Some Bounds and a Construction for Secure Broadcast Encryption

Kaoru Kurosawa[1], Takuya Yoshida[1], Yvo Desmedt[2,3] ⋆, and Mike Burmester[3]

[1] Dept. of EE, Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152-8552, Japan
{kurosawa,takuya}@ss.titech.ac.jp
[2] Center for Cryptography, Computer and Network Security, and
Department of EE & CS, University of Wisconsin – Milwaukee
P.O. Box 784, WI 53201-0784, U.S.A.
desmedt@cs.uwm.edu
[3] Information Security Group, Royal Holloway – University of London
Egham, Surrey TW20 OEX, U.K.
m.burmester@rhbnc.ac.uk

Abstract. We first present two tight lower bounds on the size of the secret keys of each user in an unconditionally secure one-time use broadcast encryption scheme (OTBES). Then we show how to construct a computationally secure multiple-use broadcast encryption scheme (MBES) from a key predistribution scheme (KPS) by using the ElGamal cryptosystem. We prove that our MBES is secure against chosen (message, privileged subset of users) attacks if the ElGamal cryptosystem is secure and if the original KPS is simulatable. This is the first MBES whose security is proved formally.

1 Introduction

Secure broadcast encryption is one of the central problems in communication and network security. In this paper we link One-Time use Broadcast Encryption Schemes (OTBESs) [5,7,6] with Key Predistribution Schemes (KPS)[10]. Both schemes are closely related but they have a different structure. In a KPS, a Trusted Authority (TA) distributes secret information to a set of users such that, each member of a privileged subset P of users can compute a specified key k_P, but no coalition F (forbidden subset) is able to recover any information on the key k_P that it is not supposed to know. In a OTBES, the TA distributes secret information to a set of users and then broadcasts a ciphertext b_P over a network. The secret information is such that each member of a particular subset P of users can decrypt b_P, but no coalition F (forbidden subset) is able to recover any information on the plaintext m_P of b_P that it is not supposed to know.

A natural way to construct an OTBES from a KPS is to use a key k_P of the KPS to encrypt the message m_P, that is

$$b_P = k_P + m_P. \tag{1}$$

⋆ A part of this research has been supported by NSF Grant NCR-9508528.

K. Ohta and D. Pei (Eds.): ASIACRYPT'98, LNCS 1514, pp. 420–433, 1998.

Stinson *et al.* [4,6] have shown that there is a tradeoff between $|B_P|$ and $|U_i|$ in OTBESs, where B_P is the set of ciphertexts b_P and U_i is the set of secrets of user i. That is, $|B_P|$ can be decreased by increasing $|U_i|$ and vice versa.

A $(\mathcal{P}, \mathcal{F})$-KPS is a KPS for which $\mathcal{P} \stackrel{\triangle}{=} \{P \mid P \text{ is a privileged subset}\}$ and $\mathcal{F} \stackrel{\triangle}{=} \{F \mid F \text{ is a forbidden subset}\}$. In particular,

- A $(t, \leq w)$-KPS is a $(\mathcal{P}, \mathcal{F})$-KPS with $\mathcal{P} = \{P \mid |P| = t\}$, $\mathcal{F} = \{F \mid |F| \leq w\}$,
- A $(\leq n, \leq w)$-KPS is a $(\mathcal{P}, \mathcal{F})$-KPS with $\mathcal{P} = 2^{\mathcal{U}}$, $\mathcal{F} = \{F \mid |F| \leq w\}$, where $\mathcal{U}$ is the set of users and $n \stackrel{\triangle}{=} |\mathcal{U}|$.

We define $(\mathcal{P}, \mathcal{F})$-OTBESs, $(t, \leq w)$-OTBESs and $(\leq n, \leq w)$-OTBESs in a similar way. Below we list some of the known KPSs and OTBESs.

Key Predistribution Schemes. Blom obtained a $(2, \leq w)$-KPS in [1] by using MDS codes (also see [10]). Blundo *et al.* obtained a $(t, \leq w)$-KPS in [3] by using symmetric polynomials. Fiat and Naor presented a $(\leq n, \leq w)$-KPS in [5]. Blundo *et al.* found tight lower bounds on $|U_i|$ for $(t, \leq w)$-KPSs [3] and for $(\leq n, \leq w)$-KPSs [2].[1] Recently, Ludy and Staddon found some bounds and constructions for some classes of $(n - w, \leq w)$-OTBESs [8]. However, there is a gap between their bounds and the constructions.

One-Time Use Broadcast Encryption Schemes. Stinson *et al.* gave constructions for $(t, \leq w)$-OTBESs [4] and $(\leq n, \leq w)$-OTBESs [6] which can realize the tradeoff between $|B_P|$ and $|U_i|$. Blundo, Frota Mattos and Stinson found a lower bound on $|B_P|$ and $|U_i|$ for $(t, \leq w)$-OTBESs which reflects the tradeoff [4]. Recently, Desmedt and Viswanathan presented a $(\leq n, \leq n)$-KPS [9]. This can be considered as a complement of the Fiat and Naor $(\leq n, \leq n)$-KPS.

In this paper, we first prove that a $(\mathcal{P}, \mathcal{F})$-KPS is equivalent to a $(\mathcal{P}, \mathcal{F})$-OTBES when $|B_P| = |M|$, where M denotes the set of messages (Theorems 1, 2). Then, by using the bounds in [3,2] for KPSs we get directly a lower bound on $|U_i|$ for $(\leq n, \leq w)$-OTBESs and a lower bound for $(t, \leq w)$-OTBESs. The former is the first lower bound for $(\leq n, \leq w)$-OTBESs. The latter is more tight than the bound of Blundo, Frota Mattos and Stinson for $|B_P| = |M|$. Both bounds are tight because the natural schemes which use equation (1) meet the equalities of our bounds. We also present a general lower bound on $|U_i|$ for KPSs which includes all the previous known bounds as special cases (Theorem 3).

Next, we show how to construct a computationally secure $(\mathcal{P}, \mathcal{F})$-Multiple use Broadcast Encryption Scheme ($(\mathcal{P}, \mathcal{F})$-MBES) from a $(\mathcal{P}, \mathcal{F})$-KPS by using the ElGamal cryptosystem. We prove (Theorem 4) that our $(\mathcal{P}, \mathcal{F})$-MBES is secure against *chosen (message, privileged subset of users) attacks* (Definition 1) if the ElGamal cryptosystem is secure and if the original $(\mathcal{P}, \mathcal{F})$-KPS is *simulatable* (Definition 3).

We then show that the Blundo *et al.* scheme, the Fiat-Naor scheme and the Desmedt-Viswanathan scheme are all simulatable (Theorems 5,6). By combining

[1] The model for broadcast encryption in [2,5] corresponds to our model for KPSs. So, for example, the bounds in [2] hold only for KPSs, and not for OTBESs.

this result with our earlier construction we get $(\mathcal{P}, \mathcal{F})$-MBESs for $(\mathcal{P}, \mathcal{F}) = (t, \leq w)$ and $(\leq n, \leq w)$ whose security is proven formally.

The proposed construction is the first MBES whose security is proven formally (Corollary 6). Furthermore, our technique can be generalized to many of the OTBESs in [6], and our argument holds for Multiple use $(\mathcal{P}, \mathcal{F})$-KPSs.

2 Mathematical Models [4,6]

Our model for key distribution and broadcast encryption consists of a Trusted Authority (TA) and a set of users $\mathcal{U} = \{1, 2, \ldots, n\}$.

2.1 Key Predistribution

In a key pre-distribution scheme, the TA generates and distributes secret information to each user. The information given to user i is denoted by u_i and must be distributed "off-band" (i.e., not using the network) in a secure manner. This secret information will enable various *privileged subsets* to compute keys.

Let $2^{\mathcal{U}}$ denote the set of all subsets of users. $\mathcal{P} \subseteq 2^{\mathcal{U}}$ will denote the collection of all privileged subsets to which the TA distributes keys. $\mathcal{F} \subseteq 2^{\mathcal{U}}$ will denote the collection of all possible coalitions (called *forbidden subsets*) against which each key is to remain secure.

Once the secret information is distributed, each user i in a privileged set P should be able to compute the key k_P associated with P. On the other hand, no forbidden set $F \in \mathcal{F}$ disjoint from P should be able to compute any information about k_P.

Let K_P denote the set of possible keys associated with P. We assume that $K_P = K$ for each $P \in \mathcal{P}$.

For $1 \leq i \leq n$, let U_i denote the set of all possible secret values that might be distributed to user i by the TA. For any subset of users $X \subseteq \mathcal{U}$, let U_X denote the cartesian product $U_{i_1} \times \cdots \times U_{i_j}$, where $X = \{i_1, \ldots, i_j\}$ and $i_1 < \cdots < i_j$. We assume that there is a probability distribution on $U_{\mathcal{U}}$, and that the TA chooses $u_{\mathcal{U}} \in U_{\mathcal{U}}$ according to this probability distribution.

We say that the scheme is a $(\mathcal{P}, \mathcal{F})$-*Key Predistribution Scheme* ($(\mathcal{P}, \mathcal{F})$-KPS) if the following conditions are satisfied:

1. Each user i in any privileged set P can compute k_P:
   $\forall i \in P$, $\forall P \in \mathcal{P}$, $\forall u_i \in U_i$, $\exists k_P \in K_P$ s.t.,
   $$\Pr[K_P = k_P \mid U_i = u_i] = 1.$$
2. No forbidden subset F disjoint from any privileged subset P has any information on k_P:
   $\forall P \in \mathcal{P}, \forall k_P \in K_P, \forall F \in \mathcal{F}$ s.t. $P \cap F = \emptyset$, $\forall u_F \in U_F$ s.t. $\Pr(U_F = u_F) > 0$,
   $$\Pr[K_P = k_P \mid U_F = u_F] = \Pr[K_P = k_P]. \qquad (2)$$

We denote a $(\mathcal{P}, \mathcal{F})$-KPS by $(U_1, \ldots, U_n, K)$.

2.2 One-Time Broadcast Encryption

We will use the notation from Section 2.1. We assume that the network is a *broadcast channel*, i.e., it is insecure, and that any information transmitted by the TA will be received by every user.

In a set-up stage, the TA generates and distributes secret information u_i to each user i off-band. At a later time, the TA will want to broadcast a message to a privileged subset P. The particular privileged subset P is, in general, not known ahead of time.

$\mathcal{P} \subseteq 2^{\mathcal{U}}$ will denote the collection of all privileged subsets to which the TA might want to broadcast a message. $\mathcal{F} \subseteq 2^{\mathcal{U}}$ will denote the collection of all possible coalitions (forbidden subsets) against which a broadcast is to remain secure.

Now, suppose that the TA wants to broadcast a message to a given privileged set $P \in \mathcal{P}$ at a later time. (The particular privileged set P is not known when the scheme is set up, except for the restriction that $P \in \mathcal{P}$.) Let M_P denote the set of possible messages that might be broadcast to P. We assume that $M_P = M$ for each $P \in \mathcal{P}$. Furthermore, we assume that there is a probability distribution on M, and that the TA chooses a *message* (i.e., a plaintext) $m_P \in M$ according to this probability distribution. Then the *broadcast* b_P (which is an element of a specified set B_P) is computed as a function of m_P and u_P.

Once b_P is broadcast, each user $i \in P$ should be able to decrypt b_P and obtain m_P. On the other hand, no forbidden set $F \in \mathcal{F}$ disjoint from P should be able to compute any information about m_P.

The security of the scheme is in terms of a single broadcast, so we call the scheme *one-time*. We say that the scheme is a $(\mathcal{P}, \mathcal{F})$-*One-Time Broadcast Encryption Scheme* ($(\mathcal{P}, \mathcal{F})$-OTBES) if the following conditions are satisfied:

1. Without knowing the broadcast b_P, no subset of users has any information about the message m_P, even if given all the secret information $U_{\mathcal{U}}$:
   $\forall P \in \mathcal{P}$, $\forall m_P \in M_P$, $\forall u_U \in U_U$ s.t. $\Pr[U_U = u_U] > 0$,
   $$\Pr[M_P = m_P \mid U_U = u_U] \; = \; \Pr[M_P = m_P]. \tag{3}$$
2. The message for a privileged user is uniquely determined by the broadcast message and the user's secret information:
   $\forall i \in P$, $\forall P \in \mathcal{P}$, $\forall u_i \in U_i$, $\forall b_P \in B_P$, $\exists m_P \in M_P$ s.t.,
   $$\Pr[M_P = m_P \mid U_i = u_i, B_P = b_P] \; = \; 1. \tag{4}$$
3. After receiving the broadcast message, no forbidden subset F disjoint from P has any information on m_P:
   $\forall P \in \mathcal{P}$, $\forall F \in \mathcal{F}$ s.t. $P \cap F = \emptyset$, $\forall m_P \in M_P$, $\forall u_F \in U_F$, $\forall b_P \in B_P$,
   $$\Pr[M_P = m_P \mid U_F = u_F, B_P = b_P] \; = \; \Pr[M_P = m_P]. \tag{5}$$

We denote a $(\mathcal{P}, \mathcal{F})$-OTBES by $(U_1, \ldots, U_n, M, \{B_P\})$.

2.3 Conventional Notation

We first consider key predistribution schemes. If $\mathcal{P}$ consists of all t-subsets of $\mathcal{U}$, then we will write $(t, \mathcal{F})$-KPS. Similarly, if $\mathcal{P}$ consists of all subsets of $\mathcal{U}$ of size at most t, we write $(\leq t, \mathcal{F})$-KPS. An analogous notation will be used for $\mathcal{F}$. Thus, for example, a $(\leq n, 1)$-KPS is a KPS for which there is a key associated with any subset of users (i.e., $\mathcal{P} = 2^{\mathcal{U}}$) and no key k_P can be computed by any individual user $i \notin P$. Note that in any $(\mathcal{P}, \mathcal{F})$-KPS, if $F \in \mathcal{F}$ and $F' \subseteq F$, then $F' \in \mathcal{F}$. Hence, a $(\mathcal{P}, w)$-KPS is a $(\mathcal{P}, \leq w)$-KPS.

The same notation is used for one-time use broadcast encryption schemes.

3 Known Results

For a random variable X, $H(X)$ denotes the entropy of X. Generally,

$$0 \leq H(X) \leq \log_2 |X|, \text{ where } X \stackrel{\triangle}{=} \{x \mid \Pr(X = x) > 0\}.$$

In particular, $H(X) = \log_2 |X|$ iff X is uniformly distributed.

3.1 A $(t, \leq w)$-KPS (The Blundo *et al.* Scheme)

Blom presented a $(2, \leq w)$-KPS in [1]. This was generalized to a $(t, \leq w)$-KPS by Blundo *et al.* as follows [3]. Let q be a prime such that $q \geq n$ (the number of users). The TA chooses a random *symmetric* polynomial in t variables over $GF(q)$ in which the degree of any variable is at most w, that is, a polynomial

$$f(x_1, \ldots, x_t) = \sum_{i_1=0}^{w} \cdots \sum_{i_t=0}^{w} a_{i_1 \cdots i_t} x_1^{i_1} \cdots x_t^{i_t},$$

where, $a_{i_1 \cdots i_t} = a_{\pi(i_1 \cdots i_t)}$ for any permutation π on $(i_1, \ldots, i_t)$. The TA computes u_i as $u_i = f(i, x_2, \ldots, x_t)$ and gives u_i to user i secretly for $1 \leq i \leq n$. The key associated with the t-subset $P = \{i_1, \ldots, i_t\}$ is $k_P = f(i_1, \ldots, i_t)$. Each user $j \in P$ can compute k_P from u_j easily. In this scheme, $|K_P| = q = |K|$ and

$$\log |U_i| = \binom{t + w - 1}{t - 1} \log |K|.$$

This scheme is optimum because Blundo *et al.* have shown that the following lower bound on $|U_i|$ applies.

Proposition 1. *[3] In a $(t, \leq w)$-KPS,*

$$\log |U_i| \geq \binom{t + w - 1}{t - 1} H(K).$$

Beimel and Chor gave a combinatorial proof of Proposition 1 [7]. Blundo and Cresti obtained the following more general lower bound.

Proposition 2. *[2] In a $(\mathcal{P}, \mathcal{F})$-KPS with $\{1, 2, \cdots, n\} \setminus P \in \mathcal{F}$ for all $P \in \mathcal{P}$,*

$$\log |U_i| \geq \tau_i H(K),$$

where $\tau_i = |\{P \in \mathcal{P} \mid i \in P\}|$

Note that Proposition 1 is obtained from Proposition 2 by letting $n = t + w$.

3.2 A $(\leq n, \leq w)$-KPS (The Fiat-Naor Scheme)

Fiat and Naor presented the following $(\leq n, \leq w)$-KPS [5]. Let q be any positive integer. For every subset $F \subseteq \mathcal{U}$ of cardinality at most w, the TA chooses a random value $s_F \in Z_q$ and gives s_F to every member of $\mathcal{U} \setminus F$ as the secret information. Then the key associated with a privileged set P is defined to be

$$k_P = \sum_{F : F \in \mathcal{F}, F \cap P = \emptyset} s_F \pmod q,$$

Here is a small example for illustration. Take $n = 3$, $q = 17$ and $w = 1$, and suppose that the TA chooses the values,

$$s_\emptyset = 11, \quad s_{\{1\}} = 8, \quad s_{\{2\}} = 3, \quad s_{\{3\}} = 8.$$

The secret information of the users is,

$$u_1 = \{s_\emptyset, s_{\{2\}}, s_{\{3\}}\}, \quad u_2 = \{s_\emptyset, s_{\{1\}}, s_{\{3\}}\}, \quad u_3 = \{s_\emptyset, s_{\{1\}}, s_{\{2\}}\}.$$

The keys determined by this information are,

$$k_{\{1,2\}} = s_\emptyset + s_{\{3\}} = 2 \bmod 17, \quad \ldots \quad , k_{\{1,2,3\}} = s_\emptyset = 11 \bmod 17.$$

In this scheme, $|K_P| = q = |K|$ and

$$\log |U_i| = \sum_{j=0}^{w} \binom{n-1}{j} \log |K|.$$

This scheme is optimum because Blundo and Cresti have shown the following Proposition and Corollary.

Proposition 3. *[2] In a $(\leq n, \mathcal{F})$-KPS,*

$$\log |U_i| \geq v_i H(K)$$

where $v_i = |\{F \in \mathcal{F} \mid i \notin F\}|$.

Corollary 1. *[2] In a $(\leq n, \leq w)$-KPS,*

$$\log |U_i| \geq \sum_{j=0}^{w} \binom{n-1}{j} H(K).$$

3.3 The $(\leq n, \leq n)$-KPS (The Desmedt-Viswanathan Scheme)

Desmedt and Viswanathan presented a $(\leq n, \leq n)$-KPS [9]. This scheme can viewed as a complement of the Fiat-Naor $(\leq n, \leq n)$-KPS. The TA initially generates $2^n - n - 1$ independent keys, i.e., one for each $P \subseteq \{1, 2, \ldots, n\}$ such that $|P| \geq 2$. Each user i receives from the TA the keys of those subsets for which $i \in P$. Hence, each user gets $2^{n-1} - 1$ keys. This scheme is optimum because of the following lower bound which follows from Corollary 1.

Corollary 2. *In a $(\leq n, \leq n)$-KPS,*

$$\log |U_i| \geq (2^{n-1} - 1)H(K).$$

(Desmedt and Viswanathan gave another direct proof [9].)

3.4 Lower Bounds for $(t, \leq w)$-OTBESs

Blundo, Frota Mattos and Stinson obtained the following lower bound for $(t, \leq w)$-OTBESs [4],

Proposition 4. *In any $(t, \leq w)$-OTBES with $t \geq w + 1$,*

$$H(B_P) + \sum_{j=1}^{w} H(U_{i_j}) \geq (2w + 1)H(M),$$

for any $P \in \mathcal{P}$.

4 New Lower Bounds on $|U_i|$

In this section we first prove that a $(\mathcal{P}, \mathcal{F})$-KPS is equivalent to a $(\mathcal{P}, \mathcal{F})$-OTBES when $|B_P| = |M|$. Then, by using the bounds in [3,2] for KPSs, we get directly a lower bound on $|U_i|$ for $(\leq n, \leq w)$-OTBESs and a lower bound for $(t, \leq w)$-OTBESs. The former is the first lower bound presented for $(\leq n, \leq w)$-OTBESs. The latter is more tight than the bound of Blundo, Mattos and Stinson for $|B_P| = |M|$. Our bounds are both tight. We also present a general lower bound on $|U_i|$ for KPSs which includes all the previous bounds as special cases.

4.1 Equivalence between KPS and OTBES

Theorem 1. *If there exists a $(\mathcal{P}, \mathcal{F})$-KPS $(U_1, \ldots, U_n, K)$, then there exists a $(\mathcal{P}, \mathcal{F})$-OTBES $(U_1, \ldots, U_n, M, \{B_P\})$ with $|B_P| = |M| = |K|$ for all $P \in \mathcal{P}$.*

Proof. Use a key k_P of the $(\mathcal{P}, \mathcal{F})$-KPS to encrypt a message m_P, that is

$$b_P = k_P + m_P,$$

and broadcast b_P. We then get a $(\mathcal{P}, \mathcal{F})$-OTBES. □

Theorem 2. *If there exists a* $(\mathcal{P}, \mathcal{F})$*-OTBES* $(U_1, \ldots, U_n, M, \{B_P\})$ *such that* $|B_P| = |M|$ *for all* $P \in \mathcal{P}$*, then there exists a* $(\mathcal{P}, \mathcal{F})$*-KPS* $(U_1, \ldots, U_n, K)$ *such that* $|K| = |M|$ *and* $H(K) = H(M)$.

Proof. From a $(\mathcal{P}, \mathcal{F})$-OTBES construct a KPS as follows. Fix $b_P \in B_P$ arbitrarily for all $P \in \mathcal{P}$. Since $|B_P| = |M|$, there is a bijection from B_P to M for any $(u_1, \ldots, u_n)$. Then there is an $\hat{m}_P \in M$ such that each member of P decrypts the b_P as $\hat{m}_P$ for any $(u_1, \ldots, u_n)$. Now take $k_P = \hat{m}_P$ in our KPS. It is easy to see that we get a $(\mathcal{P}, \mathcal{F})$-KPS with $|K| = |M|$ and $H(K) = H(M)$. □

4.2 Lower bounds for OTBESs

From Theorem 2, Proposition 1, and Corollary 1, we obtain immediately the following lower bounds on $|U_i|$ for OTBESs.

Corollary 3. *In a* $(t, \leq w)$*-OTBES, if* $|B_P| = |M|$ *for all* $P \in \mathcal{P}$*, then*

$$\log |U_i| \geq \binom{t + w - 1}{t - 1} H(M).$$

Corollary 4. *In a* $(\leq n, \leq w)$*-OTBES, if* $|B_P| = |M|$ *for all* $P \in \mathcal{P}$*, then*

$$\log |U_i| \geq \sum_{j=0}^{w} \binom{n - 1}{j} H(M).$$

These bounds are tight because the construction in the proof of Theorem 1 meets the equalities if we use the KPSs of Section 3.1 and Section 3.2.

4.3 A General Lower Bound on $|U_i|$

We generalize Proposition 1 as follows.

Theorem 3. *In a* $(\mathcal{P}, \mathcal{F})$*-KPS,*

$$\log |U_i| \geq \delta_i \log |K|,$$

where

$$\delta_i = |\{P \mid i \in P \in \mathcal{P}\ ,\ \{1, 2, \ldots, n\} \backslash P \in \mathcal{F}\}|.$$

The proof is given in Appendix.

Note that Proposition 3 is also obtained as a corollary from Theorem 3. Indeed, all the previous bounds for KPSs are obtained as corollaries to Theorem 3.

From Theorem 2 and Theorem 3, we get the following corollary.

Corollary 5. *In a* $(\mathcal{P}, \mathcal{F})$*-OTBES, if* $|B_P| = |M|$ *for all* $P \in \mathcal{P}$*, then*

$$\log |U_i| \geq \delta_i \log |M|,$$

where $\delta_i = |\{P \mid i \in P \in \mathcal{P}\ ,\ \{1, 2, \ldots, n\} \backslash P \in \mathcal{F}\}|$.

5 Multiple Use Broadcast Encryption

In this section we first show how to construct a computationally secure $(\mathcal{P}, \mathcal{F})$-Multiple use Broadcast Encryption Scheme ($(\mathcal{P}, \mathcal{F})$-MBES) from a $(\mathcal{P}, \mathcal{F})$-KPS by using the ElGamal cryptosystem. We then prove that our $(\mathcal{P}, \mathcal{F})$-MBES is secure against chosen (message, privileged subset of users) attacks if the ElGamal cryptosystem is secure and if the original $(\mathcal{P}, \mathcal{F})$-KPS is simulatable. We also show that all the KPSs considered in Section 3 are simulatable. This construction is the first $(\mathcal{P}, \mathcal{F})$-MBES whose security is proved formally. Furthermore, our technique can be generalized to many of the OTBES presented in [6].

5.1 A Proposed Construction for $(\mathcal{P}, \mathcal{F})$-MBES

Let $(U_1, \ldots, U_n, K)$ be a $(\mathcal{P}, \mathcal{F})$-KPS. The TA distributes secret information $u_1, \ldots, u_n$ to the users in the same way as for the $(\mathcal{P}, \mathcal{F})$-KPS. Let Q be a prime power such that $|K| \mid Q - 1$. Let g be a primitive $|K|$-th root of unity over $GF(Q)$. All the participants agree on Q and g. Let

$$M \stackrel{\triangle}{=} \langle g \rangle = \{m \mid m = g^x \text{ for some } x\}$$

If the TA wishes to send a message $m_p \in M$ to a privileged set $P \in \mathcal{P}$, then the TA broadcasts

$$b_P = (g^r, m_P g^{r k_P}),$$

where k_P is the key of the $(\mathcal{P}, \mathcal{F})$-KPS for P and r is a random number. Each member of P can decrypt b_P by using k_P with the ElGamal cryptosystem.

5.2 Security

Let $\boldsymbol{u}_F$ be a $\boldsymbol{u}_F \in U_F$ with $\Pr(U_F = \boldsymbol{u}_F) > 0$. We will show that the proposed construction is secure against chosen message attacks, in which the adversary can target privileged subsets of users adaptively. Informally these attacks are defined as follows. Fix a forbidden subset F (under the control of the adversary) arbitrarily. Suppose that F has obtained a broadcast b_P of a privileged subset P, $P \cap F = \emptyset$. Then F chooses several privileged subsets P_i and messages m_{P_i} adaptively, and can obtain from the TA, by using it as an oracle, the broadcast b_{P_i}, $i = 1, 2, \ldots$.

Definition 1. *A $(\mathcal{P}, \mathcal{F})$-MBES is secure against chosen (message, privileged subset of users) attacks if there is no probabilistic polynomial time algorithm (adversary) A_0 such as follows. Give as input to A_0:*

$$Q, g, \tilde{F} \in \mathcal{F}, \boldsymbol{u}_{\tilde{F}}, \tilde{P} \in \mathcal{P}, b_{\tilde{P}} = (g^r, m_{\tilde{P}} g^{r k_{\tilde{P}}})$$

with $\tilde{F} \cap \tilde{P} = \emptyset$. A_0 then chooses $P_i \in \mathcal{P}$ and $m_i \in M$ adaptively, and sends these to the TA as a query for $i = 1, 2, \ldots, l$. The TA gives back $b_{P_i} = (g^{r_i}, m_{P_i} g^{r_i k_{P_i}})$ to A_0. Finally, A_0 outputs $m_{\tilde{P}}$ with non-negligible probability for all $(\tilde{F}, \tilde{P})$.

Definition 2. *We say that the ElGamal cryptosystem is secure if there is no probabilistic polynomial time algorithm* A_1 *which on input* (Q, g, y, g^r, my^r) *outputs* m *with non-negligible probability, where* r *is a random number and* $y \in \langle g \rangle$.

Definition 3. *We say that a* $(\mathcal{P}, \mathcal{F})$*-KPS is simulatable if there is a probabilistic polynomial time algorithm (the simulator)* B *for which the following holds. On input* $(Q, g, y, P \in \mathcal{P}, \tilde{F} \in \mathcal{F})$ *with* $P \cap \tilde{F} = \emptyset$, B *outputs* $\boldsymbol{u}_{\tilde{F}}$, $g^{k_{P_1}}, \ldots, g^{k_{P_h}}$ *with probability*

$$\Pr(K_{P_1} = k_{P_1}, \ldots, K_{P_h} = k_{P_h}, u_{\tilde{F}} = \boldsymbol{u}_{\tilde{F}} \mid K_P = k_P),$$

where $y = g^{k_P}$ *and* $\{P_1, \ldots, P_h\} = \{P_i \mid P_i \in \mathcal{P}, P_i \neq P, P_i \cap \tilde{F} = \emptyset\}$.

Theorem 4. *Suppose that a* $(\mathcal{P}, \mathcal{F})$*-KPS is simulatable. Then the* $(\mathcal{P}, \mathcal{F})$*-MBES obtained by using this KPS in our construction is secure against chosen (message, privileged subset of users) attacks if the ElGamal cryptosystem is secure.*

Proof. Suppose that a $(\mathcal{P}, \mathcal{F})$-KPS is simulatable and that the proposed $(\mathcal{P}, \mathcal{F})$-MBES is not secure against chosen (message, privileged subset of users) attacks. Then there is a simulator B for the $(\mathcal{P}, \mathcal{F})$-KPS, and an adversary A_0 which breaks $b_{\tilde{P}}$ for $\tilde{P} \in \mathcal{P}$ by controlling $\tilde{F} \in \mathcal{F}$ for some $\tilde{P} \cap \tilde{F} = \emptyset$.

We will describe a probabilistic polynomial time algorithm A_1 which breaks the ElGamal cryptosystem by using A_0 and B as subroutines. Let the input to A_1 be (Q, g, y, g^r, my^r). Then there is a $k_{\tilde{P}}$ such that $y = g^{k_{\tilde{P}}}$. A_1 works as follows.

1. A_1 gives $(Q, g, y, \tilde{P}, \tilde{F})$ to B. Then B outputs $\boldsymbol{u}_{\tilde{F}}$, $g^{k_{P_1}}, \ldots, g^{k_{P_h}}$.
2. A_1 gives $(Q, g, \tilde{F}, \boldsymbol{u}_{\tilde{F}}, \tilde{P}, g^r, my^r)$ to A_0.
3. Since A_1 has $g^{k_{P_1}}, \ldots, g^{k_{P_h}}$, A_1 can answer any query of A_0.
4. Finally, A_0 outputs m with non-negligible probability.

Then A_1 can output m with non-negligible probability. This is a contradiction. □

5.3 Simulatable $(\mathcal{P}, \mathcal{F})$-KPSs

In what follows, we assume that $\binom{t+w-1}{t-1}$ is polynomial in the length of Q for the Blundo *et al.* scheme, that $\sum_{i=0}^{w} \binom{n-1}{i}$ is polynomial in the length of Q for the Fiat-Naor scheme, and that $2^{n-1} - 1$ is polynomial in the length of Q for the Desmedt-Viswanathan scheme.

Theorem 5. *The Fiat-Naor scheme and the Desmedt-Viswanathan scheme are simulatable.*

Proof. We give a proof for the Fiat-Naor scheme. The proof for the Desmedt-Viswanathan scheme is obtained in a similar way.

We shall describe a simulator B whose input is $(Q, g, y, P, \tilde{F})$, where $P \cap \tilde{F} = \emptyset$. B chooses s_{F_i} randomly for all $F_i \in \mathcal{F}$. From the $\{s_{F_i}\}$, B can obtain $\boldsymbol{u}_{\tilde{F}}$. Note that $s_{\tilde{F}} \notin \boldsymbol{u}_{\tilde{F}}$. On the other hand,

$$k_P = \sum_{F:|F|\le w, F\cap P=\emptyset} s_F = s_{\tilde{F}} + \sum_{F:F\neq\tilde{F},|F|\le w,F\cap P=\emptyset} s_F \pmod{q-1}$$

Therefore,

$$\begin{aligned} y &= g^{k_P} = g^{s_{\tilde{F}}} \cdot g^{\sum_{F:F\neq\tilde{F},|F|\le w,F\cap P=\emptyset} s_F}, \\ g^{s_{\tilde{F}}} &= y/g^{\sum_{F:F\neq\tilde{F},|F|\le w,F\cap P=\emptyset} s_F}. \end{aligned}$$

Thus B can compute $g^{s_{\tilde{F}}}$ which is consistent with k_P such that $y = g^{k_P}$. Then B can compute $g^{k_{P_i}}$ for all $P_i \in \mathcal{P}$ because B knows $\{s_F \mid F \neq \tilde{F}, F \in \mathcal{F}\}$ and $g^{s_{\tilde{F}}}$. □

Definition 4. *Let $A = \{a_{i_1\cdots i_t} \mid 0 \le i_1 \le w, \ldots, 0 \le i_t \le w\}$. We say that A is symmetric if for any $a_{i_1\cdots i_t} \in A : a_{i_1\cdots i_t} = a_{\pi(i_1\cdots i_t)}$ for all permutations π of $(i_1 \cdots i_t)$. Furthermore, let*

$$f(x_1, \ldots, x_t) = \sum_{i_1=0}^{w} \cdots \sum_{i_t=0}^{w} a_{i_1\cdots i_t} x_1^{i_1} \cdots x_t^{i_t}.$$

We say that $f(x_1, \ldots, x_t)$ is symmetric if $\{a_{i_1\cdots i_t}\}$ is symmetric.

Lemma 1. *For given $D = \{b_{j_1\cdots j_t} \mid 1 \le j_1 \le w+1, \ldots, 1 \le j_t \le w+1\}$, let*

$$a_{i_1\cdots i_t} \triangleq \sum_{j_1=1}^{w+1} \cdots \sum_{j_t=1}^{w+1} b_{j_1\cdots j_t} w_{j_1 i_1} \cdots w_{j_t i_t},$$

where $[w_{ij}] \triangleq C^{-1}$ and

$$C \triangleq \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & w+1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2^w & \cdots & (w+1)^w \end{pmatrix}.$$

Then

$$b_{j_1,\ldots,j_t} = \sum_{i_1=0}^{w} \cdots \sum_{i_t=0}^{w} a_{i_1\cdots i_t} j_1^{i_1} \cdots j_t^{i_t}.$$

Furthermore, if D is symmetric, then $\{a_{i_1\cdots i_t}\}$ is symmetric.

Theorem 6. *The Blundo et al. scheme is simulatable.*

Proof. For simplicity, suppose that the input to the simulator B is

$$\tilde{F} = \{1, 2, \dots, w\},\ P = \{v_1, \dots, v_t\},\ y = g^{k_P},\ Q,\ g.$$

B first chooses a (dummy) symmetric polynomial

$$f(x_1, \dots, x_t) = \sum_{i_1=0}^{w} \cdots \sum_{i_t=0}^{w} a_{i_1\cdots i_t} x_1^{i_1} \cdots x_t^{i_t},$$

randomly. Then $\boldsymbol{u}_{\tilde{F}} = (f(1, x_2, \dots, x_t), \dots, f(w, x_2, \dots, x_t))$. Next we consider a (real) symmetric polynomial

$$f_c(x_1, \dots, x_t) = \sum_{i_1=0}^{w} \cdots \sum_{i_t=0}^{w} \hat{a}_{i_1\cdots i_t} x_1^{i_1} \cdots x_t^{i_t} \tag{6}$$

such that $f_c(i, x_2, \dots, x_t) = f(i, x_2, \dots, x_t)$ for $1 \le i \le w$ and $f_c(v_1, \dots, v_t) = k_P$. We first show that there exists such a polynomial f_c. Let

$$J = \{(j_1 \cdots j_t) \mid 1 \le j_1 \le w+1, \dots, 1 \le j_t \le w+1\} \setminus \{(w+1 \cdots w+1)\}.$$

Then B can compute $b_{j_1\cdots j_t} = f_c(j_1, \dots, j_t)$ for all $(j_1 \cdots j_t) \in J$ by using $\boldsymbol{u}_{\tilde{F}}$. Let $c = f_c(w+1, \dots, w+1)$, where c is an unknown variable. From Lemma 1, B can compute $\{\hat{a}_{i_1\cdots i_t}\}$ from $\{b_{j_1\cdots j_t}\}$ and c. Further, it is easy to see that $\hat{a}_{i_1\cdots i_t}$ has the form

$$\hat{a}_{i_1\cdots i_t} = \alpha_{i_1\cdots i_t} + \beta_{i_1\cdots i_t} c, \tag{7}$$

for some constants $\alpha_{i_1\cdots i_t}$ and $\beta_{i_1\cdots i_t}$. Then from eq.(6), we have

$$k_P = f_c(v_1, \dots, v_t) = e_0 + e_1 c$$

for some constants e_0 and e_1. This means that there exists such an f_c. Now

$$y = g^{k_P} = g^{e_0}(g^c)^{e_1}.$$

Then $g^c = (y/g^{e_0})^{1/e_1}$. Therefore B can compute $\{g^{\hat{a}_{i_1\cdots i_t}}\}$ from equation (7). Finally B can compute $g^{k_{P_i}}$ for all $P_i \in \mathcal{P}$ by using equation (6) and $\{g^{\hat{a}_{i_1\cdots i_t}}\}$. □

Corollary 6. *Suppose that the ElGamal cryptosystem is secure. The MBESs obtained from the Blundo et al. scheme, the Fiat-Naor scheme and the Desmedt-Viswanathan scheme by using our construction, are all secure against chosen (message, privileged subset of users) attacks.*

5.4 Generalization of Our MBES

We can generalize the MBESs in Corollary 6 so that anyone can do broadcast encryption. In the Fiat-Naor based MBES, make each g^{s_F} public. In the Blundo *et al.* based MBES, make each g^{a_i} public, where a_i is the coefficient of the symmetric polynomial f. Finally in the Desmedt-Viswanathan based MBES, make each g^{k_P} public. It can be proved that these modifications maintain the security. The details will be given in the final paper.

References

1. Blom, R.: An optimal class of symmetric key generation systems. Advances in Cryptology – EUROCRYPT '84, Lecture Notes in Computer Science #209. Springer-Verlag (1985) 335–338
2. Blundo, C., Cresti, A.: Space requirements for broadcast encryption, Advances in Cryptology – EUROCRYPT '94, Lecture Notes in Computer Science #950. Springer-Verlag (1995) 287–298.
3. Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro,U., Yung, M.: Perfectly secure key distribution for dynamic conferences, Advances in Cryptology – CRYPTO '92, Lecture Notes in Computer Science #740. Springer-Verlag (1993) 471–486
4. Blundo, C., Frota Mattos, L.A., Stinson, D.R.: Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution, Advances in Cryptology – CRYPTO '96, Lecture Notes in Computer Science #1109. Springer-Verlag (1996) 387–400
5. Fiat, A., Naor, M.: Broadcast encryption, Advances in Cryptology – CRYPTO '93, Lecture Notes in Computer Science #773. Springer-Verlag (1994) 480–491
6. D.R.Stinson, On some methods for unconditionally secure key distribution and broadcast encryption, *Designs, Codes and Cryptography*, **12** (1997) 215–243
7. Beimel, A., Chor, B.: Communication in key distribution schemes, IEEE Transactions on Information Theory, **42** (1996) 19–28
8. Ludy, M., Staddon, J.: Combinatorial bounds for broadcast encryption, Advances in Cryptology – EUROCRYPT '98, Lecture Notes in Computer Science #1403. Springer-Verlag (1998) 512–526
9. Desmedt, Y., Viswanathan, V.: Unconditionally secure dynamic conference key distribution, IEEE, ISIT '98 (1998)
10. Matsumoto, T., Imai, H.: On the key predistribution systems: A practical solution to the key distribution problem. In: Pomerance, C. (ed): Advances in Cryptology – CRYPTO '87, Lecture Notes in Computer Science #293. Springer-Verlag (1988) 185–193

Proof of Theorem 3

Our proof is a generalization of the proof in [7, Theorem 3.1].

Lemma 2. *Let P and Q be distinct subsets of* $\{1, 2, \ldots, n\}$.
Let $F \stackrel{\triangle}{=} \{1, 2, \ldots, n\} \setminus Q$. *If* $|Q| \leq |P|$, *then*

$$F \cap P \neq \emptyset$$

Proof. First, suppose that $|Q| < |P|$. If $F \cap P = \emptyset$, then

$$n \geq |F \cup P| = |F| + |P| = n - |Q| + |P| > n.$$

This is a contradiction. Therefore, $F \cap P \neq \emptyset$.

Next, suppose that $|Q| = |P|$. If $F \cap P = \emptyset$, then

$$|F \cup P| = |F| + |P| = n - |Q| + |P| = n.$$

Therefore,

$$F = \{1, 2, \ldots, n\} \setminus P.$$

This means that $P = Q = \{1, 2, \ldots, n\} \setminus P$. This is a contradiction. Hence, $F \cap P \neq \emptyset$.

□

Proof of Theorem 3

For simplicity, we give a proof for $|U_1|$. Take

$$\tilde{P} \stackrel{\triangle}{=} \{P \mid 1 \in P \in \mathcal{P}\ ,\ \{1, 2, \ldots, n\} \setminus P \in \mathcal{F}\}.$$

Let $l = \delta_1 = |\tilde{P}|$ and let $\tilde{P} = \{P_1, P_2, \ldots, P_l\}$, where $|P_1| \geq |P_2| \geq \cdots \geq |P_l|$. Let $\boldsymbol{u} = (u_1, \ldots, u_n)$ be a vector of secret information of the users such that

$$\Pr[U_U = \boldsymbol{u}] > 0.$$

We define $\boldsymbol{u}_F$ similarly.

For all $k_1 \in K_{P_1}$, for all F such that $P_1 \cap F_1 = \emptyset$ and for all $\boldsymbol{u}_F$,

$$\Pr[K_{P_1} = k_1 \mid U_F = \boldsymbol{u}_F] = \Pr[K_{P_1} = k_1] > 0,$$

from equation (2). Therefore, for all $k_1 \in K_{P_1}$ there is a $\boldsymbol{u} = (u_1, \ldots, u_n)$ such that the key of P_1 reconstructed from $\boldsymbol{u}$ is k_1. Now let $\boldsymbol{k} = (k_1, \ldots, k_l)$ be any vector in $K_{P_1} \times \cdots \times K_{P_l}$. We claim that there is a $\boldsymbol{u}$ such that the key of P_i reconstructed from $\boldsymbol{u}$ is k_i for $1 \leq i \leq l$.

Suppose that our claim is false. Let $h (\leq l)$ be the maximum index such that the keys of $\{P_i\}$ are $(k_1, \ldots, k_{h-1}, k'_h, \ldots, k'_l)$ by some $\boldsymbol{u}$, where $k'_h \neq k_h$. Then $2 \leq h$ from our discussion. Let

$$F_h \stackrel{\triangle}{=} \{1, 2, \ldots, n\} \setminus P_h.$$

Then from Lemma 2 (let $Q = P_h$ and $P = P_i$),

$$F_h \cap P_i \neq \emptyset \quad \text{for } 1 \leq i \leq h-1. \tag{8}$$

Let $\boldsymbol{u}_{F_h}$ be a subvector of $\boldsymbol{u}$ which corresponds to F_h. Then $\boldsymbol{u}_{F_h}$ can compute $k_1, \ldots, k_{h-1}$ from equation (8). Suppose that

$$\Pr[K_{P_h} = k_h | U_{F_h} = \boldsymbol{u}_{F_h}] > 0.$$

This means that there exists a $\boldsymbol{u}$ such that the keys are $k_1, \ldots, k_{h-1}, k_h$. This contradicts the maximality of h. Therefore,

$$\Pr[K_{P_h} = k_h | U_{F_h} = \boldsymbol{u}_{F_h}] = 0.$$

However, this is against eq.(2).

Hence, for any $\boldsymbol{k} \in K_{P_1} \times \cdots \times K_{P_l}$, there exists a $\boldsymbol{u}$ such that the keys are $\boldsymbol{k}$. Remember that user 1 is included in any P_i from our definition of $\tilde{P}$. It follows that u_i must be distinct for each $\boldsymbol{k}$. Therefore,

$$|U_1| \geq |K_{P_1}| \times \cdots \times |K_{P_l}| = |K|^l.$$

Hence,

$$\log |U_1| \geq l \log |K| = \delta_1 \log |K|.$$