
A τ -Restricted Key Agreement Scheme

CARLO BLUNDO, PAOLO D'ARCO AND ANTONIO GIORGIO GAGGIA

*Università di Salerno, 84081 Baronissi (SA), Italy
Email: carblu@dia.unisa.it*

A one-restricted key agreement scheme is a method by which initially a trusted authority distributes private individual pieces of information to a set of users. Later, each member of any group of users of a given size, referred to as a *conference*, can compute a common key by exchanging messages over a broadcast channel all users have access to. Such schemes can be used to establish only one common key. In this paper we analyse τ -restricted key agreement schemes. Such schemes allow the computation of up to τ common keys for τ distinct conferences. For certain values of the parameters the scheme that we propose distributes less information than the trivial one obtained by considering τ copies of a one-restricted scheme.

Received April 14, 1998; revised January 15, 1999

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. From the point of view of security, most networks can be thought of as broadcast networks, in that anyone connected to the network will have access to all the information that flows through it. This leads to many problems related to the confidentiality and authenticity of information transmitted.

When a subset of users in a network, referred to as a *conference*, wishes to communicate privately, encryption algorithms can be used to provide security against eavesdropping. If conventional (private-key) cryptography is used, a common key must be shared by the members of the conference. The question is, how can we set up an efficient protocol to give each conference a key?

A key distribution scheme (KDS) 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. Usually, we have a distribution phase, in which a trusted authority (TA) distributes information in a private way to each user and a key computation phase, where a conference computes a common key. The scheme is *unconditionally secure* if any disjoint coalition of adversaries does not gain information about the conference key, even though it has access to an infinite computational power. In the last few years, various approaches have been proposed; in this paper we restrict our attention to unconditional secure KDS.

The first method is the *key predistribution scheme*. Secret information is given to each user by the TA in the distribution phase. Later, in the key computation phase, every member of a conference G can reconstruct the common key k_G from *his piece* and the conference *identity*, while every disjoint

coalition F of adversaries does not gain any information on k_G .

A basic key predistribution scheme consists of a TA, which gives privately, in the distribution phase, keys to users in such a way that each potential group that needs to communicate securely, shares a common key. This scheme is unconditionally secure against *any* disjoint coalition of adversaries and requires no key computation phase. The drawback is that the number of keys each user must keep secret can be 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 unconditionally secure, but only with respect to coalitions of a *limited size*. One such scheme was considered by Blom [1] where, using MDS codes, an efficient scheme for conferences G of size 2 and coalitions F of size b is given (other related schemes are presented in [2, 3]).

Subsequently, for conference G of size g and coalitions of adversaries F of size b , in [4], using entropy arguments, the authors proved a lower bound on the cardinality of the domain of pieces given to users and showed that the bound is tight describing a scheme meeting it. The scheme uses symmetric polynomials with g variables and degree at most b in each variable (a brief description of such a scheme is given in Appendix B).

A second approach allows interaction among the users in a conference. In the key computation phase the members of a conference G , using the secret information received in the distribution phase, interact to agree on a key by exchanging encrypted messages among themselves via a broadcast media. Any disjoint coalition of adversaries F that hears all communications is unable to gain any information about it.

This approach, which we call the *key agreement scheme*,

initiated in [4], was continued by Beimel and Chor [5, 6] and aimed to reduce the size of information each user must keep secret. In [5] the authors studied schemes for conference G of size g and coalitions of adversaries F of size b . They proved that the interaction cannot help in reducing the size of the pieces of information given to the users compared to the non-interactive model. Hence, in order to decrease the size of the secret information, we have to relax the security requirements. We can require that the key agreement scheme is secure only in a *fixed number* of times, say τ , defining τ -*restricted* key agreement schemes. In such schemes we limit to τ the number of groups of users, whose identity is not known beforehand, that can compute a common key in an unconditionally secure way. For such schemes Beimel and Chor in [5, 6] realized a one-restricted scheme, where the size of pieces given to users is smaller than in unrestricted key agreement schemes. Subsequently, using τ copies of a one-restricted scheme, they realize a scheme which is secure for τ conferences. Such an approach, even though it allows us to construct a scheme in a straightforward manner, does not give rise to a scheme which is optimal with respect to the size of the information kept by each user. In the literature a one-restricted scheme is also referred to as a *one-time* scheme, because it can be used to compute only *one* common key.

In [7] the authors presented a generalization of the one-restricted scheme described by Beimel and Chor [5, 6] using tools from design theory.

Fiat and Naor [8] introduced a new key distribution scheme referred to as the *broadcast encryption scheme*. The TA gives some predefined keys to each user in the distribution phase. At some point, the TA enables a *privileged* subset of users to recover a common key by broadcasting a message, in the key computation phase. Each user in the privileged set can recover the common key using the broadcast message and the prearranged keys he received from the TA when the system was set up. Further, any coalition of at most b users disjoint from the privileged set has no information on this common key. Broadcast encryption schemes were designed to allow a central site to broadcast secure transmissions to an arbitrary set of recipients. The common key recovered by the privileged set will later be used to decrypt broadcast messages. Broadcast encryption was further analysed in [9, 10, 11, 12, 13, 14, 15].

Other key distribution schemes are known in the literature. A survey of unconditional secure schemes can be found in [16]; while a general model for unconditional secure KDS can be found in [17].

1.1. The results

We analyse a special type of τ -restricted key agreement schemes. In general the messages exchanged among the members of a conference can depend on the previous messages and there may be several rounds of communication. In the key agreement schemes we analyse, each member of a conference independently chooses a random value and, using its secret information, computes an encrypted version

of it. Then, this user sends this encrypted version to all the other members of the conference over the broadcast channel. The conference key will be the concatenation of all these values randomly chosen by the users in the conference.

We model the problem of τ -restricted key agreement schemes with an information theoretical framework. We use Shannon entropy mainly because this 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 A we review the basic notions of entropy and mutual information.

Throughout this paper we assume that all the τ conferences that want to compute a common key are distinct (i.e. we do not allow the same conference to compute more than once a common key). This situation is close to the spirit of the non-interactive schemes. Indeed, in such schemes all members of a conference use the same key every time they want to establish a secure communication. In this paper, we extend this feature to key agreement schemes by assuming that, if the members of a conference G want to communicate for the first time, then they compute a common key k_G by exchanging messages over the broadcast channel. Subsequently, they keep a copy of it in a secure manner, in such a way that when they want to communicate again, they use the previously computed common key k_G . We provide a τ -restricted key agreement scheme which distributes less information than the trivial scheme obtained by considering τ copies of a one-restricted scheme. Such a scheme requires that users hold a *counter* which is incremented each time a conference key is generated.

Organization

In Section 2 we formally define key predistribution schemes and τ -restricted key agreement schemes using an information theoretical framework. In Section 3 we prove some lemmas used to establish the security of our protocol. In Section 4 we describe the protocol realizing a τ -restricted key agreement scheme. Finally, in Section 5 we recall the main result of the paper.

2. THE MODEL

In this section we describe both *key predistribution* and *key agreement schemes*. We formalize such models using the entropy function (see Appendix A). Thus, the security we analyse is unconditional. Our scenario consists of a TA and a set of users $\mathcal{U} = \{1, \dots, n\}$. We assume that the network is a broadcast channel, i.e. it is insecure and any information transmitted by one user will be received by every user.

A KDS is a distribution protocol, divided into two phases: a distribution phase and a key computation phase. In the distribution phase the TA gives privately some secret information (sometimes referred to as *predefined keys*) to users in \mathcal{U} . In the key computation phase some subset of users G in \mathcal{U} , referred to as a *conference*, computes a common key using the secret information received by the TA and the messages ‘seen’ over the network during such

a phase. The TA, before providing users with some private information, does not know which conference G will later recover a common key. In some cases, for example, non-interactive schemes, such messages can be considered as ‘empty’ messages or constant ones.

In this paper by a boldface italic capital letter, say X , we denote a random variable taking a value on a set denoted by the corresponding capital letter X according to some probability distribution $\{\Pr(x)\}_{x \in X}$. The values such a random variable can take are denoted by the corresponding lower case letter.

For $1 \leq i \leq n$, with U_i we denote the set of all possible secret values distributed to user i by the TA. For any $X \subseteq \mathcal{U}$, let $U_X = U_{i_1} \times \dots \times U_{i_j}$, where $X = \{i_1, \dots, i_j\}$ and $i_1 < \dots < i_j$. We assume that the TA chooses $u_{\mathcal{U}} \in U_{\mathcal{U}}$ according to the probability distribution $\{\Pr(u_{\mathcal{U}})\}_{u_{\mathcal{U}} \in U_{\mathcal{U}}}$, that in turn naturally induces a probability distribution $\{\Pr(u_G)\}_{u_G \in U_G}$ on U_G , for any set $G \subseteq \mathcal{U}$. For any set $G \subseteq \mathcal{U}$ of size g , we denote by K_G the set of all possible values of the key k_G for the conference G . The KDS and the probability distribution on U_G induce a probability distribution $\{\Pr(k_G)\}_{k_G \in K_G}$ on K_G .

In a *key predistribution scheme*, each user i in a conference G of size g is able to recover, during the key computation phase, without interaction with other users, the secret key k_G . The user i computes k_G using the secret information he received from the TA and the identities of the other users in G . Further, no disjoint coalition F of size at most b , is able to gain any information about the secret key k_G . A key predistribution scheme is formally defined as follows.

DEFINITION 2.1. *Let $\mathcal{U} = \{1, \dots, n\}$ be a set of n users and let g and b be two positive integers such that $g + b \leq n$. A (g, b) key predistribution scheme $((g, b)$ -KPS) is a distribution protocol satisfying:*

- (1) *each user i in any conference G of size g can compute k_G .*
For all $i \in G \subseteq \mathcal{U}$, with $|G| = g$, it holds that $H(\mathbf{K}_G | U_i) = 0$.
- (2) *No coalition F of b users disjoint from the conference G has any information on k_G . For all conferences G of size g and all coalitions F of size b such that $G \cap F = \emptyset$, it holds that $H(\mathbf{K}_G | U_F) = H(\mathbf{K}_G)$.*

Notice that $H(\mathbf{K}_G | U_i) = 0$ means that the information held by user i unequivocally determines the value of the common key associated with the conference G . Moreover, $H(\mathbf{K}_G | U_F) = H(\mathbf{K}_G)$, where $F \cap G = \emptyset$, means that \mathbf{K}_G and U_F are statistically independent (i.e. the information held by users in F reveals no information on the key of the conference G).

In a *key agreement scheme*, when users of a set G of cardinality g wish to generate a conference key, during the key computation phase, they communicate between themselves through the network. All messages sent by user i are denoted by $b_i \in B_i$; whereas the messages exchanged by all the users in a conference G are denoted by $B_G \in B_G$

(i.e. for $G = \{i_1, \dots, i_g\}$ we have that $B_G = B_{i_1} \times \dots \times B_{i_g}$). Since the messages are sent over a network that is a broadcast channel, they can be heard by all the users, including any coalition of adversaries. The scheme assures that each user of G , using the secret information and the broadcast message b_G , recovers the conference key, while any disjoint coalition of adversaries is unable to gain any information on k_G . A key agreement scheme is formally defined as follows.

DEFINITION 2.2. *Let $\mathcal{U} = \{1, \dots, n\}$ be a set of n users and let g and b be two positive integers such that $g + b \leq n$. A (g, b) key agreement scheme $((g, b)$ -KAS) is a distribution protocol satisfying:*

- (1) *without knowing the broadcast b_G , no subset of users has any information on k_G even given all the secret information $U_{\mathcal{U}}$.*
For all conferences $G \subseteq \mathcal{U}$ of size g , it holds that $H(\mathbf{K}_G | U_{\mathcal{U}}) = H(\mathbf{K}_G)$.
- (2) *Each user i in any conference G of size g , knowing the broadcast b_G , can compute k_G .*
For all $i \in G \subseteq \mathcal{U}$, with $|G| = g$ and for the broadcast b_G , it holds that $H(\mathbf{K}_G | U_i B_G) = 0$.
- (3) *No coalition F of size b disjoint from a conference G of size g has any information on k_G , even knowing the broadcasts of all possible conferences.*
For all conferences $G \subseteq \mathcal{U}$ of size g and all coalitions F of size b such that $G \cap F = \emptyset$ and for any broadcast $B = \cup_{G:|G|=g} b_G$, it holds that $H(\mathbf{K}_G | U_F B) = H(\mathbf{K}_G)$.

Notice that $H(\mathbf{K}_G | U_{\mathcal{U}}) = H(\mathbf{K}_G)$ means that \mathbf{K}_G and $U_{\mathcal{U}}$ are statistically independent (i.e. the information held by all users in \mathcal{U} reveals no information on the key conference k_G of the conference G). Moreover, $H(\mathbf{K}_G | U_i B_G) = 0$ means that the information u_i and the broadcast messages b_G , exchanged by all users in G , unequivocally determine the value of the common key k_G of the conference G . Finally, $H(\mathbf{K}_G | U_F B) = H(\mathbf{K}_G)$ means that \mathbf{K}_G is statistically independent from U_F and B (i.e. the information held by F and the messages exchanged by all conferences of size g do not reveal any information about the key conference k_G).

A τ -restricted key agreement scheme is a key agreement scheme in which any coalition of adversaries F of size b disjoint from G , knowing the messages exchanged by any τ conferences during the key computation phase does not gain any information on the key k_G . A τ -restricted key agreement scheme is formally defined as follows.

DEFINITION 2.3. *Let $\mathcal{U} = \{1, \dots, n\}$ be a set of n users and let g and b be two positive integers such that $g + b \leq n$. A τ -restricted (g, b) key agreement scheme $(\tau$ -restricted (g, b) -KAS) is a distribution protocol satisfying:*

- (1) *without knowing the broadcast b_G , no subset of users has any information on k_G even given all the secret information $U_{\mathcal{U}}$.*
For all conferences $G \subseteq \mathcal{U}$ of size g , it holds that $H(\mathbf{K}_G | U_{\mathcal{U}}) = H(\mathbf{K}_G)$.

(2) Each user i in any conference G of size g , knowing the broadcast b_G , can compute k_G .

For all $i \in G \subseteq \mathcal{U}$, with $|G| = g$ and for the broadcast b_G , it holds that $H(\mathbf{K}_G | \mathbf{U}_i \mathbf{B}_G) = 0$.

(3) After seeing the communication of at most τ distinct conferences, no coalition F of b users has any information on the key of one of these conferences (disjoint from F).

For any τ distinct conferences G_1, \dots, G_τ , with $|G_i| = g$ for $i = 1, \dots, \tau$, for any $b_{G_1}, \dots, b_{G_\tau}$ and any $F \subseteq \mathcal{U}$ of size b such that $F \cap G_i = \emptyset$, it holds that $H(\mathbf{K}_{G_i} | \mathbf{U}_F \mathbf{B}_{G_1}, \dots, \mathbf{B}_{G_\tau}) = H(\mathbf{K}_{G_i})$.

Notice that $H(\mathbf{K}_{G_i} | \mathbf{U}_F \mathbf{B}_{G_1} \dots \mathbf{B}_{G_\tau}) = H(\mathbf{K}_{G_i})$ means that \mathbf{K}_{G_i} is statistically independent from \mathbf{U}_F and $\mathbf{B}_{G_1}, \dots, \mathbf{B}_{G_\tau}$ (i.e. the information held by F and the messages exchanged by any τ conferences of size g do not reveal any information about the key conference k_{G_i}).

3. TECHNICAL LEMMAS

In this section we present some technical lemmas which will be useful to prove that our τ -restricted (g, b) key agreement scheme is secure.

LEMMA 3.1. Let $\mathbf{A}, \mathbf{B}, \mathbf{C}$ and \mathbf{D} be four random variables. If $H(\mathbf{A} | \mathbf{B}) = 0$, then the following two statements hold

- (1) $H(\mathbf{C} | \mathbf{B}\mathbf{D}) = H(\mathbf{C} | \mathbf{A}\mathbf{B}\mathbf{D})$
- (2) $H(\mathbf{C} | \mathbf{A}\mathbf{D}) \geq H(\mathbf{C} | \mathbf{B}\mathbf{D})$.

Proof. The hypothesis $H(\mathbf{A} | \mathbf{B}) = 0$ and equations (15) and (10) of Appendix A imply that

$$0 = H(\mathbf{A} | \mathbf{B}) \geq H(\mathbf{A} | \mathbf{B}\mathbf{D}) \geq H(\mathbf{A} | \mathbf{B}\mathbf{C}\mathbf{D}) \geq 0.$$

Hence, $H(\mathbf{A} | \mathbf{B}\mathbf{D}) = H(\mathbf{A} | \mathbf{B}\mathbf{C}\mathbf{D}) = 0$. According to (14) of Appendix A, we have

$$I(\mathbf{C}; \mathbf{A} | \mathbf{B}\mathbf{D}) = H(\mathbf{C} | \mathbf{B}\mathbf{D}) - H(\mathbf{C} | \mathbf{A}\mathbf{B}\mathbf{D})$$

and

$$I(\mathbf{A}; \mathbf{C} | \mathbf{B}\mathbf{D}) = H(\mathbf{A} | \mathbf{B}\mathbf{D}) - H(\mathbf{A} | \mathbf{B}\mathbf{C}\mathbf{D}) = 0.$$

Since, $I(\mathbf{C}; \mathbf{A} | \mathbf{B}\mathbf{D}) = I(\mathbf{A}; \mathbf{C} | \mathbf{B}\mathbf{D})$, it follows that $H(\mathbf{C} | \mathbf{B}\mathbf{D}) = H(\mathbf{C} | \mathbf{A}\mathbf{B}\mathbf{D})$. Therefore, statement 1 is satisfied. From (15) of Appendix A and statement 1 we get

$$H(\mathbf{C} | \mathbf{A}\mathbf{D}) \geq H(\mathbf{C} | \mathbf{A}\mathbf{B}\mathbf{D}) = H(\mathbf{C} | \mathbf{B}\mathbf{D}),$$

which proves statement 2. \square

In [7] it is proved that in any $(l, g+b-l)$ -KPS, with $\ell \leq g$, the users in any coalition F of size b have no information on the key associated with the l -subsets of $G \subseteq \mathcal{U}$, where $|G| = g$ and $F \cap G = \emptyset$. This is formalized in the next lemma.

LEMMA 3.2. Let \mathcal{U} be a set of n users and let $G, F \subseteq \mathcal{U}$ be two subsets of g and b users respectively, such that

$G \cap F = \emptyset$. Finally, let Y_1, \dots, Y_α be distinct l -subsets of G , where $\alpha = \binom{g}{\ell}$ and $\ell \leq g$. Then, in any $(l, g+b-l)$ -KPS we have

$$H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | \mathbf{U}_F) = \sum_{i=1}^{\alpha} H(\mathbf{K}_{Y_i}).$$

This lemma is generalized as follows.

LEMMA 3.3. Let \mathcal{U} be a set of n users. Let t and p be two integers such that $\ell \leq t \leq g$ and $1 \leq p \leq b$ and let σ be an integer such that $\sigma \leq \binom{t}{\ell}$. If $G, F \subseteq \mathcal{U}$ are two disjoint subsets of t and p users respectively and Y_1, \dots, Y_σ are distinct l -subsets of G then, in any $(l, g+b-l)$ -KPS we have

$$H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\sigma} | \mathbf{U}_F) = \sum_{i=1}^{\sigma} H(\mathbf{K}_{Y_i}).$$

Proof. Let $X, B \subseteq \mathcal{U}$ be two subsets of \mathcal{U} of cardinality g and b respectively, such that $G \subseteq X, F \subseteq B$ and $X \cap B = \emptyset$. Let $\alpha = \binom{g}{\ell}$ and let Y_1, \dots, Y_α be distinct l -subsets of X . Then, from (11) and (12) of Appendix A, we get

$$\begin{aligned} \sum_{i=1}^{\alpha} H(\mathbf{K}_{Y_i}) &\geq H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | \mathbf{U}_F) \\ &\geq H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | \mathbf{U}_B) \\ &\quad \text{(from (15) of Appendix A as } F \subseteq B) \\ &= \sum_{i=1}^{\alpha} H(\mathbf{K}_{Y_i}) \quad \text{(from Lemma 3.2).} \end{aligned}$$

Hence, $H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | \mathbf{U}_F) = \sum_{i=1}^{\alpha} H(\mathbf{K}_{Y_i})$. Setting $X_1 = \mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\sigma}$, $X_2 = \mathbf{K}_{Y_{\sigma+1}} \dots \mathbf{K}_{Y_\alpha}$ and $\mathbf{Y} = \mathbf{U}_F$ in equation (11) of Appendix A, one gets that

$$\begin{aligned} H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | \mathbf{U}_F) &= H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\sigma} | \mathbf{U}_F) \\ &\quad + H(\mathbf{K}_{Y_{\sigma+1}} \dots \mathbf{K}_{Y_\alpha} | \mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\sigma} \mathbf{U}_F). \end{aligned}$$

Since, from (11) and (12) of Appendix A, one has

$$H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\sigma} | \mathbf{U}_F) \leq \sum_{i=1}^{\sigma} H(\mathbf{K}_{Y_i})$$

and

$$H(\mathbf{K}_{Y_{\sigma+1}} \dots \mathbf{K}_{Y_\alpha} | \mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\sigma} \mathbf{U}_F) \leq \sum_{i=\sigma+1}^{\alpha} H(\mathbf{K}_{Y_i}),$$

then, $H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | \mathbf{U}_F) = \sum_{i=1}^{\alpha} H(\mathbf{K}_{Y_i})$. Therefore, the lemma holds. \square

The next lemma will be required in the analysis of the security of our schemes.

LEMMA 3.4. Let \mathcal{U} be a set of n users and let $X_1, X_2 \subseteq \mathcal{U}$ be two distinct g -subsets. Let $F \subseteq \mathcal{U}$ be a subset of size b and let $p \in X_2 \setminus X_1$. Moreover, let α and β be integers

such that $\alpha \leq \binom{g}{\ell}$ and $\beta \leq \binom{g-1}{\ell-1}$, where $2 \leq \ell \leq g$. If Y_1, \dots, Y_α are distinct l -subsets of X_1 and Z_1, \dots, Z_β are distinct l -subsets of X_2 each containing p , then, in any $(l, g + b - l + 1)$ -KPS we have the following:

$$(i) \quad H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | \mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} U_F) = \sum_{i=1}^{\alpha} H(\mathbf{K}_{Y_i}),$$

$$\text{if } F \cap X_1 = \emptyset.$$

$$(ii) \quad H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | \mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} U_F) = \sum_{i=1}^{\beta} H(\mathbf{K}_{Z_i}),$$

$$\text{if } F \cap X_2 = \emptyset.$$

Proof. We have that

$$H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | U_p) = 0. \quad (1)$$

Indeed, from (11) and (15) of Appendix A, we get

$$\begin{aligned} H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | U_p) &\leq \sum_{i=1}^{\beta} H(\mathbf{K}_{Z_i} | Z_{i-1} \dots Z_1 U_p) \\ &\leq \sum_{i=1}^{\beta} H(\mathbf{K}_{Z_i} | U_p) \\ &= 0. \end{aligned}$$

The last equality follows from property 1 of Definition 2.1 since $p \in Z_i$. Notice that, from (13) of Appendix A, we get

$$\begin{aligned} \sum_{i=1}^{\alpha} H(\mathbf{K}_{Y_i}) &\geq H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha}) \\ &\geq H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | \mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} U_F) \\ &\quad (\text{from (12) of Appendix A}) \\ &\geq H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | U_p U_F) \\ &\quad (\text{from 2 of Lemma 3.1 and (1)}) \\ &= \sum_{i=1}^{\alpha} H(\mathbf{K}_{Y_i}). \end{aligned}$$

The last equality follows from Lemma 3.3. Indeed, we are considering an $(l, g + b - l + 1)$ -KPS and $|X_1| = g$, $|F \cup \{p\}| \leq b + 1$ and $(F \cup \{p\}) \cap X_1 = \emptyset$. Therefore, $H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | \mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} U_F) = \sum_{i=1}^{\alpha} H(\mathbf{K}_{Y_i})$. Thus, statement (i) is satisfied.

Let $X'_1 = X_1 \setminus F$. To prove statement (ii) we consider two cases.

Case 1. Assume that $|X'_1| \leq \ell - 1$. Then, $F \cap Y_j \neq \emptyset$, for any $1 \leq j \leq \alpha$, and it holds that,

$$H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | U_F) = 0. \quad (2)$$

Indeed, from (11) and (15) of Appendix A, we get

$$\begin{aligned} H(\mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} | U_F) &\leq \sum_{j=1}^{\alpha} H(\mathbf{K}_{Y_j} | \mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_{j-1}} U_F) \\ &\leq \sum_{j=1}^{\alpha} H(\mathbf{K}_{Y_j} | U_F) \\ &= 0. \end{aligned}$$

The last equality is satisfied since $H(\mathbf{K}_{Y_j} | U_F) = 0$, for $j = 1, \dots, \alpha$. In fact, if $k \in F \cap Y_j$, then, from property 1 of Definition 2.1, we have $H(\mathbf{K}_{Y_j} | U_k) = 0$. Applying inequality (12) of Appendix A, we obtain that $H(\mathbf{K}_{Y_j} | U_F) = 0$. From (2) and statement 1 of Lemma 3.1, we have

$$H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | \mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} U_F) = H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | U_F).$$

From Lemma 3.3 one gets that

$$H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | U_F) = \sum_{i=1}^{\beta} H(\mathbf{K}_{Z_i}),$$

since we are considering an $(l, b + g - l + 1)$ -KPS and, by hypothesis, we have that $|X_2| = g$, $|F| < b + 1$ and $X_2 \cap F = \emptyset$. Therefore,

$$H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | \mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} U_F) = \sum_{i=1}^{\beta} H(\mathbf{K}_{Z_i}),$$

and statement (ii) is satisfied.

Case 2. Let $|X'_1| \geq \ell$ and let σ be an integer such that $\sigma \leq \binom{|X'_1|}{\ell}$. If Y'_1, \dots, Y'_σ are distinct l -subsets of X'_1 such that $\{Y'_1, \dots, Y'_\sigma\} \subseteq \{Y_1, \dots, Y_\alpha\}$ and $\{Y''_{\sigma+1}, \dots, Y''_\alpha\} = \{Y_1, \dots, Y_\alpha\} \setminus \{Y'_1, \dots, Y'_\sigma\}$, then one gets that

$$\begin{aligned} H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | \mathbf{K}_{Y_1} \dots \mathbf{K}_{Y_\alpha} U_F) \\ = H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | \mathbf{K}_{Y'_1} \dots \mathbf{K}_{Y''_\sigma} U_F). \end{aligned} \quad (3)$$

Indeed, since $Y''_j \cap F \neq \emptyset$, for $j = \sigma + 1, \dots, \alpha$, proceeding as in Case 1, one can easily see that $H(\mathbf{K}_{Y''_{\sigma+1}} \dots \mathbf{K}_{Y''_\alpha} | U_F) = 0$. Therefore, applying statement 2 of Lemma 3.1 we get (3). From statement (i) we have that

$$\begin{aligned} A &\triangleq H(\mathbf{K}_{Y'_1} \dots \mathbf{K}_{Y'_\sigma} | \mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} U_F) \\ &= \sum_{i=1}^{\sigma} H(\mathbf{K}_{Y'_i}), \end{aligned} \quad (4)$$

since we can always see the l -subsets Y'_1, \dots, Y'_σ of X'_1 as l -subsets of a g -superset of X'_1 , say X_3 , distinct from X_2 and such that $X_3 \cap F = \emptyset$ (we can add $g - |X'_1|$ users not in F to X'_1). Moreover, since we are considering an $(l, b + g - l + 1)$ -KPS, from Lemma 3.3 one can see that

$$B \triangleq H(\mathbf{K}_{Y'_1} \dots \mathbf{K}_{Y'_\sigma} | U_F) = \sum_{i=1}^{\sigma} H(\mathbf{K}_{Y'_i}). \quad (5)$$

Setting $X = \mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta}$, $Y = \mathbf{K}_{Y'_1} \dots \mathbf{K}_{Y'_\sigma}$ and $Z = U_F$, then from (14) of Appendix A and from equations (4) and (5), we have that

$$\begin{aligned} H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | \mathbf{K}_{Y'_1} \dots \mathbf{K}_{Y'_\sigma} U_F) \\ = H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | U_F) + A - B \\ = H(\mathbf{K}_{Z_1} \dots \mathbf{K}_{Z_\beta} | U_F). \end{aligned}$$

Finally, since the sets X_2 and F satisfy $|X_2| = g$, $|F| < b + 1$ and $X_2 \cap F = \emptyset$ and we are considering an $(l, b + g - l + 1)$ -KPS then, from Lemma 3.3, it follows that $H(K_{Z_1} \dots K_{Z_\beta} | U_F) = \sum_{i=1}^{\beta} H(K_{Z_i})$. Therefore, $H(K_{Z_1} \dots K_{Z_\beta} | K_{Y'_1} \dots K_{Y'_\sigma} U_F) = \sum_{i=1}^{\sigma} H(K_{Y'_i})$ and the lemma holds. \square

This lemma states that if a coalition F of adversaries knows the keys used by the l -subsets of X_2 then it has no information about the keys used by the l -subsets of X_1 if F and X_1 are disjoint. On the other hand, if a coalition F of adversaries knows the keys used by the l -subsets of X_1 then it has no information about the keys used by the l -subsets of X_2 if F and X_2 are disjoint.

4. A τ -RESTRICTED KEY AGREEMENT SCHEME

In this section we describe a protocol to realize a τ -restricted key agreement scheme that can be used by τ distinct conferences to set up a common key. For certain values of the parameters, the scheme we propose distributes less information than the trivial scheme obtained by considering τ independent copies of a one-restricted scheme.

We need some definitions and results from design theory. A *design* is a pair (V, \mathcal{B}) , where V is a set of n elements (called *points*) and \mathcal{B} is a set of subsets of V of fixed size k , where $k \geq 2$ (called *blocks*). A *parallel class* of (V, \mathcal{B}) consists of n/k blocks from \mathcal{B} which partition the set V . The design (V, \mathcal{B}) is said to be *resolvable* if the set of blocks, \mathcal{B} , can be partitioned into parallel classes. If \mathcal{B} consists of all k -subsets of V , then (V, \mathcal{B}) is called the *complete k -uniform hypergraph* on V .

We will use the following theorem of Baranyai, a proof of which can be found in [18, Theorem 36.1].

THEOREM 4.1. *The complete k -uniform hypergraph on n points is resolvable if $n \equiv 0 \pmod k$.*

In the scheme we propose there is no effective interaction among the users. Every member i of a conference G independently chooses a random value $m^{(i)}$ and uses its secret information to compute an encrypted version of $m^{(i)}$ which is broadcast. Then, the key of $G = \{i_1, \dots, i_g\}$, with $i_1 < \dots < i_g$, will be $k_G = (m^{(i_1)}, \dots, m^{(i_g)})$.

Notice that in the following the sets elements are listed sequentially in increasing order.

The protocol provided in [7], which is a one-time key agreement scheme, is a building block of our scheme. Therefore, we recall it.

A protocol for the one-restricted key agreement scheme

Let $\mathcal{U} = \{1, \dots, n\}$ be a set of n users and let $G \subseteq \mathcal{U}$ be a conference of size g . Suppose that $\ell \geq 2$ is an integer such that $g \equiv 1 \pmod{\ell - 1}$ and that $k \geq 1$ is an integer. The set-up phase consists of the TA distributing secret information corresponding to an $(\ell, b + g - \ell)$ -KPS described in Appendix B, implemented over $(Z_{p^k})^\ell$, with p prime. For an ℓ -subset of users A , we denote by k_A the key associated with A . We think of k_A as being made

up of ℓ independent keys over Z_{p^k} , which we denote by $k_{A,1}, \dots, k_{A,\ell}$. Each user h of a conference G performs the following steps.

1. Chooses a random value $m^{(h)} = (m_1^h, \dots, m_r^h) \in (Z_{p^k})^r$, where $r = \binom{g-2}{\ell-2}$.
2. Partitions the complete $(\ell - 1)$ -uniform hypergraph on $G \setminus \{h\}$ into r parallel classes C_1, \dots, C_r , which all consist of $\chi = (g - 1)/(\ell - 1)$ blocks that we denote with $B_{i,j}^h$ for $1 \leq i \leq r$ and $1 \leq j \leq \chi$.
3. For each block $B_{i,j}^h$ denote with $B(i, j, h)$ the set $B_{i,j}^h \cup \{h\} = \{x_1, \dots, x_\ell\}$ and let $\alpha_{i,j}^h$ denote the index such that $x_{\alpha_{i,j}^h} = h$.
4. Encrypts each m_i^h using the χ keys $k_{B(i,j,h), \alpha_{i,j}^h}$ by defining

$$b_{i,j}^h = k_{B(i,j,h), \alpha_{i,j}^h} + m_i^h \pmod{p^k},$$

for $1 \leq i \leq r$ and $1 \leq j \leq \chi$.

5. Broadcast the vector

$$b^{(h)} = (b_{1,1}^h, \dots, b_{1,\chi}^h, \dots, b_{r,1}^h, \dots, b_{r,\chi}^h).$$

The secret key is the value $k_G = (m^{(1)}, \dots, m^{(g)})$ which can be decrypted by anyone in G from the global broadcast $b_G = (b^{(1)}, \dots, b^{(g)})$.

The next simple example illustrates the steps of this protocol.

EXAMPLE 4.1. Suppose that $g = 5$ and $\ell = 3$. Note that $5 \equiv 1 \pmod 2$. Suppose that the conference set is $G = \{1, 2, 3, 4, 5\}$. For each user $i \in G$, we partition the two-subsets of $G \setminus \{i\}$ into $r = 3$ disjoint parallel classes. Later, we describe only the ones related to user 4.

$$\begin{aligned} C_1^4 &= \{\{1, 2\}, \{3, 5\}\}, & C_2^4 &= \{\{1, 3\}, \{2, 5\}\}, \\ C_3^4 &= \{\{1, 5\}, \{2, 3\}\}. \end{aligned}$$

Consider the computations performed by user 4. First, user 4 picks three random values (i.e. his part of the key), say $m_1^4, m_2^4, m_3^4 \in Z_{p^k}$. Next, he computes the relevant α values. These are as follows:

$$\begin{aligned} \alpha_{1,1}^4 &= 3, & \alpha_{1,2}^4 &= 2, & \alpha_{2,1}^4 &= 3 \\ \alpha_{2,2}^4 &= 2, & \alpha_{3,1}^4 &= 2, & \alpha_{3,2}^4 &= 3. \end{aligned}$$

This determines the values broadcast by user 4:

$$\begin{aligned} b^{(4)} &= (m_1^4 + k_{\{1,2,4\},3}, m_1^4 + k_{\{3,4,5\},2}, m_2^4 + k_{\{1,3,4\},3}, \\ & m_2^4 + k_{\{2,4,5\},2}, m_3^4 + k_{\{1,4,5\},2}, m_3^4 + k_{\{2,3,4\},3}). \end{aligned}$$

The security of this protocol derives from the observation that any coalition F of b users such that $F \cap G = \emptyset$, has no information about the key after the observation of the broadcast, even if they pool all their secret information. Indeed, as proved in Lemma 3.3 of [7], the $\binom{g}{\ell}$ keys used by the conference appear to any disjoint coalition to be independent random elements of Z_{p^k} . Since each of these

keys is used exactly once (the definition of the indices $\alpha_{i,j}^h$ ensures that every $k_{A,j}$ is used to encrypt exactly one $m_{i,j}$), they function as a series of one-time pads.

Now we have all the necessary tools for the description of the protocol for a τ -restricted key agreement scheme.

Protocol for the τ -restricted key agreement scheme

Let $\mathcal{U} = \{1, \dots, n\}$ be a set of n users and let $G_1, \dots, G_\tau \subseteq \mathcal{U}$ be τ distinct conferences of size g . Suppose that $\ell \geq 2$ is an integer such that $g \equiv 1 \pmod{\ell - 1}$.

Distribution phase

- The TA distributes secret information corresponding to the KPS described in Appendix B. More precisely, the TA uses $\tau - 1$ copies of an $(\ell, b + g - \ell + 1)$ -KPS, say $\Delta_1, \dots, \Delta_{\tau-1}$, implemented over $(Z_{p^{k_1}})^\ell, \dots, (Z_{p^{k_{\tau-1}}})^\ell$, respectively and an $(\ell, b + g - \ell)$ -KPS, say Δ_τ , implemented over $(Z_{p^{k_\tau}})^\ell$, with p prime and $k_i \leq k_1$, for $2 \leq i \leq \tau$.

Key computation phase

- When users in a conference G_1 want to compute a common key, they perform the steps from 1 to 5 of the protocol for the one-restricted key agreement scheme Δ_1 . For $G_1 = \{i_1, \dots, i_g\}$, $i_1 < \dots < i_g$, the final key k_{G_1} will be $(m^{(i_1)}, \dots, m^{(i_g)})$.
- When users in a conference G_t , with $2 \leq t \leq \tau$, want to compute a common key they perform the steps from 1 to 5 of the protocol for the one-restricted key agreement scheme Δ_t . Since, for $2 \leq t \leq \tau$, we have that $G_t \setminus G_{t-1} \neq \emptyset$, then let $h_t \in G_t \setminus G_{t-1}$ be the user with 'minimum' identity. Using the scheme Δ_{t-1} implemented over $(Z_{p^{k_{t-1}}})^\ell$, user h_t performs the following steps:
 1. For $r = \binom{g-2}{\ell-2}$, he chooses a random value $m^{(h_t)} = (m_1^{h_t}, \dots, m_r^{h_t}) \in (Z_{p^{\ell k_{t-1}}})^r$.
 2. Partitions the complete $(\ell - 1)$ -uniform hypergraph on $G_t \setminus \{h_t\}$ into r parallel classes C_1, \dots, C_r , which consist of all $\chi = \frac{g-1}{\ell-1}$ blocks that we denote with $B_{i,j}^{h_t}$, for $1 \leq i \leq r$ and $1 \leq j \leq \chi$.
 3. Encrypts each $m_i^{h_t}$ using the χ keys $k_{B(i,j,h_t)}$, where $B(i, j, h_t) = B_{i,j}^{h_t} \cup \{h_t\}$, by defining

$$b_{i,j}^{h_t} = k_{B(i,j,h_t)} + m_i^{h_t} \pmod{p^{\ell k_{t-1}}},$$

for $1 \leq i \leq r$ and $1 \leq j \leq \chi$.

4. Broadcasts the vector

$$b^{(h_t)} = (b_{1,1}^{h_t}, \dots, b_{1,\chi}^{h_t}, \dots, b_{r,1}^{h_t}, \dots, b_{r,\chi}^{h_t}).$$

For $G_t = \{j_1, \dots, j_g\}$, with $j_1 < \dots < j_g$ and $h_t \in G_t \setminus G_{t-1}$, the key k_{G_t} is $(m^{(j_1)}, \dots, m^{(j_g)}, m^{(h_t)})$.

Our scheme requires that users hold a counter which is incremented each time a conference key is generated.

To familiarize ourselves with the concepts used in the general construction we give an example of a two-restricted key agreement scheme.

EXAMPLE 4.2. Let $\tau = 2$, $n \geq 7$, $g = 5$ and $\ell = 3$. Suppose that the conferences $G_1 = \{1, 3, 4, 5, 6\}$ and $G_2 = \{1, 2, 3, 4, 7\}$ want to set up a common key.

Distribution phase

The TA distributes secret information corresponding to the KPS described in Appendix B. He uses a copy of a $(3, b+3)$ -KPS, say Δ_1 , implemented over $(Z_{p^{k_1}})^3$ and a copy of a $(3, b+2)$ -KPS, say Δ_2 , implemented over $(Z_{p^{k_2}})^3$, with p prime and $k_2 \leq k_1$.

Key computation phase

When users in the conference G_1 want to compute a common key, they perform the steps from 1 to 5 of the protocol for the one-restricted key agreement scheme using the scheme Δ_1 implemented over $(Z_{p^{k_1}})^3$. More precisely, each user $i \in G_1$, partitions the two-subsets of $G_1 \setminus \{i\}$ into $r = 3$ disjoint parallel classes. For example, user 1 computes the following classes:

$$C_1^1 = \{\{3, 4\}, \{5, 6\}\}, \quad C_2^1 = \{\{3, 5\}, \{4, 6\}\}, \\ C_3^1 = \{\{3, 6\}, \{4, 5\}\}.$$

Consider the computations performed by user 1. First, user 1 picks three random values (i.e. his part of the key), say $m_1^1, m_2^1, m_3^1 \in Z_{p^{k_1}}$. Next, he computes the relevant α values. These are as follows:

$$\alpha_{1,1}^1 = 1, \quad \alpha_{1,2}^1 = 1, \quad \alpha_{2,1}^1 = 1 \\ \alpha_{2,2}^1 = 1, \quad \alpha_{3,1}^1 = 1, \quad \alpha_{3,2}^1 = 1.$$

This determines the values broadcast by user 1.

$$b^{(1)} = (m_1^1 + k_{\{1,3,4\},1}, m_1^1 + k_{\{1,5,6\},1}, m_2^1 + k_{\{1,3,5\},1}, \\ m_2^1 + k_{\{1,4,6\},1}, m_3^1 + k_{\{1,3,6\},1}, m_3^1 + k_{\{1,4,5\},1}).$$

The key k_{G_1} will be $(m^{(1)}, m^{(3)}, m^{(4)}, m^{(5)}, m^{(6)})$, where $m^{(i)} = (m_1^i, m_2^i, m_3^i)$.

When users in the conference G_2 want to compute a common key, they perform the steps from 1 to 5 of the protocol for the one restricted key agreement scheme using the scheme Δ_2 implemented over $(Z_{p^{k_2}})^3$. Precisely, each user $i \in G_2$, partitions the two-subsets of $G_2 \setminus \{i\}$ into $r = 3$ disjoint parallel classes. For example, user 3 computes the following classes.

$$C_1^3 = \{\{1, 2\}, \{4, 7\}\}, \quad C_2^3 = \{\{1, 4\}, \{2, 7\}\}, \\ C_3^3 = \{\{1, 7\}, \{2, 4\}\}.$$

Then user 3 picks three random values (i.e. his part of the key), say $m_1^3, m_2^3, m_3^3 \in Z_{p^{k_2}}$. Next, he computes the relevant α values. These are as follows:

$$\alpha_{1,1}^3 = 3, \quad \alpha_{1,2}^3 = 1, \quad \alpha_{2,1}^3 = 2 \\ \alpha_{2,2}^3 = 2, \quad \alpha_{3,1}^3 = 2, \quad \alpha_{3,2}^3 = 2.$$

This determines the values broadcast by user 3

$$b^{(3)} = (m_1^3 + k_{\{1,2,3\},3}, m_1^3 + k_{\{3,4,7\},1}, m_2^3 + k_{\{1,3,4\},2}, \\ m_2^3 + k_{\{2,3,7\},2}, m_3^3 + k_{\{1,3,7\},2}, m_3^3 + k_{\{2,3,4\},2}).$$

Moreover, the user 2 $\in G_2 \setminus G_1$ (having minimum identity) performs the following computation using the information distributed with the scheme Δ_1 . Partitions the two-subsets of $G_2 \setminus \{2\}$ into $r = 3$ disjoint parallel classes

$$C_1^2 = \{\{1, 3\}, \{4, 7\}\}, \quad C_2^2 = \{\{1, 4\}, \{3, 7\}\}, \\ C_3^2 = \{\{1, 7\}, \{3, 4\}\}.$$

Then, user 2 picks three random values, say $\widehat{m}_1^2, \widehat{m}_2^2, \widehat{m}_3^2 \in \mathbf{Z}_{p^{3k_1}}$. Next, he computes the new broadcast

$$b^{(2)} = (\widehat{m}_1^2 + k_{\{1,2,3\}}, \widehat{m}_1^2 + k_{\{2,4,7\}}, \widehat{m}_2^2 + k_{\{1,2,4\}}, \\ \widehat{m}_2^2 + k_{\{2,3,7\}}, \widehat{m}_3^2 + k_{\{1,2,7\}}, \widehat{m}_3^2 + k_{\{2,3,4\}}).$$

Notice that the modular additions are done in $\mathbf{Z}_{p^{3k_1}}$. In fact, since only user 2 issues a broadcast, then we allow him to use all three entries of the key he shares with any subset of 2 users in G_2 . The key k_{G_2} will be $(m^{(1)}, m^{(2)}, m^{(3)}, m^{(4)}, m^{(7)}, \widehat{m}^{(2)})$.

4.1. The security of the scheme

In this section we show that the protocol proposed in Section 4 indeed realizes a τ -restricted KAS, that is, it satisfies Definition 2.3.

Each conference key is the concatenation of random values chosen by the users during the key computation phase. Hence, the key is independent from the *a priori* information held by the users and, for any conference G , we have that $H(\mathbf{K}_G | \mathbf{U}) = H(\mathbf{K}_G)$. Thus, condition 1 of Definition 2.3 is satisfied.

It is easy to see that each user in a conference can compute a common key. In fact, each user in a conference G broadcasts his part of the key in such a way that all other users in G are able to decrypt the broadcast value. Hence, $H(\mathbf{K}_G | \mathbf{U}_i \mathbf{B}_G) = 0$, for each conference G and each user i in G . Thus, condition 2 of Definition 2.3 is satisfied.

To prove that our scheme is secure, we have to show that if $F \cap G_i = \emptyset$

$$H(\mathbf{K}_{G_i} | \mathbf{B}_{G_1}, \dots, \mathbf{B}_{G_\tau} \mathbf{U}_F) = H(\mathbf{K}_{G_i}). \quad (6)$$

We will give a sketch of a proof that equation (6) holds for any conference G_i , with $1 < i < \tau$. The cases $i = 1$ and $i = \tau$ can be deduced from the following analysis in a straightforward way. The users in the conference G_i , for $1 < i < \tau$, use the schemes Δ_i and Δ_{i-1} . Moreover, the scheme Δ_{i-1} (respectively, Δ_i) is also used by the users in G_{i-1} (respectively, G_{i+1}). Notice that the common key k_{G_i} , computed by the conference G_i , can be thought of as $k_{G_i}^{\Delta_i} k_{G_i}^{\Delta_{i-1}}$, where $k_{G_i}^{\Delta_i}$ (respectively, $k_{G_i}^{\Delta_{i-1}}$) is the part of k_{G_i} computed using the scheme Δ_i (respectively, Δ_{i-1}). In a similar way, b_{G_i} can be thought of as $b_{G_i}^{\Delta_i} b_{G_i}^{\Delta_{i-1}}$, where

$b_{G_i}^{\Delta_i}$ (respectively, $b_{G_i}^{\Delta_{i-1}}$) is the part of the broadcast b_{G_i} computed using the scheme Δ_i (respectively, Δ_{i-1}).

Since the schemes $\Delta_1, \dots, \Delta_\tau$ are independent, the users in F could derive some information on k_{G_i} only from the broadcast messages b_{G_i} , $b_{G_{i-1}}^{\Delta_{i-1}}$ and $b_{G_{i+1}}^{\Delta_i}$. Therefore, to prove that equation (6) holds, it is enough to show that the following equality is satisfied:

$$H(\mathbf{K}_{G_i} | \mathbf{B}_{G_{i-1}}^{\Delta_{i-1}} \mathbf{B}_{G_i} \mathbf{B}_{G_{i+1}}^{\Delta_i} \mathbf{U}_F) = H(\mathbf{K}_{G_i}).$$

Intuitively, since the schemes Δ_i and Δ_{i-1} are constructed independently, then in order to prove that the equality holds it is sufficient to show that the following two equalities are satisfied:

$$H(\mathbf{K}_{G_i}^{\Delta_i} | \mathbf{B}_{G_i}^{\Delta_i} \mathbf{B}_{G_{i+1}}^{\Delta_i} \mathbf{U}_F) = H(\mathbf{K}_{G_i}^{\Delta_i})$$

and

$$H(\mathbf{K}_{G_i}^{\Delta_{i-1}} | \mathbf{B}_{G_i}^{\Delta_{i-1}} \mathbf{B}_{G_{i-1}}^{\Delta_{i-1}} \mathbf{U}_F) = H(\mathbf{K}_{G_i}^{\Delta_{i-1}}).$$

We will prove that $H(\mathbf{K}_{G_i}^{\Delta_i} | \mathbf{B}_{G_i}^{\Delta_i} \mathbf{B}_{G_{i+1}}^{\Delta_i} \mathbf{U}_F) = H(\mathbf{K}_{G_i}^{\Delta_i})$; the other equality can be proved in a similar way.

It is intuitively clear that a coalition F of users disjoint from the privileged set G_i has no information about $k_{G_i}^{\Delta_i}$ after the observation of the broadcast, even if they pool all their secret information. This is because of the property, which we proved in Lemma 3.4, that the $\binom{g}{\ell}$ keys of the scheme Δ_i used to distribute $k_{G_i}^{\Delta_i}$, as well as the $\binom{g-1}{\ell-1}$ keys of the scheme Δ_i used by the user with 'minimum' identity in $G_{i+1} \setminus G_i$ to distribute $k_{G_{i+1}}^{\Delta_i}$ appear to F to be independent random elements of $\mathbf{Z}_{p^{k_1}}$. Each of these keys is used to encrypt one element of $\mathbf{Z}_{p^{k_1}}$ and thus these keys function as a series of one-time pads. A formal proof of the security of the scheme can be obtained by a straightforward modification of the one given in [6]. Hence, condition 3 of Definition 2.3 is satisfied. Thus, our protocol realizes a τ -restricted key agreement scheme.

4.2. The information distributed

In this section we consider the amount of information given to any user in our τ -restricted key agreement scheme. We show that for certain values of the parameters the scheme we propose distributes less information than the trivial one obtained by considering τ independent copies of a one-time scheme.

In our scheme, the key computed by the users in G_1 is a random element of $(\mathbf{Z}_{p^{k_1}})^{g^r}$; while, for $2 \leq t \leq \tau$, the key computed by the users in G_t is a random element of $(\mathbf{Z}_{p^{k_t}})^{g^r} \times (\mathbf{Z}_{p^{k_{t-1}}})^{\ell^r}$. Since the key computed by all the conferences has to be taken from domains of the same size, then it must be that $p^{g^r k_1} = p^{g^r k_t} \cdot p^{\ell^r k_{t-1}}$, for $2 \leq t \leq \tau$. Hence,

$$gk_1 = gk_t + \ell k_{t-1}, \quad \text{for } 2 \leq t \leq \tau. \quad (7)$$

In the following we prove that, for any integers g and ℓ such that $2 \leq \ell \leq g$, there always exist positive integers k_1, \dots, k_τ satisfying this equation. The next lemma holds.

LEMMA 4.2. Let g and ℓ be two positive integers such that $2 \leq \ell \leq g$. Let $I_1 = 1$ and $I_t = g^{t-1} - \ell I_{t-1}$, for $2 \leq t \leq \tau$. If $gk_1 = gk_t + \ell k_{t-1}$, for $2 \leq t \leq \tau$, then it holds that $k_t = k_1 \cdot \frac{I_t}{g^{t-1}}$ for $1 \leq t \leq \tau$.

Proof. We prove this lemma by induction on t . If $t = 1$ we have that $k_1 = I_1 \cdot k_1 = k_1$. Now, suppose that the lemma is true for some $t < \tau$. Then, we prove it for $t + 1$. From (7) we have that $gk_1 = gk_{t+1} + \ell k_t$. Using the inductive hypothesis, we get $gk_{t+1} = k_1(g - \ell \frac{I_t}{g^{t-1}}) = \frac{k_1}{g^{t-1}}(g^t - \ell I_t)$. Since $I_{t+1} = g^t - \ell I_t$, then it follows that $k_{t+1} = k_1 \cdot \frac{I_{t+1}}{g^t}$. Thus, the lemma holds. \square

From this lemma it is easy to see that, for any integers g and ℓ such that $2 \leq \ell \leq g$, there always exist positive integers k_1, \dots, k_τ satisfying equation (7). For example, if we set $k_1 = g^{\tau-1}$, then it follows that $k_t = g^{\tau-t} I_t$ for $t = 2, \dots, \tau$.

In our scheme, since the key is a random element of $(Z_{p^{k_1}})^{g^\tau}$, then the entropy of the key is

$$H(\mathbf{K}) = gk_1 \binom{g-2}{\ell-2} \log p;$$

whereas, for each user i , we have that

$$H(U_i) = \ell(k_1 + \dots + k_{\tau-1}) \binom{g+b}{\ell-1} \log p \\ + \ell k_\tau \binom{g+b-1}{\ell-1} \log p.$$

The efficiency of the constructions can be measured by considering the amount of secret information stored by each user compared to the information content of the key. In our scheme, we have that

$$\frac{H(U_i)}{H(\mathbf{K})} = \frac{\ell(k_1 + \dots + k_{\tau-1}) \binom{g+b}{\ell-1}}{gk_1 \binom{g-2}{\ell-2}} + \frac{\ell k_\tau \binom{g+b-1}{\ell-1}}{gk_1 \binom{g-2}{\ell-2}};$$

whereas, in the protocol for a one-restricted key agreement scheme we have that

$$\frac{H(U_i)}{H(\mathbf{K})} = \frac{\ell \binom{g+b-1}{\ell-1}}{g \binom{g-2}{\ell-2}}, \quad (8)$$

since the information is distributed according to the $(l, b + g - l)$ -KPS of Appendix B.

Now we compare the information distributed by the TA in our protocol with the information distributed in the trivial protocol realized by considering τ independent copies of a one-restricted key agreement scheme. The following lemma holds.

LEMMA 4.3. Let τ be an integer greater than 1 and let g and ℓ be two positive integers such that $2 \leq \ell \leq g$. If $gk_1 = gk_t + \ell k_{t-1}$ for $2 \leq t \leq \tau$, then there exist integers k_1, \dots, k_τ such that

$$\frac{(k_1 + \dots + k_{\tau-1}) \binom{g+b}{\ell-1}}{k_1 \binom{g-2}{\ell-2}} + \frac{k_\tau \binom{g+b-1}{\ell-1}}{k_1 \binom{g-2}{\ell-2}} \leq \tau \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}} \quad (9)$$

if and only if $\ell^2 - (b+1)\ell - g \leq 0$.

Proof. Our proof is by induction on τ . If $\tau = 2$ it is easy to see that, setting $k_1 = g$ and $k_2 = g - \ell$, equation (7) holds and

$$\left[\frac{\binom{g+b}{\ell-1}}{\binom{g-2}{\ell-2}} + \frac{k_2 \binom{g+b-1}{\ell-1}}{k_1 \binom{g-2}{\ell-2}} \right] \leq 2 \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}}$$

is satisfied if and only if

$$g \binom{g+b}{\ell-1} \leq (g+\ell) \binom{g+b-1}{\ell-1}.$$

This inequality holds if and only if $g(b+g) \leq (g+\ell)(g+b-\ell+1)$. A simple algebra shows that the previous inequality is satisfied if and only if $\ell^2 - (b+1)\ell - g \leq 0$. Now, suppose that inequality (9) is satisfied for some $\tau > 2$. Then, we prove that such an inequality holds for $\tau + 1$. Denote with

$$A(\tau) \triangleq \frac{(k_1 + \dots + k_{\tau-1}) \binom{g+b}{\ell-1}}{k_1 \binom{g-2}{\ell-2}} + \frac{k_\tau \binom{g+b-1}{\ell-1}}{k_1 \binom{g-2}{\ell-2}},$$

and

$$B(\tau) \triangleq \tau \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}}.$$

From Lemma 4.2, setting $k_t = k_1 \frac{I_t}{g^{t-1}}$ for $1 \leq t \leq \tau$, we have that

$$\frac{(k_1 + \dots + k_{\tau-1}) \binom{g+b}{\ell-1}}{k_1 \binom{g-2}{\ell-2}} + \frac{k_\tau \binom{g+b-1}{\ell-1}}{k_1 \binom{g-2}{\ell-2}} \\ = \left(1 + \frac{I_2}{g} + \dots + \frac{I_{\tau-1}}{g^{\tau-2}} \right) \frac{\binom{g+b}{\ell-1}}{\binom{g-2}{\ell-2}} + \frac{I_\tau \binom{g+b-1}{\ell-1}}{g^{\tau-1} \binom{g-2}{\ell-2}}.$$

Since for any pair of positive integers r and s , with $r \leq s-1$, we have that $\binom{s}{r} = \binom{s-1}{r-1} + \binom{s-1}{r}$, then it follows that

$$\left(1 + \frac{I_2}{g} + \dots + \frac{I_{\tau-1}}{g^{\tau-2}} \right) \frac{\binom{g+b}{\ell-1}}{\binom{g-2}{\ell-2}} + \frac{I_\tau \binom{g+b-1}{\ell-1}}{g^{\tau-1} \binom{g-2}{\ell-2}} \\ = \left(1 + \frac{I_2}{g} + \dots + \frac{I_\tau}{g^{\tau-1}} \right) \frac{\binom{g+b}{\ell-1}}{\binom{g-2}{\ell-2}} - \frac{I_\tau \binom{g+b-1}{\ell-1}}{g^{\tau-1} \binom{g-2}{\ell-2}}.$$

Applying the inductive hypothesis, we have that

$$\left(1 + \frac{I_2}{g} + \dots + \frac{I_\tau}{g^{\tau-1}} \right) \frac{\binom{g+b}{\ell-1}}{\binom{g-2}{\ell-2}} - \frac{I_\tau \binom{g+b-1}{\ell-1}}{g^{\tau-1} \binom{g-2}{\ell-2}} \\ \leq \tau \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}},$$

if and only if $\ell^2 - (b+1)\ell - g \leq 0$. Hence, it follows that

$$\left(1 + \frac{I_2}{g} + \dots + \frac{I_\tau}{g^{\tau-1}} \right) \frac{\binom{g+b}{\ell-1}}{\binom{g-2}{\ell-2}} + \frac{I_{\tau+1} \binom{g+b-1}{\ell-1}}{g^\tau \binom{g-2}{\ell-2}} \\ \leq \tau \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}} + \frac{I_\tau \binom{g+b-1}{\ell-1}}{g^{\tau-1} \binom{g-2}{\ell-2}} + \frac{I_{\tau+1} \binom{g+b-1}{\ell-1}}{g^\tau \binom{g-2}{\ell-2}}$$

if and only if $\ell^2 - (b+1)\ell - g \leq 0$. From Lemma 4.2, we have that $I_{\tau+1} = g^\tau - \ell I_\tau$. Therefore, it results that

$$\begin{aligned} & \left(1 + \frac{I_2}{g} + \dots + \frac{I_\tau}{g^{\tau-1}}\right) \frac{\binom{g+b}{\ell-1}}{\binom{g-2}{\ell-2}} + \frac{I_{\tau+1}}{g^\tau} \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}} \\ & \leq (\tau+1) \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}} + \frac{I_\tau}{g^{\tau-1}} \frac{\binom{g+b-1}{\ell-2}}{\binom{g-2}{\ell-2}} - \ell \frac{I_\tau}{g^\tau} \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}} \end{aligned}$$

if and only if $\ell^2 - (b+1)\ell - g \leq 0$. It is immediate to see that

$$\left(1 + \frac{I_2}{g} + \dots + \frac{I_\tau}{g^{\tau-1}}\right) \frac{\binom{g+b}{\ell-1}}{\binom{g-2}{\ell-2}} + \frac{I_{\tau+1}}{g^\tau} \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}} = A(\tau+1)$$

and

$$(\tau+1) \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}} = B(\tau+1).$$

Hence, to prove that $A(\tau+1) \leq B(\tau+1)$, it is enough to show that

$$\frac{I_\tau}{g^{\tau-1}} \frac{\binom{g+b-1}{\ell-2}}{\binom{g-2}{\ell-2}} - \ell \frac{I_\tau}{g^\tau} \frac{\binom{g+b-1}{\ell-1}}{\binom{g-2}{\ell-2}} \leq 0.$$

Elementary algebra shows that this inequality holds if and only if $\ell^2 - (b+1)\ell - g \leq 0$. Thus, the lemma holds. \square

From the previous lemma, one can easily see that, for certain values of the parameters, our τ -restricted KAS distributes less information to the users than the trivial scheme obtained by considering τ copies of a one-restricted KAS. Indeed, as shown in Lemma 4.3, our scheme is better if and only if $\ell^2 - (b+1)\ell - g \leq 0$. There always exist values for which the previous inequality holds. In fact, this inequality is satisfied if and only if

$$2 \leq \ell \leq \left\lfloor \frac{b+1 + \sqrt{(b+1)^2 + 4g}}{2} \right\rfloor,$$

from which one gets that our scheme is better than the trivial one, if and only if $2 \leq \ell \leq \min\{g, b+1\}$, provided that $g \equiv 1 \pmod{\ell-1}$.

5. CONCLUSIONS

In this paper we have analysed τ -restricted key agreement schemes. Such schemes allow the computation of τ common keys for τ distinct conferences. We have presented a protocol which utilizes τ suitable key predistribution schemes as building blocks to realize a τ -restricted key agreement scheme. For certain values of the parameters, the scheme that we have presented distributes less information than the trivial one obtained by considering τ copies of a one-restricted key agreement scheme.

ACKNOWLEDGEMENTS

The authors are partially supported by the Italian Ministry of University and Scientific Research (MURST). We would

like to thank the anonymous referees for their careful reading and useful comments and suggestions which improved the readability of the paper.

REFERENCES

- [1] Blom, R. (1984) An optimal class of symmetric key generation systems. *Lecture Notes in Computer Science*, **209**, 335–338.
- [2] Gong, L. and Wheeler, D. J. (1990) A matrix key-distribution scheme. *J. Cryptology*, **2**, 51–59.
- [3] Matsumoto, T. and Imai, H. (1987) On the key predistribution system: a practical solution to the key distribution problem. *Lecture Notes in Computer Science*, **239**, 185–193.
- [4] Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U. and Yung, M. (1993) Perfectly-secure key distribution for dynamic conferences. *Lecture Notes in Computer Science*, **740**, 471–486.
- [5] Beimel, A. and Chor, B. (1994) Interaction in key distribution schemes. *Lecture Notes in Computer Science*, **773**, 444–455.
- [6] Beimel, A. and Chor, B. (1996) Communication in key distribution schemes. *IEEE Trans. Inform. Theory*, **42**, 19–28.
- [7] Blundo, C., Frota Mattos, L. A. and Stinson, D. R. (1998) Generalized Beimel–Chor schemes for broadcast encryption and interactive key distribution. *Theor. Comput. Sci.*, **200**, 313–334.
- [8] Fiat, A. and Naor, M. (1994) Broadcast encryption. *Lecture Notes in Computer Science*, **773**, 480–491.
- [9] Berkovits, S. (1992) How to broadcast a secret. *Lecture Notes in Computer Science*, **547**, 536–541.
- [10] Blundo, C. and Cresti, A. (1995) Space requirements for broadcast encryption. *Lecture Notes in Computer Science*, **950**, 287–298.
- [11] Blundo, C. and Cresti, A. (1996) Broadcast encryption schemes with disenrollment capability. *5th Italian Conf. Theoretical Computer Science*, pp. 176–191. World Scientific, Singapore.
- [12] Blundo, C., Frota Mattos, L. A. and Stinson, D. R. (1996) Multiple key distribution maintaining user anonymity via broadcast channels. *J. Comput. Security*, **3**, 309–323.
- [13] Blundo, C., Frota Mattos, L. A. and Stinson, D. R. (1996) Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution. *Lecture Notes in Computer Science*, **1109**, 387–400.
- [14] Chor, B., Fiat, A. and Naor, M. (1994) Tracing traitors. *Lecture Notes in Computer Science*, **839**, 257–270.
- [15] Just, M., Kranakis, E., Krizanc, D. and van Oorschot, P. (1994) Key distribution via true broadcasting. In *Proc. 2nd ACM Conf. on Computer and Communications Security*, pp. 81–88.
- [16] Stinson, D. R. (1997) On some methods for unconditionally secure key distribution and broadcast encryption. *Designs, Codes and Cryptography*, **12**, 215–243.
- [17] Blundo, C. and Cresti, A. (1998) *Lower Bounds for Unconditional Secure Key Distribution Schemes*. Submitted for publication.
- [18] Van Lint, J. H. and Wilson, R. M. (1992) *A Course in Combinatorics*. Cambridge University Press, Cambridge.
- [19] Cover, T. M. and Thomas, J. A. (1991) *Elements of Information Theory*. Wiley, New York.

APPENDIX A. INFORMATION THEORY CONCEPTS

In this appendix we review the information theoretic concepts used in our definitions and proofs. For a complete treatment of the subject the reader is advised to consult [19].

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

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

(all logarithms in this paper are to the base 2). The entropy satisfies $0 \leq H(X) \leq \log |X|$, where $H(X) = 0$ if and only if there exists $x_0 \in X$ such that $\Pr(X = x_0) = 1$; whereas, $H(X) = \log |X|$ if and only if $\Pr(X = x) = 1/|X|$ for all $x \in X$.

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

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

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

$$H(X|Y) \geq 0. \quad (10)$$

Given $n + 1$ random variables, X_1, \dots, X_n, Y , the entropy of $X_1 \dots X_n$ given Y can be written as

$$H(X_1 \dots X_n | Y) = H(X_1 | Y) + H(X_2 | X_1 Y) + \dots \\ \dots + H(X_n | X_1 \dots X_{n-1} Y). \quad (11)$$

The *mutual information* between X and Y is defined by

$$I(X; Y) = H(X) - H(X|Y)$$

and satisfies the following properties:

$$I(X; Y) = I(Y; X) \quad \text{and} \quad I(X; Y) \geq 0,$$

from which one gets

$$H(X) \geq H(X|Y), \quad (12)$$

with equality if and only if X and Y are independent. Therefore, given n random variables, X_1, \dots, X_n , it holds that

$$H(X_1, \dots, X_n) \\ = \sum_{i=1}^n H(X_i | X_1, \dots, X_{i-1}) \leq \sum_{i=1}^n H(X_i). \quad (13)$$

Given three random variables, X, Y and Z , the *conditional mutual information* between X and Y given Z can be written as

$$I(X; Y|Z) = H(X|Z) - H(X|Z Y) \\ = H(Y|Z) - H(Y|Z X) \\ = I(Y; X|Z). \quad (14)$$

Since the conditional mutual information $I(X; Y|Z)$ is always non-negative we get

$$H(X|Z) \geq H(X|Z Y). \quad (15)$$

APPENDIX B. A KEY PREDISTRIBUTION SCHEME

In this section we describe the (g, b) -KPS given in [4]. Let $\mathcal{U} = \{1, \dots, n\}$ be a set of n users and $G \subseteq \mathcal{U}$ a conference of size g . Let p be a prime such that $p \geq n$ (the number of users). The TA chooses n distinct random numbers $s_i \in \mathbb{Z}_p$ and gives s_i to user i ($1 \leq i \leq n$). These values s_i do not need to be secret and can be thought of as the ‘identity’ of user i . Thus, for example, it is sufficient to take $s_i = i$ for $1 \leq i \leq n$. Next, the TA constructs a random symmetric polynomial in g variables with coefficients from \mathbb{Z}_p , in which the degree of any variable is at most b :

$$f(x_1, \dots, x_g) = \sum_{i_1=0}^b \dots \sum_{i_g=0}^b a_{i_1, \dots, i_g} x_1^{i_1} \dots x_g^{i_g}.$$

The fact that f is symmetric is equivalent to $a_{i_1, \dots, i_g} = a_{\pi(i_1), \dots, \pi(i_g)}$ for all permutations π of $\{1, \dots, g\}$.

Then, for $1 \leq i \leq n$, the TA computes a polynomial g_i in $g - 1$ variables x_2, \dots, x_g by setting $x_1 = s_i$ in $f(x_1, \dots, x_g)$. The coefficients of g_i comprise the secret information which is given to user i . The key associated with the g -subset $G = \{i_1, \dots, i_g\}$ is

$$k_G = f(s_{i_1}, \dots, s_{i_g}) \bmod p.$$

Each user $i_j \in G$ can compute

$$k_G = g_{i_j}(s_{i_1}, \dots, s_{i_{j-1}}, s_{i_{j+1}}, \dots, s_{i_g}) \bmod p.$$

It can be shown that no subset of b users disjoint from G can compute any information about k_G (see [4]). Also, it is not hard to see that $H(K_G) = \log p$, for all G of size g , and

$$H(U_i) = \binom{g+b-1}{g-1} \log p$$

for $1 \leq i \leq n$.