A Unified Model for Unconditionally Secure Key Distribution

Stelvio Cimato[1], Paolo D'Arco[1], and Antonella Cresti[2]

[1] Dipartimento di Informatica ed Applicazioni
Università di Salerno, 84081 Baronissi (SA), Italy
e-mail: {cimato, paodar}@dia.unisa.it

[2] Dipartimento di Scienze dell'Informazione
Università di Roma "La Sapienza", 00198 Roma, Italy
e-mail: cresti@dsi.uniroma1.it

Abstract. A key distribution scheme is a method by means of which a trusted party distributes 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. In this paper we present a model for unconditionally secure key distribution schemes, i.e., schemes whose security is independent of the power of the adversary. We prove lower bounds on the amount of information the trusted party has to generate and each user has to keep secret in such schemes, and we show that some previous unconditionally secure models for key distribution fall in our model. As a consequence, the lower bounds given in the literature for these models can be seen as corollaries of our results. Hence, the main contribution of the paper consists in pointing out a sort of common structure underlying some apparently different key distribution techniques.

Key words. Key distribution, information theory, broadcast encryption.

1 Introduction

Secure Communication. Historically secure communication is the first issue studied in Cryptography. Despite many years of researches and scientific contributions, it is still a major area of interest in the cryptographic community. Indeed, the increase in bandwith, size, and usage of traditional communication networks and distributed systems, and the spread diffusion of different typologies of devices for wireless communications, have provided new possibilities as well as new security challenges that require technological answers. A growing application area is *conferencing*, where a group of users or entities of a certain network collaborate interactively in a common task. Such a task can be a simple chat among friends, a business meeting, a video conference among formal representatives of many countries, a task-force operation in a highly dangerous environment and so on. All of the above tasks might require secure communication.

Public key algorithms provide certainly a solution and can be employed in order to get secure communication. However, due to the large sizes of the groups of users that might be involved in such tasks, and due to the efficiency of symmetric algorithms, which are in terms of computation several orders of magnitude better than public key algorithms, in practice symmetric algorithms are preferible. Therefore, assuming the group of users agrees on securing its communication by means of symmetric primitives, the preliminary problem that must be solved is how to establish common keys. Several methods have been proposed in the literature: The reader is referred to [47, 59] for a detailed overview, and to [9] for a simple introduction to the key establishment problem. In this paper our attention will focus only on some unconditionally secure key distribution schemes.

Key Distribution Schemes. A key distribution scheme is a method by means of which a trusted party distributes 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. The scheme is said to be *unconditionally secure* if its security is independent of the power of the adversary.

A basic and straightforward unconditional secure scheme consists in distributing common keys to the users: more precisely, each user gets from the trusted party one key for each group in which he belongs to. The drawback of this solution is that the trusted party has to generate an *exponential* number of keys, one for each possible subset of the set of users, and each user has to store an *exponential* number of keys. Given the high complexity of such a distribution mechanism, schemes where security is traded with complexity were introduced. In [6], Blom proposed a scheme where keys are still unconditionally secure, but only with respect to coalitions of a limited size. This approach enables saving upon the number of keys the trusted party has to generate and the user must store. Schemes related to [6] were given in [33, 46].

Later on, generalizing the approach of [6] for pairs of users, Blundo et al. [13], considered unconditionally secure key distribution schemes for groups of users of a given size. Their schemes have two parameters: t denoting the size of the groups that share a common key, and w denoting the size of the coalitions of adversaries. These schemes are referred to as *w-secure t-conference key distribution schemes*. Moreover, the authors proved a tight lower bound on the size of the user's piece of information. The bound establishes that the basic scheme, Blom's scheme [6], and Blundo's et. al scheme [13], are the best that can be done, since both can be seen as special cases of w-secure t-conference key distribution schemes. To reduce the amount of information the trusted party has to generate and the users have to keep secret in an unconditionally secure key distribution scheme, unconditionally secure *key agreement schemes* were introduced in [13]. Basically, in these schemes, interaction among users is allowed in order to compute a common key. Unfortunately, Beimel and Chor [2, 3] showed that it does not help in decreasing user memory storage requirements.

Berkovitz first [5] and Fiat and Naor later on [29] proposed a new key distribution paradigm, designed for broadcast transmissions. In this setting, a central broadcast site broadcasts a message enabling a *privileged* subset of users to recover a common key which can be used for secure broadcast transmissions. The common key is secure against coalitions of at most k users disjoint from the privileged set. In [7], by using an information theoretic approach, the authors generalized the model given in [29], and showed that the first scheme therein presented, referred to as the *zero-message* scheme, is optimal with respect to both the amount of information each user stores, and to the amount of information the center has to generate.

Chiou and Chen [20] also considered the problem of broadcasting a secure key to a group of users. A different implementation of their scheme was subsequently given in [44]. Different approaches for broadcasting a common key, based on secret sharing schemes, were given in [5, 43]. The drawback of such schemes is that they are *one-time*, i.e., they can be used only once; afterwards, the common key is not secure anymore. Broadcast encryption was further analyzed in [35, 21, 60, 16, 45, 8].

Just et al. [35] proposed a scheme, based on the one given in [5], which preserves users' anonimity. Indeed, the broadcast message sent by the broadcaster in order to provide the common key to the privileged group, does not contain any information regarding the users in the group. Moreover, each user in the privileged set computes the common key from the broadcast message but gets no infomation about the identity of any other user of the group. The drawback of this scheme is that it is also one time. Other results on broadcast encryption schemes preserving users' anonymity can be found in [14].

In [16, 15] the authors describe some variations and generalizations of the Beimel-Chor scheme, including broadcast encryption schemes as well as key agreement schemes. An excellent survey of unconditionally secure key distribution schemes was given in [60].

In order to deal with security concerns related to the use of a *single* trusted party in key distribution schemes, a distributed implementation of some key distribution schemes was proposed in [42]. Recently, a different model for the distribution of the center was proposed in [51]. The unconditionally secure version of this model has been subsequently studied in [12, 24, 10, 25].

Other research directions. Due to the large number of possible applications, broadcast encryption has become a major topic in Cryptography, and it has evolved in several directions. These directions include multicast communications [65, 18, 19, 54, 55, 27], where the privileged subset of recipients *dynamically* changes by means of join and remove operations; traitor tracing [22, 53, 28, 17, 63, 4, 32, 30, 56, 58, 36, 37], where the emphasis is on catching dishonest users who set up illegal decrypting devices; and revoking schemes [1, 50, 39, 49, 34, 40], which allow efficient and fast revocation of a small group of users. Moreover, several schemes presented in the literature achieve more than one of the above-mentioned aspects, e.g., broadcast plus traitor tracing capabilities [31, 62, 61, 64], or revocation and tracing capabilities [50, 49, 34]. Very recently, some papers have considered a setting in which packets can get lost during transmission [52, 66, 57, 41], i.e., the traditional assumption of a reliable underlying network in the design of broadcast-like encryption schemes, has been removed. Finally, [26], has reviewed and extended existing broadcast encryption schemes, in order to gain fault tolerance and to remove the need for trust in the broadcaster, assumption which may not hold in a variety of applicative settings.

Contribution of this paper. In this paper we provide a concise model, based on an information theoretical framework, for unconditionally secure key distribution schemes. Basically, we show that unconditionally secure key predistribution schemes, key agreement schemes, and broadcast encryption schemes, can be seen as instances of a unique model. Notice that in [60], the author did some steps towards a unified description of unconditionally secure key distribution schemes. In a certain way, this paper continues and generalises the unifying description process therein started. Moreover, we prove tight lower bounds on the amount of information each user in such a model has to keep secret, and on the amount of secret information the trusted party has to generate extending the results in [7]. Finally, we point out that previous lower bounds for key predistribution schemes, key agreement and broadcast encryption schemes, can be seen as corollaries of our results.

Organization of the Paper. In Section 2, using an information theoretic framework, we give the definition of a model for unconditional secure key distribution schemes. In Section 3, we prove lower bounds on the amount of information the center has to generate and each user has to keep secret in the scheme, pointing out relations among the number of keys held by each user and the parameters describing the security of the scheme. Finally, in Sections 4, we analyze unconditionally secure key predistribution schemes, key agreement schemes, and broadcast encryption schemes, respectively. We show how they can be seen as instances of our model for unconditionally secure key distribution schemes, and we show that previous lower bounds for these schemes can be derived as corollaries of our results.

2 The Model

In this section we present a unifying model for unconditional secure key distribution schemes relying on an information theorethic framework. We use the entropy approach mainly because it leads to a simple, compact, and elegant description of the scheme, and because this approach takes into account all the probability distributions on the keys. In Appendix, some basic concepts and properties of entropy are introduced.

Informal description. Our scenario consists of a center $\mathcal{C}$, also referred to as *Trusted Authority*, a set of users $\mathcal{U} = \{1, \ldots, n\}$, and two collections, say $\mathcal{P}$ and $\mathcal{F}$, of subsets of $\mathcal{U}$. $\mathcal{P}$ denotes the *privileged* subsets of users, enabled to compute a common key; $\mathcal{F}$ denotes the *forbidden* subsets, not allowed to gain any information about the keys. A key distribution scheme is divided into two phases: a *distribution phase* and a *key computation phase*. During the distribution phase, the center $\mathcal{C}$ gives some information, sometimes referred to as *predefined* keys, to the users in $\mathcal{U}$. In the key computation phase, a privileged subset $P \in \mathcal{P}$ of users, from the information received from the center during the distribution phase, and from the "view" of the communication the users in P have during the execution of such a phase, recovers a common key k_P. The view consists of the concatenation of all messages sent either by the same users in P or by the trusted authority. The common key k_P is unconditionally secure against any forbidden set $F \in \mathcal{F}$ of users disjoint from P, i.e., the users in F have no information on this common key, even if they have an infinite computational power.

During the distribution phase the center does not know which privileged subset will later recover a common key.

TOPOLOGY OF THE NETWORK. We assume that the network is synchronous. The center shares a *secure point-to-point channel* with every user. Moreover, users and center have access to an authenticated broadcast channel.

FORMAL DESCRIPTION. Let U_i be the set of possible values user i can receive. The center, during the distribution phase, for $i = 1, \ldots, n$, distributes to user i a piece of information $u_i \in U_i$, chosen according to the probability distribution[1] $\{Pr_{\mathbf{U}_i}(u)\}_{u \in U_i}$. Let K_P denote the set of possible values the common key k_P can assume, according to the probability distribution $\{p_{\mathbf{K}_P}(k)\}_{k \in K_P}$, and let $H(\mathbf{K}_P)$ be the entropy of such a probability distribution. Finally, let V_i be the set of possible concatenations of messages v_i that can be seen by user i along the broadcast channel. Such v_i's are sampled in V_i according to the probability distribution $\{Pr_{\mathbf{V}_i}(v)\}_{v \in V_i}$, induced by the information held by each user, and by the algorithm which defines the key computation phase. Let $H(\mathbf{V}_i)$ be the entropy of this probability distribution. In the key computation phase, every user i in the privileged subset P, computes the common key k_P by using the information received from the center during the distribution phase and v_i.

Using the above concepts and notation, we can state the following definition:

Definition 2.1 *Let $\mathcal{U} = \{1, \ldots, n\}$ be a set of n users, let $\mathcal{P} \subseteq 2^{\mathcal{U}}$ be a family of privileged subsets of users, and let $\mathcal{F} \subseteq 2^{\mathcal{U}}$ be a family of forbidden subset of users. A* $(\mathcal{P}, \mathcal{F})$ key distribution scheme *($(\mathcal{P}, \mathcal{F})$-KDS, for short) is a distribution protocol divided into two phases, a distribution phase and a key computation phase, such that:*

1. Every user i in a privileged subset P can compute the common key k_P by using the private information u_i and his own view v_i. More precisely: *For any $P \in \mathcal{P}$ and for any $i \in P$, it holds that*
$$H(\mathbf{K}_P | \mathbf{U}_i \mathbf{V}_i) = 0.$$
2. Any forbidden coalition of users has absolutely no information on the common key k_P, even if it has access to the views users belonging to privileged subsets have had during the executions of the key computation phases. More precisely: *For any $P \in \mathcal{P}$ and for all $F \in \mathcal{F}$ such that $F \cap P = \emptyset$, it holds that*
$$H(\mathbf{K}_P | \mathbf{U}_F \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_{|\mathcal{P}|}}) = H(\mathbf{K}_P).$$

Notice that Definition 2.1 deals with a *passive* adversary, i.e., coalitions of users only try to get information on common keys by using their own private information and the transcript of the communication which has taken place along the public channel. Active attacks are not considered.

The above model implies some simple consequences which we state as remarks for the reader convenience and to simplify the proofs of the results provided later on.

Remark 1. Notice that, from Property 2 of Definition 2.1, it easily follows that, for any $j = 1, 2, \ldots, |\mathcal{P}|$,

$$H(\mathbf{K}_P | \mathbf{U}_F \ \mathbf{V}_{P_{i_1}} \ldots \mathbf{V}_{P_{i_j}}) = H(\mathbf{K}_P) \text{ and } H(\mathbf{K}_P | \mathbf{V}_{P_{i_1}} \ldots \mathbf{V}_{P_{i_j}}) = H(\mathbf{K}_P). \quad (1)$$

Remark 2. Definition 2.1 does not say anything about the entropies of the random variables $\mathbf{K}_P$ and $\mathbf{K}_{P'}$, for different $P, P' \in \mathcal{P}$. For example, we could have either $H(\mathbf{K}_P) > H(\mathbf{K}_{P'})$ or $H(\mathbf{K}_P) \leq H(\mathbf{K}_{P'})$. Our results apply to the general case of arbitrary entropies on the keys, but for clarity we assume that all entropies are equal, i.e., $H(\mathbf{K}_P) = H(\mathbf{K}_{P'})$. We denote this entropy simply by $H(\mathbf{K})$.

[1] In this paper with a boldface capital letter, say $\mathbf{X}$, we denote a random variable taking value on a set denoted by the corresponding capital letter X, according to some probability distribution $\{Pr_{\mathbf{X}}(x)\}_{x \in X}$. The values such a random variable can take are denoted by the corresponding lower letter. Moreover, if for $i = 1, \ldots, n$, $\mathbf{X}_i$ (x_i) is a random variable (value) and $W = \{j_1, \ldots, j_m\} \subseteq \{1, \ldots, n\}$ is a subset of indices, then $\mathbf{X}_W$ (x_W) denotes the random variable $\mathbf{X}_{j_1} \ldots \mathbf{X}_{j_m}$ (the value $x_{j_1} \ldots x_{j_m}$).

3 Lower Bounds

In this section we prove some lower bounds on the amount of information each user in any $(\mathcal{P}, \mathcal{F})$ key distribution scheme has to keep secret, and the center has to generate. Before proving our results, we need some technical lemmas.

Lemma 3.1 *Let* $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$, *and* $\mathbf{W}$ *be four random variables. If* $H(\mathbf{X}|\mathbf{YW}) = 0$, *then the following inequalities hold:*

$$1. \quad H(\mathbf{Y}|\mathbf{W}) \geq H(\mathbf{X}|\mathbf{W}) \quad 2. \quad H(\mathbf{Y}) \geq H(\mathbf{X}|\mathbf{W}) \quad 3. \quad H(\mathbf{Z}|\mathbf{XW}) \geq H(\mathbf{Z}|\mathbf{YW}).$$

Proof: Property *1.* simply follows from (8) and (10) of Appendix A. Indeed, from (8), we have that $I(\mathbf{X};\mathbf{Y}|\mathbf{W}) = H(\mathbf{X}|\mathbf{W}) - H(\mathbf{X}|\mathbf{YW}) = H(\mathbf{X}|\mathbf{W})$. Then, from (10), we have that $H(\mathbf{Y}|\mathbf{W}) \geq I(\mathbf{X};\mathbf{Y}|\mathbf{W}) = H(\mathbf{X}|\mathbf{W})$. Property *2.* directly follows from Property *1.*, applying (7) of Appendix A. Indeed, $H(\mathbf{Y}) \geq H(\mathbf{Y}|\mathbf{W}) \geq H(\mathbf{X}|\mathbf{W})$. Finally, Property *3.* can be shown by noticing that, from (10) of Appendix A and $H(\mathbf{X}|\mathbf{YW}) = 0$, we have that $H(\mathbf{Z}|\mathbf{XYW}) = H(\mathbf{Z}|\mathbf{YW})$. Indeed, $0 = H(\mathbf{X}|\mathbf{YW}) \geq I(\mathbf{X};\mathbf{Z}|\mathbf{YW}) = H(\mathbf{Z}|\mathbf{YW}) - H(\mathbf{Z}|\mathbf{XYW}) \geq 0$. Therefore, applying (9) of Appendix A, and using the above equality, we have that $H(\mathbf{Z}|\mathbf{XW}) \geq H(\mathbf{Z}|\mathbf{XYW}) = H(\mathbf{Z}|\mathbf{YW})$. □

The first implication of the above model is *independence of the keys.* More precisely, if a key k_X is secure against a set of users Z, then it is independent of all the keys k_{Y_i} the users in Z can compute and of the public available information. Such a result holds because Property 2 of Definition 2.1 requires independence of each key from the private information u_Z, held by Z, and the public available information $v_{P_1} \ldots v_{P_{|\mathcal{P}|}}$. Since keys k_{Y_i} *can be computed* by Z from u_Z and the public available information, they cannot give to Z more information than the one Z already has. Formally, we can state the result as follows:

Lemma 3.2 *Let* $\mathcal{U}$ *be a set of* n *users, let* r *be an integer, and let* $\mathcal{P}, \mathcal{F} \subseteq 2^{\mathcal{U}}$. *Finally, let* $X, Y_1, \ldots, Y_r, Z \subseteq \mathcal{U}$ *such that* $X, Y_1, \ldots, Y_r \in \mathcal{P}$, $Z \in \mathcal{F}$, $Z \cap X = \emptyset$ *and, for* $i = 1, \ldots, r$, $Z \cap Y_i \neq \emptyset$. *Then, in any* $(\mathcal{P}, \mathcal{F})$ *key distribution scheme it holds that*

$$H(\mathbf{K}_X|\mathbf{K}_{Y_1} \ldots \mathbf{K}_{Y_r} \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_{|\mathcal{P}|}}) = H(\mathbf{K}_X).$$

Proof: Notice that, from (7) of Appendix A we have $H(\mathbf{K}_X) \geq H(\mathbf{K}_X|\mathbf{K}_{Y_1} \ldots \mathbf{K}_{Y_r} \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_{|\mathcal{P}|}})$. Therefore, to prove the lemma, it is enough to show that $H(\mathbf{K}_X|\mathbf{K}_{Y_1} \ldots \mathbf{K}_{Y_r} \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_{|\mathcal{P}|}}) \geq H(\mathbf{K}_X)$. To this aim notice that, from (4) and (9) of Appendix A, and from *1* of Definition 2.1, we have that

$$H(\mathbf{K}_{Y_1} \ldots \mathbf{K}_{Y_r}|\mathbf{U}_Z \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_{|\mathcal{P}|}}) \leq \sum_{j=1}^{r} H(\mathbf{K}_{Y_j}|\mathbf{U}_Z \mathbf{V}_{Y_j}) = 0.$$

Therefore, setting $\mathbf{X} = \mathbf{K}_{Y_1} \ldots \mathbf{K}_{Y_r}$, $\mathbf{Y} = \mathbf{U}_Z$, $\mathbf{Z} = \mathbf{K}_X$, and $\mathbf{W} = \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_{|\mathcal{P}|}}$, we get

$$\begin{aligned} H(\mathbf{K}_X|\mathbf{K}_{Y_1} \ldots \mathbf{K}_{Y_r} \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_{|\mathcal{P}|}}) &\geq H(\mathbf{K}_X|\mathbf{U}_Z \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_{|\mathcal{P}|}}) \text{ (from } \mathit{3.} \text{ of Lemma 3.1)} \\ &= H(\mathbf{K}_X) \text{ (from } \mathit{2.} \text{ of Definition 2.1)} \end{aligned}$$

which proves the lemma. □

This result plays an important role in the rest of the paper. Indeed, we prove two lower bounds on the amount of information each user has to keep secret and both are derived by using independence of the keys and some assumptions on the structure of the pair $(\mathcal{P}, \mathcal{F})$.

The first lower bound holds when, for any $P \in \mathcal{P}$, the family $\mathcal{F}$ *contains the complement* of P with respect to $\mathcal{U}$. The bound basically says that user i has to keep secret at least as many predefined keys as given by the number of privileged subsets P in which he belongs to. The intuition behind the result is the following: For each privileged subset P, k_P is independent of all the keys of the other privileged subsets Q. Indeed, $Q \neq P$ implies $Q \cap \mathcal{U} \setminus P \neq \emptyset$. Since the complement of P is forbidden, k_P and k_Q are independent. In particular, keys associated with overlapping privileged subsets are jointly independent. Since the privileged subsets P which user i belongs to are overlapping at least in i, then it follows that the user has to store at least as much information as provided by the keys associated with all the privileged subsets P in which he belongs to. The intuition can be formalised has follows:

Theorem 3.3 *Let $\mathcal{U}$ be a set of n users and let $\mathcal{P}, \mathcal{F} \subseteq 2^{\mathcal{U}}$ be two collections of privileged and forbidden subsets such that, for any privileged subset $P \in \mathcal{P}$, it holds that $\mathcal{U} \setminus P \in \mathcal{F}$. Then, in any $(\mathcal{P}, \mathcal{F})$ key distribution scheme, the entropy $H(\mathbf{U}_i)$, for $i = 1, \ldots, n$, satisfies*

$$H(\mathbf{U}_i) \geq \pi_i H(\mathbf{K}),$$

where $\pi_i = |\{P \in \mathcal{P} \ : \ i \in P\}|$.

Proof: Let us assume that $\{P \in \mathcal{P} : i \in P\} = \{P_1, \ldots, P_{\pi_i}\}$. Properties (4) and (9) of Appendix A, and Property *2.* of Definition 2.1 imply that

$$H(\mathbf{K}_{P_1} \ldots \mathbf{K}_{P_{\pi_i}} | \mathbf{U}_i \ \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_\pi}) \leq \sum_{j=1}^{\pi_i} H(\mathbf{K}_{P_j} | \mathbf{U}_i \ \mathbf{V}_{P_j}) = 0.$$

Setting $\mathbf{X} = \mathbf{K}_{P_1} \ldots \mathbf{K}_{P_{\pi_i}}$, $\mathbf{Y} = \mathbf{U}_i$, $\mathbf{W} = \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_\pi}$, and applying Property *2.* of Lemma 3.1, it holds that

$$\begin{aligned} H(\mathbf{U}_i) &\geq H(\mathbf{K}_{P_1} \ldots \mathbf{K}_{P_{\pi_i}} | \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_\pi}) \\ &= H(\mathbf{K}_{P_1} | \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_\pi}) + \sum_{\ell=2}^{\pi_i} H(\mathbf{K}_{P_\ell} | \mathbf{K}_{P_1} \ldots \mathbf{K}_{P_\ell} \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_\pi}) \quad \text{(from (4) of App. A)} \\ &= H(\mathbf{K}_{P_1}) + \sum_{\ell=2}^{\pi_i} H(\mathbf{K}_{P_\ell} | \mathbf{K}_{P_1} \ldots \mathbf{K}_{P_\ell} \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_\pi}) \quad \text{(from property (1))}. \end{aligned}$$

Let us define, for $2 \leq \ell \leq \pi_i$, the subsets $X = P_\ell$, $Z = \mathcal{U} \setminus P_\ell$ and, for $j = 1, \ldots, \ell - 1$, the subsets $Y_j = P_j$. It is not difficult to see that these subsets satisfy the hypothesis of Lemma 3.2. Hence, $H(\mathbf{K}_{P_\ell} | \mathbf{K}_{P_1} \ldots \mathbf{K}_{P_{\ell-1}} \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_\pi}) = H(\mathbf{K}_{P_\ell})$. Therefore,

$$H(\mathbf{U}_i) \quad \geq \quad \sum_{\ell=1}^{\pi_i} H(\mathbf{K}_{P_\ell}) = \pi_i H(\mathbf{K}).$$

Thus, the theorem holds. □

To set up a cryptographic protocol we need random bits. This resource is usually referred to as the *randomness* of the scheme. The randomness of a scheme can be measured in different way. Knuth and Yao [38] proposed the following approach: Let `Alg` be an algorithm that generates the probability distribution $P = \{p_1, \ldots, p_n\}$, using only independent and unbiased random bits. Denote by $T(\texttt{Alg})$ the average number of random bits used by `Alg` and let $T(P) = min_{\texttt{Alg}} T(\texttt{Alg})$. The value $T(P)$ is a measure of the average number of random bits needed to simulate the source described by the probability distribution P. In [38] it has been shown the following result

Theorem 3.4 $H(\mathbf{P}) \leq T(\mathbf{P}) < H(\mathbf{P}) + 2.$

Thus, the entropy of a random source is *very close* to the average number of unbiased random bits necessary to simulate the source. Hence, it is a natural measure of the randomness.

Let $R(\mathcal{F},\mathcal{P})$ be the randomness needed to set-up a key distribution scheme. Denoting by $\mathbf{K} = \mathbf{K}_1,\ldots,\mathbf{K}_{|\mathcal{P}|}$, by $\mathbf{U} = \mathbf{U}_1,\ldots,\mathbf{U}_n$, and by $\mathbf{V} = \mathbf{V}_1,\ldots,\mathbf{V}_n$, and applying the above result, it holds that

$$R(\mathcal{F},\mathcal{P}) \geq H(\mathbf{K},\mathbf{U},\mathbf{V}).$$

However, applying properties (4) and (7), we have that

$$\begin{aligned} H(\mathbf{K},\mathbf{U},\mathbf{V}) &= H(\mathbf{U},\mathbf{V}) + H(\mathbf{K}|\mathbf{UV}) \\ &\geq H(\mathbf{UV}) \\ &\geq H(\mathbf{U}). \end{aligned}$$

Notice that in all the constructions we will describe later on, during the key computation phase, users do not flip random bits. Therefore, it holds that $H(\mathbf{UV}) = H(\mathbf{U})$.

Using exactly the same technique we have applied in Theorem 3.3, it is easy to see that $H(\mathbf{U}) \geq |\mathcal{P}|H(\mathbf{K})$. Therefore, if the keys are uniformly chosen in $\mathcal{K}$, then it holds that $R(\mathcal{F},\mathcal{P}) \geq H(\mathbf{U}) \geq |\mathcal{P}|\log|\mathcal{K}|$. This means that the center has to generate at least $|\mathcal{P}|$ keys, each of size $\log|\mathcal{K}|$, in order to construct the scheme. In Section 4.1 we will give a protocol for a key predistribution scheme meeting this bound.

The second lower bound we present holds when the family $\mathcal{P}$ of privileged sets consists of all possible sets of users, i.e., $\mathcal{P} = 2^{\mathcal{U}}$, and we only have restrictions on the collection of forbidden subsets of users $\mathcal{F}$. A $(2^{\mathcal{U}},\mathcal{F})$ key distribution scheme will be simply called *$\mathcal{F}$-resilient key distribution scheme.*

Theorem 3.5 *Let $\mathcal{U}$ be a set of n users, and let $\mathcal{F} \subseteq 2^{\mathcal{U}}$. In any $\mathcal{F}$-resilient key distribution scheme, the entropy $H(\mathbf{U}_i)$, for $i = 1,\ldots,n$, satisfies*

$$H(\mathbf{U}_i) \geq f_i H(\mathbf{K}),$$

where $f_i = |\{F \in \mathcal{F} \ : \ i \notin F\}|$.

Proof: Assume that $\mathcal{F}_i = \{F \in \mathcal{F},\ i \notin F\} = \{F_1,\ldots,F_{f_i}\}$, and let $\mathcal{X}_i = \{X_j = \mathcal{U}\backslash F_j \ : \ F_j \in \mathcal{F}_i,\ j = 1,\ldots,f_i\}$ be the collection of complementary subsets. It follows that $|\mathcal{X}_i| = f_i$ and user i belongs to every subset $X \in \mathcal{X}_i$. The result can be easily derived by repeating the proof of Theorem 3.3. □

Along the same line, we can show that $R(\mathcal{F},\mathcal{P}) \geq H(\mathbf{U}) \geq |\mathcal{F}|H(\mathbf{K})$. Notice that, Theorems 3.3 and 3.5 give the same bound only when $\mathcal{F} = \mathcal{P} = 2^{\mathcal{U}}$.

A w-resilient key distribution schemes is a particular case of an $\mathcal{F}$-resilient key distribution scheme. In such a scheme, each common key is secure against coalitions of at most w users, i.e., $\mathcal{F} = \{F \in 2^{\mathcal{U}} \ : \ |F| \leq w\}$. Hence, for $i = 1,\ldots,n$, we have that $f_i = |\{F \in \mathcal{F},\ i \notin F\}| = \sum_{j=0}^{w} \binom{n-1}{j}$. The next corollary is an immediate consequence of Theorem 3.5.

Corollary 3.6 *Let $\mathcal{U}$ be a set of n users, and let $w < n$ be an integer. In any w-resilient key distribution scheme, the entropy $H(\mathbf{U}_i)$, for $i = 1,\ldots,n$, satisfies*

$$H(\mathbf{U}_i) \geq \sum_{j=0}^{w} \binom{n-1}{j} H(\mathbf{K}).$$

The above bound is met by a w-resilient key distribution scheme given by Fiat and Naor in [29].

4 Embedding Previous Models

In this section we show that some previous models for unconditionally secure key distribution can be seen as instances of our general model. More precisely, we show that unconditionally secure key predistribution schemes, key agreement schemes and broadcast encryption schemes, fall in our model.

4.1 Key Predistribution Schemes

A *Key Predistribution Scheme* (KPS, for short) is defined as follows: A trusted center **C**, during a *distribution phase*, gives to the users in $\mathcal{U}$ some information, which has to be kept secret. Later on, during a *key computation phase*, a specified privileged subset of users computes a common key by using the information received from the center during the distribution phase and some public available information, like the *identities* of the other users belonging to the privileged subset. The key is secure against disjoint coalitions of users. Various key predistribution schemes have been proposed in the past: the basic scheme, Blom's scheme [6], the *Zero-Message Broadcast Encryption Scheme* (see, [29, 7]) and the *Non-Interactive w-Secure g-Conference Key Distribution Scheme* (see, [13, 33, 46]) are all examples of such schemes. As the name suggests, keys are in a certain way *predistributed* to the users during the distribution phase of the scheme. It is easy to see that a KPS can be seen as an instance of our model for key distribution, where the "view" v_i can be considered as an "empty" view or a constant one. Therefore, a KPS is modeled by the following two relations:

- For any $P \in \mathcal{P}$ and for any $i \in P$, it holds that $H(\mathbf{K}_P|\mathbf{U}_i) = 0$.
- For any $P \in \mathcal{P}$ and for all $F \in \mathcal{F}$, such that $F \cap P = \emptyset$, it holds that $H(\mathbf{K}_P|\mathbf{U}_F) = H(\mathbf{K}_P)$.

It is immediate to see that the bounds provided in Section 3 directly apply also to KPSs.

In [13] the authors considered key distribution schemes for groups of users of a given size. Their scheme has two parameters: g, the size of the subsets that can share a common key, and w, the size of the coalitions of adversaries. Hence, $\mathcal{P} = \{P \in 2^{\mathcal{U}} : |P| = g\}$ and $\mathcal{F} = \{F \in 2^{\mathcal{U}} : |F| \leq w\}$. Such schemes were referred to as *non-interactive w-secure g-conference scheme.* The authors proved a tight lower bound on the size of the user's secret information. The protocol meeting the bound uses symmetric multi-variate polynomials and is a generalization of Blom's scheme [6].

We can show that the lower bound given in [13] can be simply derived from Theorem 3.3. Indeed, let $n = |\mathcal{U}|$, and let w and g be two integers such that $g + w \leq n$. First, notice that if Σ is a non-interactive w-secure g-conference scheme for n users, then Σ is also a non-interactive w-secure g-conference scheme for $n' < n$ users. Therefore, without loss of generality, let us restrict our attention to the first $w+g$ users, and let us denote this ground set of users by $G = \{1, \ldots, w+g\}$. Let $\mathcal{P} = \{P \in 2^G : |P| = g\}$ and let $\mathcal{F} = \{F \in 2^G : |F| \leq w\}$. For any privileged subset $P \in \mathcal{P}$ it holds that $G \backslash P \in \mathcal{F}$. Therefore, we can apply Theorem 3.3 from which we get that $H(\mathbf{U}_i) \geq \pi_i H(\mathbf{K})$, where $\pi_i = |\{P \in \mathcal{P} : i \in P\}|$, for every $1 \leq i \leq w+g$. In this case, $\pi_i = \binom{g+w-1}{w-1}$. Hence, we get that $H(\mathbf{U}_i) \geq \binom{g+w-1}{w-1} H(\mathbf{K})$, which is the same bound given in [13].

An $\mathcal{F}$-resilient key predistribution scheme is described by the following protocol, which is a generalization of the zero-message broadcast encryption scheme given by Fiat and Naor [29]. By means of this scheme, the users in any privileged subset $P \subseteq \{1, \ldots, n\}$ can compute a common key k_P, using the information received during the distribution phase of the protocol from the center and the knowledge of the composition of P. Such a common key k_P is secure against any coalition of users $F \in \mathcal{F}$.

Distribution Phase

1. For each $F \in \mathcal{F}$ the center uniformly chooses a value $s_F \in \mathbf{Z}_q$.
2. The center distributes the value s_F to each user i such that $i \notin F$.

Key Computation Phase

1. The common key k_P of the privileged set $P \in 2^{\mathcal{U}}$ is the sum modulo q of all the values s_F's such that $F \in \mathcal{F}$ and $F \cap P = \emptyset$.

It is easy to see that the above protocol realizes an $\mathcal{F}$-resilient key predistribution scheme. Indeed, each user in a privileged set P can compute the same common key k_P. Moreover, the users in any forbidden subset $F \in \mathcal{F}$, with $F \cap P = \emptyset$, will be missing the value s_F and therefore they will be unable to compute the common key k_P. In this protocol only $|\{F \in \mathcal{F} \ : \ i \notin F\}|$ elements of $\mathbf{Z}_q$ are kept secret by each user. Hence, since Theorem 3.5 holds also in the case of key predistribution schemes, this protocol is optimal with respect to the size of secret information held by each user in the scheme. Moreover, the center, in order to realize such a scheme, generates $|\mathcal{F}|$ values. Hence, this protocol is also optimal with respect to the amount of information the center has to generate and send during the distribution phase.

4.2 Key Agreement Schemes

A *Key Agreement Scheme* (KAS, for short) allows interaction among the users in order to establish common keys and is defined as follows: A trusted center $\mathbf{C}$, during a *distribution phase*, gives to the users in $\mathcal{U}$ some private information. Later on, during a *key computation phase*, a specified privileged subsets of users can compute a common key by using the information received from the center, during the distribution phase, and the messages they send to each other in such a phase. The resulting common key is secure against any disjoint coalition of users, even if such coalitions know *all* the messages exchanged by *all* the possible privileged subsets.

It is easy to see that such a model is an instance of our model for unconditionally secure key distribution schemes. In this case, the view each player gets, is given by the concatenation of all the messages sent by the players belonging to the privileged subset[2]. Therefore, the lower bounds of Section 3 directly apply to key agreement schemes as well. More precisely, we have that:

- If $\mathcal{U}\backslash P \in \mathcal{F}$ for $P \in \mathcal{P}$, then $H(\mathbf{U}_i) \geq \pi_i H(\mathbf{K})$, where $\pi_i = |\{P \in \mathcal{P} : i \in P\}|$.
- If $\mathcal{P} = 2^{\mathcal{U}}$ and $\mathcal{F} \subset 2^{\mathcal{U}}$, then $H(\mathbf{U}_i) \geq f_i H(\mathbf{K})$, where $f_i = |\{F \in \mathcal{F} \ : \ i \notin F\}|$.
- If $\mathcal{P} = 2^{\mathcal{U}}$ and $\mathcal{F} = \{F \in 2^{\mathcal{U}} \ : \ |F| \leq w\}$, then $H(\mathbf{U}_i) \geq \sum_{j=0}^{w} \binom{n-1}{j} H(\mathbf{K})$.

According to the previous bounds, one can easily see, as already noticed by Beimel and Chor [2, 3], that interaction does not help in decreasing the size of the pieces of information given to the users in a key agreement scheme, compared to a non-interactive scheme. Hence, in order to decrease the size of the secret information, held by each user, we have to relax the security requirements. One way is to require a scheme to be secure only a fixed number of times, say ℓ times. In other words, we limit to ℓ the number of privileged subsets that can compute a common key. A ℓ-time $(\mathcal{P}, \mathcal{F})$ key agreement scheme can be defined as follows[3]:

- For any $P \in \mathcal{P}$ and for any $i \in P$, it holds that $H(\mathbf{K}_P|\mathbf{U}_i\mathbf{V}_i) = 0$.
- For any $P \in \mathcal{P}$, for all $F \in \mathcal{F}$ such that $F \cap P = \emptyset$, and for all $j_1, \ldots, j_\ell \in \{1, 2, \ldots, |\mathcal{P}|\}$, it holds that $H(\mathbf{K}_P|\mathbf{U}_F\mathbf{V}_{P_{j_1}} \ldots \mathbf{V}_{P_{j_\ell}}) = H(\mathcal{K}_P)$.

According to the previous definition, at most ℓ privileged sets can subsequently recover a common key, but which sets will reconstruct a common key is non known a-priori. Hence, the center has to distribute pieces of information so that any possible subset in $\mathcal{P}$ could be able to reconstruct a common key.

A one-time key agreement scheme, with $\mathcal{P} = \{X \subseteq \mathcal{U} : |X| = t\}$ and $\mathcal{F} = \{X \subseteq \mathcal{U} : |X| \leq w\}$, can be found in [13]. Considering t independent executions of this protocol, Beimel and Chor [2, 3] realized, at the expenses of round complexity, a key agreement scheme which distributes less information to the users than the one-time scheme proposed in [13].

Since ℓ-time $(\mathcal{P}, \mathcal{F})$ key agreement schemes are an instance of our model for unconditional key distribution, the bounds given in Section 3 directly apply to ℓ-time key agreement schemes as well. More precisely, we have that:

- If $\mathcal{U}\backslash P \in \mathcal{F}$ for all $P \in \mathcal{P}$, then it holds that $H(\mathbf{U}_i) \geq \min\{\ell, \pi_i\} H(\mathbf{K})$, where $\pi_i = |\{P \in \mathcal{P} : i \in P\}|$.

[2]Notice that few issues of practical nature are not covered by the definition. Since a KAS allows interaction among users, 'active' attacks could be applied, e.g., an attacker may send forged messages to some users. Our model, as stated in Section 2, just deals with KAS schemes unconditionally secure against a passive adversary.

[3]When $\ell = |\mathcal{P}|$, we get the definition of a non-restricted unconditionally secure KAS scheme.

- If $\mathcal{P} = 2^{\mathcal{U}}$ and $\mathcal{F} \subset 2^{\mathcal{U}}$, then $H(\mathbf{U}_i) \geq \min\{\ell, f_i\} H(\mathbf{K})$, where $f_i = |\{F \in \mathcal{F} \ : \ i \notin F\}|$.
- If $\mathcal{P} = 2^{\mathcal{U}}$ and $\mathcal{F} = \{F \in 2^{\mathcal{U}} \ : \ |F| \leq w\}$, then $H(\mathbf{U}_i) \geq \min\left\{\ell, \sum_{j=0}^{w} \binom{n-1}{j}\right\} H(\mathbf{K})$.

Hence, the entropy of the secret information stored by each user i is lower bounded by $\min\{\ell, c_i\} H(\mathcal{K})$, for some parameter c_i depending on the user i. It is worthwhile to notice that if $\ell \geq c_i$, for each $i \in \mathcal{U}$, then these bounds coincide with those stated for key predistribution schemes. showing that, also in this case, no advantage comes from allowing interaction among users. Moreover, in any ℓ-time key agreement scheme there is an additional cost for sending messages. On the other hand, if for some $i \in \mathcal{U}$, it holds that $\ell < c_i$, then we can construct an ℓ-time key agreement scheme simply by putting together ℓ copies of a 1-time key agreement scheme. Such an approach, even though allows us to construct a scheme in a straightforward manner, does not always give rise to scheme optimal with respect to the amount of information kept secret by each user. A better construction can be found in [11].

4.3 Broadcast Encryption Schemes

In a *Broadcast Encryption Scheme* (BES, for short) a trusted center **C**, during a *distribution phase*, gives some private information to a set of users $\mathcal{U}$. Later on, the center enables a *privileged* subset $P \subseteq \mathcal{U}$ of users to recover a common key k_P, in such a way that coalitions of at most w users, disjoint from P, gains no information on it. The center enables the privileged users to recover a key by broadcasting a message b_P, computed as a function of the privileged set P, the information given to the users in the distribution phase, and the common key k_P. During the *key computation phase*, each user in P computes the key k_P using b_P and the information received during the distribution phase. In a BES scheme the center, during the distribution phase, does not know which subset will be enabled. Moreover, this privileged subset can dynamically change.

It is easy to see that such a model is also an instance of our model for unconditional key distribution. In this case the view $V_i = b_P$ for all $i \in \mathcal{U}$. Therefore, setting $\alpha = 2^{|\mathcal{U}|} - 1$, a BES is modeled by the following two properties:

- For any $P \subseteq \mathcal{U}$ and for any $i \in P$, it holds that $H(\mathbf{K}_P | \mathbf{U}_i \mathbf{V}_P) = 0$.
- For any $P \subseteq \mathcal{U}$ and for all $F \subseteq \mathcal{U}$ such that $|F| \leq w$ and $F \cap P = \emptyset$, it holds that $H(\mathbf{K}_P | \mathbf{U}_F \mathbf{V}_{P_1} \ldots \mathbf{V}_{P_\alpha}) = H(\mathbf{K}_P)$.

Since broadcast encryption can be seen as a particular case of our model for key distribution, then the bounds provided in Section 3 directly apply to BES as well. In our model, a w-resilient broadcast encryption scheme is just an $\mathcal{F}$-resilient scheme where $\mathcal{F} = \{F \in 2^{\mathcal{U}} \ : \ |F| \leq w\}$. Fiat and Naor [29] gave the first example of a w-resilient broadcast encryption scheme. In [7] the authors generalized the model given in [29] by using an information theoretic approach, and they showed that the zero-message scheme presented in [29] is optimal with respect to both the number of private keys associated with each user, and to the number of keys generated by the center.

Remark 3. Notice that, the theorems given in Section 3 state that unconditionally secure key distribution schemes have severe memory requirements. As a consequence, in order to design broadcast encryption schemes with smaller memory requirements, then complexity assumptions must be considered. Along this line, Fiat and Naor [29] proposed w-resilient broadcast encryption schemes, for a set of n users, requiring less information to be kept secret by each user than the one required by the previous theorems. These computationally secure schemes are based on unproven complexity assumptions such as "one-way function exists" or "extracting prime roots modulo a composite is hard". The best scheme presented in [29] distributes to each user $O(w \log w \log n \log |K|)$ bits.

As previously reported, Fiat and Naor [29] constructed a zero-message unconditionally secure broadcast encryption scheme in which the center is not required to broadcast any message. The users in any privileged subset P can non-interactively compute a common key as function of the set P and of the secret information they receive from the center[4]. The protocol they proposed is exactly the $\mathcal{F}$-resilient key distribution scheme we have described before, in the special case in which

[4]This scheme, as pointed out by Stinson [60], can be actually considered a key predistribution scheme.

$\mathcal{F} = \{F \in \mathcal{U} : 0 \leq |F| \leq w\}$. With such a scheme, each user holds $\sum_{i=0}^{w} \binom{n-1}{i}$ values from $\mathbf{Z}_q$, and the center has to generate $\sum_{i=0}^{w} \binom{n}{i}$ values. Since the bound provided by Corollary 3.6 holds also in the case of broadcast encryption schemes, then, assuming that the common keys are uniformly chosen in $\mathbf{Z}_q$, the above protocol is optimal with respect to the amount of information (equivalently, the number of secret values) which has to be kept secret by each user. This protocol is also optimal with respect to the amount of information the center has to generate during the distribution phase. Indeed, by using a technique similar to the one employed in Theorem 3.3 we can prove that the center, in order to construct the scheme, has to generate at least $\sum_{i=0}^{w} \binom{n}{i}$ keys, each of size $\log q$.

5 Conclusions

In this paper we have presented a concise model for unconditionally secure key distribution schemes, based on an information theoretical framework. We have shown that some previous unconditionally secure models for key distribution can be seen as instances of this model. Moreover, we have shown how previous bounds on the amount of information that has to be generated by the center to set up the scheme, and must be kept secret by the users, can be obtained as corollaries of our results. Hence, this paper points out a common structure underlying some apparently different key distribution techniques.

A Information Theory Background

In this appendix we review some information theoretic concepts we have used in our definitions and proofs. For a complete treatment of the subject the reader is referred to [23].

Given a random variable $\mathbf{X}$, taking values on a set X according to the probability distribution $\{Pr(x)\}_{x \in X}$, we define the *entropy* of $\mathbf{X}$, denoted by $H(\mathbf{X})$, as

$$H(\mathbf{X}) = -\sum_{x \in X} Pr(x) \log Pr(x)$$

(all logarithms in this paper are to relative to the base 2). The entropy satisfies the following property

$$0 \leq H(\mathbf{X}) \leq \log |X|, \tag{2}$$

where $H(\mathbf{X}) = 0$ if and only if there exists $x_0 \in X$ such that $Pr(\mathbf{X} = x_0) = 1$; whereas, $H(\mathbf{X}) = \log |X|$ if and only if $Pr(\mathbf{X} = x) = 1/|X|$, for all $x \in X$.

Given two random variables $\mathbf{X}$ and $\mathbf{Y}$, taking values on sets X and Y, respectively, according to the joint probability distribution $\{Pr(x, y)\}_{x \in X, y \in Y}$ on their cartesian product, the *conditional entropy* $H(\mathbf{X}|\mathbf{Y})$ is defined as

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y \in Y} \sum_{x \in X} Pr(y) Pr(x|y) \log Pr(x|y).$$

From the definition of conditional entropy it is easy to see that

$$H(\mathbf{X}|\mathbf{Y}) \geq 0. \tag{3}$$

Given $n+1$ random variables, $\mathbf{X}_1, \ldots, \mathbf{X}_n, \mathbf{Y}$, the entropy of $\mathbf{X}_1 \ldots \mathbf{X}_n$ given $\mathbf{Y}$ can be written as

$$H(\mathbf{X}_1 \ldots \mathbf{X}_n|\mathbf{Y}) = H(\mathbf{X}_1|\mathbf{Y}) + H(\mathbf{X}_2|\mathbf{X}_1\mathbf{Y}) + \cdots + H(\mathbf{X}_n|\mathbf{X}_1 \ldots \mathbf{X}_{n-1}\mathbf{Y}). \tag{4}$$

The *mutual information* between $\mathbf{X}$ and $\mathbf{Y}$ is defined by

$$I(\mathbf{X}; \mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}) \tag{5}$$

and satisfies the following properties:

$$I(\mathbf{X}; \mathbf{Y}) = I(\mathbf{Y}; \mathbf{X}), \tag{6}$$

and

$$I(\mathbf{X};\mathbf{Y}) \geq 0,$$

from which it is easy too see that

$$H(\mathbf{X}) \geq H(\mathbf{X}|\mathbf{Y}), \tag{7}$$

with equality if and only if $\mathbf{X}$ and $\mathbf{Y}$ are independent. Given three random variables, $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$, the *conditional mutual information* between $\mathbf{X}$ and $\mathbf{Y}$ given $\mathbf{Z}$ can be written as

$$I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) = H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{Z}\ \mathbf{Y}) = H(\mathbf{Y}|\mathbf{Z}) - H(\mathbf{Y}|\mathbf{Z}\ \mathbf{X}) = I(\mathbf{Y};\mathbf{X}|\mathbf{Z}). \tag{8}$$

Since the conditional mutual information $I(\mathbf{X};\mathbf{Y}|\mathbf{Z})$ is always non-negative, it holds that

$$H(\mathbf{X}|\mathbf{Z}) \geq H(\mathbf{X}|\mathbf{Z}\ \mathbf{Y}). \tag{9}$$

Moreover, from (8) and (3), we obtain

$$H(\mathbf{X}|\mathbf{Z}) \geq I(\mathbf{X};\mathbf{Y}|\mathbf{Z}). \tag{10}$$

References

[1] J. Anzai, N. Matsuzaki, and T. Matsumoto, *A Quick Group Key Distribution Scheme with Entity Revocation*, Advances in Cryptology - Asiacrypt '99, Lecture Notes in Computer Science, Vol. 1716, pp. 333-347.

[2] A. Beimel and B. Chor. *Interaction in Key Distribution Schemes*, In Proceeding of Crypto 93. Lecture Notes in Computer Science, Vol. 773, ,pp 444–455.

[3] A. Beimel and B. Chor. *Communication in Key Distribution Schemes*, IEEE Transactions on Information Theory, Vol. 42, pp 19–28, 1996

[4] O. Berkman, M. Parnas, and J. Sgall, *Efficient Dynamic Traitor Tracing*, Proc. of the 11-th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2000), pp. 586–595, 2000.

[5] S. Berkovits. *How to Broadcast a Secret*, In Proc. Eurocrypt 91, Lecture Notes in Computer Science, Vol. 547, pp 536–541, 1992.

[6] R. Blom. *An Optimal Class of Symmetric Key Generation Systems*, Proc. Eurocrypt 84, Lecture Notes in Computer Science, Vol. 209, pp 335–338, 1994.

[7] C. Blundo and A. Cresti. *Space Requirements for Broadcast Encryption*, Proc. Eurocrypt '94, Lecture Notes in Computer Science, Vol. 950, pp 287–298, 1994.

[8] C. Blundo and A. Cresti. *Broadcast Encryption Schemes with Disenrollment Capability*, Fifth Italian Conference on Theoretical Computer Science, Word Scientific, pp 176–191, 1996

[9] C. Blundo and P. D'Arco, *The Key Establishment Problem*, FOSAD01, Springer-Verlag, 2002.

[10] C. Blundo, P. D'Arco, V. Daza and C. Padró. *Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures*, Proceedings of the Information Security Conference (ISC 2001), Lecture Notes in Computer Science, vol. 2200, pp. 1-17, Springer-Verlag , 2001.

[11] C. Blundo, P. D'Arco, A. Giorgio Gaggia. *A τ-restricted Key Agreement Scheme*, The Computer Journal , Vol. 42, n. 1, pp. 51-61, 1999.

[12] C. Blundo, P. D'Arco and C. Padró. *A Ramp Model for Distributed Key Distribution Schemes*, to appear on Discrete Applied Mathematics.

[13] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. *Perfectly-Secure Key Distribution for Dynamic Conferences*, In Proc. Crypto 92, Lecture Notes in Computer Science, Vol. 740, pp 471–486, 1993.

[14] C. Blundo, Luiz A. Frota Mattos, and D. R. Stinson. *Multiple Key Distribution Maintaining User Anonymity via Broadcast Channels*, Journal of Computer Security, Vol 3, pp 309–323, 1996.

[15] C. Blundo, Luiz A. Frota Mattos, and D. R. Stinson. *Trade-offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution*, In Proc. CRYPTO '96, Lecture Notes in Computer Science, Vol. 1109, pp 387–400, 1996.

[16] C. Blundo, Luiz A. Frota Mattos, and D. R. Stinson. *Generalized Beimel-Chor Schemes for Broadcast Encryption and Interactive Key Distribution*, Theoretical Computer Science, Volume 200, Issues 1-2 28, pp 313-334, 1998.

[17] D. Boneh and M. Franklin, *An Efficient Public Key Traitor Scheme*, Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science, vol. 1666, pp. 338–353, 1999.

[18] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, *Issue in Multicast Security: A Taxonomy and Efficient Constructions*, Infocom '99, pp. 708–716, 1999.

[19] R. Canetti, T. Malkin, and K. Nissim, *Efficient Communication-Storage Tradeoffs for Multicast Encryption*, Advances in Cryptology - Eurocrypt '99, Lecture Notes in Computer Science, vol. 1592, pp. 459–474, 1999.

[20] G. H. Chiou and W. T. Chen. *Secure Broadcasting Using the Secure Lock*, IEEE Transaction on Software Engineering, Vol. 15, 929–934, 1989.

[21] B. Chor, A. Fiat, and M. Naor. *Tracing Traitors*, Proc. Crypto 94, Lecture Notes in Computer Science, Vol. 839, pp 257–270, 1994.

[22] B. Chor, A. Fiat, M. Naor and B. Pinkas, *Traitor Tracing*, IEEE Transactions on Information Theory, vol. 46, No. 3, pp. 893–910, May 2000.

[23] T. M. Cover and J. A. Thomas. *Elements of Information Theory.* John Wiley & Sons, 1991.

[24] P. D'Arco, *On the Distribution of a Key Distribution Center*, Proceedings of the Italian Conference on Theoretical Computer Science (ICTCS 2001), Lecture Notes in Computer Science, vol. 2202, pp. 357-369, Springer-Verlag , 2001,

[25] P. D'Arco and D. Stinson, *On Unconditionally Secure Robust Distributed Key Distribution Centers*, Proceedings di ASIACRYPT 2002, Lecture Notes in Computer Science, Vol. 2501, pp. 346-363, Springer Verlag, 2002.

[26] P. D'Arco and D. Stinson, *Fault Tolerant and Distributed Broadcast Encryption*, Proceedings of the Cryptographers' Track RSA Conference 2003 (CT-RSA 2003), Lecture Notes in Computer Science, Vol. 2612, pp. 262-279, Springer Verlag, 2003.

[27] G. Di Crescenzo and O. Kornievskaia, *Efficient Multicast Encryption Schemes*, Security in Communication Network (SCN02), Lecture Notes in Computer Science, 2002.

[28] C. Dwork, J. Lotspiech, and M. Naor, *Digital Signets: Self-Enforcing Protection of Digital Information*, Proceedings of the 28-th Symposium on the Theory of Computation, pp. 489–498, 1996.

[29] A. Fiat and M. Naor, *Broadcast Encryption*, Proceedings of Crypto '93, Lecture Notes in Computer Science, vol. 773, pp. 480-491, 1994.

[30] A. Fiat and T. Tessa, *Dynamic Traitor Tracing*, Journal of Cryptology, Vol. 14, pp. 211–223, 2001.

[31] E. Gafni, J. Staddon, and Y. L. Yin, *Efficient Methods for Integrating Traceability and Broadcast Encryption*, Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science, vol. 1666, p. 372–387, 1999.

[32] J. Garay, J. Staddon, and A. Wool, *Long-Lived Broadcast Encryption*, Advances in Cryptology - Crypto 2000, Lecture Notes in Computer Science, vol. 1880, pp. 333–352, 2000.

[33] L. Gong and D.J. Wheeler. *A Matrix Key-Distribution Scheme*, Journal of Cryptology, Vol. 2, pp 51–59, 1990.

[34] D. Halevy and A. Shamir, *The LSD Broadcast Encryption Scheme*, Advances in Cryptology - Crypto '02, Lecture Notes in Computer Science, vol. 2442, pp. 47-60, 2002.

[35] M. Just, E. Kranakis, D. Krizanc, P. van Oorschot. *Key Distribution via True Broadcasting*, Proc. 2nd ACM Conference on Computer and Communications Security, pp 81–88, 1994.

[36] A. Kiayias and M. Yung, *Traitor Tracing with Constant Transmission Rate*, Advances in Cryptology - Eurocrypt '02, Lecture Notes in Computer Science, vol. 2332, pp. 450-465, 2002.

[37] A. Kiayias and M. Yung, *Self Protecting Pirates and Black-Box Traitor Tracing*, Advances in Cryptology - Crypto '01, Lecture Notes in Computer Science, vol.2139 , pp. 63-79, 2001.

[38] Knuth D. E. and Yao A. C., *The Complexity of Nonuniform Random Number Generation*, Algorithms and Complexity, Academic Press, pp. 357–428, 1976.

[39] R. Kumar, S. Rajagopalan, and A. Sahai, *Coding Constructions for Blacklisting Problems without Computational Assumptions*, Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science, Vol. 1666, pp. 609–623, 1999.

[40] H. Kurnio, R. Safani-Naini, and H. Wang, *A Group Key Distribution Scheme with Decentralised User Join*, Security in Communication Network (SCN02), Lecture Notes in Computer Science, 2002.

[41] H. Kurnio, R. Safani-Naini, and H. Wang, *A Secure Re-keying Scheme with Key Recovery Property*, ACISP 2002, Lecture Notes in Computer Science, Vol. 2384, pp. 40–55, 2002.

[42] K. Kurosawa, K. Okada, and K. Sakano, *Security of the Center in Key Distribution Schemes*, Advances in Cryptology - Asiacrypt '94, Lecture Notes in Computer Science, vol. , pp. , 1994.

[43] C. Laih, J. Lee, and L. Harn. A New Threshold Scheme and its Applications in Designing the Conference Key Distribution Cryptosystem. *Information Processing Letters*, **32** (1989), 95–99.

[44] C. H. Lin, C. C. Chang, and R. C. Lee. A Conference Key Broadcasting System Using Sealed Locks. *Information Systems*, **17** (1992), 323-328.

[45] M. Luby and J. Staddon, *Combinatorial Bounds for Broadcast Encryption*, Advances in Cryptology - Eurocrypt '98, Lecture Notes in Computer Science, vol. 1403, pp. 512–526, 1998.

[46] T. Matsumoto and H. Imai, *On the Key Predistribution System: A Practical Solution to the Key Distribution Problem*, Proc. Crypto 87, Lecture Notes in Computer Science, Vol. 239, pp 185–193, 1987.

[47] A.J. Menezes, P.C. Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[48] C. J. Mitchell and F. C. Piper, *Key Storage in Secure Networks*, Discrete Applied Mathematics, vol. 21, pp. 215–228, 1988.

[49] D. Naor, M. Naor, and J. Lotspiech, *Revocation and Tracing Schemes for Stateless Receivers* Advances in Cryptology - Crypto '01, Lecture Notes in Computer Science, vol. 2139, pp. 41–62, 2001.

[50] M. Naor and B. Pinkas, *Efficient Trace and Revoke Schemes*, Financial Cryptography 2000, Lecture Notes in Computer Science, vol. 1962, pp. 1–21, 2000.

[51] M. Naor, B. Pinkas, and O. Reingold. *Distributed Pseudo-random Functions and KDCs*, Advances in Cryptology - Eurocrypt'99, Lecture Notes in Computer Science, vol. 1592, pp. 327–346, 1999.

[52] A. Perrig, D. Song, and J. D. Tygar, *ELK, a new Protocol for Efficient Large-Group Key Distribution*, in IEEE Symposium on Security and Privacy (2000).

[53] B. Pfitzmann, *Trials of Traced Traitors*, Information Hiding, Lecture Notes in Computer Science, vol. 1174, pp. 49-64, 1996.

[54] R. Poovendran and J. S. Baras, *An Information Theoretic Analysis of Rooted-Tree Based Secure Multicast Key Distribution Schemes*, Advances in Cryptology, Crypto '99, vol. 1666, pp. 624-638, 1999.

[55] R. Safavi-Naini and H. Wang, *New Constructions for Multicast Re-Keying Schemes Using Perfect Hash Families*, 7th ACM Conference on Computer and Communication Security, ACM Press, pp. 228–234, 2000.

[56] R. Safavi-Naini and Y. Wang, *Sequential Traitor Tracing*, Lecture Notes in Computer Science, vol. 1880, p. 316–332, 2000.

[57] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin and D. Dean, *Self-Healing Key Distribution with Revocation*, IEEE Symposium on Security and Privacy, May 12-15, 2002, Berkeley, California.

[58] J. N. Staddon, D.R. Stinson and R. Wei, *Combinatorial properties of frameproof and traceability codes*, IEEE Transactions on Information Theory vol. 47, pp. 1042-1049, 2001.

[59] D.R. Stinson, *Cryptography: Theory and Practise*, CRC Press, 1995 (2nd Edition, 2002).

[60] D. R. Stinson. *On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption.* Designs, Codes and Cryptography, 12 (1997), 215–243.

[61] D. R. Stinson and T. van Trung, *Some New Results on Key Distribution Patterns and Broadcast Encryption*, Designs, Codes and Cryptography, vol. 15, pp. 261–279, 1998.

[62] D. R. Stinson and R. Wei, *Key preassigned traceability schemes for broadcast encryption*, Proceedings of SAC'98, Lecture Notes in Computer Science, vol. 1556, pp. 144-156, 1999.

[63] D. R. Stinson and R. Wei, *Combinatorial properties and constructions of traceability schemes and frameproof codes*, SIAM Journal on Discrete Mathematics, vol. 11, pp. 41–53, 1998.

[64] D. R. Stinson and R. Wei, *An Application of Ramp Schemes to Broadcast Encryption*, Information Processing Letters, Vol. 69, pp. 131–135, 1999.

[65] D. M. Wallner, E. J. Harder, and R. C. Agee, *Key Management for Multicast: Issues and Architectures*, Internet Draft (draft-wallner-key-arch-01.txt), ftp://ftp.ieft.org/internet-drafts/draft-wallner-key-arch-01.txt.

[66] C. Wong, and S. Lam, *Keystone: A Group Key Management Service*, in International Conference on Telecommunications, ICT 2000.