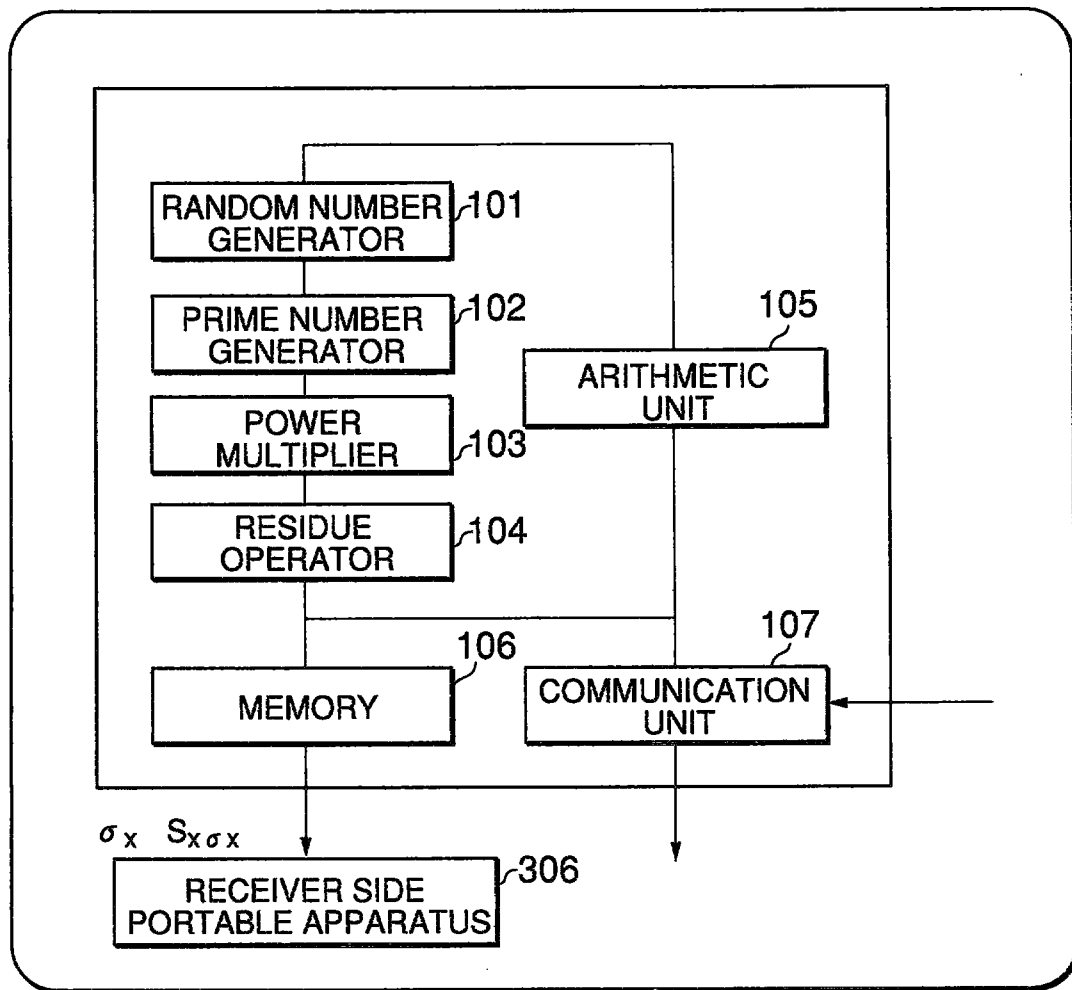


FIG. 3

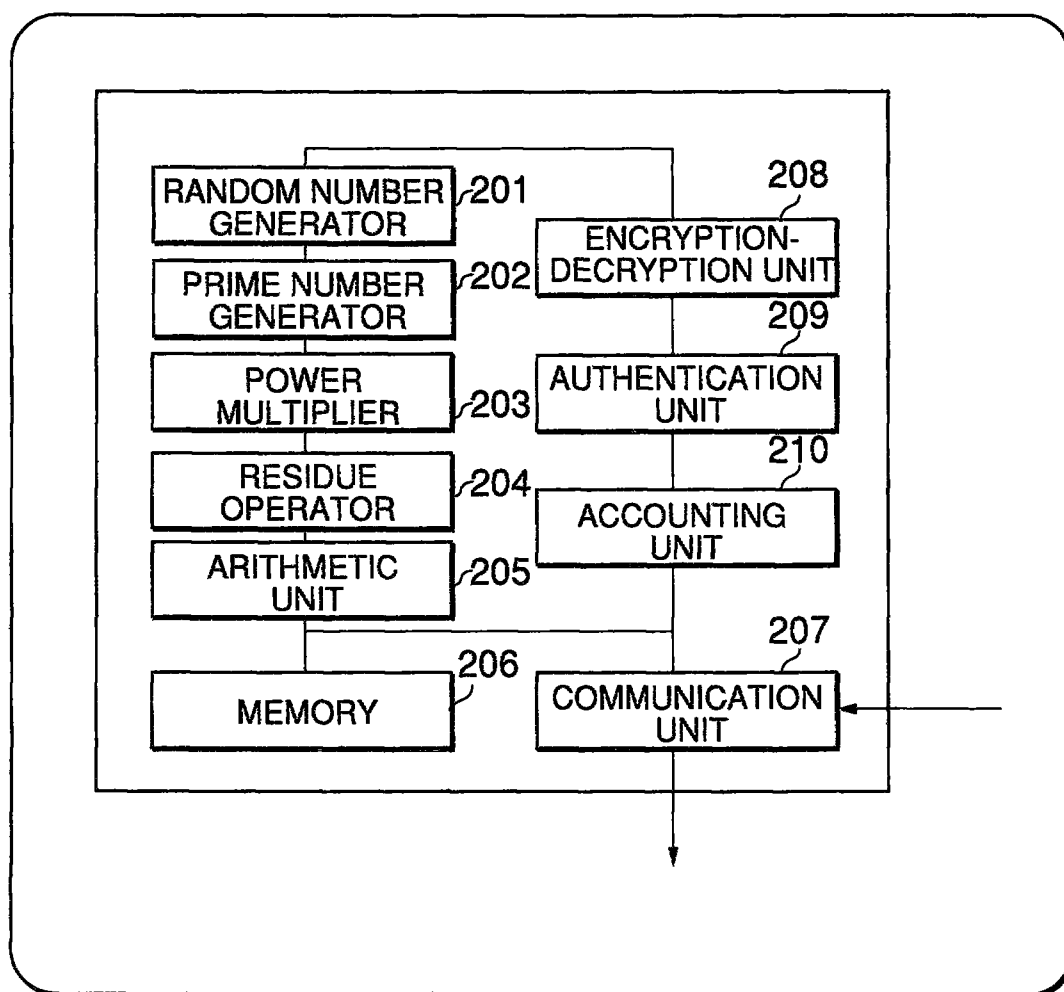


FIG. 4

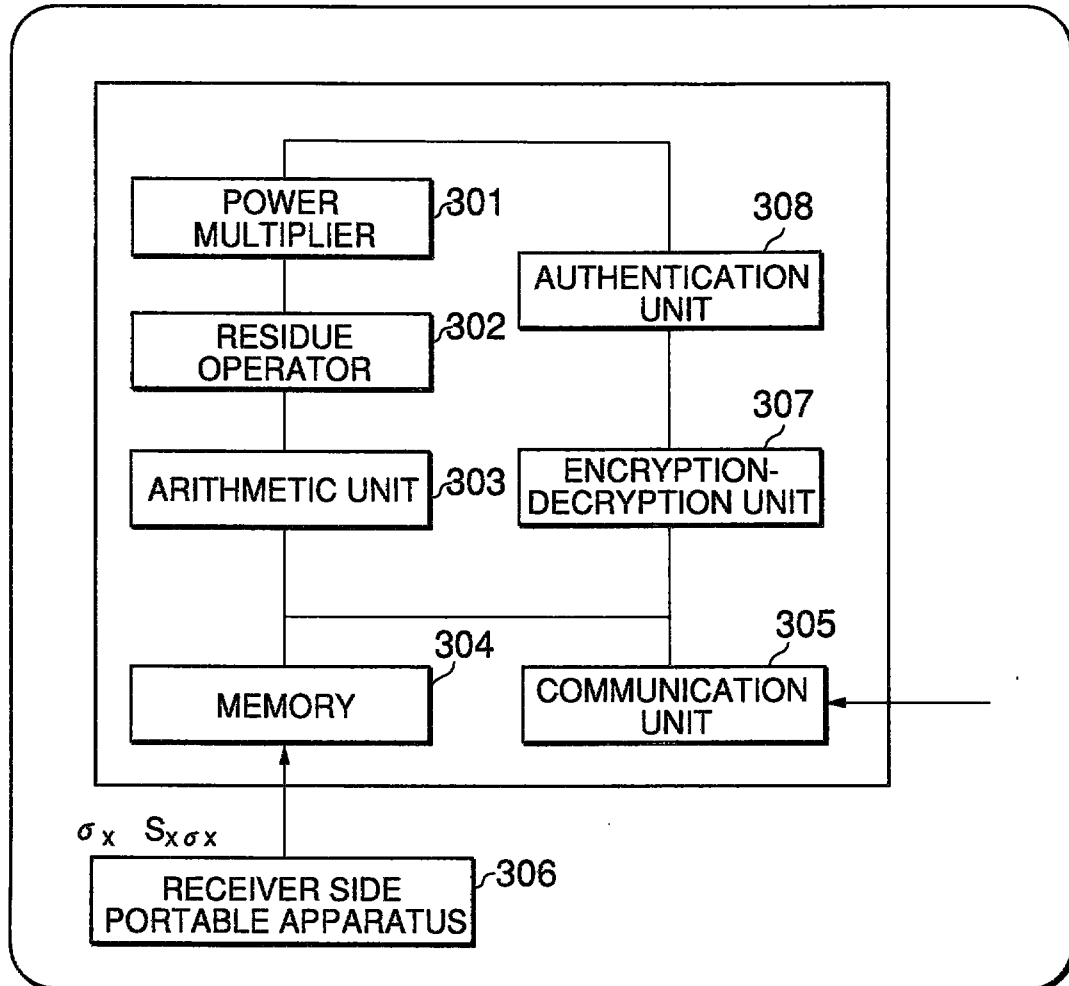


FIG. 5

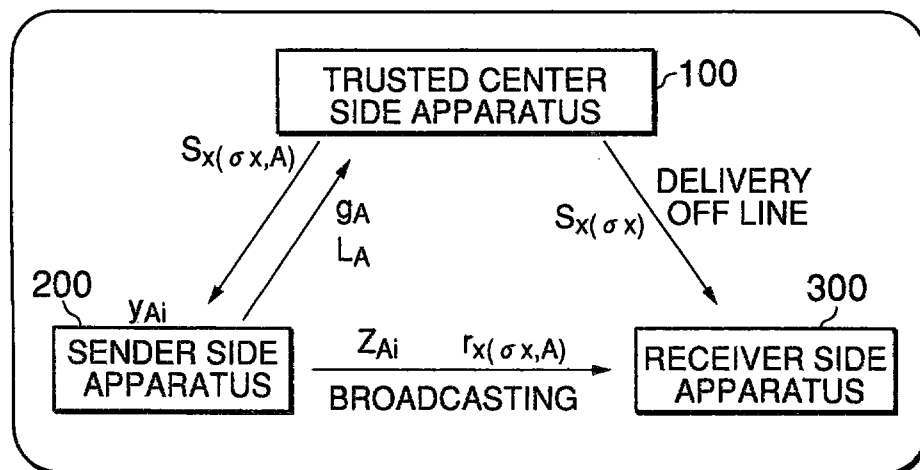


FIG. 6

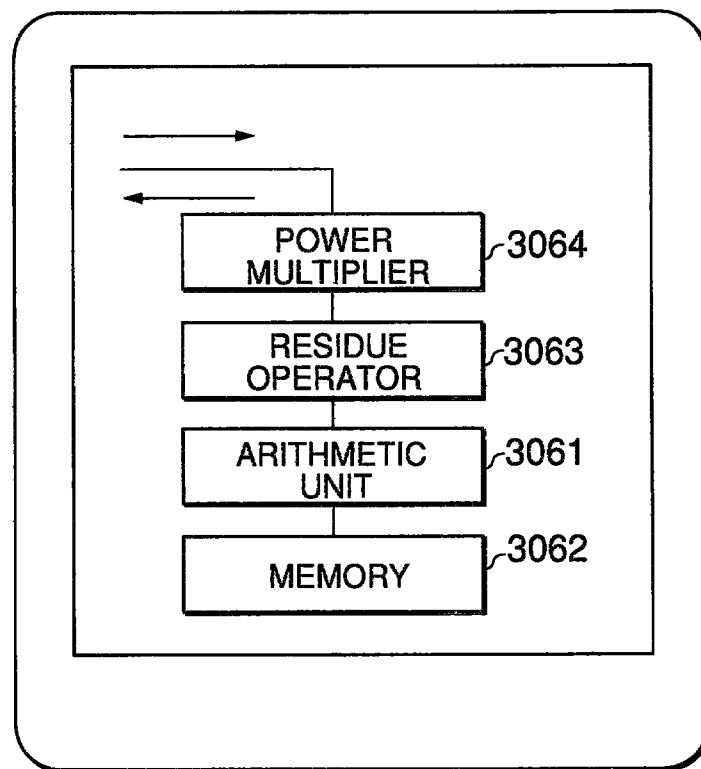


FIG. 7

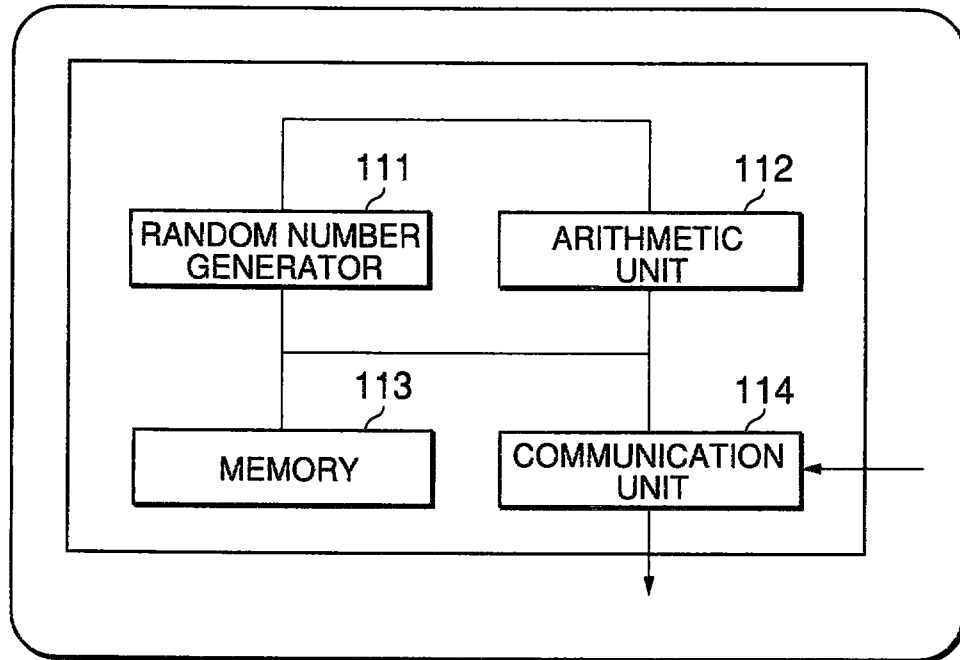


FIG. 8

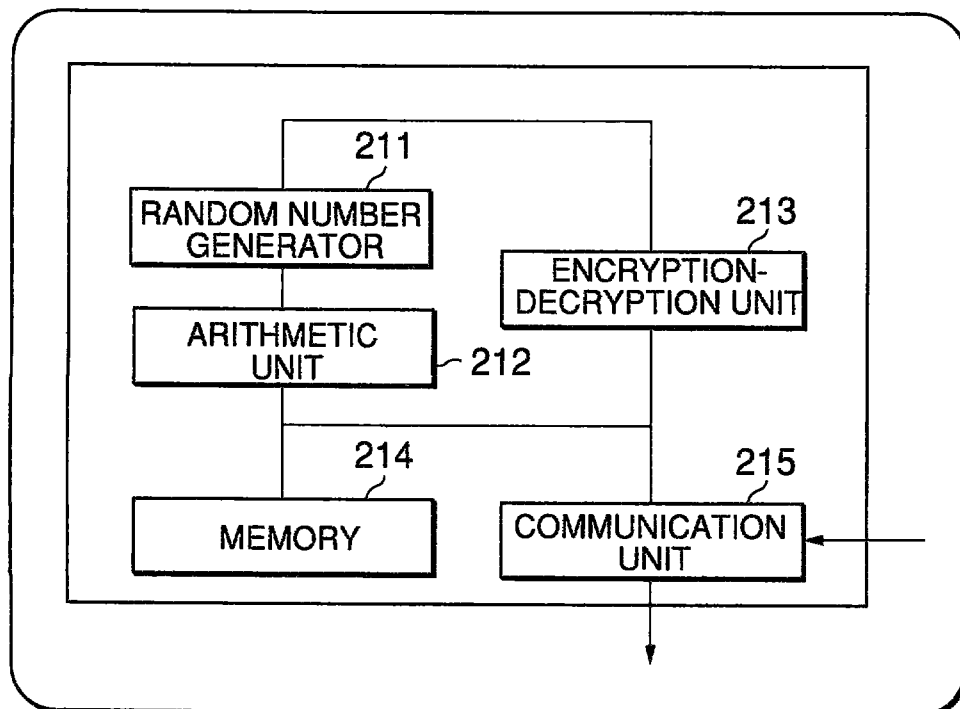
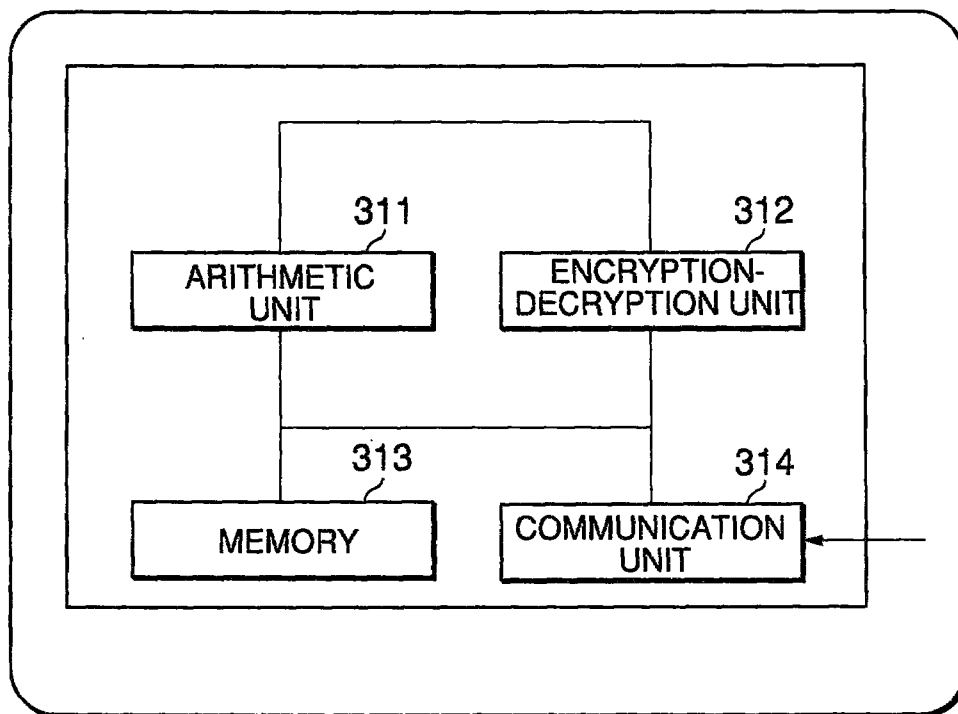


FIG. 9



- 1 -

METHOD AND SYSTEM FOR DISTRIBUTING ENCRYPTION AND  
DECRYPTION KEYS IN  
SECURE BROADCAST COMMUNICATION

5

Background of the Invention

1. Field of the Invention

The present invention relates to a technique of distributing a key for decryption in secure broadcast communication to restricted receivers.

2. Description of Related Art

10 Conventionally, as techniques of secure broadcast communication, some systems have been proposed.

For example, there is known a copied key method described in an article, S.J. Kent: "Security Requirements and Protocols for a Broadcast Scenario", IEEE Trans. Commun., COM-29, 6, pp. 778 - 786 (1981).

15 This copied key method is a fundamental system for secure broadcast communication, and is simple extension of the conventional one-to-one individual cipher communication. Namely, in this method, copies of one kind of key are distributed to a sender and a plurality of regular receivers. The sender encrypts information by use of the distributed copy key and sends  
20 the encrypted information. Each of the regular receivers uses the distributed copy key to decrypt the encrypted information.

Further, there is known a technique of distributing a common key using an individual key assigned for every receiver. For example, a system of key distribution by multiplexing-demultiplexing of an information  
25 sequence using the Chinese remainder theorem is described in an article, Lee, Tokiwa, et al: "A Multi-Address Communication Using a Method of

REPLACEMENT SHEET

07 JAN 1999

Multiplexing and Demultiplexing, 1986 Symposium on encryption and information security". Also, Mambo et al: "A Secure Broadcast Communication Method with Short Messages", IEICE TRNS. FUNDAMENTALS, VOL. E77-A, No. 8 AUGUST 1994 describes such a  
5 technique.

The system of multiplexing-demultiplexing an information sequence by use of the Chinese remainder theorem performs the following processes.

(1) Key generation process:

10 For receivers  $i$  ( $1 \leq i \leq s$ ),  $s$  integers  $g_1, g_2, \dots, g_s$  ( $r \leq s$ ) which are relatively prime to one another are generated, and  $g_i$  is distributed in advance to  $i$ -th receiver as secret key of that receiver  $i$ .

(2) Encryption process:

An information sequence of  $s$  items to be multiplexed is expressed  
15 as  $M_1, M_2, \dots, M_s$ . The sender calculates a multiplexed sentence  $F$  to be sent by:

$$F = \sum_{i=1}^k A_i G_i M_i \bmod G$$

and broadcasts it. Here,  $G$ ,  $G_i$ , and  $A_i$  are defined as follows:

$$G = \prod_{i=1}^k g_i$$

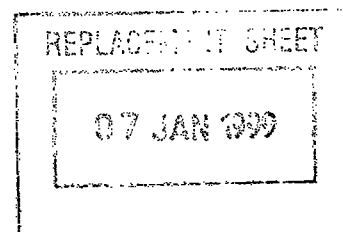
$$G_i = G / g_i$$

$$A_i G_i \equiv 1 \pmod{g_i}$$

20 and  $A_i$  is the smallest integer which satisfies the above equations.

(3) Decryption process:

Using  $g_i$ , the receiver  $i$  demultiplexes  $M_i$  from  $F$  by the following equation,



$$M_i = F \bmod g_i$$

Here,  $M_i$  is a common key to be distributed to the receiver  $i$ . Thus, according to this system, the copy key can be distributed in secret to the restricted receivers only.

5           Next, the system described in the literature, Mambo et al: "A Secure Broadcast Communication Method with Short Messages", IEICE TRNS. FUNDAMENTALS, VOL. E77-A, No. 8 AUGUST 1994 performs following processes.

(1) Key generation process:

10           A trusted center produces following information.

Secret key:

$$P = 2p + 1, Q = 2q + 1: \text{prime number} \quad (p, q: \text{prime number})$$
$$e_i \in \mathbb{Z}, 0 < e_i < L \quad (1 \leq i \leq m)$$

Public key:

$$g \in \mathbb{Z}, 0 < g < N$$
$$N = PQ$$
$$v_i = g^{e_i} \bmod N \quad (1 \leq i \leq m)$$

15           For  $\sigma \in S$ , the center calculates  $s_\sigma$  that satisfies:

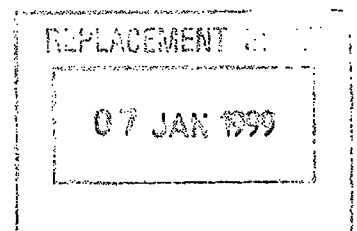
$$s_\sigma \sum_{i=1}^k e_{\sigma(i)} \equiv 1 \pmod{L}$$

and distributes it as secret key of a receiver  $U_\sigma$ . Here, the set  $S$  is defined as  $S = \{f \mid \text{one to one map } f: A\{1, 2, \dots, k\} \rightarrow B\{1, 2, \dots, m\}, m > k\}$ .

(2) Key distribution process:

20           A sender selects an integer  $r$  at random, and, in order to have a common key  $K$  defined as:

$$K = g^r \bmod N$$



in common with restricted receivers, calculates  $z_i$  that satisfies:

$$z_i = v_i^r \bmod N \quad (1 \leq i \leq m)$$

and broadcasts  $z_i$  ( $1 \leq i \leq m$ ).

The receiver  $U\sigma$  uses the following equation:

5 
$$K = \left( \prod_{i=1}^k z_{\sigma(i)} \right)^{s\sigma} \bmod N$$

to calculate the common key  $K$ .

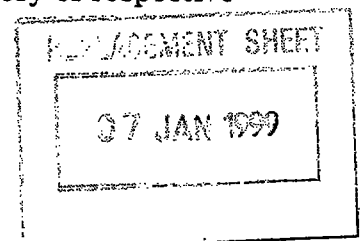
### Summary of the Invention

In the above-described conventional method of key distribution by  
10 multiplexing using the Chinese remainder theorem, common key data for  
respective receivers are arranged serially and transmitted. Thus, broadcast  
data length becomes longer in proportion to the number of the receivers.  
Accordingly, it is not suitable for communication for millions of receivers or  
more, such as satellite broadcasting.

15 On the other hand, according to the system described in the above-  
referred literature, Mambo et al: "A Secure Broadcast Communication  
Method with Short Messages", IEICE TRNS. FUNDAMENTALS, VOL. E77-  
A, No. 8 AUGUST 1994, data for distributing the common key can be  
shortened. In this system, however, it is not possible to have the key  
20 commonly used among restricted receivers belonging to any set of receivers.

Further, in all systems, when there are a plurality of senders,  
receivers must obtain the above-described user secret key for respective  
senders, and manage them.

Thus, an object of the present invention is to provide a key  
25 distribution system in which a receiver can receive delivery of respective



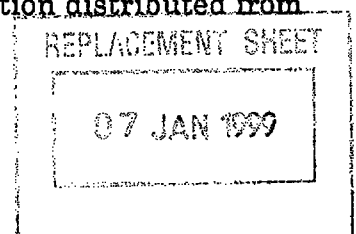
common keys from a plurality of senders by means of only one secret key. A further object is to make it possible that, in such a key distribution system, a common key for data decryption can be commonly owned only among any sender and any set of receivers, and to shorten broadcast data for distributing  
5 a common key even when the number of receivers are large.

To attain the above objects, the present invention provides a method of key distribution having an encryption-decryption key of secure broadcast communication commonly used among a plurality of senders and a plurality of receivers in a communication system comprising apparatuses of  
10 said plurality of senders and apparatuses of said plurality of receivers, wherein:

in an apparatus of a trusted center provided separately from said senders and said receivers, first key information, which is common to said plurality of senders and is used for a key commonly used among said senders  
15 and said receivers, is produced and distributed to prescribed receivers, while second key information which is used for a key commonly used among said senders and said receivers is produced and distributed to said senders;

in apparatuses of said senders, third key information, which is used by said receivers together with said first key information to calculate an  
20 encryption-decryption key used by the sender in question in broadcast communication, is produced using the second key information distributed from said trusted center and is sent to said receivers who have a key in common with said sender; and

in an apparatus of a receiver, the encryption-decryption key which  
25 is used for broadcast communication by the sender who distributed said third key information is obtained using the first key information distributed from



said trusted center and the third key information distributed from said sender.

According to the present method of key distribution, it is sufficient for each receiver to have only the first key information distributed from the trusted center as a user secret key. When an encryption-decryption key of a new sender is to be obtained, it is not necessary to receive distribution of new user secret key.

In detail, the present invention provides a method of key distribution, in which an encryption-decryption key for secure broadcast communication performed by said sender is distributed to receivers, in a communication system comprising apparatuses of a plurality of senders and apparatuses of a plurality of receivers, and an apparatus of a trusted center, comprising:

a step, in which, in the apparatus of the trusted center,

$$e_i \in Z \quad (1 \leq i \leq m)$$

are produced as trusted center secret key,

$$t_A \in Z$$

is produced as sender registration key of a sender A, and, as receiver secret key,  $\sigma_x \in S_{km}$  and

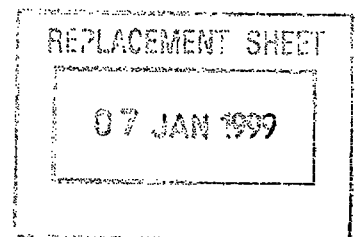
$$s_x(\sigma_x) \in Z$$

are produced (here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$  defined as:

$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \\ \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m \}$$

it is expressed as:

$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A),$$



with " $\sim$ " becoming an equivalence relation on  $S_{km}$ , leading to an expression:

$$\tilde{S}_{km} = S_{km} / \sim$$

), and the receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  are distributed to the receiver x;

a step, in which, in the apparatus of the sender A,

5 sender secret key  $g_A$ ,  $L_A$ , and a finite Abelian group  $G_A$  satisfying:

$$\begin{aligned} g_A &\in G_A \\ L_A &= \text{ord}_{G_A}(g_A) \end{aligned}$$

are produced (here,

$$\text{ord}_{G_A}(g)$$

means the least positive integer a satisfying:

10 
$$g^a = 1 (\in G_A)$$

), and the sender secret key  $g_A$  is sent to said trusted center;

a step, in which, in the apparatus of the trusted center, receiver registration data:

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

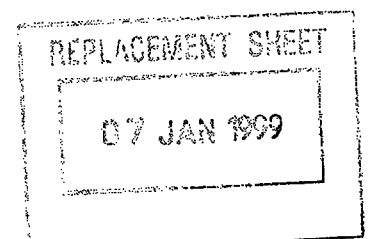
15 is calculated from the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and the receiver secret key  $s_x(\sigma_x)$ ,  $\sigma_x$ , and the receiver registration data  $s_x(\sigma_x, A)$  is sent to the sender A, and key distribution data:

$$y_{Ai} = g_A^{u_i} (\in G_A) \quad (1 \leq i \leq m)$$

is calculated from  $g_A$  received from the sender A, the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and this key distribution data  $y_{Ai}$  is sent to  
20 the sender A;

a step, in which, in the apparatus of the sender A, random integers  $r$ ,  $r'$  are produced, receiver registration key  $r_x(\sigma_x, A)$  satisfying:

$$r_x(\sigma_x, A) s_x(\sigma_x, A) = r' \pmod{L_A}$$



is calculated from the receiver registration data  $s_x(\sigma_x, A)$  received from said trusted center, the sender secret key  $L_A$ , and the random integer  $r'$ ; the receiver registration key  $r_x(\sigma_x, A)$  is sent to the receiver  $x$ ; and key distribution data defined as:

5 
$$z_{Ai} = y_{Ai}^{r'} \quad (\in G_A) \quad (1 \leq i \leq m)$$

is calculated from the key distribution data  $y_{Ai}$  received from said trusted center, and the random integer  $r$ , and the key distribution data  $z_{Ai}$  is broadcasted to each receiver; and

a step, in which, in the apparatus of the receiver  $x$ , an encryption-  
10 decryption key  $K_A$  used for broadcast communication is calculated using:

$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \quad (\in G_A)$$

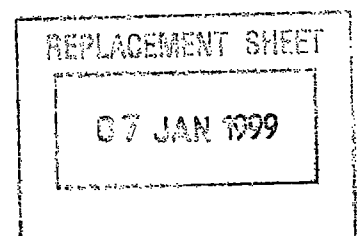
from the receiver registration key  $r_x(\sigma_x, A)$  received from the sender, the key distribution data  $z_{Ai}$ , and the receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$ , with the encryption-decryption key  $K_A$  being produced by the sender  $A$ , using:

15 
$$K_A = g_A^{r'} \quad (\in G_A).$$

According to this method of key distribution, it is not necessary for the receivers to own private keys which are different for respective senders. Further, in secure broadcast communication, even when the number of receivers is large, the length of the key distribution data can be made short.

20 Further, in the present method of key distribution, the receiver secret key is made secret from the senders and the sender secret key is more reliably made secret from the receivers since the sender registration key is owned only by the trusted center in secret. Accordingly, security against impropriety is improved.

25



### Brief Description of the Drawings

Fig. 1 is a block diagram showing a configuration of a key distribution system according to an embodiment of the present invention;

Fig. 2 is a block diagram showing a configuration of a trusted center side apparatus according to a first embodiment of the present invention;

Fig. 3 is a block diagram showing a configuration of a sender side apparatus according to the first embodiment of the present invention;

Fig. 4 is a block diagram showing a configuration a receiver side apparatus according to the first embodiment of the present invention;

Fig. 5 is a view showing information flow caused by key distribution process in the first embodiment of the present invention;

Fig. 6 is a block diagram showing a configuration of a receiver side apparatus according to a second embodiment of the present invention;

Fig. 7 is a block diagram showing a configuration of a trusted center side apparatus according to a fifth embodiment of the present invention;

Fig. 8 is a block diagram showing a configuration of a sender side apparatus according to the fifth embodiment of the present invention; and

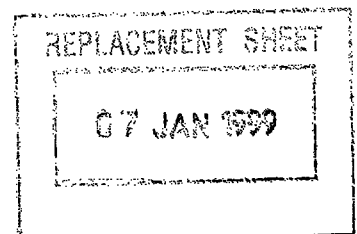
Fig. 9 is a block diagram showing a configuration of a receiver side apparatus according to the fifth embodiment of the present invention.

### Detailed Description

In the following, there will be described a key distribution system according to an embodiment of the present invention.

Firstly, the first embodiment will be described.

Fig. 1 shows a configuration of a key distribution system according to the present embodiment of the invention.



As shown in the figure, the present system comprises a trusted center side apparatus 100, sender side apparatuses 200, and receiver side apparatuses 300. These apparatuses are connected to one another via communication lines 400. The trusted center side apparatus 100 is the one  
5 and only apparatus used by the trusted center organization in the system, while the system has a plurality of sender side apparatuses 200 and a plurality of receiver side apparatuses 300.

Fig. 2 shows a configuration of the trusted center side apparatus 100.

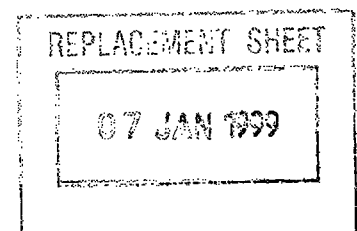
10 As shown in the figure, the trusted center side apparatus 100 comprises a random number generator 101, a prime number generator 102, a power multiplier 103, a remainder computing unit 104, an arithmetic unit 105, a memory 106, and a communication unit 107. The trusted center side apparatus 100 is connected to receiver side portable apparatuses 306 which  
15 are delivered to receivers off line.

Fig. 3 shows a configuration of the sender side apparatus 200.

As shown in the figure, the sender side apparatus 200 comprises a random number generator 201, a prime number generator 202, a power multiplier 203, a remainder computing unit 204, an arithmetic unit 205, a  
20 memory 206, a communication unit 207, an encryption-decryption unit 208, an authentication unit 209, and an accounting unit 210.

Fig. 4 shows a configuration of the receiver side apparatus 300.

As shown in the figure, the receiver side apparatus 300 comprises a power multiplier 301, a remainder computing unit 302, an arithmetic unit  
25 303, a memory 304, a communication unit 305, a receiver side portable apparatus 306 which has been delivered off line from the trusted center, an



encryption-decryption unit 307, and an authentication unit 308.

In the following, three processes will be described, i.e., a preparation process, a key distribution process, and an encryption-decryption process.

5 First, the preparation process will be described.

(1) Preparation process

(i) A sender A uses the random number generator 201, the prime number generator 202, the power multiplier 203, the remainder computing unit 204 and the arithmetic unit 205 within the sender side apparatus 200, to  
10 produce the following keys, and makes only public key open to the public.

Secret key:

$P_A, Q_A$  : prime numbers

$L_A = lcm(ord_{P_A}(g_A), ord_{Q_A}(g_A))$

$g_A \in Z, 0 < g_A < N_A$

$r, r' \in Z, 0 < r, r' < L_A$

Public key:

$N_A (= P_A Q_A)$

15 The secret key is stored in the memory 206. Further, pieces of the secret key  $g_A, L_A$  are sent to the trusted center by means of the communication unit 207.

(ii) The reliable trusted center uses the arithmetic unit 105 within the trusted center side apparatus 100 to generate the following information.

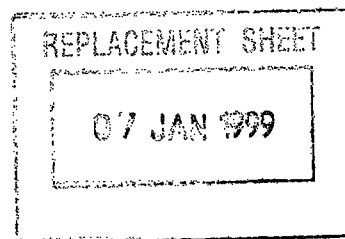
20 Trusted center secret key:

$e_i \in Z (1 \leq i \leq m)$

Sender registration key for the sender A:

$t_A \in Z, 0 < t_A < L_A$

Receiver secret key for a receiver x:



$$s_x(\sigma_x) \in Z, \quad 0 < t_A < L_A$$

All these are stored in the memory 106 together with  $\sigma_x$ .

Here, for a set:

$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \\ \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m \}$$

5 when  $\sigma, \sigma' \in S_{km}$ , it is assumed that:

$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$$

Here, " $\sim$ " becomes an equivalence relation on  $S_{km}$ , and

$$\tilde{S}_{km} = S_{km} / \sim$$

Further, the trusted center takes the receiver secret key  $s_x(\sigma_x)$  from  
10 the memory 106, stores it in the receiver side portable apparatus 306  
together with  $\sigma_x$ , and delivers that apparatus to the receiver x off line. Of  
course, it may be delivered to the receiver in another way.

Next, the key distribution process will be described.

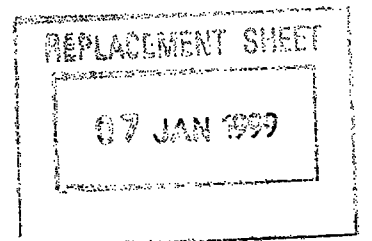
## (2) Key distribution process

15 Fig. 5 shows information flow among the trusted center, senders  
and receivers in the present key distribution process.

(i) The trusted center uses the remainder computing unit 104 and the  
arithmetic unit 105 within the trusted center side apparatus 100 to calculate  
receiver registration key  $s_x(\sigma_x, A)$  defined as:

20 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \bmod L_A$$

from  $L_A$  received from the sender A, trusted center secret key  $e_i$ ,  $\sigma_x$ , receiver  
secret key  $s_x(\sigma_x)$  and the sender registration key  $t_A$ , and sends it to the sender  
A using the communication unit 107.



Further, the trusted center uses the power multiplier 103, the remainder computing unit 104 and the arithmetic unit 105 to calculate sender key distribution data  $y_{Ai}$  of the sender A:

$$y_{Ai} = g_A^{u_i} \bmod N_A \quad (1 \leq i \leq m)$$

- 5 from  $g_A$  received from the sender A, sender public key  $N_A$  of the sender A, and trusted center public key  $e_i$ , and sends it to the sender A by means of the communication unit 107.

- (ii) The sender A generates random integers  $r, r'$  by means of the random number generator 201 within the sender side apparatus 200, and  
10 stores them in the memory 206. Further, the sender A uses the power multiplier 203, the remainder computing unit 204 and the arithmetic unit 205 to calculate data encryption key  $K_A$  defined by:

$$K_A = g_A^{rr'} \bmod N_A$$

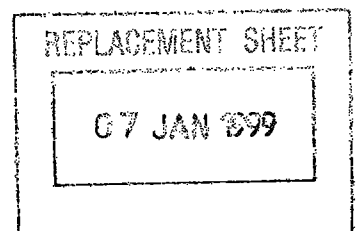
- from these random integers  $r, r'$ , his own secret key  $g_A$  and his own public key  
15  $N_A$ , and stores it in the memory 206. Then, for the purpose of having the key  $K_A$  in common with the receiver  $x$ , the sender A uses the remainder computing unit 204 and the arithmetic unit 205 to calculate receiver registration key  $r_x(\sigma_x, A)$  of the receiver  $x$ , satisfying:

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

- 20 from his own secret key  $L_A$ , the random number  $r'$  and the receiver registration key  $s_x(\sigma_x, A)$ , and sends it to the receiver by means of the communication unit 207.

- Further, the sender A uses the power multiplier 203, the remainder computing unit 204 and the arithmetic unit 205 within the sender side  
25 apparatus 200 to calculate receiver key distribution data  $z_{Ai}$  defined by:

$$z_{Ai} = y_{Ai}^r \bmod N_A \quad (1 \leq i \leq m)$$



from his own public key  $N_A$ , the random number  $r$  and  $y_{Ai}$  received from the trusted center, and broadcasts it to the receivers by means of the communication unit 207.

In the above process, the trusted center performs a part of the processes for producing  $r_x(\sigma_x, A)$  and  $z_{Ai}$ , for one thing, to keep  $\sigma_x$  of the receiver  $x$ , the receiver secret key  $s_x(\sigma_x)$  and the sender registration number  $t_A$  secret from the sender  $A$  so as to prevent improprieties by the sender  $A$ .

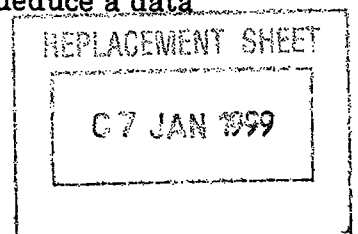
(iii) The receiver  $x$  uses the power multiplier 301, the remainder computing unit 302 and the arithmetic unit 303 within the receiver side apparatus 300 to calculate the data encryption key  $K_A$  by the expression:

$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \bmod N_A$$

from the key distribution data  $z_{Ai}$  received from the sender  $A$ , the receiver registration key  $r_x(\sigma_x, A)$ ,  $\sigma_x$  and the receiver secret key  $s_x(\sigma_x)$  delivered from the trusted center and the sender public key  $N_A$  opened to the public, and stores it in the memory 304.

By the above-described process, the sender  $A$  and the receiver  $x$  can have the key  $K_A$  in common. Similarly, for any other sender and any other receiver, it is possible to have a key in common. In that case, receiver key distribution data  $z_{Ai}$  broadcasted by each sender is the same for each receiver.

Further, in the above-described process, the receiver  $x$  receives the key distribution data  $z_{Ai}$  and the receiver registration key  $r_x(\sigma_x, A)$  from the sender  $A$ . These  $z_{Ai}$  and  $r_x(\sigma_x, A)$  have been produced under the effect of the sender registration number  $t_A$  of the sender  $A$ , and  $t_A$  is kept secret from the receiver. Thus, owing to the use of the above-described sender registration number  $t_A$ , it becomes very difficult for the receiver  $x$  to deduce a data



encryption key  $K_B$  of another sender B from the key distribution data  $z_{Ai}$  and the receiver registration key  $r_x(\sigma_x, A)$  received from the sender A and key distribution data  $z_{Bi}$  broadcasted by the sender B.

In the following, the encryption-decryption process will be  
5 described.

(3) Encryption-decryption process

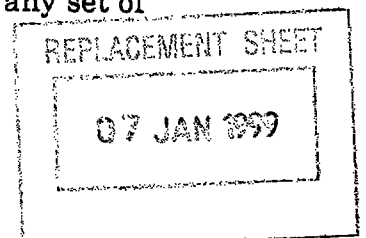
(i) The sender A uses the encryption-decryption unit 208 within the sender side apparatus 200 to encrypt data P with the common key  $K_A$  produced in the key distribution process. Then, the sender A sends a cipher  
10 text  $C=E(K_A: P)$  to a receiver by means of the communication unit 207.

(ii) The receiver uses the communication unit 305 within the receiver side apparatus 300 to receive the public key C, and uses the encryption-decryption unit 307 to decrypt the public key C with the common key  $K_A$  stored in the memory 304, so as to obtain the original data.

15 The above is the first embodiment of the present invention.

In the conventional technique, when a sender newly enters a key distribution system, it is necessary for the sender to produce  $\sigma_x$  and receiver secret key  $s_x(\sigma_x)$  by himself and to deliver them to a receiver off line. On the other hand, according to the key distribution system of the first embodiment,  
20 it suffices for a sender who newly enters the system to produce the sender secret key  $P_A$ ,  $Q_A$ ,  $L_A$ ,  $g_A$  and the sender public key  $N_A$ . Further, receiver secret key owned by a receiver is same for all the senders. Thus, when a receiver wishes to receive data from a new sender, it is not necessary to obtain new receiver secret key.

25 Further, the receiver registration key  $r_x(\sigma_x, A)$  makes it possible to have a common key in common with receivers belonging to any set of



receivers, for data encryption and decryption concerning them only. Even when the number of receivers is large, it is not necessary to correspondingly lengthen the key distribution data  $z_{Ai}$  broadcasted for distribution of a common keys.

5 In the above processes, it is possible alternatively that the sender sends the sender secret key  $L_A$  to the trusted center in advance, and in the step of the preparation process, the trusted center generates the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and the receiver secret key  $s_x(\sigma_x)$  satisfying:

$$\begin{aligned} e_i &\in Z, \quad 0 < e_i < L_A, \quad (1 \leq i \leq m) \\ t_A &\in Z, \quad 0 < t_A < L_A \\ 10 \quad s_x(\sigma_x) &\in Z, \quad 0 < s_x(\sigma_x) < L_A, \end{aligned}$$

and, in the step of the key distribution process, the trusted center calculates the receiver registration key  $s_x(\sigma_x, A)$  by:

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \mod L_A$$

from the sender secret key  $L_A$ , the trusted center secret key  $e_i$ , the sender registration key  $t_A$  and the receiver secret key  $s_x(\sigma_x)$ .  
15

Next, a second embodiment of the present invention will be described.

In the second embodiment of the present invention, the receiver side portable apparatus 300 of the above first embodiment is provided with a power multiplier 3064, a remainder computing unit 3063, an arithmetic unit  
20 3061 and a memory 3062 as shown in Fig. 6. Further, the process of calculating the data encryption key  $K_A$  in the receiver side apparatus 300 of the above first embodiment is partly performed in the receiver side portable

REPLACEMENT SHEET

07 JAN 1999

apparatus 306.

Namely, in the second embodiment, (1) in the step of the preparation process, the trusted center stores  $\sigma_x$  and the receiver secret key  $s_x(\sigma_x)$  in the receiver side portable apparatus 306 (such as an IC card (a smart  
5 card)), and delivers them to the receiver x.

Then, (2) in the key distribution process, the receiver x outputs the key distribution data  $z_{Ai}$  stored in the memory within the receiver side apparatus 300 to the receiver side portable apparatus 306. Next, within the receiver side portable apparatus 306, the receiver x uses the power multiplier  
10 3064 and the remainder computing unit 3063 to calculate:

$$\xi_x(\sigma_x, A) = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \bmod N_A$$

from  $\sigma_x$ , the receiver secret key  $s_x(\sigma_x)$ , the key distribution data  $z_{Ai}$  and the sender public key  $N_A$ , and outputs the calculated result  $\xi_x(\sigma_x, A)$  to the receiver side apparatus 300.

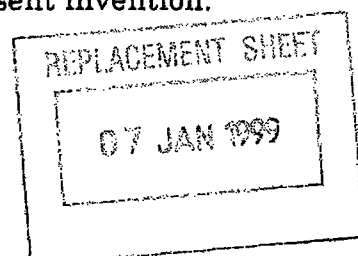
15 Next, the receiver x uses the power multiplier 301, the remainder computing unit 302 and the arithmetic unit 303 within the receiver side apparatus 300 to calculate the data encryption key  $K_A$  by:

$$K_A = \xi_x(\sigma_x, A)^{r_x(\sigma_x, A)} \bmod N_A$$

from  $\xi_x(\sigma_x, A)$  outputted to the receiver side apparatus 300, the receiver  
20 registration key  $r_x(\sigma_x, A)$  stored in the memory 304, and the sender public key  $N_A$ , and stores it in the memory 304.

Thus,  $\sigma_x$  and the receiver secret key  $s_x(\sigma_x)$  are prevented from being outputted outside the receiver side portable apparatus 306, so that these are prevented from being stolen by electronic duplicating or the like.

25 The above is the second embodiment of the present invention.



Next, a third embodiment of the present invention will be described.

The third embodiment of the present invention is different from the above-described first embodiment in that the value of  $r$  in the equation:

$$K_A = g_A^{r'} \bmod N_A$$

5 is changed periodically every short time period, and  $z_{Ai}$  obtained by using the changed  $r$  is broadcasted periodically for update of the data encryption-decryption key  $K_A$  calculated in the sender side apparatus 200 and in the receiver side apparatus 300.

Further, in the present embodiment, the value of  $r'$  is made to be  
10 characteristic to sending data so as to identify data broadcasted by a sender. Namely, a registration key  $r_x(\sigma_x, A)$  which the receiver  $x$  received from a sender to decrypt certain broadcast data or a set of broadcast data is characteristic to that broadcast data. To obtain another broadcast data or another set of broadcast data, the receiver  $x$  must receive another  $r_x(\sigma_x, A)$  for  
15 that broadcast data or that set of broadcast data.

The above is the third embodiment of the present invention.

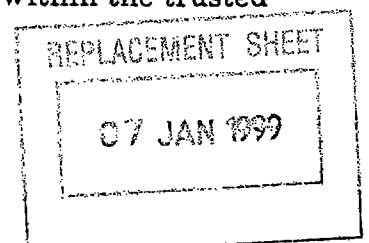
Next, a fourth embodiment of the present invention will be described.

The fourth embodiment is different from the above-described first  
20 embodiment in that authentication of receivers is performed so as to charge receivers who have a common key  $K_A$  in common for fee-charging data  $P$  encrypted with the key  $K_A$  and sent by a sender.

Namely, in the fourth embodiment of the present invention, following processes are further performed.

25 (1) Preparation process

(i) The trusted center uses the arithmetic unit 105 within the trusted



center side apparatus 100 to produce a number  $UID_x$  for the receiver  $x$  in advance, and stores it in the receiver side portable apparatus 306 together with the receiver secret key  $s_x(\sigma_x)$ , and delivers that apparatus. Further  $UID_x$  is stored in the memory 106, so as to correspond to  $s_x(\sigma_x)$ .

5 (ii) The sender  $A$  uses the arithmetic unit 205 within the sender side apparatus 200 to produce his own number  $BIDA$ , and stores it in the memory 206. The sender  $A$  sends  $BIDA$  to the trusted center by means of the communication unit 207.

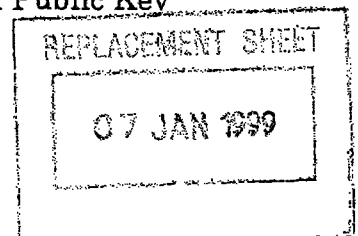
(iii) The trusted center receives  $BIDA$ , the number of the sender  $A$ ,  
10 using the communication unit 107 within the trusted center side apparatus 100, and stores it in the memory 106 so as to correspond to the sender registration key  $t_A$ .

(iv) The receiver  $x$  uses the authentication unit 308 within the receiver side apparatus 300 to produce information for authentication from the  
15 receiver secret key  $s_x(\sigma_x)$ , and sends it to the sender  $A$ .

(v) The sender  $A$  confirms the information for authentication by means of the authentication unit 209 within the sender side apparatus 200.

As the method of authentication, any conventionally-known authentication method may be employed in which authentication is not  
20 effected as long as the receiver does not know  $s_x(\sigma_x)$ . However, it is necessary for the sender to be prevented from knowing the receiver private key  $s_x(\sigma_x)$  itself.

For example, authentication of the receiver  $x$  may be performed as in the following processes according to a method employing a signature using  
25 the RSA algorithm (described in an article by, R. L. Rivest, A. Shamir, L. Adelman: "A Method for Obtaining Digital Signatures and Public Key



Cryptosystems", Commun. of the ACM, Vol. 21, No. 2, pp. 120-126, 1978).

(1) The trusted center uses the arithmetic unit 105 within the trusted center side apparatus 100 to produce  $(y_x, n_x)$  satisfying:

$$\begin{aligned} s'_x y_x &\equiv 1 \pmod{\text{lcm}(p_x - 1, q_x - 1)} \\ n_x &= p_x q_x \quad (p_x, q_x : \text{prime numbers}) \end{aligned}$$

5 for the receiver  $x$ , and deliver them to the sender in advance. Here, for a function  $\pi$  which has been opened,  $s'_x$  is defined as  $s'_x = \pi(s_x(\sigma_x))$ .

(2) The receiver  $x$  uses the authentication unit 308 within the receiver side apparatus 300 to calculate a hash value  $(h(w); 0 < h(W) < n_x)$  of broadcast data  $W$  using a unidirectional hash function  $h$  as public key, and produces a  
10 signature for  $h(W)$  by the following expression:

$$\text{sgn}_x(h(W)) = h(W)^{s'_x} \pmod{n_x}$$

using the private key  $s'_x$ , and sends it to the sender by means of the communication unit 305 together with a data sending request.

(3) The sender uses the authentication unit 209 within the sender side  
15 apparatus 200 to confirm that:

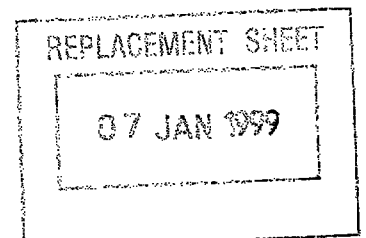
$$\text{sgn}_x(h(W))^{y_x} = h(W) \pmod{n_x}$$

is satisfied.

After the authentication, the sender  $A$  uses the communication unit 207 within the sender side apparatus 200 to send his own number BIDA and  
20 UID $_x$ , the number of the receiver  $x$ , to the trusted center.

The trusted center uses the arithmetic unit 105 within the trusted center side apparatus 100 to calculate the receiver registration data  $s_x(\sigma_x, A)$  expressed by:

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \pmod{LA}$$



from the sender registration key  $t_A$  and the receiver secret key  $s_x(\sigma_x)$  corresponding to the sender number BIDA and the receiver number UIDx received respectively, and sends it to the sender A.

The sender uses the remainder computing unit 204 and the  
5 arithmetic unit 205 within the sender side apparatus 200 to calculate the receiver registration key  $r_x(\sigma_x, A)$  satisfying:

$$r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

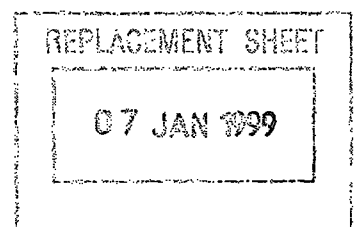
from the receiver registration key  $s_x(\sigma_x, A)$  received from the trusted center, and sends it to the receiver by means of the communication unit 207. At  
10 that time, in the case that data to be delivered being encrypted with the common key  $K_A$  (namely, the data which the receiver requested to the sender) is chargeable, the sender A charges the receiver x by means of the accounting unit 210.

The above is the fourth embodiment of the present invention.

15 Next, a fifth embodiment of the present invention will be described.

The fifth embodiment of the present invention is an extension of the copy key system described in the Description of Related Art to the system shown in Fig. 1 which includes a plurality of senders, a plurality of receivers and a trusted center.

20 Fig. 7 shows a configuration of a trusted center side apparatus 100 according to the fifth embodiment of the present invention. As shown in the figure, the trusted center side apparatus 100 comprises a random number generator 111, an arithmetic unit 112, a memory 113, and a communication unit 114. Further, Fig. 8 shows a configuration of a sender side apparatus  
25 200 according to the fifth embodiment of the present invention. As shown in the figure, the sender side apparatus 200 comprises a random number



generator 211, an arithmetic unit 212, an encryption-decryption unit 213, a memory 214, and a communication unit 215. Further, Fig. 9 shows a configuration of a receiver side apparatus 300 according to the fifth embodiment of the present invention. As shown in the figure, the receiver side apparatus 300 comprises an arithmetic unit 311, an encryption-decryption unit 312, a memory 313, and a communication unit 314.

In the present embodiment, firstly, the following process is performed as a preparation process.

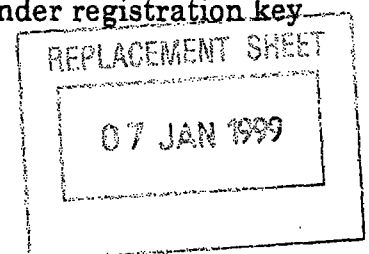
(1) Preparation process

- 10 (i) The trusted center uses the random number generator 111 within the trusted center side apparatus 100 to generate a secret key  $K_0$  and stores it in the memory 113. Also, the trusted center distributes it to senders and receivers.
- (ii) The sender A uses the random number generator 211 within the sender side apparatus 200 to generate sender registration key BIDA, and sends it to the receivers by means of the communication unit 215.

Thereafter, the following process is performed as a key distribution process.

(2) Key distribution process

- 20 (i) The sender A uses the arithmetic unit 212 within the sender side apparatus 200 to calculate a common key  $KA' = F(K_0, BIDA)$  from the secret key  $K_0$  and the sender registration key BIDA, using a suitable one-way function  $F$ .
- (ii) The receiver uses the arithmetic unit 312 within the receiver side apparatus 300 to calculate the common key  $KA' = F(K_0, BIDA)$  from the secret key  $K_0$  distributed from the trusted center and the sender registration key



BIDA received from the sender, using the one-way function  $F$ .

(iii) The sender A uses the random number generator 211 within the sender side apparatus 200 to produce a suitable integer  $r$  and sends it to the receiver by means of the communication unit 215. Further, the sender A  
5 calculates a data encryption-decryption key  $DK=F'(r, KA)$  from the integer  $r$  and the common key  $KA$  using a suitable function  $F'$ , and stores it in the memory 214.

(iv) The receiver uses the arithmetic unit 312 within the receiver side apparatus 300 to calculate the data encryption-decryption key  $DK=F'(r, KA)$   
10 from the integer  $r$  received from the sender A and the common key  $KA$ , and stores it in the memory 314.

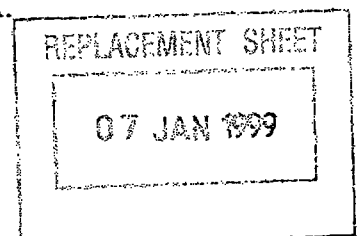
After the distribution of the data encryption-decryption key  $DK$  by the key distribution process, an encryption-decryption process is performed as described in the following.

15 (3) Encryption-decryption process

(i) The sender A encrypts data  $P$  to be delivered with the data encryption-decryption key  $DK$  using the encryption-decryption unit 213 within the sender side apparatus 200, and sends it to the receiver  $x$  by means of the communication unit 215.

20 (ii) The receiver receives the encrypted delivered data  $P$  by the communication unit 314 within the receiver side apparatus 300, and decrypts it with the data encryption-decryption key  $DK$  using the encryption-decryption unit 312.

In the above-described fifth embodiment of the present invention  
25 also, a single piece of secret key suffices for a receiver to have respective common keys of a plurality of senders in common with them.



Next, a sixth embodiment of the present invention will be described.

In the sixth embodiment of the present invention, senders and receivers have a common key in common among them, through cipher communication using respective keys of the receivers.

5           Configurations of the whole system, a trusted center side apparatus 100, a sender side apparatus 200, and a receiver side apparatus 300 according to the present embodiment are similar to those in the above-described fifth embodiment of the present invention.

          In the present embodiment, the following process is performed as a  
10   preparation process.

(1) Preparation process

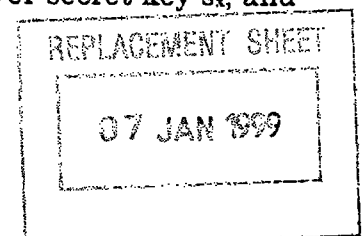
(i)       The trusted center uses the random number generator 111 within the trusted center side apparatus 100 to produce secret key  $s_x$  of the receiver  $x$ , and delivers it to the receiver. Further, the trusted center uses the  
15   random number generator 111 to produce BIDA, the number of the sender  $A$ , and distributes it to the sender  $A$  and the receiver  $x$ .

(ii)      The sender  $A$  uses the random number generator 211 within the sender side apparatus 200 to produce the common key  $K_A$ .

          Thereafter, the following process is performed as a key distribution  
20   process.

(2) Key distribution process

(i)       The trusted center uses the arithmetic unit 112 within the trusted center side apparatus 100 to calculate a session key  $K_{Ax}$ , which is to be used in a session between the receiver  $x$  and the sender  $A$  and defined as  $K_{Ax}=F(s_x, K_A)$  using a suitable one-way function  $F$ . The trusted center calculates  $K_{Ax}$   
25   from BIDA, the number of the sender  $A$ , and the receiver secret key  $s_x$ , and



stores it in the memory 113.

(ii) The receiver x uses the arithmetic unit 312 within the receiver side apparatus 300 to calculate  $K_{Ax}=F(s_x, BIDA)$  from the number of the sender A BIDA and his own secret key  $s_x$  using the one-way function  $F$ , and stores it in  
5 the memory 313.

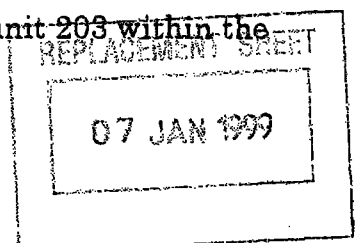
(iii) The sender A uses the encryption-decryption unit 213 within the sender side apparatus 200 to encrypt the common key  $K_A$  with the session key  $K_{Ax}$  to obtain key distribution data  $K_{Cx}$ , and sends the key distribution data  $K_{Cx}$  to the receiver by means of the communication unit 215. Further,  
10 the sender A uses the random number generator 211 to produce a suitable integer  $r$ , and sends it to the receiver by means of the communication unit 215. In addition, the sender A uses the arithmetic unit 212 to calculate a data encryption-decryption key  $DK=F'(r, K_A)$  from the integer  $r$  and the common key  $K_A$  using a suitable function  $F'$ , and stores it in the memory 214.

(iv) The receiver x receives the key distribution data  $K_{Cx}$  from the sender A, and uses the encryption-decryption apparatus 303 within the receiver side apparatus 300 to decrypt the key distribution data  $K_{Cx}$  with the session key  $K_{Ax}$ . Then, the receiver x uses the arithmetic unit 302 to calculate the data encryption-decryption key  $DK=F'(r, K_A)$  from the decrypted  
15 common key  $K_A$  and the received integer  $r$ , using the function  $F'$ , and stores it in the memory 303.

After the distribution of the data encryption-decryption key  $DK$  by the key distribution process, an encryption-decryption process is performed as described in the following.

25 (3) Encryption-decryption process

(i) The sender A uses the encryption-decryption unit 203 within the



sender side apparatus 200 to encrypt data P to be delivered with the data encryption-decryption key DK, and sends it to the receiver x by means of the communication unit 205.

(ii) The receiver x receives the encrypted delivered data P through the communication unit 305 within the receiver side apparatus 300. Then, the receiver x uses the encryption-decryption unit 303 to decrypt the received data P with the data encryption-decryption key DK.

The sender A may change the value of the common key  $K_A$  periodically so as to change the value of the data encryption-decryption key DK periodically.

According to the above-described sixth embodiment of the present invention also, the receiver can have respective common keys of a plurality of senders in common with them, by means of single piece of secret key.

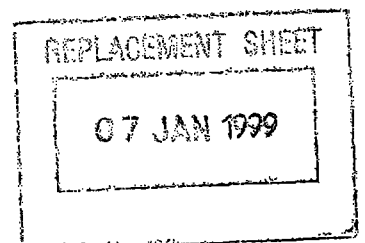
Next, a seventh embodiment of the present invention will be described.

Similarly to the above-described sixth embodiment, in the seventh embodiment of the present invention, senders and receivers have a common key in common among them by cipher communication using respective keys of the receivers.

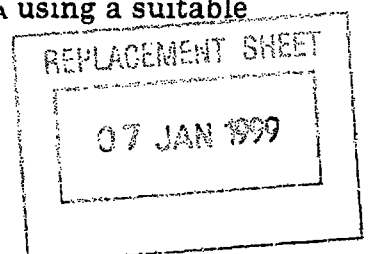
Configurations of the whole system, a trusted center side apparatus 100, a sender side apparatus 200, and a receiver side apparatus 300 according to the present embodiment are similar to those in the above-described fifth embodiment of the present invention.

In the present seventh embodiment, the following process is performed as a preparation process.

(1) Preparation process



- (i) The trusted center uses the random number generator 111 and the arithmetic unit 112 within the trusted center side apparatus 100 to produce a private key  $s_x$  and public key  $p_x$  of the receiver  $x$  according to a suitable open key cryptographic system  $E$  and sends  $s_x$  to the receiver. Further, the
- 5 trusted center produces BIDA, a number of the sender  $A$ , using the random number generator 111, and delivers or sends it to the sender  $A$  and the receiver  $x$ .
- (ii) The sender  $A$  uses the random number generator 211 within the sender side apparatus 200 to produce a common key  $K_A$ , and stores it in the
- 10 memory 114.
- Thereafter, the following process is performed as a key distribution process.
- (2) Key distribution process
- (i) The sender  $A$  uses the encryption-decryption unit 213 within the sender side apparatus 200 to calculate a key distribution data  $K_{Cx}=E(p_x, K_A)$
- 15 from the receiver public key  $p_x$  and the common key  $K_A$  employing a suitable above-described public key cipher system  $E$ . Then, the sender  $A$  sends  $K_{Cx}$  to the receiver  $x$  by means of the communication unit 215.
- (ii) The receiver  $x$  uses the encryption-decryption unit 313 within the receiver side apparatus 300 to encrypt, with his own private key  $s_x$ , the key
- 20 distribution data  $K_{Cx}$  received from the sender  $A$ , and stores the encrypted common key  $K_A$  in the memory 314.
- (iii) The sender  $A$  uses the random number generator 211 within the sender side apparatus 200 to generate a suitable integer  $r$ , and sends it to the receiver  $x$  by means of the communication unit 215. Further, the sender  $A$
- 25 uses the arithmetic unit 212 to calculate the data encryption-decryption key  $DK=F(r, K_A)$  from the integer  $r$  and the common key  $K_A$  using a suitable



function  $F$ , and stores it in the memory 214.

- (iv) The receiver  $x$  uses the arithmetic unit 312 within the receiver side apparatus 300 to calculate the data encryption-decryption key  $DK=F(r, K_A)$  from the common key  $K_A$  and the integer  $r$  received from the sender, using  
5 the function  $F$ , and stores it in the memory 314.

After the distribution of the data encryption-decryption key  $DK$  by the key distribution process, an encryption-decryption process is performed as described in the following.

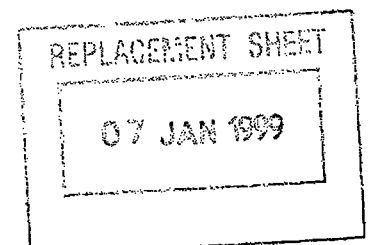
(3) Encryption-decryption process

- 10 (i) The sender  $A$  uses the encryption-decryption unit 213 within the sender side apparatus 200 to encrypt data to be delivered  $P$  with the data encryption-decryption key  $DK$ , and sends it to the receiver  $x$  by means of the communication unit 213.
- (ii) The receiver  $x$  receives the encrypted delivered data  $P$  through the  
15 communication unit 314 within the receiver side apparatus 300. Then, the receiver  $x$  decrypts the data  $P$  with the data encryption-decryption key  $DK$  using the encryption-decryption unit 312.
- (iii) The sender  $A$  changes the value of the common key  $K_A$  periodically so as to change the data encryption-decryption key  $DK$ .

20 According to the above-described seventh embodiment of the present invention also, the receiver can have respective common keys of a plurality of senders in common with them, using a single piece of secret key.

Next, an eighth embodiment of the present invention will be described.

25 The eighth embodiment of the present invention is similar to the above-described sixth and seventh embodiments except that sending of the



key distribution data  $K_{C_x}$  from the sender to the receiver is modified as described in the following.

Namely, in the present eighth embodiment, the sender A separates the set of all of the receivers into some subsets. Next, in sending key  
5 distribution data  $K_{C_i}$  ( $1 \leq i \leq n$ ,  $n$ : the number of the receivers) to the receivers, the sender assigns communication channels to the above-described subsets of the receivers respectively, and sends the key distribution data  $K_{C_i}$  to the receivers through the communication unit 215 within the sender side apparatus 200.

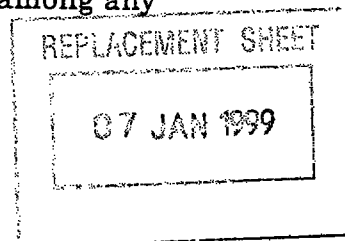
10 On the other hand, any receiver  $x$  receives the key distribution data  $K_{C_x}$  by the communication unit 314 within the receiver side apparatus 300 through the communication channel assigned to the subset to which he belongs.

The embodiments of the present invention have been described  
15 above.

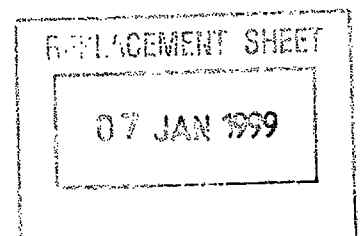
Each of the above-described processes performed by the trusted center side apparatus 100, the sender side apparatus 200, and the receiver side apparatus 300 may be performed by a computer which executes programs describing procedures for performing respective processes. In that  
20 case, each program describing a procedure for performing a process may be stored in a storing medium to be supplied to each computer.

As described above, according to the present invention, a receiver can receive distribution of respective common keys of a plurality of senders, using only one receiver secret key.

25 Further, in some inventions disclosed herein, it is possible to have a common key for data encryption and decryption in common among any

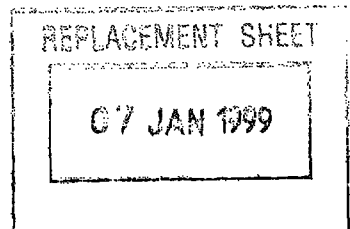


sender and receivers belonging to any set of receivers. Further, even if the number of the receivers is large, it is possible to realize common key distribution using short broadcast communication data for distribution of a common key.

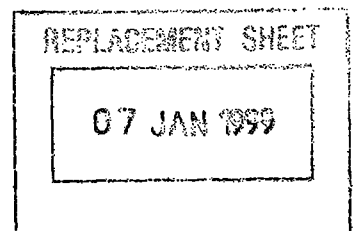


What is claimed is:

- 1 1. A method of key distribution having an encryption-decryption  
2 key of secure broadcast communication in common among a plurality of  
3 senders and a plurality of receivers in a communication system  
4 comprising apparatuses of said plurality of senders and apparatuses of  
5 said plurality of receivers, wherein:
  - 6 in an apparatus of a trusted center provided separately from  
7 said senders and said receivers, first key information which is common  
8 to said plurality of senders and is used for having a key in common  
9 among said senders and said receivers, is produced and distributed to  
10 prescribed receivers, while second key information which is used for a  
11 key in common among said senders and said receivers is produced and  
12 distributed to said senders;
  - 13 in an apparatus of a sender, third key information, which is  
14 used by said receivers together with said first key information to  
15 calculate an encryption-decryption key used by the sender in question  
16 in broadcast communication, is produced using the second key  
17 information distributed from said trusted center and is sent to said  
18 receivers who have the encryption-decryption key in common with said  
19 sender; and
  - 20 in an apparatus of a receiver, the encryption-decryption key  
21 which is used for broadcast communication by the sender who  
22 distributed said third key information is obtained using the first key  
23 information distributed from said trusted center and the third key  
24 information distributed from said sender.



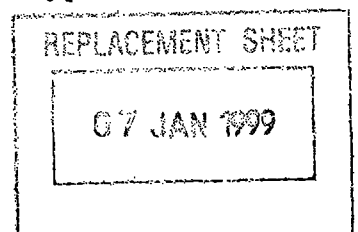
1     2.         A method of key distribution having an encryption-decryption  
2     key of secure broadcast communication in common among a plurality of  
3     senders and a plurality of receivers in a communication system  
4     comprising an apparatus of a trusted center, apparatuses of said  
5     plurality of senders and apparatuses of said plurality of receivers,  
6     comprising:  
7         a first step, in the apparatus of the trusted center, of producing  
8     receiver secret key  $s_x$  of receiver  $x$  so as to correspond to a subset  $S'$  of a  
9     finite set  $S$ , and distributing the receiver secret key  $s_x$  to said receiver  $x$ ,  
10    while producing sender registration key  $t_A$  of a sender  $A$ ;  
11         a second step, in the apparatus of the sender  $A$ , of producing  
12    sender secret key  $g_A$  of the sender  $A$  and calculating an encryption-  
13    decryption key  $K_A$  from the sender secret key  $g_A$ ;  
14         a third step, in cooperation between the apparatus of the  
15    trusted center and the apparatus of the sender  $A$ , of producing key  
16    distribution data  $W$  by a function of at least the sender secret key  $g_A$  and  
17    the sender registration key  $t_A$ , while producing receiver registration key  
18     $r_x$  of the receiver  $x$  for the sender  $A$  by a function of at least the receiver  
19    private key information  $s_x$  and the sender registration key  $t_A$ ;  
20         a fourth step, in the apparatus of the sender  $A$ , of sending the  
21    receiver registration key  $r_x$  to the receiver  $x$  and broadcasting the key  
22    distribution data  $W$  to each receiver; and  
23         a fifth step, in the apparatus of the receiver  $x$ , of calculating  
24    the encryption-decryption key  $K_A$  from the receiver private key  
25    information  $s_x$  distributed from the trusted center and the key  
26    distribution data  $W$  and the receiver registration key  $r_x$  received from  
27    the sender  $A$ , the encryption-decryption key  $K_A$  being to be used for  
28    secure broadcast communication performed by the sender  $A$ ;



29            wherein said receiver secret key  $s_x$ , the key distribution data  $W$ ,  
30    and the receiver registration key  $r_x$  are produced in such a relation that  
31    the encryption-decryption key  $K_A$  can be derived from said receiver  
32    secret key  $s_x$ , the key distribution data  $W$ , and the receiver registration  
33    key  $r_x$ , and other information opened to each receiver.

1    3.        The method of key distribution according to Claim 2, wherein:  
2            said second step is one in which, in the apparatus of the sender  
3    A, variable information  $r_A$  and  $r_A'$  for changing the encryption-  
4    decryption key are produced, and the encryption-decryption key  $K_A$  is  
5    calculated by a function of the variable information  $r_A$  and  $r_A'$  acting on  
6    the secret key  $g_A$ , the variable information  $r_A$  being for changing the  
7    encryption-decryption key periodically, and the variable information  $r_A'$   
8    being for changing the encryption-decryption key for every broadcast  
9    content; and  
10           said third step is one in which:  
11           in the apparatus of the trusted center, data  $W'$  is produced by a  
12    function of the sender secret key  $g_A$  and the sender registration key  $t_A$ ,  
13    and sent to the sender A, while data  $r_x'$  is produced by a function of the  
14    receiver secret key  $s_x$  of the receiver  $x$  and the sender registration key  $t_A$ ,  
15    and sent to the sender A; and  
16           in the apparatus of the sender A, the key distribution data  $W$  is  
17    produced by a function of the variable information  $r_A$  acting on the data  
18     $W'$ , and the receiver registration key  $r_x$  of the receiver  $x$  for the sender A  
19    is produced by a function of the variable information  $r_A'$  acting on the  
20    data  $r_x'$ .

1    4.        A method of key distribution for having an encryption-



2 decryption key of secure broadcast communication in common among a  
3 plurality of senders and a plurality of receivers in a communication  
4 system comprising an apparatus of a trusted center, apparatuses of said  
5 plurality of senders and apparatuses of said plurality of receivers,  
6 comprising:

7 a first step for distributing receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  to the  
8 receiver x, in which, in the apparatus of the trusted center,

9 
$$e_i \in Z \quad (1 \leq i \leq m)$$

10 are produced as a trusted center secret key;

11 
$$t_A \in Z$$

12 is produced as a sender registration key of a sender A;  $\sigma_x \in Sk_m$  and

13 
$$s_x(\sigma_x) \in Z$$

14 are produced (here, when  $\sigma, \sigma' \in Sk_m$  for  $S_{km}$ :

15 
$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \rightarrow B = \{1, 2, \Lambda, m\}, 0 < k < m \}$$

16 it is expressed by the following expression:

17 
$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$$

18 “ $\sim$ ” being an equivalence relation on  $S_{km}$ , to lead to the following  
19 expression:

20 
$$\tilde{S}_{km} = S_{km} / \sim$$

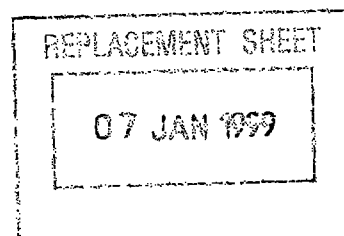
21 ), a second step, in which, in an apparatus of the sender A, are  
22 produced sender secret keys  $g_A$ ,  $L_A$ , and a finite Abelian group  $G_A$   
23 satisfying:

24 
$$g_A \in G_A$$
  
$$L_A = \text{ord}_{G_A}(g_A)$$

25 (here,

26 
$$\text{ord}_{G_A}(g)$$

27 means a least positive integer a which satisfies:



28  $g^a = 1 (\in G_A)$

29 ), and the sender secret key  $g_A$  is sent to the trusted center;

30 a third step, in which, in the apparatus of the trusted center,  
31 receiver registration data defined by the following expression:

32 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

33 is calculated from the trusted center secret key  $e_i$ , the sender  
34 registration key  $t_A$ , and the receiver secret key  $s_x(\sigma_x)$ ,  $\sigma_x$ ; and the  
35 receiver registration data  $s_x(\sigma_x, A)$  is sent to the sender A, while key  
36 distribution data defined as:

37 
$$y_{Ai} = g_A^{u_i} (\in G_A) \quad (1 \leq i \leq m)$$

38 is calculated from the  $g_A$  received from the sender A, the trusted center  
39 secret key  $e_i$ , and the sender registration key  $t_A$ ; and the key  
40 distribution data  $y_{Ai}$  is sent to the sender A;

41 a fourth step, in which, in the apparatus of the sender A,  
42 integers  $r, r'$  are produced; a receiver registration key  $r_x(\sigma_x, A)$   
43 satisfying:

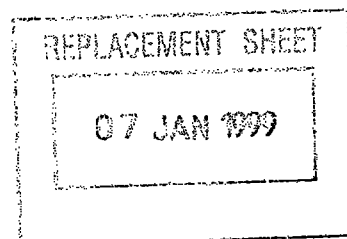
44 
$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

45 is calculated from the receiver registration data  $s_x(\sigma_x, A)$  received from  
46 the trusted center, the sender secret key  $L_A$ , and the integer  $r'$ ; and the  
47 receiver registration key  $r_x(\sigma_x, A)$  is sent to the receiver x; while key  
48 distribution data defined as:

49 
$$z_{Ai} = y_{Ai}^r (\in G_A) \quad (1 \leq i \leq m)$$

50 is calculated from the key distribution data  $y_{Ai}$  received from the  
51 trusted center and the integer  $r$ ; and the key distribution data  $z_{Ai}$  is  
52 broadcasted to each receiver; and

53 a fifth step, in which, in an apparatus of the receiver x, an  
54 encryption-decryption key  $K_A$  is calculated by:



$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} (\in G_A)$$

from the receiver registration key  $r_x(\sigma_x, A)$  received from the sender, the key distribution data  $z_{Ai}$ , the receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  distributed from the trusted center; the encryption-decryption key  $K_A$  being generated by the sender A employing:

$$K_A = g_A^{K'} (\in G_A)$$

to be used for broadcast communication.

5. A method of key distribution having an encryption-decryption key of secure broadcast communication in common among a plurality of senders and a plurality of receivers in a communication system comprising an apparatus of a trusted center, apparatuses of said plurality of senders and apparatuses of said plurality of receivers, comprising:

a first step, in which, in the apparatus of the trusted center,

$$e_i \in Z \quad (1 \leq i \leq m)$$

is produced as a trusted center secret key;

$$t_A \in Z$$

is produced as a sender registration key of a sender A;  $\sigma_x \in S_{km}$  and

$$s_x(\sigma_x) \in Z$$

are produced as receiver secret keys of a receiver x;

(here, when  $\sigma, \sigma' \in S_{km}$  for a set defined as:

$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m \}$$

it is expressed by the following expression:

$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$$

and, in that case, " $\sim$ " becomes an equivalence relation on  $S_{km}$ , which



\* C L H S \*

REPLACEMENT SHEET

07 JAN 1999

19 leads to the following expression:

20 
$$\bar{S}_{km} = S_{km} / \sim$$

21 ); and the receiver secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$  are sent to the receiver x;

22 a second step, in which, in an apparatus of the sender A,

$P_A, Q_A$ : prime numbers

23 
$$L_A = \text{lcm}(\text{ord}_{P_A}(g_A), \text{ord}_{Q_A}(g_A))$$

$$g_A \in Z, \quad 0 < g_A < N_A$$

$$r, r' \in Z, \quad 0 < r, r' < L_A$$

24 are produced as sender secret keys;

25 
$$N_A (= P_A Q_A)$$

26 is produced as a sender public key; and the sender secret key  $g_A$  is sent  
27 to the trusted center;

28 a fourth step, in which, in the apparatus of the trusted center,  
29 receiver registration data defined as:

30 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

31 is calculated from the trusted center secret key  $e_i$ , the sender  
32 registration key  $t_A$ , and the receiver secret keys  $s_x(\sigma_x)$ ,  $\sigma_x$ ; and the  
33 receiver registration data  $s_x(\sigma_x, A)$  is sent to the sender A; while key  
34 distribution data defined as:

35 
$$y_{Ai} = g_A^{u_i} \bmod N_A \quad (1 \leq i \leq m)$$

36 is calculated from  $g_A$  received from the sender A, the trusted center  
37 secret key  $e_i$ , and the sender registration key  $t_A$ ; and the key  
38 distribution data  $y_{Ai}$  is sent to the sender A;

39 a fifth step, in which, in the apparatus of the sender A, integers  
40  $r, r'$  are produced; and a receiver registration key  $r_x(\sigma_x, A)$  satisfying:

41 
$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

42 is calculated from the receiver registration data  $s_x(\sigma_x, A)$  received from  
43 the trusted center, the sender secret key  $L_A$ , and the integer  $r'$ ; and the



REPLACEMENT SHEET

07 JAN 1999

44 receiver registration key  $r_x(\sigma_x, A)$  is sent to the receiver x; while key  
45 distribution data defined as:

46 
$$z_{Ai} = y_{Ai}^r \bmod N_A \quad (1 \leq i \leq m)$$

47 is calculated from the key distribution data  $y_{Ai}$  received from the  
48 trusted center and the integer r; and the key distribution data  $z_{Ai}$  is  
49 broadcasted to each receiver; and

50 a sixth step, in which, in an apparatus of the receiver x, an  
51 encryption-decryption key  $K_A$  is calculated by:

52 
$$K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \bmod N_A$$

53 from the receiver registration key  $r_x(\sigma_x, A)$  received from the sender, the  
54 key distribution data  $z_{Ai}$ , and the receiver secret keys  $\sigma_x, s_x(\sigma_x)$   
55 distributed from the trusted center; the encryption-decryption key  
56 being generated by the sender A using:

57 
$$K_A = g_A^{r'} \bmod N_A$$

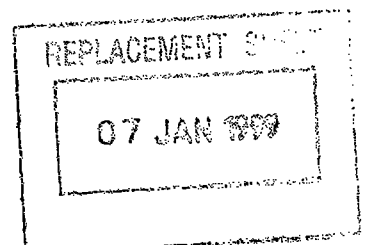
58 to be used for broadcast communication.

1 6. The method of key distribution according to Claim 5, further  
2 comprising:

3 a seventh step, in which, in said apparatus of the sender A,  
4 said secret key  $L_A$  is generated and sent to the trusted center before the  
5 apparatus of the trusted center performs the first step of generating the  
6 trusted center secret key  $e_i$ , the sender identification  $t_A$ , and the  
7 receiver secret key  $s_x(\sigma_x)$ ;

8 wherein:

9 in said first step, in the apparatus of the trusted center, the  
10 trusted center information  $e_i$ , the sender identification  $t_A$ , and the  
11 receiver secret key  $s_x(\sigma_x)$  are produced from the sender secret key  $L_A$



12 received from the sender so as to satisfy:

$$\begin{aligned} & e_i \in Z, \quad 0 < e_i < L_A, \quad (1 \leq i \leq m) \\ & t_A \in Z, \quad 0 < t_A < L_A \\ & s_x(\sigma_x) \in Z, \quad 0 < s_{x, \sigma_x} < L_A, \end{aligned}$$

14 and,

15 in said fourth step, in the apparatus of the trusted center, the  
16 receiver registration data  $s_x(\sigma_x, A)$  is calculated from the sender secret  
17 key  $L_A$ , the trusted center secret key  $e_i$ , the sender registration key  $t_A$ ,  
18 and the receiver secret key  $s_x(\sigma_x)$  so as to satisfy:

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \mod L_A.$$

1 7. The method of key distribution according to Claim 5, further  
2 comprising:

3 an eighth step, in which, in the apparatus of the sender A, a  
4 value of the integer  $r$  is changed; and a value of the encryption-  
5 decryption key  $K_A$  is recalculated in accordance with the changed  
6 integer  $r$ ; while the key distribution data  $z_{Ai}$  is recalculated in  
7 accordance with the changed integer  $r$  and broadcasted to each receiver  
8 again; and

9 a ninth step, in which, in the apparatus of the receiver  $x$ , the  
10 encryption-decryption key  $K_A$  is recalculated in accordance with the key  
11 distribution data  $z_{Ai}$  broadcasted again.

1 8. The method of key distribution according to Claim 5, wherein:  
2 in said fifth step, in the apparatus of the sender A, a value of  
3 the integer  $r'$  is generated in accordance with each piece of information  
4 or each kind of information to be encrypted and broadcasted; and



REPLACEMENT SHEET

07 JAN 1999

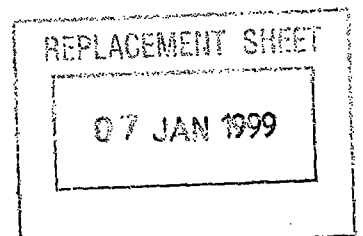
5 encryption-decryption keys  $K_A$  are calculated for respective information  
6 or respective kinds of information in accordance with respective values  
7 of the integer  $r'$  generated in accordance with the information or kinds  
8 of information; while pieces of receiver registration key  $r_x(\sigma_x, A)$  are  
9 calculated in accordance with respective integers  $r'$  generated in  
10 accordance with respective said information or kinds of information on  
11 which the receiver  $x$  is allowed to perform decryption, and the said  
12 pieces of receiver registration key  $r_x(\sigma_x, A)$  are sent to the receiver  $x$ ; and  
13 in said sixth step, in the apparatus of the receiver  $x$ ,  
14 encryption-decryption key  $K_A$  for said information or kinds of  
15 information on which said receiver  $x$  is allowed to perform decryption  
16 are calculated in accordance with respective pieces of receiver  
17 registration key  $r_x(s_x, A)$  received.

1 9. The method of key distribution according to Claim 5, further  
2 comprising:

3 a tenth step in which, in the apparatuses of the sender  $A$  and  
4 the receiver  $x$ , possession of the receiver secret key  $s_x(\sigma_x)$  by said  
5 receiver  $x$  is authenticated according to a system by which the receiver  
6 secret key  $s_x(\sigma_x)$  is made secret from the sender  $A$ , before the fifth step  
7 for sending the receiver registration key  $r_x(\sigma_x, A)$  from the sender  $A$  to  
8 the receiver  $x$ .

1 10. The method of key distribution according to Claim 5, further  
2 comprising:

3 an eleventh step in which, in the apparatus of the sender  $A$ , a  
4 fee for information or a kind of information, which is encrypted with the  
5 encryption-decryption key  $K_A$  corresponding to the receiver registration



6 key  $r_x(\sigma_x, A)$  and broadcasted, is calculated as accounting information  
7 for the receiver A, said eleventh step being performed when the fifth  
8 step is performed for sending the receiver registration key  $r_x(\sigma_x, A)$  from  
9 the sender A to the receiver x.

1 11. A method of key distribution having an encryption-decryption  
2 key of secure broadcast communication in common among a plurality of  
3 senders and a plurality of receivers in a communication system  
4 comprising apparatuses of said plurality of senders and apparatuses of  
5 said plurality of receivers, comprising:

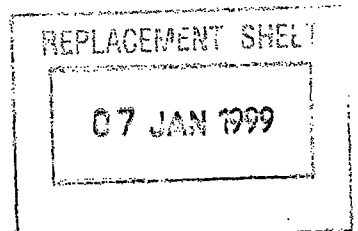
6 a first step, in which, in an apparatus of a trusted center  
7 provided separately from said apparatuses of senders and said receivers,  
8 a secret key  $K_0$  is generated and distributed to each sender and each  
9 receiver;

10 a second step, in which, in an apparatus of a sender A, a sender  
11 registration key BIDA is generated and sent to the receivers, while a  
12 common key  $K_A' = F(K_0, BIDA)$  is calculated from the secret key  $K_0$   
13 distributed from the trusted center and the sender registration key  
14 BIDA using a given one-way function F;

15 a third step, in which, in the apparatuses of the receivers, the  
16 common key  $K_A'$  is calculated from the secret key  $K_0$  distributed from  
17 the trusted center and the sender registration key BIDA received from  
18 the sender A using said one-way function F;

19 a fourth step, in which, in the apparatus of the sender A, an  
20 integer  $r$  is produced and sent to the receivers; and

21 a fifth step, in which, in the apparatuses of the receivers, an  
22 encryption-decryption key  $K_A$  is calculated by  $K_A = F'(r, K_A')$  from the  
23 integer  $r$  received from the sender A and the common key  $K_A'$  using a



24 given function  $F'$ , the encryption-decryption key  $K_A$  being calculated by  
25 the sender A using  $K_A = F'(r, K_A')$ .

1 12. A method of key distribution having an encryption-decryption  
2 key of secure broadcast communication in common among a plurality of  
3 senders and a plurality of receivers in a communication system  
4 comprising apparatuses of said plurality of senders and apparatuses of  
5 said plurality of receivers, comprising:

6 a first step, in which, in an apparatus of a trusted center  
7 provided separately from said apparatuses of senders and said receivers,  
8 a personal key  $s_x$  for a receiver  $x$  is produced, and distributed to the  
9 sender A and the receiver  $x$ ;

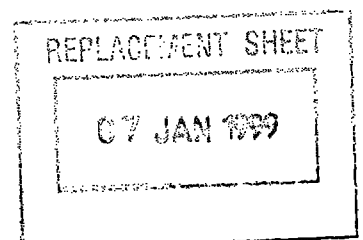
10 a second step, in which, in an apparatus of the sender A, a  
11 common key  $K_A$  is produced, and said common key  $K_A$  is owned in  
12 common with the receiver  $x$  by cipher communication using the personal  
13 key  $s_x$  for the receiver  $x$ , which has been distributed from the trusted  
14 center;

15 a third step, in which, in the apparatus of the sender A,  
16 information  $r$  is produced and sent to the receiver  $x$ ; and

17 a fourth step, in which, in each of the apparatuses of the  
18 receiver  $x$  and the sender A, an encryption-decryption key  $DK$  is  
19 calculated in accordance with an expression,  $DK = F(r, K_A)$ .

1 13. The method of key distribution according to Claim 12, further  
2 comprising:

3 a fifth step, in which, in the apparatus of the sender A, the  
4 common key  $K_A$  is changed, and the changed common key  $K_A$  is owned in  
5 common with the receiver  $x$  by cipher communication using the personal



6 key  $s_x$  for the receiver  $x$ ; and

7 a sixth step, in which, in each of the apparatuses of the sender  
8 A and the receiver  $x$ , the encryption-decryption key  $DK$  is recalculated  
9 by  $DK=F(r, K_A)$  in accordance with the changed common key  $K_A$ .

1 14. The method of key distribution according to Claim 12, further  
2 comprising:

3 a seventh step, in which, in the apparatus of the sender A, the  
4 information  $r$  is changed, and the changed information  $r$  is informed to  
5 the receivers; and

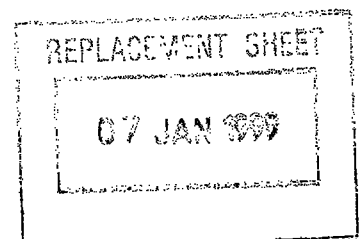
6 an eighth step, in which, in each of the apparatuses of the  
7 sender A and the receivers, the encryption-decryption key  $DK$  is  
8 recalculated by  $DK=F(r, K_A)$  in accordance with the changed  
9 information  $r$ .

1 15. The method of key distribution according to Claim 12, further  
2 comprising:

3 a ninth step, in which, in the apparatus of the sender A, key  
4 information for the receiver  $x$  to calculate said encryption-decryption  
5 key  $DK$  is sent through a given communication channel which is  
6 different from a communication channel for broadcasting information  
7 encrypted with the encryption-decryption key  $DK$ .

1 16. A key distribution system for having an encryption-decryption  
2 key used for secure broadcast communication in common among senders  
3 and receivers, wherein:

4 said system comprises a trusted center apparatus, a plurality  
5 of sender apparatuses, and a plurality of receiver apparatuses;



6 said trusted center apparatus comprises:

7 means for producing:

8 
$$e_i \in Z \quad (1 \leq i \leq m)$$

9 as a trusted center secret key;

10 
$$t_A \in Z$$

11 as a sender registration key of a sender A; and  $\sigma_x \in S_{km}$  and

12 
$$s_x(\sigma_x) \in Z$$

13 (here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$  defined as:

14 
$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \\ \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m \}$$

15 it is expressed by the following expression:

16 
$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$$

17 and, in that case, " $\sim$ " becomes an equivalence relation on  $S_{km}$ , leading  
18 to the following definition:

19 
$$\tilde{S}_{km} = S_{km} / \sim$$

20 ); and for distributing the receiver secret keys  $\sigma_x, s_x(\sigma_x)$  to said receiver  
21 apparatus used by the receiver x;

22 means for calculating receiver registration data defined by:

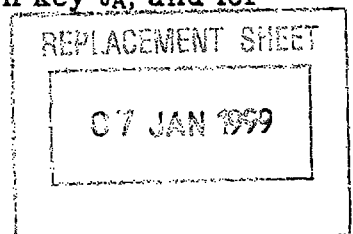
23 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

24 from the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and  
25 the receiver secret keys  $s_x(\sigma_x), \sigma_x$ , and for sending the receiver  
26 registration data  $s_x(\sigma_x, A)$  to said sender apparatus used by the sender  
27 A; and

28 means for calculating key distribution data defined by:

29 
$$y_{Ai} = g_A^{u_i} \quad (\in G_A) \quad (1 \leq i \leq m)$$

30 from  $g_A$  received from said sender apparatus used by the sender A, the  
31 trusted center secret key  $e_i$ , and the sender registration key  $t_A$ , and for



32 sending the key distribution data  $y_{Ai}$  to said sender apparatus used by  
33 the sender A;

34 said sender apparatus used by the sender A comprises:

35 means for producing sender secret keys  $g_A$ ,  $L_A$ , and a finite  
36 Abelian group  $G_A$ , satisfying:

37 
$$g_A \in G_A$$
$$L_A = \text{ord}_{G_A}(g_A)$$

38 (here,

39 
$$\text{ord}_{G_A}(g)$$

40 means a least positive integer  $a$  satisfying:

41 
$$g^a = 1 (\in G_A)$$

42 ), and for sending the sender secret key  $g_A$  to said trusted center  
43 apparatus;

44 means for producing integers  $r$ ,  $r'$ , calculating receiver  
45 registration key  $r_x(\sigma_x, A)$  satisfying:

46 
$$r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

47 from the receiver registration data  $s_x(\sigma_x, A)$  received from said trusted  
48 center apparatus, the sender secret key  $L_A$ , and the integer  $r'$ ; and for  
49 sending the receiver registration key  $r_x(\sigma_x, A)$  to said receiver apparatus  
50 of the receiver  $x$ ; and

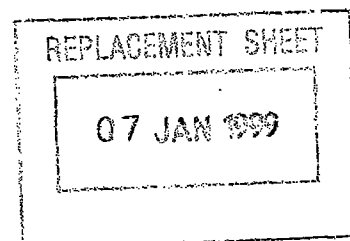
51 means for calculating key distribution data defined as:

52 
$$z_{Ai} = y_{Ai}' (\in G_A) \quad (1 \leq i \leq m)$$

53 from the key distribution data  $y_{Ai}$  received from said trusted center  
54 apparatus, and the integer  $r$ ; and for broadcasting the key distribution  
55 data  $z_{Ai}$  to said plurality of receiver apparatuses; and

56 said receiver apparatus of the receiver  $x$  comprises:

57 means for calculating encryption-decryption key  $K_A$  by the  
58 following expression:



$$K_A = \left( \prod_{i=1}^k z_{A\sigma_i(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} (\in G_A),$$

said encryption-decryption key  $K_A$  being generated by said sender apparatus of the sender A by the following expression:

$$K_A = g_A^{r'} (\in G_A).$$

17. A trusted center apparatus which supports distribution of an encryption-decryption key from a sender apparatus to a receiver apparatus, having said encryption-decryption key used in secure broadcast communication in common among senders and receivers, comprising:

means for producing:

$$e_i \in Z \quad (1 \leq i \leq m)$$

as a trusted center secret key;

$$t_A \in Z$$

as a sender registration key of a sender A; and, as receiver secret keys of a receiver x,  $\sigma_x \in S_{km}$  and:

$$s_x(\sigma_x) \in Z$$

(here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$ :

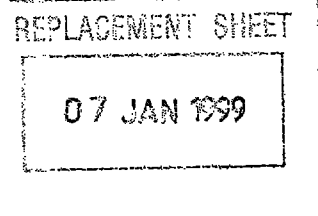
$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m \}$$

it is expressed by the following expression:

$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A),$$

with " $\sim$ " being an equivalence relation on  $S_{km}$ , which lead to an expression:

$$\tilde{S}_{km} = S_{km} / \sim,$$



22 and for distributing the receiver secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$  to said receiver  
23 apparatus used by the receiver x;

24 means for calculating receiver registration data defined by:

25 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

26 from the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and  
27 the receiver secret keys  $s_x(\sigma_x)$ ,  $\sigma_x$ ; and for sending the receiver  
28 registration data  $s_x(\sigma_x, A)$  to said sender apparatus used by the sender  
29 A; and

30 means for calculating key distribution data defined as:

31 
$$y_{Ai} = g_A^{u_i} (\in G_A) \quad (1 \leq i \leq m)$$

32 from  $g_A$  received from said sender apparatus of the sender A, the trusted  
33 center secret key  $e_i$ , and the sender registration key  $t_A$ ; and for sending  
34 the key distribution data  $y_{Ai}$  to said sender apparatus of the sender A.

1 18. A sender apparatus which distributes an encryption-decryption  
2 key to a receiver apparatus being supported by a trusted center  
3 apparatus, having said encryption-decryption key used in secure  
4 broadcast communication in common among senders and receivers,  
5 comprising:

6 means for producing sender secret key  $g_A$ ,  $L_A$ , and a finite  
7 Abelian group  $G_A$  satisfying:

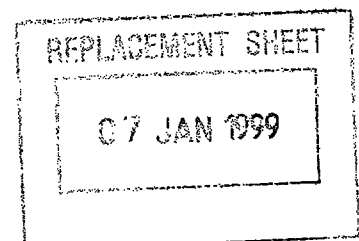
8 
$$g_A \in G_A$$
  
$$L_A = \text{ord}_{G_A}(g_A)$$

9 (here,

10 
$$\text{ord}_{G_A}(g)$$

11 means a least positive integer a satisfying:

12 
$$g^a = 1 (\in G_A)$$



13 ); and for sending the sender secret key  $g_A$  to said trusted center  
14 apparatus;

15 means for producing integers  $r, r'$ ; calculating a receiver  
16 registration key  $r_x(\sigma_x, A)$  satisfying:

$$17 \quad r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

18 from the receiver registration data  $s_x(\sigma_x, A)$ , the sender secret key  $L_A$ ,  
19 and the integer  $r$ , and for sending the receiver registration key  $r_x(\sigma_x, A)$   
20 to said receiver apparatus used by the receiver  $x$ ;

21 means for calculating key distribution data defined as:

$$22 \quad z_{Ai} = y_{Ai}^r \quad (\in G_A) \quad (1 \leq i \leq m)$$

23 from key distribution data  $y_{Ai}$  received from said trusted center  
24 apparatus, and the integer  $r$ ; and for broadcasting the key distribution  
25 data  $z_{Ai}$  to a plurality of said receiver apparatuses as objects of  
26 broadcast communication; and

27 means for calculating an encryption-decryption key  $K_A$  used for  
28 broadcast communication, in accordance with:

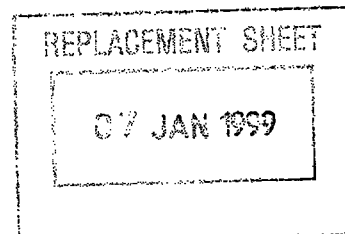
$$29 \quad K_A = g_A^{r'} \quad (\in G_A).$$

1 19. A receiver apparatus which receives an encryption-decryption  
2 key from a sender apparatus being supported by a trusted center  
3 apparatus, having said encryption-decryption key used in secure  
4 broadcast communication in common among senders and receivers,  
5 comprising:

6 means for calculating the encryption-decryption key  $K_A$  used  
7 for the broadcast communication by an expression:

$$8 \quad K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A)s_x(\sigma_x, A)} \quad (\in G_A)$$

9 from a receiver registration data  $r_x(\sigma_x, A)$  and a key distribution data  $z_{Ai}$



10 received from the sender apparatus used by a sender A, and receiver  
11 secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$  received from the trusted center apparatus, the  
12 encryption-decryption key  $K_A$  being generated by said sender apparatus  
13 of the sender A using an expression:

14 
$$K_A = g_A^{r'} (\in G_A).$$

1 20. A receiver apparatus which receives an encryption-decryption  
2 key from a sender apparatus being supported by a trusted center  
3 apparatus, having said encryption-decryption key used in secure  
4 broadcast communication in common among senders and receivers,  
5 comprising:

6 a main apparatus and an auxiliary apparatus;

7 wherein:

8 said auxiliary apparatus comprises:

9 means for connection with said trusted center apparatus;

10 storing means for taking in and storing receiver secret keys

11  $s_x(\sigma_x)$ ,  $\sigma_x$  produced by said trusted center apparatus;

12 means for connection with said main apparatus, and

13 means for taking in key distribution data  $z_{Ai}$  received by said

14 main apparatus from said sender apparatus used by a sender A;

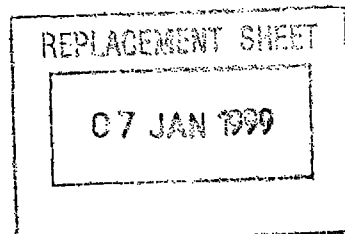
15 calculating:

16 
$$\xi_x(\sigma_x, A) = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \bmod N_A$$

17 from the key distribution data  $z_{Ai}$  and the receiver secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$   
18 stored in said storing means; and for outputting a result  $\xi_x(\sigma_x, A)$  of the  
19 calculation to said main apparatus; and

20 said main apparatus comprises:

21 means for outputting the key distribution data  $z_{Ai}$  received



22 from said sender apparatus of the sender A to said auxiliary apparatus;  
23 and

24 means for calculating encryption-decryption key  $K_A$  used in  
25 broadcast communication, using an expression:

26 
$$K_A = \xi_x(\sigma_x, A)^{r_x(\sigma_x, A)} \bmod N_A$$

27 from a receiver registration key  $r_x(\sigma_x, A)$  received from the sender  
28 apparatus of the sender A, and  $\xi_x(\sigma_x, A)$  output from the auxiliary  
29 apparatus, the encryption-decryption key  $K_A$  being generated by said  
30 sender apparatus of the sender A, using an expression:

31 
$$K_A = g_A^{r'} (\in G_A).$$

1 21. An auxiliary apparatus used being connected with a trusted  
2 center apparatus and a plurality of receiver apparatuses, in a  
3 communication system comprising a plurality of sender apparatuses  
4 which perform broadcast communication, said plurality of receiver  
5 apparatuses, and said trusted center apparatus which supports  
6 distribution of an encryption-decryption key of a sender apparatus used  
7 in secure broadcast communication to a receiver apparatus; said  
8 auxiliary apparatus comprising:

9 means for connection with said trusted center apparatus;

10 storing means for taking in and storing receiver secret keys  
11  $s_x(\sigma_x)$ ,  $\sigma_x$  for a receiver x, produced by said trusted center apparatus;

12 means for connection with said receiver apparatus used by the  
13 receiver x; and

14 means for taking in key distribution data  $z_{Ai}$  received by said  
15 receiver apparatus used by the receiver x from said sender apparatus  
16 used by the sender A; for calculating:



\* C L M S \*

REPLACEMENT SHEET

07 JAN 1999

$$\xi_x(\sigma_x, A) = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \bmod N_A$$

18 from the key distribution data  $z_{Ai}$  and the receiver secret keys  $\sigma_x, s_x(\sigma_x)$   
 19 stored in said storing means; and for outputting a calculation result  
 20  $\xi_x(\sigma_x, A)$  to said receiver apparatus of the receiver x.

1 22. A storing medium which stores a program for making an  
 2 information processing apparatus execute a process for supporting  
 3 distribution of an encryption-decryption key from sender apparatuses to  
 4 receiver apparatuses, having said encryption-decryption key used in  
 5 secure broadcast communication in common among senders and  
 6 receivers, wherein:

7 said program makes the information processing apparatus  
 8 execute:

9 a step of producing:

$$e_i \in Z \quad (1 \leq i \leq m)$$

11 as a trusted center secret key,

$$t_A \in Z$$

13 as a sender registration key of a sender A, and, as receiver secret keys of  
 14 a receiver x,  $\sigma_x \in S_{km}$  and:

$$s_x(\sigma_x) \in Z$$

16 (here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$  defined as:

$$S_{km} = \{ \sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\} \\ \rightarrow B = \{1, 2, \Lambda, m\}, \quad 0 < k < m \}$$

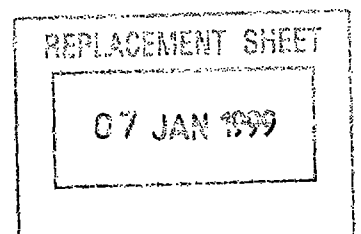
18 it is expressed by the following expression:

$$\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A),$$

20 with " $\sim$ " becoming an equivalence relation on  $S_{km}$ , leading to an  
 21 expression:



\* C L H S \*



22  $\tilde{S}_{km} = S_{km} / \sim$

23 ); and of distributing the receiver secret keys  $\sigma_x$ ,  $s_x(\sigma_x)$  to said receiver  
24 apparatus used by the receiver x;

25 a step of calculating receiver registration data defined as:

26 
$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

27 from the trusted center secret key  $e_i$ , the sender registration key  $t_A$ , and  
28 the receiver secret keys  $s_x(\sigma_x)$ ,  $\sigma_x$ ; and of sending the receiver  
29 registration data  $s_x(\sigma_x, A)$  to said sender apparatus used by the sender  
30 A; and

31 a step of calculating key distribution data  $y_{Ai}$  defined as:

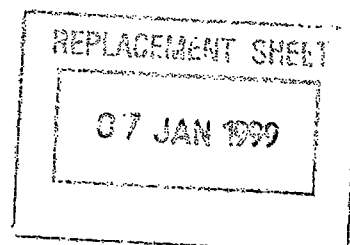
32 
$$y_{Ai} = g_A^{u_i} (\in G_A) \quad (1 \leq i \leq m)$$

33 from  $g_A$  received from said sender apparatus used by the sender A, the  
34 trusted center secret key  $e_i$ , and the sender registration key  $t_A$ ; and of  
35 sending the key distribution data  $y_{Ai}$  to said sender apparatus used by  
36 the sender A.

1 23. A storing medium which stores a program for making an  
2 information processing apparatus execute a process in sender  
3 apparatuses which distribute an encryption-decryption key to receiver  
4 apparatuses, being supported by a trusted center apparatus, having  
5 said encryption-decryption key used in secure broadcast communication  
6 in common among senders and receivers, wherein:

7 said program makes the information processing apparatus  
8 execute:

9 a step of producing sender secret keys  $g_A$ ,  $L_A$ , and a finite  
10 Abelian group  $G_A$  satisfying:



11  $g_A \in G_A$   
12  $L_A = \text{ord}_{G_A}(g_A)$

13 (here,

14  $\text{ord}_{G_A}(g)$

15 means a least positive integer a satisfying:

16  $g^a = 1 (\in G_A)$

17 ), and of sending the sender secret key  $g_A$  to said trusted center  
18 apparatus;

19 a step of producing integers  $r, r'$ ; calculating receiver  
20 registration key  $r_x(\sigma_x, A)$  satisfying:

21  $r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$

22 and sending the receiver registration key  $r_x(\sigma_x, A)$  to said receiver  
23 apparatus used by the receiver  $x$ ;

24 a step of calculating key distribution data defined as:

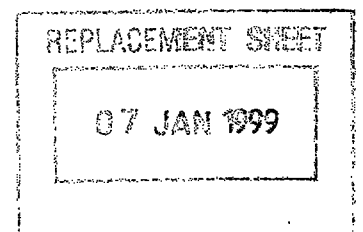
25  $z_{Ai} = y_{Ai}^{r'} (\in G_A) \quad (1 \leq i \leq m)$

26 from key distribution data  $y_{Ai}$  received from said key administration  
27 apparatus, and the integer  $r$ ; and broadcasting the key distribution data  
28  $z_{Ai}$  to said plurality of receiver apparatuses as objects of broadcast  
29 communication; and

30 a step of calculating an encryption-decryption key  $K_A$  used in  
31 broadcast communication, using:

$K_A = g_A^{rr'} (\in G_A).$

- 1 24. A storing medium which stores a program for making an  
2 information processing apparatus execute a process in receiver  
3 apparatuses which receive an encryption-decryption key distributed  
4 from sender apparatuses, being supported by a trusted center apparatus,  
5 having said encryption-decryption key used in secure broadcast



6 communication in common among senders and receivers, wherein:

7 said program makes the information processing apparatus  
8 execute:

9 a step of calculating an encryption-decryption key  $K_A$  used for  
10 broadcast communication, using an expression:

$$11 \quad K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} (\in G_A)$$

12 from a receiver registration key  $r_x(\sigma_x, A)$  received from said sender  
13 apparatus used by a sender A, key distribution data  $z_{Ai}$ , and a receiver  
14 secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  distributed from the trusted center, the  
15 encryption-decryption key  $K_A$  being generated by said sender apparatus  
16 used by the sender A, using:

$$17 \quad K_A = g_A^{r'} (\in G_A).$$

1 25. A key distribution system for having an encryption-decryption  
2 key used for secure broadcast communication in common among senders  
3 and receivers, wherein:

4 said system comprises a trusted center apparatus, a plurality  
5 of sender apparatuses, and a plurality of receiver apparatuses;

6 said trusted center apparatus comprises:

7 means for producing:

$$8 \quad e_i \in Z \quad (1 \leq i \leq m)$$

9 as a trusted center secret key,

$$10 \quad t_A \in Z$$

11 as a sender registration key of a sender A, and, as receiver secret keys of  
12 a receiver x,  $\sigma_x \in S_{km}$  and

$$13 \quad s_x(\sigma_x) \in Z$$

14 (here, when  $\sigma, \sigma' \in S_{km}$  for a set  $S_{km}$  defined as:



\* C L M S \*

REPLACEMENT SHEET

07 JAN 1999

15  $S_{km} = \{\sigma \mid \text{one to one map } \sigma : A = \{1, 2, \Lambda, k\}$   
 $\rightarrow B = \{1, 2, \Lambda, m\}, 0 < k < m\}$

16 it is expressed by:

17  $\sigma \sim \sigma' \stackrel{\text{def}}{\Leftrightarrow} \sigma(A) = \sigma'(A)$

18 with " $\sim$ " becoming an equivalence relation on  $S_{km}$ , leading to the  
 19 following expression:

20  $\tilde{S}_{km} = S_{km} / \sim$

21 ), and of distributing the receiver secret key  $\sigma_x$ ,  $s_x(\sigma_x)$  to said receiver  
 22 apparatus used by a receiver x;

23 means for calculating:

24  $s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$

25 from the key distributor secret key  $e_i$ , the sender registration key  $t_A$ ,  
 26 and the receiver secret keys  $s_x(\sigma_x)$ ,  $\sigma_x$ , and sending the receiver  
 27 registration data  $s_x(\sigma_x, A)$  to said sender apparatus used by the sender  
 28 A; and

29 means for calculating key distribution data  $y_{Ai}$ :

30  $y_{Ai} = g_A^{u_i} \bmod N_A \quad (1 \leq i \leq m)$

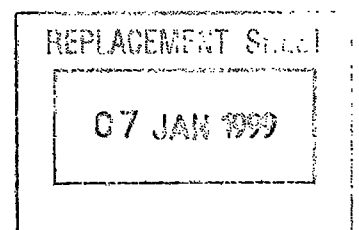
31 from  $g_A$  received from the sender A, the trusted center secret key  $e_i$ , and  
 32 the sender registration key  $t_A$ , and sending the key distribution data  $y_{Ai}$   
 33 to said sender apparatus used by the sender A;

34 said sender apparatus used by the sender A comprises:

35 means for producing:

36  $P_A, Q_A$ : prime numbers  
 $L_A = \text{lcm}(\text{ord}_{P_A}(g_A), \text{ord}_{Q_A}(g_A))$   
 $g_A \in \mathbb{Z}, 0 < g_A < N_A$   
 $r, r' \in \mathbb{Z}, 0 < r, r' < L_A$

37 as sender secret keys of the sender A,



38  $N_A (= P_A Q_A)$

39 as a sender public key of the sender A, and sending the sender secret  
40 key  $g_A$  to said trusted center apparatus;

41 means for generating  $r, r'$ , calculating receiver registration key  
42  $r_x(\sigma_x, A)$  satisfying:

$$43 \quad r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

44 from receiver registration data  $s_x(\sigma_x, A)$  received from the trusted center,  
45 the sender secret key  $L_A$ , and the integer  $r'$ , and sending the receiver  
46 registration key  $r_x(\sigma_x, A)$  to said receiver apparatus used by the receiver  
47 x; and

48 means for calculating key distribution data defined as:

$$49 \quad z_{Ai} = y_{Ai}^{r'} \pmod{N_A} \quad (1 \leq i \leq m)$$

50 from key distribution data  $y_{Ai}$  received from the trusted center, and the  
51 integer  $r$ , and broadcasting the key distribution data  $z_{Ai}$  to said  
52 plurality of receiver apparatuses as objects of broadcast  
53 communication;

54 and,

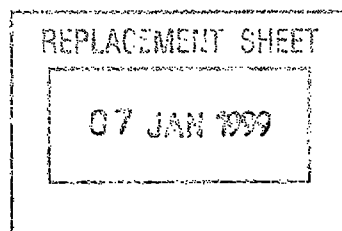
55 said receiver apparatus used by the receiver x comprise:

56 means for calculating an encryption-decryption key  $K_A$  for  
57 broadcast communication, using:

$$58 \quad K_A = \left( \prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \pmod{N_A}$$

59 from the receiver registration key  $r_x(\sigma_x, A)$  received from said sender  
60 apparatus used by the sender A, the key distribution data  $z_{Ai}$ , and the  
61 receiver secret keys  $\sigma_x, s_x(\sigma_x)$  distributed from the trusted center, said  
62 encryption-decryption key  $K_A$  being generated by said sender apparatus  
63 used by the sender A, using:

$$64 \quad K_A = g_A^{r'} \pmod{N_A}.$$



**METHOD AND SYSTEM FOR DISTRIBUTING ENCRYPTION AND  
DECRYPTION KEYS IN  
SECURE BROADCAST COMMUNICATION**

65

**Abstract of the Disclosure**

It is made possible to obtain a common key owned in common with a plurality of senders, using only one receiver secret key. A trusted center produces the receiver secret key of a receiver, so as to correspond to a subset consisting of two or more elements from a  
70 suitable finite set  $Z$ , and distributes it the receiver. Further, the trusted center produces identification information  $t_A$  for a sender. The sender produces an encryption-decryption key  $K_A$  from his own sender secret key. Keeping the receiver secret key and the identification information  $t_A$  secret from the sender, the trusted center cooperates  
75 with the sender to produce data related to each element of the finite set  $Z$  and the sender secret key, and data related to a subset corresponding to the receiver secret key and related to the sender secret key, and broadcasts these data. The receiver  $x$  calculates the encryption-decryption key  $K_A$  from the received data and his own receiver secret  
80 key.

**Figure 1**

