JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 15, 653-667 (1999)

Authorization-based Group-oriented Secure Broadcasting System

TZONG-CHEN WU AND YUH-SHIHNG CHANG
Department of Information Management
National Taiwan University of Science and Technology
Taipei, Taiwan 106, R.O.C.

This paper presents an authorization-based group-oriented secure broadcasting system based on the ID-based system proposed by Tsujii and Itoh. In the proposed system, any broadcasting secret in ciphertext form is addressed to "group" instead of "individual". First of all, the broadcaster defines the message authorization strategy among the individuals in the destination group by considering the characteristics or restrictions of the secret, such as timeliness, integrity, or importance etc. Afterwards, the broadcaster broadcasts the secret in ciphertext form to the destination group such that the individuals in the destination group only can recover the secret by means of authentication, following a predefined message authorization strategy. In general, the broadcaster can define the message authorization strategy for a secure broadcast as one of the following: (1) restricted 1-out-of-n, so that only the specified individual in the destination group can recover it; (2) unrestricted 1-out-of-n, so that any individual in the destination group can recover it; (3) n-out-of-n, so that all individuals in the destination group should collaborate together to recover it; (4) restricted t-out-of-n, so that only the specified t individuals in the destination group should collaborate together to recover it; and (5) unrestricted t-out-of-n, so that any t individuals in the destination group can collaborate together to recover it. The security of the proposed system is based on the difficulty of computing discrete logarithms over GF(p). Also, some possible conspiracy attacks on the proposed system are analyzed.

Keywords: secure broadcasting, authorization-based, group-oriented, ID-based system, authentication, discrete logarithms

1. INTRODUCTION

Due to the prevalence of computer and communication networks, cryptographic techniques, such as DES [5] and RSA [17], have been widely applied to network systems to meet the requirements of privacy and secrecy. There are two available approaches for network communications: point-to-point and point-to-multipoint. The point-to-multipoint approach is also referred to "broadcast" [22]. One useful property of a broadcast channel is that a single transaction from the broadcaster can be received simultaneously by several recipients over communication links; it hence requires less interaction time as compared to the point-to-point approach [13]. A broadcasting cryptoscheme allows authorized or legal recipients to recover broadcasting secrets whereas unauthorized or illegal recipients obtain no useful knowledge. Many application systems (for instance, video text system, electronic mail and electronic conferencing) use broadcasting cryptoschemes to achieve both efficiency and secrecy [6, 15].

Received October 3, 1996; accepted December 16, 1997.
Communicated by Jean-Lien C. Wu.

In the past decade, several broadcasting cryptoschemes have been developed [2-4, 11, 21, 24]. However, most of them are individual-oriented. That is, secrets in ciphertext form are addressed to individuals, and each individual takes full authority for recovering those secrets. In 1987, Desmedt [7] first introduced the concept of group-oriented cryptography. A group-oriented cryptosystem provides the following features: (1) secrets in ciphertext form are addressed to "group" instead of "individual"; (2) only certain subsets of authorized individuals in the destination group can recover the secrets. Hence, all the individuals in the same destination group share the group authority for recovering the dedicated secrets. Straightforwardly, a group-oriented cryptosystem will be more efficient when broadcasting channels are involved.

In an authorization-based group-oriented secure broadcasting system, the broadcaster specifies the message authorization strategy among the individuals in the destination group by considering the characteristics or restrictions of the broadcast message (such as timeliness, integrity, importance etc.) before broadcasting the ciphertext of the secret. The individuals in the destination group can only recover the secret by means of authentication, following a predefined message authorization strategy. In general, the broadcaster can define the message authorization strategy for a secure broadcast as one of the following:

(1) restricted high-authorized (i.e., restricted 1-out-of-n): only the specified individual in the destination group can recover it;
(2) unrestricted high-authorized (i.e., unrestricted 1-out-of-n): any individual in the destination group can recover it;
(3) low-authorized (i.e., n-out-of-n): all the individuals in the destination group should collaborate together to recover it;
(4) restricted threshold-authorized (i.e., restricted t-out-of-n): only the specified t individuals in the destination group should collaborate together to recover it; and
(5) unrestricted threshold-authorized (i.e., unrestricted t-out-of-n): any t individuals in the destination group can collaborate together to recover it.

Note that most previously developed group-oriented secure broadcasting cryptoschemes or systems [1, 7, 8, 12, 14] only provide some, not all, of the message authorization strategies stated above.

The main ideas behind the design of an ID-based system are that the personal identity of a user is regarded as the public key for that user, and that the corresponding secret key is derived from the personal identity by applying a trapdoor one-way function [20]. In practical applications, the personal identity may be the user's name, E-mail address, identification number, or some knowledge about the user. An ID-based system has the significant advantage that it enables any two users to communicate securely and to authenticate each other without extra key exchange. Furthermore, it simplifies the problem of key management. Some well-known ID-based systems can be found in [20, 23].

In this paper, we intend to propose an authorization-based group-oriented secure broadcasting system that employs all the message authorization strategies defined above. The proposed system preserves the merits of both the group-oriented cryptography and the ID-based system. Since the proposed system is mainly inspired by Tsujii and Itoh's ID-based system [23], we first briefly review their system in the next section. The proposed system is described in section 3. In section 4, we discuss security analyses for the proposed system, including some possible attacks caused by outside intruders or inside impostors in the destination group. Finally, we give conclusions in section 5.

2. REVIEW OF TSUJII AND ITOH'S ID-BASED SYSTEM

We will first define the following vector operations to improve the presentation of Tsujii and Itoh's ID-based system. Let p, g and r be integers, and let $A=\{a_1, a_2, ..., a_c\}$ and $B=\{b_1, b_2, ..., b_c\}$ be c-dimensional integer vectors.

Definition 1. $A \bmod p = (a_1 \bmod p, a_2 \bmod p, ..., a_c \bmod p)$.

Definition 2. $g^A \bmod p = (g^{a_1} \bmod p, g^{a_2} \bmod p, ..., g^{a_c} \bmod p)$.

Definition 3. $A^r \bmod p = (a_1^r \bmod p, a_2^r \bmod p, ..., a_c^r \bmod p)$.

Definition 4. $A^B \bmod p = \prod_{i=1}^{c} (a_i)^{b_i} \bmod p$.

Assume there exists a key generation center (KGC) in the system. The tasks of KGC are to define the system's secret and public parameters and to generate secret keys for registering users in the initialization stage. Tsujii and Itoh's ID-based system works as follows:

Initialization: Initially, KGC chooses a large prime p, a generator a over Galois field GF(p), and a one-to-one function $f: Z_2^k \to Z_2^c$, where k is the length of the user's identity and $k < c$. Note that in order to withstand a conspiracy attack [23], c should be greater than the maximum number of users in the system. After that, KGC uses Merkle and Hellman's scheme [16] to generate a c-dimensional vector $A = (a_1, a_2, ..., a_c) \in Z_{p-1}^c$, such that

$$A \cdot I \neq A \cdot J (\bmod\ p-1), \text{ for } I \neq J, \tag{1}$$

where I and J are c-dimensional binary vectors, and computes

$$H = \alpha^A \bmod p. \tag{2}$$

Here, A is used as the secret key, and H is used as the public key for KGC. The parameters p, α, k and H are made public to all users in the system while A is kept secret. When a user U_i wants to join the system, he/she first generates a k-dimensional binary vector for his/her identity, denoted as

$$ID_i = (x_{i1}, x_{i2}, ..., x_{ik}), \text{ for } x_{ij} \in \{0,1\},$$

and registers ID_i to KGC. Then, KGC computes U_i's extended identity as

$$EID_i = f(ID_i) = (y_{i1}, y_{i2}, ..., y_{ic}), \text{ for } y_{ij} \in \{0,1\},$$

generates the secret key for U_i as

$$s_i = A \cdot EID_i \ (\mathrm{mod}\ p - 1), \tag{3}$$

and sends s_i to U_i via a highly secure channel.

In the following, we will describe how to generate an A satisfying Eq. (1). First, KGC randomly generates a superincreasing sequence $\{b_i\}$ (for $i = 1, 2, ..., c$) satisfying $\sum_{i=1}^{c} b_i < p - 1.$ Afterwards, KGC selects an integer d such that $\gcd(d, p - 1) = 1$ and computes

$$a_i = b_i \cdot d (\mathrm{mod}\ p - 1), \tag{4}$$

for $i = 1, 2, ..., c$. The vector $A = (a_1, a_2,..., a_c)$ is what we want.

Encryption: Suppose U_j wants to send a secret message m to U_i. U_j first computes U_i's extended identity $EID_i = f(ID_i)$, randomly chooses an integer $r \in Z_{p-1}$, and encrypts m as

$$c_1 = \alpha^r \bmod p, \tag{5}$$

$$c_2 = m \cdot (H^{EID_i})^r \ (\mathrm{mod}\ p). \tag{6}$$

Afterwards, U_j sends the ciphertext (c_1, c_2) of m to U_i.

Decryption: Upon receiving the ciphertext (c_1, c_2) of m sent by U_j, U_i uses his/her secret key s_i to recover m as

$$m = (c_1)^{-s_i} \cdot c_2 \bmod p, \tag{7}$$

Now, we will show that U_i can recover m by Eq. (7). From Eq. (3), we have

$$\alpha^{s_i} = \alpha^{A \cdot EID_i} = H^{EID_i} (\mathrm{mod}\ p). \tag{8}$$

By Eqs. (5), (6) and (8), the correctness of Eq. (7) can be verified as

$$\begin{aligned}(c_1)^{-s_i} \cdot c_2 &= (\alpha^r)^{-s_i} \cdot c_2 (\mathrm{mod}\ p) \\ &= (\alpha^{s_i})^{-r} \cdot m \cdot (H^{EID_i})^r (\mathrm{mod}\ p) \\ &= (H^{EID_i})^{-r} \cdot m \cdot (H^{EID_i})^r (\mathrm{mod}\ p) \\ &= m (\mathrm{mod}\ p).\end{aligned}$$

In Tsujii and Itoh's ID-based system, any malicious user of the system will face the discrete logarithm problem in finding the system's secret parameter or another user's secret key. Moreover, conspiratorial users cannot directly solve A by presenting their secret keys s_i's to each other because the number of unknown variables, i.e., a_i's, is always greater than the number of equations in the equation system formed by Eq. (3). The reader is encouraged to refer to the same paper [23] for detailed security analyses of Tsujii and Itoh's ID-based system.

3. THE PROPOSED SYSTEM

As in Tsujii and Itoh's ID-based system, the proposed system requires a key generation center, KGC. The proposed system consists of two phases: a preparation phase and an application phase. In the preparation phase, KGC generates secret and public information for the system, the registering group and the individuals in that group, respectively. In the application phase, the broadcaster first defines the message authorization strategy for the secret, then encrypts the secret, and finally broadcasts the ciphertext of the secret to the destination group. The individuals in the destination group can only recover the secret by means of authentication, following a predefined message authorization strategy. These two phases are explained in the following.

3.1 The Preparation Phase

The preparation phase includes two stages: initialization and registration. In the initialization stage, KGC defines the system parameters. The public parameters of the system are stored in a public directory while the secret parameters of the system are kept secret by KGC itself. In the registration stage, KGC generates the secret and the public parameters for the registering group and its individuals. The public parameters are also stored in the public directory, the secret parameters for the groups are maintained by KGC, and the secret parameters for the individuals are kept secret by the individuals themselves. These two stages are described in the following.

Initialization: KGC performs the following steps to generate the secret and the public parameters for the system:

Step 1: Select two large primes p ($> 2^{512}$) and q ($> 2^{160}$), where q is a prime divisor of $\frac{p-1}{2}$.
Step 2: Select a generator α in GF(p) with order q.
Step 3: Select a constant c, such that c is greater than both the maximum number of groups joining the system and the maximum number of individuals in the groups.
Step 4: Use Merkle and Hellman's scheme [16] to generate a c-dimensional vector $A_S = (a_1, a_2, \ldots, a_c) \in Z_q^c$, such that

$$A_S \cdot I \neq A_S \cdot J (\bmod\ q), \text{ for } I \neq J, \tag{9}$$

where I and J are c-dimensional binary vectors.
Step 5: Compute

$$H_S = \alpha^{A_S} \bmod p. \tag{10}$$

Step 6: Choose two one-way hashing functions $f: Z_p \to Z_q^c$ and $h: Z_p \to Z_q$.
Step 7: Create a public directory, and put the parameters p, q, α, f, h, c, and H_S in it while keeping A_S secret.

When the system has been set up, KGC can accept the registration of a group and its individuals. The registration stage is stated as follows.

Registration: Let G with the identity GID be the registering group and U_i with the identity ID_i be one of the individuals in G. KGC performs the following steps to generate the secret and the public parameters for G and all the U_i's in G:

Step 1: For the registering group G, do the following:
1-1: Use Merkle and Hellman's scheme [16] to generate a c-dimensional vector $A_G \in Z_q^c$ for G, and compute

$$H_G = \alpha^{A_G} \bmod p. \tag{11}$$

1-2: Compute G's extended identity $EGID = f(GID)$.
1-3: Randomly select a c-dimensional vector $R_G \in Z_q^c$, generate a group key for G as

$$s_G = A_S \cdot (R_G + EGID) \bmod q, \tag{12}$$

and compute

$$v_G = (H_S)^{R_G} \bmod p. \tag{13}$$

Step 2: For each U_i in G, do the following:
2-1: Compute U_i's extended identity $EID_i = f(ID_i)$.
2-2: Randomly select a c-dimensional vector $R_i \in Z_q^c$, generate a personal key for U_i as

$$s_i = A_G \cdot (R_i + EID_i) \bmod q, \tag{14}$$

and compute

$$v_i = (H_G)^{R_i} \bmod p. \tag{15}$$

Step 3: Solve Φ_G using the following equation:

$$s_G = (A_G \cdot \Phi_G + \sum_{U_i \in G} s_i) \bmod q. \tag{16}$$

Step 4: Compute

$$y_G = (H_G)^{-\Phi_G} \bmod p. \tag{17}$$

Step 5: Deliver (s_G, s_i) to each U_i in G through a highly secure channel, and put H_G, y_G, v_G, v_i's in the public directory.

Note that, for security reasons, KGC can discard the secret parameters A_S, A_G, R_G, Φ_G, and R_i when no more new groups or individuals want to join the system. The parameters generated by the preparation phase are summarized below:

(1) Public transformation function: f, h.

(2) Secret information for KGC: A_S.
(3) Public information for KGC: p, q, α, H_S.
(4) Secret information for G: A_G, s_G, Φ_G, R_G.
(5) Public information for G: GID, H_G, y_G, v_G.
(6) Secret information for each U_i in G: s_i, R_i.
(7) Public information for each U_i in G: ID_i, v_i.

3.2 The Application Phase

The application phase includes two stages: encryption and decryption. The encryption stage deals with the task of encrypting a secret according to the message authorization strategy of the secret, and the decryption stage deals with the task of decrypting the ciphertext of the secret, following a predefined message authorization strategy. These stages are described below.

Encryption: Let U_b be the broadcaster, G be the destination group and B be the group to whom U_b belongs. Suppose U_b wants to broadcast a secret $m \in Z_p$ to G. The broadcasting transaction is formatted as {broadcaster, recipients, message authorization strategy, ciphertext}. U_b performs the following steps to originate the broadcasting transaction for m:

Step 1: Define the message authorization strategy for m.
Step 2: Generate G's extended identity $EGID = f(GID)$.
Step 3: Randomly select an integer $r \in Z_p$ and compute

$$c_1 = \alpha^{-r} \bmod p. \tag{18}$$

Step 4: Solve c_2 using the following equation:

$$h(m) = s_b \cdot c_1 - r \cdot c_2 \bmod q. \tag{19}$$

Step 5: According to the predefined message authorization strategy for m, perform one of the following cases:
Case 1. Restricted 1-out-of-n authorization strategy:
5-1: Let $U_i \in G$ with identity ID_i be the specified recipient.
5-2: Generate U_i's extended identity $EID_i = f(ID_i)$.
5-3: Compute

$$c_3 = (m + ID_i)((H_G)^{EID_i} \cdot v_i)^r \bmod p. \tag{20}$$

5-4: Broadcast $\{B.U_b, G.U_i$, restricted 1-out-of-n, $(c_1, c_2, c_3)\}$.
Case 2. Unrestricted 1-out-of-n authorization strategy:
5-5: Compute

$$c_3 = (m + GID)((H_S)^{EGID_i} \cdot v_G)^r \bmod p. \tag{21}$$

5-6: Broadcast $\{B.U_b, G,$ unrestricted 1-out-of-n, $(c_1, c_2, c_3)\}$.

Case 3. n-out-of-n authorization strategy:

5-7: Compute

$$c_3 = (m + GID)((H_S)^{EGID} \cdot v_G \cdot y_G)^r \bmod p. \tag{22}$$

5-8: Broadcast $\{B.U_b, G, n$-out-of-$n, (c_1, c_2, c_3)\}$.

Case 4. Restricted t-out-of-n authorization strategy:

5-9: Let $U_1, U_2, ..., U_t$ with the identities $ID_1, ID_2, ..., ID_t$, respectively, be the specified individuals in G.

5-10: Construct a polynomial $Q(x)$ with degree t-1 by interpolating on points $(ID_i, (H_G)^{EID_i} \cdot v_i)^{-r} \bmod p)$'s (for $i = 1, 2, ..., t$).

Let $Q(x) = k + e_1x + e_2 x^2 + ... + e_{t-1} x^{t-1} \bmod p$.

5-11: Compute

$$c_3 = (m + GID) \cdot k \bmod p. \tag{23}$$

5-12: Broadcast $\{B.U_b, G.\{U_1, U_2, ..., U_t\}$, restricted t-out-of-n, $(c_1, c_2, c_3)\}$.

Case 5. Unrestricted t-out-of-n authorization strategy:

5-13: Randomly generate a polynomial $Q(x)$ with degree t-1 as

$$Q(x) = k + e_1x + e_2 x^2 + ... + e_{t-1} x^{t-1} \bmod p.$$

5-14: Compute the shadows δ_i's for all individuals U_i's in G as follows:

$$\begin{aligned} Q(ID_1) &= \delta_1, \\ Q(ID_2) &= \delta_2, \\ &\vdots \\ Q(ID_n) &= \delta_n. \end{aligned}$$

5-15: Compute

$$d_i = (\delta_i + ID_i)((H_G)^{EID_i} \cdot v_i)^r \bmod p. \tag{24}$$

5-16: Compute c_3 as Eq. (23).

5-17: Broadcast $\{B.U_b, G,$ unrestricted t-out-of-n, $(c_1, c_2, c_3, d_1, d_2, ..., d_n)\}$.

Note that Cases 1 and 3 are special cases of Case 4 whereas Cases 2 and 3 are special cases of Case 5. However, for the sake of efficient implementation, we will differentiate these cases from each other in our presentation. Furthermore, the broadcaster may define different threshold values t for the message authorization strategies specified in Cases 4 and 5.

Decryption: Upon receiving the message broadcasted by U_b, the individuals in G can only recover the secret m with authentication from the ciphertext by following the predefined message authorization strategy. The procedures for decrypting the ciphertext of m are as follows:

Step 1: According to the predefined message authorization strategy for m, perform one of the following cases:

Case 1. Restricted 1-out-of-n authorization strategy:

1-1. Let $U_i \in G$ with identity ID_i be the specified recipient.

1-2. U_i uses the personal key s_i to recover the secret as

$$m = (c_3 \cdot (c_1)^{s_i} - ID_i) \bmod p. \tag{25}$$

Case 2. Unrestricted 1-out-of-n authorization strategy:

1-3. Any individual in G uses the group key s_G to recover the secret as

$$m = (c_3 \cdot (c_1)^{s_G} - GID) \bmod p. \tag{26}$$

Case 3. n-out-of-n authorization strategy:

1-4. Each individual $U_i \in G$ computes

$$w_i = (c_1)^{s_i} \bmod p. \tag{27}$$

1-5. All the individuals in G collaborate to recover the secret as

$$m = ((c_3 \cdot \prod_{U_i \in G} w_i) - GID) \bmod p. \tag{28}$$

Case 4. Restricted t-out-of-n authorization strategy:

1-6. Let $U_1, U_2, ..., U_t$ be the t specified individuals in G that can recover the secret.

1-7. These t individuals cooperate to reconstruct $Q(x)$ by interpolating on points $(ID_i, (c_1)^{s_i} \bmod p)$'s (for $i = 1, 2, ..., t$), and obtain $k = Q(0)$.

1-8. Recover the secret as

$$m = (c_3 \cdot k^{-1} - GID) \bmod p. \tag{29}$$

Case 5. Unrestricted t-out-of-n authorization strategy:

1-9. Any t individuals in G use their personal keys s_i's to compute their shadows δ_i's as

$$\delta_i = (d_1 \cdot (c_1)^{s_i} - ID_i) \bmod p. \tag{30}$$

1-10. These t individuals cooperate to reconstruct $Q(x)$ by interpolating on points (ID_i, δ_i)'s and obtain $k = Q(0)$.

1-11. Recover the secret as in Eq.(29).

Step 2. Authenticate the recovered m as follows:

2-1. Generate U_b's extended identity $EID_b = f(ID_b)$.

2-2. Check if the following equality holds:

$$\alpha^{h(m)} = (v_b \cdot (H_B)^{EID_b})^{c_1} (c_1)^{c_2} (\text{mod } p). \tag{31}$$

If the equality holds, then the recovered m is verified.

In the following, we will first show that the individuals in the destination group can only recover the secret m by following the message authorization strategy defined by the broadcaster.

Case 1: Restricted 1-out-of-n

From Eqs. (14) and (15), we have

$$\begin{aligned} \alpha^{s_i} &= \alpha^{A_G \cdot R_i} \cdot \alpha^{A_G \cdot EID_i} (\text{mod } p) \\ &= (H_G)^{R_i} (H_G)^{EID_i} (\text{mod } p) \\ &= v_i \cdot (H_G)^{EID_i} (\text{mod } p). \end{aligned} \tag{32}$$

From Eqs. (20) and (32), we have

$$\begin{aligned} c_3 \cdot (c_1)^{s_i} - ID_i &= c_3 \cdot (\alpha^{-r})^{s_i} - ID_i (\text{mod } p) \\ &= c_3 \cdot (\alpha^{s_i})^{-r} - ID_i (\text{mod } p) \\ &= c_3 \cdot (v_i \cdot (H_G)^{EID_i})^{-r} - ID_i (\text{mod } p) \\ &= (m + ID_i)((H_G)^{EID_i} \cdot v_i)^r \cdot (v_i \cdot (H_G)^{EID_i})^{-r} - ID_i (\text{mod } p) \\ &= (m + ID_i) - ID_i = m (\text{mod } p), \text{ which implies Eq.(25).} \end{aligned}$$

Case 2: Unrestricted 1-out-of-n

From Eqs. (12) and (13), we have

$$\begin{aligned} \alpha^{S_G} &= \alpha^{A_S \cdot R_G} \cdot \alpha^{A_S \cdot EGID} (\text{mod } p) \\ &= (H_S)^{R_G} (H_S)^{EGID} (\text{mod } p) \\ &= (v_G)(H_S)^{EGID} (\text{mod } p). \end{aligned} \tag{33}$$

From Eqs. (21) and (33), we have

$$\begin{aligned} c_3 \cdot (c_1)^{S_G} - GID &= c_3 \cdot (\alpha^{-r})^{S_G} - GID (\text{mod } p) \\ &= c_3 \cdot (\alpha^{S_G})^{-r} - GID (\text{mod } p) \\ &= c_3 \cdot (v_G \cdot (H_S)^{EGID})^{-r} - GID (\text{mod } p) \\ &= (m + GID)((H_S)^{EGID} \cdot v_G)^r \cdot (v_G \cdot (H_S)^{EGID})^{-r} - GID (\text{mod } p) \\ &= (m + GID) - GID = m (\text{mod } p), \text{ which implies Eq. (26).} \end{aligned}$$

Case 3: n-out-of-n

From Eq. (27), we have

$$\prod_{U_i \in G} w_i = (c_1)^{\sum_{U_i \in G} s_i} = (\alpha^{-r})^{\sum_{U_i \in G} s_i} \tag{34}$$
$$= (\alpha^{\sum_{U_i \in G} s_i})^{-r} (\text{mod } p).$$

From Eq. (16), we have

$$\alpha^{S_G} = \alpha^{A_G \cdot \Phi_G} \cdot \alpha^{\sum_{U_i \in G} s_i}$$
$$= (H_G)^{\Phi_G} \cdot \alpha^{\sum_{U_i \in G} s_i} (\text{mod } p)$$
$$= y_G^{-1} \cdot \alpha^{\sum_{U_i \in G} s_i} (\text{mod } p),$$

which implies

$$\alpha^{\sum_{U_i \in G} s_i} = \alpha^{S_G} \cdot y_G (\text{mod } p). \tag{35}$$

From Eqs. (22), (34) and (35), we have

$$c_3 \cdot \prod_{U_i \in G} w_i - GID = c_3 \cdot (\alpha^{\sum_{U_i \in G} s_i})^{-r} - GID (\text{mod } p)$$
$$= c_3 \cdot (v_G \cdot (H_S)^{EGID} \cdot y_G)^{-r} - GID (\text{mod } p)$$
$$= (m + GID)((H_S)^{EGID} \cdot v_G \cdot y_G)^{r} \cdot (v_G \cdot (H_S)^{EGID} \cdot y_G)^{-r} - GID (\text{mod } p)$$
$$= (m + GID) - GID = m (\text{mod } p), \text{ which implies Eq. (28)}$$

Case 4: Restricted t-out-of-n

Since $(c_1)^{s_i} = (v_i \cdot (H_G)^{EID_i})^{-r} (\text{mod } p)$, steps 5-10 in the **Encryption** procedure and steps 1-7 in the **Decryption** procedure will construct the same polynomial $Q(x)$. Thus, these t individuals in G will obtain $k = Q(0)$ which is the same as that generated by the broadcaster. Thus,

$$c_3 \cdot k^{-1} - GID = (m + GID) \cdot k \cdot k^{-1} - GID = m (\text{mod } p),$$

which implies Eq. (29).

Case 5: Unrestricted t-out-of-n

Since $(c_1)^{s_i} = (v_i \cdot (H_G)^{EID_i})^{-r} (\text{mod } p)$, each U_i in G will obtain the shadow δ_i by Eq. (24) which is the same as that generated by the broadcaster. This implies that any t individuals in G can obtain $k = Q(0)$ which is the same as that generated by the broadcaster, as shown in Shamir's scheme [19]. Thus, they can recover the secret m as discussed in Case 4.

Next, we will show that the individuals in the destination group can authenticate the recovered m. From Eqs. (19), we have

$$\alpha^{h(m)} = \alpha^{s_b \cdot c_1} \cdot \alpha^{-r \cdot c_2} (\text{mod } p)$$
$$= (v_b \cdot (H_B)^{EID_b})^{c_1} (c_1)^{c_2} (\text{mod } p),$$

which implies Eq. (31). Thus, the individuals in the destination group can authenticate the recovered m by verifying Eq. (31). Note that the purpose of using the one-way hashing function h in Eq. (19) is to avoid a chosen-plaintext attack against any ElGamal-like digital signature scheme [10].

4. SECURITY ANALYSIS

The attackers of a group-oriented cryptosystem may be outside intruders or inside impostors. Outside intruders attack the system using knowledge of only the system's public parameters and broadcasting transactions. Inside impostors are individuals in the destination group, and they may attack the system using knowledge of system's public parameters, broadcasting transactions, and their own secret parameters (for instance, the personal keys and the group key). Attacks plotted by inside impostors often proceed with conspiratorial cooperation using 1-out-of-n or t-out-of-n message authorization strategies. Some possible attacks against the proposed system are analyzed as follows:

Attack 1: An outside intruder tries to reveal KGC's secret parameter, i.e., A_S.
Cryptanalysis of Attack 1: The intruder may directly compute A_S from Eq. (10) using knowledge of all available public parameters. However, he will face the discrete logarithm problem in trying to compute A_S from Eq. (10) [9, 10, 18].

Attack 2: An outside intruder tries to reveal G's secret parameters, i.e., A_G, R_G, Φ_G and s_G.
Cryptanalysis of Attack 2: As analyzed in **Attack 1**, the intruder will face the discrete logarithm problem in trying to directly compute A_G, R_G, Φ_G and s_G from Eqs. (11), (13), (17) and (33), respectively. Unless the intruder knows A_S and R_G (protected by the discrete logarithm assumption) in advance, he cannot solve s_G from Eq. (12).

Attack 3: An outside intruder tries to reveal any individual U_i's secret parameters, i.e., s_i and R_i.
Cryptanalysis of Attack 3: Unless the intruder knows A_G and R_i (protected by the discrete logarithm assumption) in advance, he cannot solve s_i from Eq. (14). Also, the intruder will face the discrete logarithm problem in trying to directly compute s_i from Eq. (32) with knowledge of all the available public parameters.

Attack 4: An outside intruder tries to impersonate the broadcaster U_b to broadcast a fake secret to the individuals in G.
Cryptanalysis of Attack 4: The intruder can thoroughly impersonate U_b if he knows s_b. However, as analyzed in **Attack 3**, s_b is protected by the discrete logarithm assumption. Also, the intruder will face the discrete logarithm problem, as discussed in [10], when it tries to compute c_1 and c_2 while satisfying Eq. (31) for a given fake secret m.

Attack 5: Some inside impostors try to reveal KGC's secret parameter, i.e., A_S.
Cryptanalysis of Attack 5: The impostors who know s_G still must first reveal R_G and then solve A_S from Eq. (12). As analyzed in **Attack 2**, R_G is protected by the discrete logarithm assumption.

Attack 6: Some inside impostors in G try to reveal another individual U_x's secret parameters, i.e., s_x and R_x.
Cryptanalysis of Attack 6: Let U_1, U_2, ..., U_t be the impostors in G. As analyzed in **Attacks 2** and **3**, the impostors cannot compute s_x from Eq. (14) unless they know A_G and R_x (both of which are protected by the discrete logarithm assumption) in advance. It is possible that EID_x might be a linear combination of the impostors' extended identities, i.e.,

$$EID_x = \left(\sum_{i=1}^{t} z_i \cdot EID_i\right) \bmod 2. \tag{36}$$

From Eq. (14), we have

$$\begin{aligned}\sum_{i=1}^{t} z_i \cdot s_i &= A_G \cdot \left(\sum_{i=1}^{t} z_i \cdot R_i\right) + A_G \cdot \left(\sum_{i=1}^{t} z_i \cdot EID_i\right) (\bmod\ q) \\ &= A_G \cdot \left(\sum_{i=1}^{t} z_i \cdot R_i\right) + A_G \cdot EID_x (\bmod\ q).\end{aligned}$$

On the other hand, if

$$R_x = \left(\sum_{i=1}^{t} z_i \cdot R_i\right) \bmod 2, \tag{37}$$

then s_x will be a linear combination of these impostors' personal keys. Thus, they can easily obtain U_x's personal key as

$$s_x = \left(\sum_{i=1}^{t} z_i \cdot s_i\right) \bmod q.$$

However, the probability that both Eqs. (36) and (37) will be satisfied is $\frac{2^t}{2^c} \times \frac{1}{2^c}$, where c is the dimension of the EID_i's and R_i's. Based on progress in contemporary cryptology, the proposed system will be secure against such an attack if $c \geq 128$.

Attack 7: Some inside impostors try to impersonate U_b to broadcast a fake secret to the other individuals in the same group.
Cryptanalysis of Attack 7: As analyzed in **Attack 6**, the impostors will face the discrete logarithm problem in trying to reveal U_b's personal key s_b. Without knowing s_b, the impostors may compute c_1 and c_2 while satisfying Eq. (31) for a given fake secret m. As analyzed in **Attack 4**, the impostors will face the discrete logarithm in trying to compute such c_1 and c_2.

5. DISCUSSION AND CONCLUDING REMARKS

We have presented an authorization-based group-oriented secure broadcasting sysstem based on Tsujii and Itoh's ID-based system. The proposed system provides five message authorization strategies: restricted 1-out-of-n, unrestricted 1-out-of-n, n-out-of-n, restricted

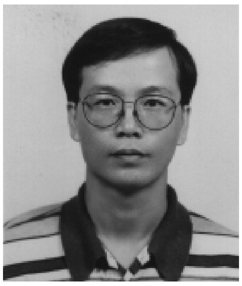
t-out-of-n, and unrestricted t-out-of-n. The broadcaster can choose one of the message authorization strategies, according to the characteristics or restrictions of the secret, to encrypt a secret, so that the individuals in the destination group can only recover the secret by means of authentication, following a predefined message authorization strategy. Except for the unrestricted t-out-of-n message authorization strategy, the broadcaster only needs to broadcast the ciphertext (c_1, c_2, c_3) to the destination group to achieve both message encryption and authentication. However, the broadcaster is required to broadcast additional n shadows to the destination group for the unrestricted t-out-of-n message authorization strategy.

The proposed system preserves the merits of Tsujii and Itoh's ID-based system. However, by introducing the random vectors R_G and R_i into the registration stage to generate the group's and its individuals' secret keys, the proposed system is more secure, especially against conspiracy attacks plotted by inside impostors.

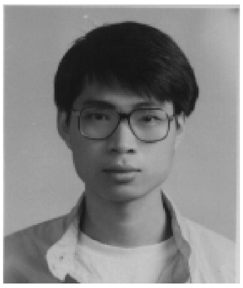
REFERENCES

1. C. C. Chang and H. C. Lee, "A new generalized group-oriented cryptoscheme without trusted centers," *IEEE Journal on Selected Area in Communications*, Vol. 11, No. 5, 1993 , pp. 725-729.
2. C. C. Chang and C. H. Lin, "A cryptosystem for secure broadcasting," in *Proceedings of National Science Council*, R.O.C., Vol. 12, No. 4, 1988, pp. 233-239.
3. C. C. Chang and T. C. Wu, "Broadcasting cryptosystem in computer networks using interpolating polynomials," *Computer Systems Science & Engineering*, Vol. 6, No. 3, 1991, pp. 185-188
4. C. H. Chiou and W. T. Chen, "Secure broadcasting using secure lock", *IEEE Transactions on Software Engineering*, Vol. SE-15, No. 8, 1989, pp. 929-934.
5. Data Encryption Standard, *Federal Information Processing Standard Publication 46*, National Technical Information Service, Springfield, VA. 1977.
6. D. W. Davis and W. L. Price, *Security for Computer Networks*, John Wiley & Sons, Chichester, 1984.
7. Y. Desmedt, "Society and group oriented cryptography: A new concept," *Advances in Cryptology - CRYPTO'87*, 1988, pp. 120-127.
8. Y. Desmedt and Y. Frankel, "Threshold cryptosystems," *Advances in Cryptology – CRYPTO'89*, 1990, pp. 307-315.
9. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, 1976, pp. 644-654.
10. T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, No. 4, 1985, pp. 469-472.
11. A. Fiat and M. Naor, "Broadcast encryption", *Advances in Cryptology – CRYTPO'93*, 1994, pp. 480-491.
12. Y. Frankel, "Practical protocol for large group oriented networks," *Advances in Cryptology—EUROCRYPT'89*, 1990, pp. 56-61.
13. I. S. Gopal and J. M. Jaffe, "Point-to-multipoint communication over broadcast links, " *IEEE Transactions on Communications*, Vol. COM-32, No. 9, 1984, pp. 1034-1044.
14. T. Hwang, "Protocols for group oriented secret sharing," *Information Processing Letters*,

Vol. 42, No. 4, 1992, pp. 179-182.
15. S. T. Kent, "Security requirements and protocols for a broadcast scenario," *IEEE Transactions on Communications*, Vol. COM-29, No. 6, 1981, pp. 778-786.
16. R. C. Merkle and M.E. Hellman, "Hiding information and signatures in trapdoor knapsack," *IEEE Transactions on Information Theory*, Vol. IT-24, No. 5, 1978, pp. 525-530
17. R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signature and public-key cryptosystem," *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120-126.
18. K. H. Rosen, *Elementary Number Theory and Its Applications*, Addison Wesley, 1993.
19. A. Shamir, "How to share a secret," *Communications of the ACM*, Vol. 22, No. 11, 1979, pp. 612-613.
20. A. Shamir, "Identity-based cryptosystems and signature scheme," *Advances in Cryptology – CRYPTO'84*, 1985, pp. 47-53.
21. G. J. Simmons, "How to (selectively) broadcast a secret," in *Proceedings of IEEE Symposium on Security & Privacy*, 1985, pp. 108-113.
22. A. Tanenbaum, *Computer Networks*, Prentice-Hall, Englewood Cliffs, New Jersey, 1988.
23. S. Tsujii and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem, " *IEEE Journal on Selected Areas in Communications*, Vol. 7, No. 4, 1989, pp. 467-473.
24. T. C. Wu and Y. S. Yen, "Cryptosystem for selectively broadcasting separate secrets," *Computer Systems Science & Engineering*, Vol. 8, No. 2, 1993, pp. 121-124.



Tzong-Chen Wu (吳宗成) received the B.S. degree in information engineering from National Taiwan University in 1983, the M.S. degree in applied mathematics from National Chung Hsing University in 1989, and the Ph.D. in computer science and information engineering from National Chiao Tung University in 1992. From August 1992 to January 1997, he was an associate professor in the Department of Information Management, National Taiwan University of Science and Technology. Since February 1997, he has been a professor in the Department of Information Management, National Taiwan University of Science and Technology. Professor Wu is a member of IEEE, ACM, and the Chinese Cryptology and Information Security Association (CCISA). His current research interests include data security, cryptography, network security, and data engineering.



Yuh-Shihng Chang (張裕幸) received the B.S. degree in information management from Tamkang University in 1989, and the M.S. degree in resource management from the National Defense Management College in 1991. Now, he is a Ph.D. candidate in the Department of Information Management, National Taiwan University of Science and Technology. His current research interests include data security, cryptography, and network security.