Space Requirements for Broadcast Encryption

Carlo Blundo[1,*] AND Antonella Cresti[2,**]

[1] Dipartimento di Informatica ed Applicazioni,
Università di Salerno, 84081 Baronissi (SA), Italy

[2] Dipartimento di Scienze dell'Informazione,
Università di Roma "La Sapienza", 00198 Roma, Italy

Abstract. Fiat and Naor [5] presented at Crypto '93 a new encryption scheme designed for broadcast transmissions. The feature of this scheme is to allow a central broadcast site to broadcast secure transmissions to an arbitrary set of recipients. In this paper we model the problem of unconditionally secure broadcast encryption schemes with an information theoretic framework. We obtain tight limitations both on the number of private keys associated with each user and on the number of keys generated by the center. Finally, we consider the model where interaction is allowed in the common key computation phase proving that the interaction cannot help in decreasing the size of the pieces of information given to the users in the broadcast encryption schemes.

1 Introduction

Key distribution is a central problem in cryptographic systems, and is a major component of the security subsystem of distributed systems, communication systems, and data networks. If users of a group wish to communicate using symmetric encryption, they must share a common key. A key distribution scheme is a method to distribute pieces of information among a set of users in such a way that each group of them can compute a common key for secure communication.

Various key distribution schemes have been proposed so far. A basic and straightforward perfectly-secure scheme (which is useful in small systems) consists of distributing initial keys to users in such a way that each potential group of users that need to communicate securely, shares a common key. When we

[*] This work has been done while the author was visiting the Department of Computer Science and Engineering of the University of Nebraska-Lincoln, NE-68588, U.S.A.. C. Blundo research's is supported by Italian Ministry of University and Scientific Research in the framework of the project: "Algoritmi, Modelli di Calcolo e Strutture Informative" and by the National Council of Research.

[**] This work has been done while the author was visiting the Laboratoire d'Informatique, Ecole Normale Supérieure, 75230 Paris Cédex 05, France

allow all possible subsets of a given size to share a common key the number of keys each user has to hold becomes prohibitively large.

Given the high complexity of such a distribution mechanism, a natural step is to trade complexity for security. We may still require that keys are perfectly secure, but only with respect to an adversary controlling coalitions of a limited size. This novel approach was initiated in Blom's work [2] for the case of session keys (other related schemes are given in [7, 8]). Recently, Blundo, De Santis, Herzberg, Kutten, Vaccaro, and Yung [3] considered key distribution for dynamic conferences of a given size. Their scheme has two parameters: t, the size of the conference (group), and k, the size of adversary coalitions. They proved a lower bound on the size of the user's piece of information of $\binom{k+t-1}{t-1}$ times the size of the common key. They then established the optimality of this bound, by describing a scheme which meets this limitation.

Fiat and Naor [5] considered the following scenario for key distribution. There is a center C and a set of users $\mathcal{U}$. The center gives some predefined keys to users in $\mathcal{U}$. At some point the center wants to enable a *privileged* subset of users to recover a common key in such a way that coalitions of users that are not in the privileged class have no information on this common key. The center enables the privileged users to share a key by broadcasting a message. In such a scheme the center, before providing users with prearranged keys, does not know which subset to enable. Moreover, this privileged subset can *dynamically* change. Fiat and Naor [5] presented k-resilient broadcast encryption schemes, that is schemes secure against a coalition of at most k non-privileged users. They constructed *zero-message* unconditionally secure schemes in which the center is not required to broadcast any message in order for the member of the privileged class to generate a common key. In a zero-message scheme each user in the privileged set computes the common key from the information he receives from the center and from the other privileged users' identities. Since the unconditionally secure protocol presented in [5] for the scheme has severe memory requirements, Fiat and Naor [5] proposed schemes requiring less keys to be held by each user, but these schemes are based on unproven complexity assumptions such as "one-way function exists" or "extracting prime roots modulo a composite is hard".

Our objective is to model the problem of unconditionally secure broadcast encryption schemes by using an information theoretic framework. First, we consider a scenario in which any privileged subset of users enabled by the center belongs to a family of *possible* privileged sets and the coalitions of non-privileged users belong to a predefined family. Then, we study the case in which the family of privileged users consists of all possible subsets of users. In this way, we put restrictions only on the family of coalitions of non-privileged users. In particular, when this family consists of all possible subsets of users of cardinality at most k this scheme reduces to the k-resilient broadcast encryption scheme described by Fiat and Naor [5]. We model such schemes by using the Shannon entropy[3] mainly because this leads to a simple, compact, and elegant description of the schemes and because this approach takes into account all probability distribu-

[3] For a complete treatment of the subject the reader is advised to consult [4, 6].

tions on the keys. We analyze the relations among the number of keys held by each user, the number of keys generated by the center, and the security of the scheme. First, we give an information-theoretic definition of the problem. Then, we obtain tight limitations both on the number of private keys associated with each user and on the number of keys generated by the center. As a consequence of our results, if one wants to design schemes with memory requirements smaller than those in [5], then one has to resort to unproven complexity assumptions such as "one-way function (maybe, with suitable algebraic properties) exists." That is, one has to trade smaller memory requirements with unproven complexity assumptions. Finally, we compare the interactive to the non-interactive setting. We show that interaction cannot decrease the size of the pieces of information given to the users in the broadcast encryption schemes. In order to decrease the size of the pieces of information we relax the security requirement. We suppose that the interactive broadcast encryption scheme be secure only a fixed number of times, say ℓ. In this setting the common key among a set of privileged user can be computed at most ℓ times. If we use more than ℓ times the scheme, then there could be some leaking of information on the $(\ell+1)$-th common key. In the case of one-time interactive broadcast encryption we propose a scheme where the user's information in any privileged set of cardinality t is only $2(n-1)/t$ times the size of the common key.
Due to the space limit on this extended abstract, all proofs are omitted. Ask either author for the complete version.

2 Zero-Message Broadcast Encryption

In this section we give a definition of broadcast encryption using an information theoretic framework. Consider the following scenario consisting of a center **C** and a set of users $\mathcal{U}$. The center gives some predefined keys to users in $\mathcal{U}$. At some point **C** wants to enable a *privileged* subset X of users to recover a common key in such a way that coalitions of users that are not in the privileged set X have no information on this common key. In such a scheme the privileged set ranges into a family of *possible* privileged sets. The center, before providing users with some prearranged keys, does not know which subset to enable. Moreover, this privileged subset can *dynamically* change. In this section we deal with zero-message broadcast encryption schemes, that is schemes in which the center is not required to broadcast any message in order for the member of a privileged class to generate a common key.

Suppose that the set of users is $\mathcal{U} = \{U_1, U_2, \dots, U_n\}$. The distribution scheme, that is the algorithm used by the center to generate the pieces of information distributed to the users, is randomized. Assume that the center's algorithm is fixed. The center generates n pieces $u_1, u_2, \dots, u_n$. The piece u_i denotes the information given by the center to U_i. To maintain the notation simpler, we will denote both the users and the sets of possible values of their pieces with the same capital letter; therefore the letter U_i will denote both the user U_i and the set where the possible pieces for U_i are taken. Given a set

$X = \{i_1, i_2, \ldots, i_r\} \subseteq \{1, 2, \ldots, n\}$, where $i_1 < i_2 < \ldots < i_r$, denote with U_X the set $U_{i_1} \times \cdots \times U_{i_r}$. The center's algorithm defines a probability distribution on $U_1 \times \cdots \times U_n$, that, in turn, naturally induces a probability distribution $\{p_{U_X}(u)\}_{u \in U_X}$ on U_X, for any set $X \in 2^{[n]}$. (We denote with $2^{[n]}$ the family of all sets of elements in $\{1, 2, \ldots, n\}$, that is $2^{[n]} = 2^{\{1,2,\ldots,n\}}$.)

Let $H(U_X) = H(U_{i_1} \ldots U_{i_r})$ be the entropy[4] of the probability distribution on $U_X = U_{i_1} \times \cdots \times U_{i_r}$. Let $\mathcal{T} \subseteq 2^{[n]}$ be the family of sets of indices representing the privileged sets of users and $\mathcal{V} \subseteq 2^{[n]}$ the family of sets of indices representing the coalitions of non-privileged users. Let $T = \{i_1, \ldots, i_t\} \in \mathcal{T}$ be a set of t elements. We denote with k_T the common key of the users $\{U_{i_1}, \ldots, U_{i_t}\}$. The common key k_T is computed by privileged users $\{U_{i_1}, \ldots, U_{i_t}\}$ using only their information and identities. We denote by $\mathcal{K}_T$ the set of all possible values of the common key k_T. For any $T = \{i_1, \ldots, i_t\} \in \mathcal{T}$, the probability distribution on $U_1 \times \cdots \times U_n$ naturally induces a probability distribution on $\mathcal{K}_T$, since each U_{i_j} deterministically computes the common key k_T using the information u_{i_j} received by the center and the indices in the set T. Let $\{p_{\mathcal{K}_T}(k)\}_{k \in \mathcal{K}_T}$ be the *a priori* probability that the common key among users $U_{i_1}, \ldots, U_{i_t}$ is $k \in \mathcal{K}_T$, and let $H(\mathcal{K}_T)$ be its entropy.

2.1 $(\mathcal{T}, \mathcal{V})$ Broadcast Encryption

In this section we consider zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption schemes. These schemes, for privileged sets of users represented by $\mathcal{T}$, are secure against coalition of non-privileged set of users represented by $\mathcal{V}$. In these schemes the center is not required to broadcast any message in order for the member of the privileged class to generate a common key. Since in such schemes the users compute the common key without any interaction we will refer to this situation as *non-interactive* model. A zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme can be defined as follows.

Definition 1. Let $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ be a set of n users and let $\mathcal{T}, \mathcal{V} \subseteq 2^{[n]}$. A *zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme* for $\mathcal{U}$ is a distribution protocol such that for any $T = \{i_1, \ldots, i_t\} \in \mathcal{T}$, there hold

1. *Any privileged user can non-interactively compute the common key k_T.* Formally, for all $i \in T$, we have $H(\mathcal{K}_T | U_i) = 0$.
2. *Any coalition of non-privileged users has absolutely no information on the common key k_T.* Formally, for all $V \in \mathcal{V}$ such that $V \cap T = \emptyset$, we have $H(\mathcal{K}_T | U_V) = H(\mathcal{K}_T)$.

Definition 1 does not say anything on the entropies of random variables $\mathcal{K}_T$ and $\mathcal{K}_{T'}$, for different $T, T' \in \mathcal{T}$. For example, we could have either $H(\mathcal{K}_T) > H(\mathcal{K}_{T'})$ or $H(\mathcal{K}_T) \leq H(\mathcal{K}_{T'})$. Our results apply to the general case of arbitrary entropies on keys, but for clarity we state our results for the simpler case that

[4] For definition and properties of information theoretic quantities we refer to [4, 6].

all entropies on keys are equal, i.e. $H(\mathcal{K}_T) = H(\mathcal{K}_{T'})$. We denote this common entropy by $H(\mathcal{K})$.

In a zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme the knowledge of "some" keys does not convey any information on another key. This is formalized by next lemma.

Lemma 2. *Let $\mathcal{U} = \{U_1, U_2, ..., U_n\}$ be a set of n users and let r be an integer. Let $X, Y_1, ..., Y_r, Z \subseteq \{1, 2, \ldots, n\}$ such that $X, Y_1, \ldots, Y_r \in \mathcal{T}$, $Z \in \mathcal{V}$, $Z \cap X = \emptyset$, and $Z \cap Y_i \neq \emptyset$, for $i = 1, \ldots, r$. Then, in any zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme for $\mathcal{U}$ it holds that $H(\mathcal{K}_X | \mathcal{K}_{Y_1} \ldots \mathcal{K}_{Y_r}) = H(\mathcal{K}_X)$.*

The above lemma states that if a key is secure against a set of users Z, then it is independent from all other keys known by such a set of users.

The next theorem states a lower bound on the size of the information held by each user in the scheme.

Theorem 3. *Let $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ be a set of n users and let $\mathcal{T}, \mathcal{V} \subseteq 2^{[n]}$. Suppose that for any privileged set $T \in \mathcal{T}$ it holds that $\{1, 2, \ldots, n\} \backslash T \in \mathcal{V}$. Then, in any zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme for $\mathcal{U}$, for $i = 1, \ldots, n$, the entropy $H(U_i)$ satisfies*

$$H(U_i) \geq \tau_i H(\mathcal{K}),$$

where $\tau_i = |\{T \in \mathcal{T} \ : \ i \in T\}|$.

In the analysis of $(\mathcal{T}, \mathcal{V})$ broadcast encryption schemes we are interested also in the number of keys that the center has to generate in order to construct the scheme. To this aim, we define $\gamma(\mathcal{U}, \mathcal{T}, \mathcal{V}, H(\mathcal{K}), \Delta)$ to be the number of keys generated by the center **C** in a zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme Δ for a set $\mathcal{U}$ of users, given that the entropy on the secret keys is $H(\mathcal{K})$. Since we are interested in the minimum number of keys the center has to generate, we define

$$\gamma(\mathcal{U}, \mathcal{T}, \mathcal{V}) = \inf_{\mathcal{S}, \mathcal{P}} \gamma(\mathcal{U}, \mathcal{T}, \mathcal{V}, H(\mathcal{K}), \Delta),$$

where $\mathcal{S}$ is the space of all zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption schemes for $\mathcal{U}$ and $\mathcal{P}$ is the space of all non-trivial probability distributions on $\mathcal{K}$.

Next theorem provides a lower bound on the number of keys generated by the center in any zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme for a set $\mathcal{U}$ of n users.

Theorem 4. *Let $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ be a set of n users and let $\mathcal{T}, \mathcal{V} \subseteq 2^{[n]}$. Suppose that for any privileged set $T \in \mathcal{T}$ it holds that $\{1, 2, \ldots, n\} \backslash T \in \mathcal{V}$. Then, in any zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme for $\mathcal{U}$ we have*

$$\gamma(\mathcal{U}, \mathcal{T}, \mathcal{V}) \geq |\mathcal{T}|.$$

A possible protocol for a zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme, when for any privileged set $T \in \mathcal{T}$ it holds that $\{1,2,\ldots,n\}\backslash T \in \mathcal{V}$, can be easily realized as follows. For each subset $T \in \mathcal{T}$ the center uniformly chooses a key $k_T \in \mathbf{Z}_{2^m}$ and gives it to each user U_i where $i \in T$. In such a protocol each user U_i, for $i = 1, \ldots, n$, holds $\tau_i = |\{T \in \mathcal{T} : i \in T\}|$ keys and the center has to generate $|\mathcal{T}|$ keys. From Theorems 3 and 4 immediately follows that this protocol is optimal both respect the keys held by each user and the keys generated by the center.

2.2 $\mathcal{V}$-Resilient Broadcast Encryption

We consider the case in which the family of privileged sets consist of all possible sets of users, that is, $\mathcal{T} = 2^{[n]}$. In this situation there are only restrictions on the coalitions of non-privileged users $\mathcal{V}$. A $(2^{[n]}, \mathcal{V})$ broadcast encryption scheme will be simply called *$\mathcal{V}$-resilient broadcast encryption scheme.*

The next theorem states a lower bound on the size of the information held by each user in any zero-message $\mathcal{V}$-resilient broadcast encryption scheme.

Theorem 5. *Let $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ be a set of n users and let $\mathcal{V} \subseteq 2^{[n]}$. In any zero-message $\mathcal{V}$-resilient broadcast encryption scheme for $\mathcal{U}$, the entropy $H(U_i)$, for $i = 1, \ldots, n$, satisfies*

$$H(U_i) \geq v_i H(\mathcal{K}),$$

where $v_i = |\{V \in \mathcal{V} \ : \ i \notin V\}|$.

In the following we analyze the number of keys generated by the center to set up a zero-message $\mathcal{V}$-resilient broadcast encryption scheme. In this case the minimum number of keys $\gamma(\mathcal{U}, \mathcal{T}, \mathcal{V})$ the center has to generate will be denoted by $\gamma(\mathcal{U}, \mathcal{V})$.

The next theorem provides a lower bound on the number of keys generated by the center in any zero-message $\mathcal{V}$-resilient broadcast encryption scheme for a set $\mathcal{U}$ of n users.

Theorem 6. *Let $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ be a set of n users and let $\mathcal{V} \subseteq 2^{[n]}$. In any zero-message $\mathcal{V}$-resilient broadcast encryption scheme for $\mathcal{U}$ we have*

$$\gamma(\mathcal{U}, \mathcal{V}) \geq |\mathcal{V}|.$$

We can construct a protocol for a $\mathcal{V}$-resilient scheme generalizing the scheme proposed by Fiat and Naor [5] for zero-message k-resilient broadcast encryption. This protocol is optimal with respect to both the keys held by each user and the keys generated by the center. The protocol is the following.

Protocol 1

1. For each $V \in \mathcal{V}$ the center uniformly chooses a key $k_V \in \mathbf{Z}_{2^m}$.
2. The center distributes the key k_V to each user U_i such that $i \notin V$.
3. The common key $\mathcal{K}_T$ of the privileged set $T \in 2^{[n]}$ will be the exclusive or of all the keys k_V such that $V \subseteq \{1, 2, \ldots, n\} \backslash T$.

In the above protocol only $v_i = |\{V \in \mathcal{V} \ : \ i \notin V\}|$ elements of $\mathbf{Z}_{2^m}$ are kept by each user. Moreover, the center, in order to realize such a scheme, generates $v = |\mathcal{V}|$ keys. Thus, the proposed protocol is optimal as stated by next theorem.

Theorem 7. Protocol 1 *is optimal with respect to both the keys held by each user and the keys generated by the center.*

2.3 k-Resilient Broadcast Encryption

Fiat and Naor [5] presented k-resilient broadcast encryption schemes, that is schemes secure against a coalition of at most k non-privileged users. They constructed zero-message unconditionally secure broadcast encryption schemes. In our model, a zero-message k-resilient broadcast encryption scheme can be viewed as a zero-message $\mathcal{V}$-resilient broadcast encryption scheme where $\mathcal{V} = \{V \in 2^{[n]} : |V| \leq k\}$.

The next corollary states a lower bound on the size of the information held by each user in a zero-message k-resilient broadcast encryption scheme.

Corollary 8. *Let $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ be a set of n users and let $k < n$ be an integer. In any zero-message k-resilient broadcast encryption scheme for $\mathcal{U}$, the entropy $H(U_i)$ satisfies*

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

In the following we analyze the number of keys generated by the center to set up a zero-message k-resilient broadcast encryption scheme for a set of n users. In this case the minimum number of keys $\gamma(\mathcal{U}, \mathcal{T}, \mathcal{V})$ the center has to generate will be denoted by $\gamma(n, k)$.

The next corollary provides a lower bound on the number of keys generated by the center in any zero-message k-resilient broadcast encryption scheme for a set of n users.

Corollary 9. *Let $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ be a set of n users and let $k < n$ be an integer. In any zero-message k-resilient broadcast encryption scheme for a set on n users $\gamma(n, k)$ satisfies*

$$\gamma(n, k) \geq \sum_{j=0}^{k} \binom{n}{j}.$$

A possible protocol for zero-message k-resilient broadcast encryption schemes is the one proposed by Fiat and Naor [5]. For each subset $B \subset \{1,2,\ldots,n\}$, such that $0 \leq |B| \leq k$ the center generates a key k_B and gives it to each user U_i where $i \in \{1,2,\ldots,n\}\backslash B$. The common key of the privileged set $\{U_{i_1},\ldots,U_{i_t}\}$ is the exclusive or of all the keys k_B, where $B \subseteq \{1,2,\ldots,n\}\backslash\{i_1,\ldots,i_t\}$. In such a protocol each user holds $\sum_{i=0}^{k}\binom{n-1}{i}$ keys and the center has to generate $\sum_{i=0}^{k}\binom{n}{i}$ keys. This protocol is optimal with respect to both the keys held by each user and the keys generated by the center.

3 Interactive Zero-Message Schemes

In Section 2 we proved lower bounds on the information held by each user in a non-interactive zero-message broadcast encryption scheme. In this section we study the case in which we allow interaction among users to set up a common key. We extend the definitions of Section 2 to interactive zero-message broadcast encryption schemes and show that the interaction cannot decrease the size of the pieces of information given to the users in the broadcast encryption schemes. So, in order to decrease the size of the pieces of information we have to relax the security requirement. We require that the interactive broadcast encryption scheme be secure only a fixed number of times, say ℓ. Finally, we propose a 1-time interactive zero-message k-resilient broadcast encryption scheme where the user's information in any privileged set of cardinality t is only $2(n-1)/t$ times the size of the common key.

Let $\mathcal{U} = \{U_1,\ldots,U_n\}$ be a set of users. The algorithm used by the center to generate the pieces of information that will be distributed to the users, as well as the users' algorithm to set up the common key, are randomized. Assume that the center's algorithm and the users' algorithms are fixed.

In an interactive zero-message broadcast encryption scheme, each user U_i in a privileged set gets a message γ_i from all other users in the same set, based on the users' keys. Let Γ_i be the set of all possible messages of U_i. Given a set $T = \{i_1,i_2,\ldots,i_t\} \subseteq \{1,2,\ldots,n\}$, where $i_1 < i_2 < \ldots < i_t$, denote with Γ_T the set $\Gamma_{i_1} \times \cdots \times \Gamma_{i_t}$. The center's algorithm and the users' algorithms define a probability distribution on $\Gamma_1 \times \cdots \times \Gamma_n$, that, in turn, naturally induces a probability distribution $\{p_{\Gamma_T}(\gamma)\}_{\gamma\in\Gamma_T}$ on Γ_T, for any set $T \in 2^{[n]}$.

Let $H(\Gamma_T) = H(\Gamma_{i_1}\ldots\Gamma_{i_r})$ be the entropy of the probability distribution on $\Gamma_T = \Gamma_{i_1} \times \cdots \times \Gamma_{i_t}$. Given a set $T = \{i_1,\ldots,i_t\} \in 2^{[n]}$, with k_T we denote the common key established by users $U_{i_1},\ldots,U_{i_t}$, whereas with $\mathcal{K}_T$ we denote the set of all possible values of the common key k_T.

Formally, we define an interactive zero-message $(\mathcal{T},\mathcal{V})$ broadcast encryption scheme for n users as follows.

Definition 10. Let $\mathcal{U} = \{U_1,U_2,\ldots,U_n\}$ be a set of n users and let $\mathcal{T},\mathcal{V} \subseteq 2^{[n]}$. An *interactive zero-message* $(\mathcal{T},\mathcal{V})$ *broadcast encryption scheme* for $\mathcal{U}$ is a distribution protocol such that for any $T = \{i_1,\ldots,i_t\} \in \mathcal{T}$, there hold

1. *Any privileged user can interactively (after an exchange of messages among the users in T) compute the common key k_T.*
   Formally, for all $i \in T$, we have $H(\mathcal{K}_T|U_i\ \Gamma_i) = 0$.
2. *Any coalition of non-privileged users in $\mathcal{V}$ even knowing the conversations of all the possible privileged sets, has absolutely no information on the common key $\mathcal{K}_T$.*
   Formally, for all $V \in \mathcal{V}$ such that $V \cap T = \emptyset$, we have $H(\mathcal{K}_T|U_S\ \Gamma_{T_1} \dots \Gamma_{T_{|\mathcal{T}|}}) = H(\mathcal{K}_T)$.

As we have done in section 2, it is possible to define both interactive $\mathcal{V}$-resilient and interactive k-resilient schemes. We can prove that, under the hypothesis of Definition 10, the same bounds of Section 2 hold. Hence, we get

1. In any interactive zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme for $\mathcal{U}$, if for any $T \in \mathcal{T}$ we have $\{1, 2, \dots, n\} \backslash T \in \mathcal{V}$, then the entropy $H(U_i)$, for $i = 1, \dots, n$, satisfies $H(U_i) \geq \tau_i H(\mathcal{K})$, where $\tau_i = |\{T \in \mathcal{T} \ :\ i \in T\}|$.
2. In any interactive zero-message $\mathcal{V}$-resilient broadcast encryption scheme for $\mathcal{U}$, the entropy $H(U_i)$, for $i = 1, \dots, n$, satisfies $H(U_i) \geq v_i H(\mathcal{K})$, where $v_i = |\{V \in \mathcal{V} \ :\ i \notin V\}|$.
3. In any interactive zero-message k-resilient broadcast encryption scheme for $\mathcal{U}$, with $k < n$, the entropy $H(U_i)$ satisfies $H(U_i) \geq \sum_{j=0}^{k} \binom{n-1}{j} H(\mathcal{K})$.

We have seen that the interaction cannot decrease the size of the pieces of information given to the users in the broadcast encryption schemes. So, in order to decrease the size of the information distributed, we relax the security requirement. We allow that the interactive broadcast encryption scheme be secure only a fixed number of times, say ℓ. In this situation at most ℓ sets can subsequently recover a common key, but which set will be enabled to reconstruct the common key is not known a-priori. Hence, the center has to distribute pieces of information in such a way that any possible set could be a privileged set (akin to what happen in the general case of interactive zero-message broadcast encryption). An ℓ-time interactive broadcast encryption scheme is defined as follows.

Definition 11. Let $\mathcal{U} = \{U_1, U_2, \dots, U_n\}$ be a set of n users and let $\mathcal{T}, \mathcal{V} \subseteq 2^{[n]}$. An *$\ell$-time interactive zero-message $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme* for $\mathcal{U}$ is a distribution protocol such that for any $T = \{i_1, \dots, i_t\} \in \mathcal{T}$, there hold

1. *Any privileged user can interactively (after an exchange of messages among the users in T) compute the common key k_T.*
   Formally, for all $i \in T$, we have $H(\mathcal{K}_T|U_i\ \Gamma_i) = 0$.
2. *Any coalition of non-privileged users in $\mathcal{V}$ even knowing the conversations of any ℓ among all the possible privileged sets, has absolutely no information on the common key k_T.*
   Formally, for all $V \in \mathcal{V}$ such that $V \cap T = \emptyset$ and for all $j_1, \dots, j_\ell \in \{1, 2, \dots, n\}$, we have $H(\mathcal{K}_T|U_S\ \Gamma_{T_1} \dots \Gamma_{T_\ell}) = H(\mathcal{K}_T)$.

Beimel and Chor [1] proposed an interactive k-secure t-conference key distribution scheme (for definition and notation on k-secure t-conference key distribution schemes see [3, 1]) such that for a domain of key $\mathcal{K}$ the cardinality of pieces of every user is $|\mathcal{K}|^{2+2(k-1)/t}$. Their protocol is based on the non-interactive k-secure t-conference scheme proposed by Blom [2]. In the protocol we propose, the domain of keys for a privileged set of size t will be of cardinality q^t and, since the Blom's scheme is used, q must be a prime power greater than or equal to $\sqrt{n}$. Basically, our protocol, depicted in Figure 1., is that proposed by Beimel and Chor [1] adapted to handle the case of one-time interactive zero-message k-resilient broadcast encryption.

The protocol for 1-time interactive zero-message k-resilient broadcast encryption schemes for n users is the following.

Protocol 2

PREPROCESSING PHASE

1. The center distribute to any user U_i a independent key $k_{i,\mathrm{C}} \in \mathbf{Z}_q$, where $q \geq \sqrt{n}$ is a prime power.
2. The center distributes other keys to users according to the Blom's non-interactive $(n-2)$-secure 2-conference scheme for n users with keys taken from $\mathbf{Z}_{q^2}$.

KEY-COMPUTATION PHASE

3. Let $T \in 2^{[n]}$. Each user U_i, with $i \in T$, randomly chooses a key $k_i \in \mathbf{Z}_q$.
4. If $T = \{i\}$, then the user U_i sends to C the message $k_i + k_{i,\mathrm{C}} \bmod q$.
5. If $|T| > 1$, then the common key k_T is computed as follows.

   5.1. Each pair of user U_i, U_j, with $i, j \in T$, reconstruct a common key $k_{i,j} \in \mathbf{Z}_{q^2}$. View the joint key as consisting of two sub-keys $k'_{i,j}$ $k''_{i,j}$, both in $\mathbf{Z}_q$.

   5.2. Each user U_i, with $i \in T$, broadcasts to each other user U_j, where $j \in T \backslash \{i\}$, the values

$$k_i + k'_{i,j} \bmod q \text{ if } i < j$$
$$k_i + k''_{i,j} \bmod q \text{ if } i > j.$$

   5.3. The common key k_T is the concatenation of the random k_i's, with $i \in T$. Hence, for $T = \{i_1, i_2, \ldots, i_t\}$, the key k_T will be

$$k_T = k_{i_1} \circ k_{i_2} \circ \cdots \circ k_{i_t}$$

Figure 1.

The above protocol realizes a 1-time interactive zero-message k-resilient broadcast encryption scheme as stated in the next theorem.

Theorem 12. Protocol 2 *realizes a one-time interactive zero-message k-resilient broadcast encryption scheme for a set of n users in which the domain of pieces of every user is $q^{2(n-1)}$ and the common key of each privileged set T of size t is chosen in a set of cardinality q^t.*

Clearly, a scheme for an ℓ-time interactive zero-message k-resilient broadcast encryption scheme can be constructed by considering ℓ copies of the scheme realized with Protocol 2.

4 Broadcast Encryption

In this section we analyze broadcast encryption schemes, that is schemes secure against coalitions of non-privileged users in which the center is required to broadcast some messages in order for the member of the privileged set to generate a common key.

The center, in a preprocessing phase, knowing neither the privileged set nor the value of the common key, generates and distributes some keys to participants in $\mathcal{U}$. The center, in the broadcast-encryption phase, on input the set $T = \{i_1, \ldots, i_t\}$, the common key k_T and the informations given to users in the preprocessing phase, computes the messages $b_{i_1}, \ldots, b_{i_t}$ and broadcasts it to users $U_{i_1}, \ldots, U_{i_t}$ respectively. At the end of the broadcast encryption phase, only the users U_i's, with $i \in T$, are able to compute the common key k_T. The common key k_T will be secure against every non-privileged set of user. A natural requirement is that any coalition of non-privileged users has absolutely no information on the common key k_T even knowing the broadcast messages of all other coalition of users. Let us denote with B_i the set of all possible broadcast messages for user U_i, and let $B_T = B_{i_1} \times \cdots \times B_{i_t}$. For any $T \in \mathcal{T}$, the probability distribution on $\mathcal{K}_T$ induces a probability distribution $\{p_{B_T}(b)\}_{b \in B_T}$ on B_T. Let $H(B_T)$ be its entropy.

We define a $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme as follows.

Definition 13. Let $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ be a set of n users and let $\mathcal{T}, \mathcal{V} \subseteq 2^{[n]}$. A $(\mathcal{T}, \mathcal{V})$ *broadcast encryption scheme* for $\mathcal{U}$ is a distribution protocol such that for any $T = \{i_1, \ldots, i_t\} \in \mathcal{T}$, there hold

1. *Before knowing the broadcast messages any subset of users has no information on the value of the common key k_T.*
   Formally, for all $X \subseteq \{1, 2, \ldots, n\}$ it holds that $H(\mathcal{K}_T | U_X) = H(\mathcal{K}_T)$.
2. *After seeing the broadcast message, any privileged user can compute the common key k_T.*
   Formally, for all $i \in T$, it holds that $H(\mathcal{K}_T | U_i B_i) = 0$.
3. *Any coalition of non-privileged users has absolutely no information on the common key k_T, even knowing the broadcast messages of all the possible privileged sets.*
   Formally, for all $V \in \mathcal{V}$ such that $V \cap T = \emptyset$, it holds that $H(\mathcal{K}_T | U_V B_{T_1} \ldots B_{T_{|T|}})$ $= H(\mathcal{K}_T)$.

The next simple theorem states a lower bound on the size of each broadcast message in a $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme.

Theorem 14. *Let $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ be a set of n users and let $\mathcal{T}, \mathcal{V} \subseteq 2^{[n]}$. In any $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme for $\mathcal{U}$, the entropy $H(B_i)$ satisfies $H(B_i) \geq H(\mathcal{K})$.*

As we have done in section 2, it is possible, in this more general setting, to define $\mathcal{V}$-resilient broadcast encryption schemes as well as k-resilient broadcast encryption schemes. We can prove that, under the hypothesis of Definition 13, the same bounds of Section 2 hold. Hence, we get

1. In any $(\mathcal{T}, \mathcal{V})$ broadcast encryption scheme for $\mathcal{U}$, if for any $T \in \mathcal{T}$ we have $\{1, 2, \ldots, n\} \backslash T \in \mathcal{V}$, then, for $i = 1, \ldots, n$, the entropy $H(U_i)$ satisfies $H(U_i) \geq \tau_i H(\mathcal{K})$, where $\tau_i = |\{T \in \mathcal{T} \ : \ i \in T\}|$.
2. In any $\mathcal{V}$-resilient broadcast encryption scheme for $\mathcal{U}$, for $i = 1, \ldots, n$, the entropy $H(U_i)$ satisfies $H(U_i) \geq v_i H(\mathcal{K})$, where $v_i = |\{V \in \mathcal{V} \ : \ i \notin V\}|$.
3. In any k-resilient broadcast encryption scheme for $\mathcal{U}$, with $k < n$, the entropy $H(U_i)$ satisfies $H(U_i) \geq \sum_{j=0}^{k} \binom{n-1}{j} H(\mathcal{K})$.

References

1. A. Beimel and B. Chor, *Interaction in Key Distribution Schemes*, in "Advances in Cryptology - CRYPTO 93", D.R. Stinson Ed., "Lecture Notes in Computer Science", Vol. 773, Springer-Verlag, Berlin, 1994, pp. 444–457.
2. R. Blom, *An Optimal Class of Symmetric Key Generation Systems*, in "Advances in Cryptology - Eurocrypt 84" "Lecture Notes in Computer Science", Vol. 209, Springer-Verlag, Berlin, 1984, pp. 335–338.
3. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, *Perfectly-Secure Key Distribution for Dynamic Conferences*, in "Advances in Cryptology - CRYPTO 92", E. Brickell Ed., "Lecture Notes in Computer Science", Vol. 740, Springer-Verlag, Berlin, 1993, pp. 478–493.
4. I. Csiszár and J. Körner, *Information Theory. Coding Theorems for Discrete Memoryless Systems,* Academic Press, 1981.
5. A. Fiat and M. Naor, *Broadcast Encryption*, in "Advances in Cryptology - CRYPTO 93", D.R. Stinson Ed., "Lecture Notes in Computer Science", Vol. 773, Springer-Verlag, Berlin, 1994, pp. 480–491.
6. R. G. Gallager, *Information Theory and Reliable Communications*, John Wiley & Sons, New York, NY, 1968.
7. L. Gong and D.J. Wheeler, *A Matrix Key-Distribution Scheme*, Journal of Cryptology, Vol. 2, 1990, pp. 51–59.
8. T. Matsumoto and H. Imai, *On the Key Predistribution System: A Practical Solution to the Key Distribution Problem*, in "Advances in Cryptology - CRYPTO 87", "Lecture Notes in Computer Science", Vol. 239, Springer-Verlag, Berlin, 1987, pp. 185–193.