Communication in Key Distribution Schemes*

Amos Beimel[†] Benny Chor[‡]

Department of Computer Science
Technion, Haifa 32000, Israel

Abstract

A (g, b) *key distribution scheme* allows conferences of g users to generate secret keys, such that disjoint coalitions of b users cannot gain any information on the generated key (in the information theoretic sense). In this work, we study the relationships between communication and space efficiency of key distribution schemes. We prove that communication does not help in the context of *unrestricted schemes*. On the other hand, we show that for restricted schemes, which are secure only when used by a limited number of conferences, communication can substantially improve the space efficiency. We also present lower bounds on the space efficiency of restricted schemes.

Index Terms – Key Distribution, communicating protocols, space efficiency, one time schemes, cryptography.

*An extended abstract of this paper appears in "Advances in Cryptology – Crypto '93", Springer-Verlag, LNCS 773, D.R. Stinson, ed., pp. 444–455.

†Email: beimel@cs.technion.ac.il; Url: http://www.cs.technion.ac.il/~beimel .

‡Supported by the Fund for Promotion of Research at the Technion. Email: benny@cs.technion.ac.il.

1 Introduction

In various multiuser systems, the need for generating a secret, common to a subset of the users, arises occasionally. Such key can be used, for example, in establishing a secure private key cryptosystem among the members of the subset. A *non-communicating key distribution scheme* for conferences of size g which is secure against any disjoint coalition of b users is denoted (g, b)-scheme. This is a scheme where an off-line server initially distributes n pieces of information, one per user. Each user receives his piece discretely. After this initial distribution takes place, the users can reconstruct keys in a secure fashion. That is:

1. Every member of a "good" conference (set) G of g users can reconstruct a key from his piece (and the conference identity). This reconstruction requires no communication (either among users or with the server). The key that every user in G reconstructs is the same, and is called the key of the conference G.

2. Every "bad" coalition B of b users does not gain any information on the key of any disjoint conference G.

It might help the reader to remember that the size of conferences is denoted by g which stands for "$g$ood" users, and the size of coalitions is denoted by b which stands for "$b$ad" users.

It is clear that non-communicating schemes require initial distribution of pieces of information to the users. The (space) efficiency of a scheme is measured by the cardinality of the domain of pieces. The cardinality is a function of the cardinality of the domain of possible keys, $|S|$, the number of users, n, the size of conferences g, and the size of coalitions b.

Blom [1] was the first to consider non-communicating schemes for conference of size 2 and coalitions of size b. He presented an efficient $(2, b)$ scheme, based on MDS codes. The pieces in Blom's scheme are taken from a domain of cardinality $|S|^{b+1}$ (where S is the domain of keys). Matsumoto and Imai [2] suggested the use of symmetric linear functions for (g, b) schemes. Blundo, De Santis, Herzberg, Kutten, Vaccaro and Yung [3] present (g, b) schemes, based on symmetric multinomials. Their multinomials have g variables and degree at most b in each variable. The pieces in their scheme are taken from a domain of cardinality $|S|^{\binom{g+b-1}{g-1}}$. For large values of g and b, this expression is quite large. However, using entropy arguments, Blundo et. al. [3] prove a tight lower bound on the cardinality of the domain of pieces. Therefore, their scheme is space-optimal. In this work, we apply direct arguments (no entropy) to prove the same lower bound. Our proof has two advantages. First, in our opinion, it is more intuitive and less technical. Second, it actually applies to a weaker notion of security, thereby providing a stronger result. This stronger result is used in proving our lower bound on communicating schemes which is described in the next paragraph. Other works dealing with non-communicating schemes in our setting are [4, 5, 6, 7].

The large lower bound (for big conferences and coalitions) raises the question whether communication could be of help in reducing the size of pieces. Communication has some subtle implications on the security requirement (see section 5 for details). Just like the non-communicating schemes, we require that even if conferences communicate in order to generate keys, these keys remain secure with respect to disjoint coalitions of size b. Since no secure channels among users can be assumed, communication takes place via a broadcast media. One problem which arises is that the communication of one conference could leak information on the keys of *other* conferences. Therefore, we require that even if a "bad" coalition heard the communication of all the conferences, the coalition does not gain any information on keys of (disjoint) conferences. We argue that this is the right security requirement for communicating schemes. We prove that, regrettably, such unrestricted communicating schemes require pieces from a domain as large as non-communicating schemes.

This negative result motivates the introduction of *restricted* communicating schemes. These schemes can be used only for a limited number of conferences, whose identity is not known beforehand. We construct an efficient one-time secure scheme, where the size of the domain of pieces is of cardinality $|S|^{2+2\cdot(b-1)/g}$. This is a substantial improvement over the $|S|^{g+b-1}$ cardinality in the one-time secure communicating scheme of [3]. (The fact that this scheme is only one-time secure was not mentioned in [3]). Following [3], our schemes are *non-interactive*: Each user sends messages which depend only on his piece of information and not on messages received from other users. Other, less efficient, one time secure communicating schemes are presented in [8, 9]. We prove a lower bound of $|S|^{1+\lfloor b/(g-1)\rfloor}$ on the cardinality of the domain of pieces in every one time (g,b)-scheme. We use τ copies of the one-time scheme to construct a scheme which is secure for τ conferences. The cardinality of the domain of pieces in this scheme is $|S|^{\tau(2+2\cdot(b-1)/g)}$. We show that the domain of pieces of every user in a communicating (g,b) scheme, which is secure for τ conferences, is at least $\max\left\{|S|^{\tau}, |S|^{\tau^{(1-1/g)(b-1)/g}}\right\}$. Hence, the dependence on τ of the domain of pieces in our scheme cannot be completely avoided.

We contrast our results with known ones in the computational model, where attacks of coalitions are restricted to probabilistic polynomial time computations. Diffie and Hellman [10], in their pioneering work on public key cryptography, introduced a communicating scheme of key generation for conferences of size two[1]. This communicating scheme requires no server and no pieces. In this scheme a given communication *uniquely* determines the key, but it is (presumably) intractable for a third user to compute the key from the communication (of course, in our setting this information enables other users to find the conference

[1]Let p be a prime number, and let α be a primitive element in the field $\mathrm{GF}(p)$. User i (respectively j) chooses a random number $r_i \in \mathrm{GF}(p)$ (respectively r_j) and sends the message $m_i = \alpha^{r_i}$ (respectively $m_j = \alpha^{r_j}$). The joint key of users i and j is $\alpha^{r_i \cdot r_j}$, which i easily computes from m_j and r_i using the equality $m_j^{r_i} = \alpha^{r_i \cdot r_j}$.

key). On the other hand, even in the computational model, a non-communicating scheme requires pieces taken from a domain which is at least as large as the domain of keys. So in the computational model, communication does reduce the size of pieces, up to complete elimination. Fiat and Naor [11] present a non-communicating $(n-1,1)$-scheme in the computational model. In their scheme, which is based on the assumed intractability of extracting root modulo composites (RSA), the domain of pieces has the same cardinality as the domain of keys. Recall that in the computationally unbounded model a non-communicating $(n,1)$-scheme requires that the domain of pieces is at least of cardinality $|S|^n$.

The remainder of this paper is organized as follows. In Section 2 we give formal definition of communicating and non-communicating schemes. In Section 3 we present our proof of the lower bound for weak non-communicating schemes. In Section 4 we use this result to prove a lower bound for unrestricted communicating schemes. In Section 5 we define restricted communicating schemes. In Section 6 we prove lower bounds for restricted communicating schemes, and in Section 7 we describe some efficient constructions.

2 Definition of Key Distribution Schemes

In this section, we present formal definition of *communicating* and *non-communicating* key distribution schemes. We start with the communicating schemes.

Definition 2.1: Let $\{1,\ldots,n\}$ be a set of users, g and b be positive integers such that $g+b \leq n$, S be a set of keys, and $\mathcal{P}$ be an a-priori probability distribution on S. Let R be a set of random inputs. For every i $(1 \leq i \leq n)$ let U_i denote a domain of pieces for user i. An *unrestricted communicating* (g,b) *key distribution scheme* (later denoted by (g,b) scheme) with n users and domain of keys S is a function $\mathcal{U} : R \rightarrow U_1 \times U_2 \times \ldots \times U_n$. A server distributes the vectors $\{\mathcal{U}(r) \ : \ r \in R\}$ to the users according to some a-priori probability distribution on the random inputs. We denote by $\mathcal{U}_i(r)$ the i-th coordinate of $\mathcal{U}(r)$. This coordinate is the piece of user i. When users of a set G (of cardinality g) wish to generate a conference key, each user in G chooses a local random input for this conference. Then, the users communicate among themselves over a broadcast channel. We denote the resulting communication by C_G (it is a function of the g pieces and the local random inputs). As the messages are sent over a broadcast channel, they can be heard by all the users (including the users *not* in G). The key distribution function $\mathcal{U}$ and the conversations satisfy the following requirements:

reconstruction requirement At the end of the conversation, each member of G can deterministically reconstruct a key from the conversation and his piece. The key that every member of G reconstructs is the same, and is denoted by $s_G(r, \vec{r}_G)$, where r is the random input of the server, and $\vec{r}_G$ is the vector of random inputs of the users in G. Since the random input of the server and the random inputs of the users determine the pieces and the communication then describing the key as a function of the random inputs is appropriate.

unrestricted security requirement Every ("bad") coalition B of cardinality b, having their pieces and random inputs, and knowing the conversations of *all* possible conferences, does not gain any information on the key of any disjoint subset G_0 (i.e. $G_0 \cap B = \emptyset$). That is, for every vector of pieces $\langle u_1, \ldots, u_n \rangle$ which is distributed with positive probability, every set of random inputs $\vec{r}_B$ to coalition members, every possible key $s \in S$, and every set of possible consistent conversations $C_1, \ldots, C_{\binom{n}{g}}$ of all sets of cardinality g:

$$\Pr\left[\ s_{G_0}(r, \vec{r}_{G_0}) = s\ |\vec{r}_B \wedge \bigwedge_{j \in B} (\mathcal{U}_j(r) = u_j)\ \wedge \bigwedge_{|G|=g} (C_G(\mathcal{U}_G(r), \vec{r}_G) = C_G)\ \right] = \mathcal{P}(s)\ .$$

The probability is taken over r – the random input of the server, and over $\vec{r}$ – the random inputs of all the users for all conferences; $\vec{r}_B$ is the restriction of $\vec{r}$ to the coalition B.

The security property implies that for every conference G of cardinality g, it holds that $\Pr\left[\ s_G(r, \vec{r}_G) = s\ \right] = \mathcal{P}(s)$, where the probability is taken over r, the random input of the server,r, and $\vec{r}_G$ the random inputs of the users of G. In other words, the conference key of G is a random variable, which is distributed according to the a-priori probability distribution on the keys. It is *not* guaranteed that keys of different conferences are *independent* random variables. The security requirement does imply some independence between the keys. For example, it is true that every $b+1$ keys are independent. Otherwise, there are b users knowing the first b keys, and therefore gain some information on the $(b+1)$ key of a disjoint conference. In the rest of this paper we assume that the a-priori probability of each key is positive. That is, for every key $s \in S$ it holds that $\mathcal{P}(s) > 0$.

We now define non-communicating schemes, which are a special case of communicating schemes.

Definition 2.2: A *non communicating (g, b) key distribution scheme* with n users and domain of keys S is a (g, b) scheme, in which every set G of cardinality g can generate a key which depends only on the vector of pieces (and not on any communication), and every user $i \in G$ can reconstruct G's key from his piece. In this case the random input of the server determines the key of every set G. That is, s_G is only a function of r. The security requirement reduces to:

$$\Pr\left[\ s_{G_0}(r) = s\ |\ \bigwedge_{j \in B} (\mathcal{U}_j(r) = u_j)\ \right] = \mathcal{P}(s)\ .$$

We now consider a weakening of the security requirement. Instead of requiring that the conditional probability (given any pieces of a bad set B) of every key equals the a-priory probability, we will only require that this conditional probability is positive. We claim that this security requirement is *not* reasonable, since every "bad" coalition B could gain a lot of information. The reason we do define weak schemes is because we show that the lower bounds on the size of the pieces hold even for these weak schemes. To simplify this discussion, we will only consider non-communicating weak schemes.

Definition 2.3: A *weak non-communicating* (g, b) *key distribution scheme* is a non-communicating (g, b) scheme in which the security property is relaxed:

weak security property Let B be a coalition of b (bad) users, and let G be a conference of g (good) users, such that $G \cap B = \emptyset$. Then the users in B, having their pieces, cannot rule out any key of G. In other words, for every vector of pieces $\vec{u} = \langle u_1, \ldots, u_n \rangle$ which is dealt with positive probability, and every possible key $s \in S$, there exists a vector of pieces $\vec{u'}$ that agrees with $\vec{u}$ on the pieces of B, but the key of the set G according to the vector $\vec{u'}$ is s. Formally,

$$\Pr\ [\ s_G(r) = s \mid \bigwedge_{j \in B} \mathcal{U}_j(r) = u_j] > 0$$

where the probability is taken over the random input of the server.

It is obvious that unrestricted non-communicating schemes are a special case of weak non-communicating schemes. Therefore, every lower bound for weak schemes implies the same lower bound for unrestricted non-communicating schemes.

3 A Lower Bound for Non-Communicating Schemes

Blundo et. al. [3] prove a tight lower bound on the size of the pieces in every non-communicating key distribution scheme. Their proof is based on the entropy function, and, in our opinion, does not reveal the intuition behind this lower bound. We present a simpler proof of this lower bound, which is not based on entropy. Furthermore, in our proof we only use the weak security requirement. That is, even weak (g, b) schemes, where the entropy of the keys may be very low, must have large domain of pieces. Thus, our proof yields a stronger result than the lower bound of [3]. We use this stronger result in the sequel.

Theorem 3.1: [3] Let $\mathcal{U}$ be a weak non-communicating (g, b) scheme with n users and domain of keys S. Let U_i be the domain of pieces of user i in $\mathcal{U}$. Then for every i $(1 \leq i \leq n)$:

$$|U_i| \geq |S|^{\binom{g+b-1}{g-1}}.$$

Proof: Consider a (g, b) scheme with a domain of keys S. Without loss of generality, we assume that there are *exactly* $g + b$ users, which we denote by $\{1, \ldots, g + b\}$. We prove the lower bound on the domain of pieces of user 1. Let $G_1, \ldots, G_\ell$ be all the sets of cardinality

g that contain user 1, where $\ell = \binom{g+b-1}{g-1}$. Let $\vec{s} = \langle s_1, s_2, \ldots, s_\ell \rangle$ be any vector in S^ℓ. We claim that there exists a vector of pieces $\vec{u} = \langle u_1, \ldots, u_{g+b} \rangle$ (which is dealt with positive probability), such that for every $1 \leq i \leq \ell$ the key of the set G_i reconstructed from the pieces in $\vec{u}$ equals s_i. Otherwise, let i ($i \leq \ell$) be a maximal index such that there exist keys $s'_i, \ldots, s'_\ell \in S$ (where $s'_i \neq s_i$) and there exists a vector of pieces $\vec{u'} = \left\langle u'_1, \ldots, u'_{g+b} \right\rangle$, which is dealt with positive probability, such that the keys in $\vec{s'} = \langle s_1, \ldots, s_{i-1}, s'_i, \ldots, s'_\ell \rangle$ are reconstructed from the pieces in $\vec{u'}$. Such index $i \geq 2$ exists since for $i = 1$, there is some vector of pieces from which G_1 reconstructs the key s_1. Consider the set $B = \{1, \ldots, g+b\} \setminus G_i$, which contains exactly b users. Since the set B intersects G_j for every $j \neq i$, the users in B can reconstruct the keys of the conferences $G_1, \ldots, G_{i-1}, G_{i+1}, \ldots, G_\ell$. Therefore, the pieces from $\vec{u}'$ of the users in B determine that the reconstructed keys of the conferences $G_1, \ldots, G_{i-1}$ are $s_1, \ldots, s_{i-1}$, respectively. Suppose there is a positive probability that G_i's key equals s_i, given the pieces $u'_i, i \in B$. Then in particular there is a vector of pieces giving rise with non-zero probability to the keys $s_1, s_2, \ldots, s_{i-1}, s_i$. This contradicts the maximality of i. Therefore

$$\Pr[\ s_{G_i}(r) = s_i \ \mid \ \bigwedge_{j \in B} \mathcal{U}_j(r) = u'_j\ ] = 0$$

But this violates the weak security property of the (g, b) scheme, a contradiction to our assumption.

Hence for every $\vec{s} \in S^\ell$, there is a vector of pieces $\vec{u}$ for the users, in which the vector of reconstructed keys for the sets $G_1, \ldots, G_\ell$ is $\vec{s}$. Since user 1 computes the keys of the sets $G_1, \ldots, G_\ell$ from his piece, it follows that his piece must be different for every pair of different vectors of keys for the sets $G_1, \ldots, G_\ell$. There are $|S|^\ell$ possible vectors of keys, therefore there are at least $|S|^\ell$ different pieces for user 1. That is, $|U_1| \geq |S|^\ell = |S|^{\binom{g+b-1}{g-1}}$, as claimed. $\square$

We remark that if the keys of all sets were independent random variables then using the same ideas of this proof, we can prove a lower bound of $|S|^{\binom{n}{g-1}}$. Another observation is that we can consider a key distribution scheme in which only some pre-defined subsets of size g can reconstruct a key. Our proof actually supplies a lower bound for this setting as well.

Lemma 3.2: Let $\mathcal{U}$ be a (weak) non-communicating (g, b) scheme with exactly $g+b$ users and domain of keys S, in which user i is a member of at least ℓ sets that can reconstruct a key. Let U_i be the domain of pieces of user i in $\mathcal{U}$ then

$$|U_i| \geq |S|^\ell \ .$$

Notice that ℓ can be at most $\binom{g+b-1}{g-1}$.

Using symmetric degree b multinomials with g variables, Blundo et. al [3] have constructed an unrestricted non-communicating (g, b) scheme with domains of pieces $|U_i| = |S|^{\binom{g+b-1}{g-1}}$ with uniform a-priori distribution on the keys (provided that $|S| \geq n$ and $|S|$ is a prime power). So the lower bound is tight (except for small domains of keys).

4 Removing Communication from Unrestricted Schemes

In this section we show how to transform an unrestricted communicating scheme into a weak non-communicating key distribution scheme, without changing the domain of pieces. Therefore, the lower bound on the cardinality of the domain of pieces applies to unrestricted communicating schemes as well.

Theorem 4.1: Let $\mathcal{U}$ be an unrestricted communicating (g, b) key distribution scheme with $n \geq g + b$ users and domain of keys S. Let $U_1, \ldots, U_n$ be the domains of pieces of the users in $\mathcal{U}$. Then for every user i:

$$|U_i| \geq |S|^{\binom{g+b-1}{g-1}} .$$

Proof: The idea of the proof is to fix, for every set G of g users, a possible communication C_G (i.e. one that is exchanged with positive probability when G communicates in order to generate a conference key). The vector of all these communications is public knowledge. Now the server deals only vectors of pieces that are consistent with all the communications C_G's. When a member of a set G wishes to determine a conference key, he applies the reconstruction function to his piece and the fixed communication C_G. This way, no communication is required. In the rest of proof, we show first how to choose communications for different conferences such that they are consistent among themselves. This implies the existence of vectors of pieces that are consistent with all the communications. Once this is done, it is clear that the non-communicating scheme has the reconstruction property. We then prove that the resulting non-communicating scheme has the weak security property. Therefore it is a weak non-communicating (g, b) scheme.[2] By Theorem 3.1 the cardinality of the domain of pieces of every user in the resulting weak non-communicating scheme is at least $|S|^{\binom{g+b-1}{g-1}}$. But the domain of the pieces in the non-communicating scheme is not larger than that of the communicating scheme. Therefore, the lower bound on the size of the pieces applies to the original communicating scheme as well.

To complete the proof, we first show how to choose a set of communications C_G (for all G's) in a consistent way. To do this, we first fix an arbitrary vector of pieces $\vec{u}$ which is dealt by the server in the original scheme with positive probability. We also fix the local random input of each user. Each communication C_G is the one determined when the users of G hold pieces from $\vec{u}$, and have the fixed random inputs. It is clear that $\vec{u}$ is consistent with all these conversations. The server in the new scheme chooses at random a vector of pieces that is consistent with the communications. That is, the server chooses a vector of

[2] In this proof we do not define the probability distribution under which the server distributes the consistent vectors of pieces. We only require that every consistent vector is distributed with positive probability. It is possible to define a probability distribution on the consistent vectors, such that the induced (g, b) scheme will have the unrestricted security property.

pieces from the (non-empty) set of vectors of pieces $\vec{v}$ for which there exists a vector of local random inputs $\vec{r}$ for the users, such that every conference G of g users, holding the pieces of $\vec{v}$, and having the random inputs $\vec{r}_G$, communicate C_G (where $\vec{r}_G$ is the restriction of $\vec{r}$ to the members of G).

We now show that the resulting non-communicating scheme is weakly secure. Let G be any conference of cardinality g, and B be a disjoint coalition of cardinality b. By the security property of the communicating scheme, it follows that for every vector of pieces that is consistent with the fixed conversations, and every key $s \in S$, there exists a vector of pieces which is consistent with the given pieces of the users in B, such that the reconstructed key of conference G equals s. That is, the non-communicating scheme has the weak security property, as claimed. $\square$

We can define the notion of weak security for unrestricted communicating schemes in a similar manner to Definition 2.3. The lower bound of Theorem 4.1 is also applicable to such weak unrestricted communicating schemes.

5 Definition of Restricted Communicating Schemes

By Theorem 4.1, communication cannot decrease the size of the pieces of information given to the users in key distribution schemes. In order to decrease the size of the pieces of information, we relax the security requirement. We require that the key distribution schemes should be secure only for a limited number of conferences. Which conference will generate a key is not known a-priori, so the distributed pieces should accommodate any combination of conferences (up to the limit on their number). We will show that if this limit is relatively small then the size of the pieces can be substantially reduced. For example, if the scheme is only required to be secure for a single conference, then for $g = b = n/2$ we present a scheme whose domain of pieces is of cardinality $|S|^4$, regardless of n. Recall that for unrestricted schemes with these parameters, the cardinality of the domain of pieces is $|S|^{2^{\Omega(n)}}$ (Theorem 4.1).

Before going any further, we remark that the notion of key distribution schemes restricted to a limited number of conferences is meaningful only with respect to communicating schemes. For non-communicating schemes, the generation of a conference key does not add any information to any user (either in the conference or not). Therefore a one-time secure non-communicating scheme would also be secure in the unrestricted sense, and no saving can be expected. On the other hand, the communication in communicating schemes is heard by all users (not only conference members), and could reduce the uncertainty of the remaining pieces. After sufficiently many communications take place, no uncertainty is left, and the pieces become useless for additional conferences. This implies that the amount of initial secrecy in restricted communicating schemes can be smaller than that of unrestricted schemes. The proof that unrestricted communicating schemes and unrestricted non-communicating schemes have the same space efficiency (Theorem 4.1) is not applicable for restricted schemes. It is indeed possible, for example, to transform a one-time secure communicating scheme into a non-communicating scheme, using the technique of Theorem 4.1. However, this would yield a non-communicating scheme which is secure only with respect to a single *fixed* conference, depending on the one initiating the communication.

We start with the precise definition of τ-restricted key distribution scheme. Then we prove fairly close upper and lower bounds on the size of the pieces in such schemes.

Definition 5.1: A *τ-restricted communicating (g, b)-scheme* is a communicating (g, b)-scheme in which the security property is replaced by the following one:

τ-restricted security property Let B be a subset of b (bad) users. Then the users in B, having their pieces and random inputs and knowing the conversations sent by any τ conferences, do not gain any information on the key of any one of these conferences (which is disjoint to B). That is, for every vector of pieces $\langle u_1, \ldots, u_n\rangle$ which is dealt with positive probability, every combination of τ sets of users of cardinality g, denoted by $G_0, \ldots, G_{\tau-1}$, every coalition B of b users, such that $G_0 \cap B = \emptyset$, every set of random inputs $\vec{r}_B$ to coalition members, every possible key $s \in S$, and every possible consistent conversations $C_0, \ldots, C_{\tau-1}$ sent by the users of $G_0, \ldots, G_{\tau-1}$ respectively:

$$\Pr[\ s_{G_0}(r, \vec{r}_{G_0}) = s \mid \vec{r}_B \wedge \bigwedge_{j\in B} (\mathcal{U}_j(r) = u_j) \wedge \bigwedge_{0\leq j\leq \tau-1} (C_{G_j}(\mathcal{U}_{G_j}(r), \vec{r}) = C_j)\ ] = \mathcal{P}(s)$$

The probability is taken over r – the random input of the server, and $\vec{r}$ – the random inputs of all the users for all conferences; $\vec{r}_B$ is the restriction of $\vec{r}$ to the coalition B. We denote 1-restricted scheme by *one-time scheme.*

6 Lower Bounds for Restricted Communicating Schemes

In this section, we present lower bounds on the cardinality of the domain of pieces in restricted key distribution schemes. We first give a simple lower bound for every τ-restricted (g, b) scheme. We show that for $\tau \leq \binom{g+b-1}{g-1}$ the cardinality of the domains of pieces in any τ-restricted (g, b) scheme is at least $|S|^\tau$. Therefore, for $\tau \geq \binom{g+b-1}{g-1}$ the unrestricted non-communicating scheme of [3] are space optimal even with respect to τ-restricted schemes. In addition, this shows that for restricted schemes with smaller τ, some dependence on the size of τ is unavoidable. We improve this bound for the case $\tau \leq (b/g)^g$. In particular, for one time schemes we prove a $|S|^{1+\lfloor b/(g-1)\rfloor}$ lower bound (the upper bound is $|S|^{2+2(b-1)/g}$).

We first present a simple lower bounds for τ-restricted schemes.

Lemma 6.1: Let $\tau \leq \binom{g+b-1}{g-1}$. In every τ-restricted (g, b)-scheme with n users and domain of keys S, the cardinality of the domain of pieces of every user is at least $|S|^\tau$.

Proof: Again, we limit the number of users to $g+b$. Using the same ideas as in the proof of Theorem 4.1, we transform a τ-restricted (g,b)-scheme into a weak non-communicating (g,b)-scheme in which τ pre-defined sets can reconstruct a key. That is, we fix consistent conversations of the τ sets. The server generates vectors of pieces consistent with these conversations. The original scheme is secure for τ conferences, therefore by fixing τ conversations, we get a secure scheme in which these τ sets can reconstruct a key without any communication. Since $\tau \le \binom{g+b-1}{g-1}$, there are τ sets that contain user i. Choosing τ sets containing user i as the pre-defined sets, we apply Lemma 3.2 to the transformed scheme. By this lemma the cardinality of the domain of pieces of user i in the transformed scheme at least $|S|^\tau$. By the transformation, the cardinality of the domain of pieces in the transformed scheme is at most the cardinality of the domain of pieces in the τ-restricted secure scheme. Therefore, the cardinality of the domain of pieces of every user in the τ-restricted scheme is at least $|S|^\tau$. □

We now improve the previous lower bound for schemes in which $\tau \le (b/g)^g$. The proof of this lower bound uses entropy and mutual information. For definitions of these information theoretic terms, the reader can refer to [12, 13, 14]. In the proof we use the following proposition of Maurer [15] and Ahlswede and Csiszar [16]. Its context is a system where two (coin flipping) users, each with private piece of information, execute a protocol by communicating over a broadcast channel. After the execution of the protocol, the two users generate a common key, such that a third user overhearing all the communication does not have any information on the key. In this circumstances, the conditional mutual information (measuring the information known to the two users but not to the third user) of the initial pieces is at least the entropy (uncertainty) of the generated key. The proposition is proven by showing that the mutual information of any random variable held by the two users cannot be increased after a conversation on a broadcast channel. In the proposition $\mathcal{U}_i$ is the random variable which denotes the piece of user i, and S is a random variable which denotes the key.

Proposition 6.2: **[16, 15]** Let $\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3$ be random variables, held by users $1, 2, 3$ respectively. Users 1 and 2 communicate on a broadcast channel according to some protocol. Denote the communication by the random variable M. After the execution of the protocol users 1 and 2 agree on a key S known to both of them, such that user 3 has no information on the key. That is, $H(\,S \mid \mathcal{U}_1, M) = H(\,S \mid \mathcal{U}_2, M) = 0$, while $H(\,S \mid \mathcal{U}_3, M) = H(S)$. Then, $I(\,\mathcal{U}_1 \,;\, \mathcal{U}_2 \mid \mathcal{U}_3) \ge H(S)$.

We first deal with $(2,b)$-schemes. In the non-communicating $(2,b)$-scheme of Blom [1], the cardinality of the domain of pieces is $|S|^{b+1}$. In Lemma 6.3 we prove that $|S|^{b+1}$ is a lower bound even for *one-time* $(2,b)$-schemes. Thus, in this case communication does not help even if we consider only one-time schemes.

Lemma 6.3: Let $\mathcal{U}$ be a one time $(2,b)$ scheme with $n \ge b+2$ users and domain of keys

S. Assume the a-priory probability of each key in S is uniform. Then the cardinality of the domain of pieces of every user in the scheme $\mathcal{U}$ is at least $|S|^{b+1}$.

Proof: Without loss of generality, we prove that $|U_1| \geq |S|^{b+1}$, where U_1 is the domain of pieces of user 1 in the scheme $\mathcal{U}$. We start with a one-time $(2, b)$ scheme $\mathcal{U}$. For every i, we construct a new scheme with 3 users. In the new scheme user 1 receives $\mathcal{U}_1$, the piece of users 1 in $\mathcal{U}$, user 2 receives $\mathcal{U}_i$, the piece of user i in $\mathcal{U}$, and user 3 receives the pieces of users $i+1, \ldots, b+2$ from $\mathcal{U}$. In the new scheme users 1 and 2 can generate the key of the old users $\{1, i\}$. Since user 3 receives at most b pieces of the old scheme, he has no information on the generated key. Therefore, we are in the scenario of Proposition 6.2. We conclude that for every i $(2 \leq i \leq b+2)$:

$$I(\, \mathcal{U}_1 \,;\, \mathcal{U}_i \mid \mathcal{U}_{i+1} \ldots \mathcal{U}_{b+2} \,) \geq H(S) \; .$$

On the other hand, by definition

$$\begin{aligned}
\sum_{i=2}^{b+2} I(\, \mathcal{U}_1 \,;\, \mathcal{U}_i \mid \mathcal{U}_{i+1} \ldots \mathcal{U}_{b+2}) &= \sum_{i=2}^{b+2} H(\, \mathcal{U}_1 \mid \mathcal{U}_{i+1} \ldots \mathcal{U}_{b+2}) - \sum_{i=2}^{b+2} H(\, \mathcal{U}_1 \mid \mathcal{U}_i \mathcal{U}_{i+1} \ldots \mathcal{U}_{b+2}) \\
&= H(\mathcal{U}_1) - H(\, \mathcal{U}_1 \mid \mathcal{U}_2 \ldots \mathcal{U}_{b+2} \,) \\
&\leq H(\mathcal{U}_1) \; .
\end{aligned}$$

Combing the last two arguments together, we deduce that

$$H(\mathcal{U}_1) \geq \sum_{i=2}^{b+2} I(\, \mathcal{U}_1 \,;\, \mathcal{U}_i \mid \mathcal{U}_{i+1} \ldots \mathcal{U}_{b+2} \,) \geq (b+1)\, H(S) \; .$$

It holds that $H(\mathcal{U}_1) \leq \log |U_1|$, and since we assume uniform distribution on S then $H(S) = \log |S|$. Thus,

$$\log |U_1| \geq H(\mathcal{U}_1) \geq (b+1)\, H(S) = (b+1) \log |S| \; ,$$

which yields the claimed bound $|U_1| \geq |S|^{b+1}$. □

The proof of Lemma 6.3 (with respect to the domain U_1) does not require that every pair of users should be able to reconstruct a key. It only requires that user 1 and every other user can generate a key. It is also interesting to notice that any scheme meeting this lower bound satisfies $H(\, \mathcal{U}_1 \mid \mathcal{U}_2 \ldots \mathcal{U}_{b+2} \,) = 0$, so every $b+1$ users can reconstruct the pieces of all the other users. We now use Lemma 6.3 to prove a lower bound for every conference size g and various values of τ.

Theorem 6.4: Let τ, g, b be positive integers such that $\tau \leq \binom{g+b-1}{g-1}$. Consider a τ-restricted (g, b)-scheme with $n \geq g + b$ users and domain of keys S, which are distributed with the uniform a-priory probability distribution. The cardinality of the domain of pieces of every user in the scheme is at least $|S|^e$, where

$$e = \max\left\{\tau, \tau^{1-1/(g-1)}(b-1)/g\right\} \; .$$

For $\tau = 1$ the lower bound is $|S|^{1+\lfloor b/(g-1) \rfloor}$.

Proof: If $(b-1)/g \le \tau^{1/(g-1)}$, then $|S|^\tau \ge |S|^{\tau^{(1-1/(g-1))}(b-1)/g}$, and the lower bound follows from Lemma 6.1. Otherwise, we convert the τ-restricted (g, b) scheme into a one time $(2, c)$ scheme (where c is a function of b, g and τ) such that the key in the new scheme is taken from a domain of cardinality $|S|^\tau$. To complete the proof, we apply the lower bound of Lemma 6.3.

In this conversion, we start with a τ-restricted (g, b) key distribution scheme, denoted $\mathcal{U}$, with $g+b$ users. Define $a = \left\lceil (g-1)\tau^{1/(g-1)} \right\rceil$, and $c = \lfloor (g+b-1)/a \rfloor - 1$. We construct a one time $(2, c)$ scheme, called $\mathcal{U}'$, with $\lfloor (g+b-1)/a \rfloor + 1 = c+2$ users. The new scheme is defined as follows: The piece of user 0 is $\mathcal{U}'_0(r) = \mathcal{U}_0(r)$ and for every $1 \le i \le \lfloor (g+b-1)/a \rfloor$ the piece of user i is $\mathcal{U}'_i(r) = \left\langle \mathcal{U}_{a(i-1)+1}(r), \ldots, \mathcal{U}_{ai}(r) \right\rangle$. That is, in the new scheme user 0 holds the piece of user 0 from the old scheme, and user i gets the pieces of a disjoint users of the original scheme. The number of original pieces we use is $a \lfloor (g+b-1)/a \rfloor + 1 \le g+b$, so this construction is possible. We consider the conference $\{i, j\}$ in the new scheme where $i > j$ (it is possible that $j = 0$). Since user i holds a pieces of the original scheme and $a \ge (g-1)\tau^{1/(g-1)}$ there are

$$\binom{a}{g-1} \ge (a/(g-1))^{g-1} \ge \tau$$

conferences of g original users, such that user i holds $g-1$ of their pieces and user j holds one piece. For every such conference, the users i and j in the new scheme can generate the original key of the conference. That is, the conference $\{i, j\}$ in the new scheme can generate τ original keys. We view these keys as one new key taken from a domain of cardinality $|S|^\tau$.

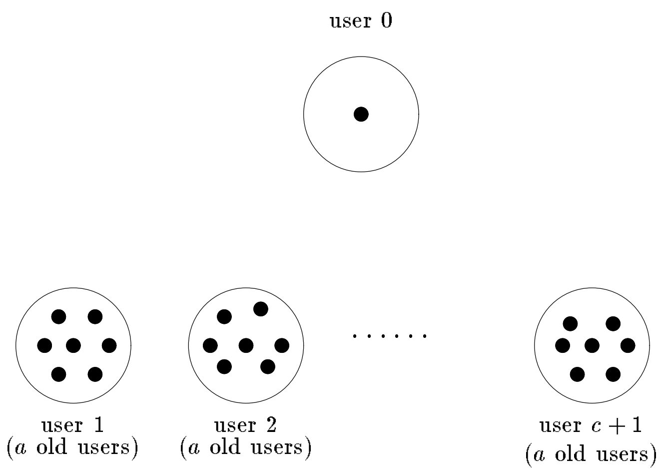

Figure 1: An illustration of the new scheme

We claim that this new key is distributed uniformly even in the conditional space where pieces of c new users (coalition members) are given. Denote the τ original conferences of size $g-1$ by $G_1, G_2, \ldots, G_\tau$, and the generated keys by $s_1, s_2, \ldots, s_\tau$ respectively. Consider a coalition C of c new users (not including i or j). If the coalition C has gained information on the concatenation of these keys then there exists an index i such that the pieces of C, the τ conversations, and the keys $s_1, \ldots, s_{i-1}$ reveal some information on the key s_i in the original scheme. This in turn, implies that in the original scheme there are pieces to all the users except G_i that, together with the communications, reveal some information on the key s_i. But this coalition contains b original users, which contradicts the τ-restricted security of $\mathcal{U}$, the original scheme.

Therefore, the scheme $\mathcal{U}'$ is a one time $(2, \lfloor (b+g-1)/a \rfloor - 1)$ scheme in which the key is distributed uniformly over a domain of cardinality $|S|^\tau$. Applying the lower bound of Lemma 6.3 to user 0, we conclude that U_0 – the domain of pieces of user 0 (in the new and original scheme) – satisfies

$$|U_0| \geq |S|^{\tau(\lfloor (b+g-1)/a \rfloor)} > |S|^{\tau^{1-1/(g-1)}(b-1)/g} .$$

If $\tau = 1$ then $a = g-1$. Thus, $|U_0| \geq |S|^{\lfloor (b+g-1)/(g-1) \rfloor} = |S|^{1+\lfloor b/(g-1) \rfloor}$. $\square$

We remark that the lower bound of Lemma 6.1 applies to weak τ-restricted schemes as well. On the other hand, the lower bound of Theorem 6.4 holds only for uniform a-priori distribution on the keys. For schemes where the keys are distributed with an arbitrary a-priori probability distributions, the lower bound is $2^{H(S)\cdot(1+\lfloor b/(g-1) \rfloor)}$. It is an open problem whether the lower bound of $|S|^{1+\lfloor b/(g-1) \rfloor}$ holds for weak one time schemes as well. Since Theorem 6.4 is proven by reduction to Lemma 6.3 then proving a $|S|^{b+1}$ lower bound for weak one time $(2, b)$ schemes suffices for proving the lower bound for every g.

7 Upper Bounds for Restricted Schemes

Blundo et. al. [3] present a one-time (g, b)-scheme in which the domain of pieces of each user is of cardinality $|S|^{g+b-1}$. (In [3] it is not pointed out that this scheme is only one-time secure). We improve their one-time scheme, and present a one-time key distribution scheme in which the domain of pieces of each user is of cardinality $|S|^{2+2(b-1)/g}$. To construct τ-restricted schemes, we use τ independent copies of our one-time scheme.

Lemma 7.1: Let S be a domain of keys of cardinality q^g, such that q is a prime-power which is greater or equal to $\sqrt{n}$. There exists a one-time (g, b) scheme with n users and domain of keys S (with uniform a-priori probability distribution) in which the cardinality of the domain of pieces of every user is $|S|^{2+2\cdot(b-1)/g}$.

Proof: For clarity of the exposition, we first assume that $n = g+b$. In this case let $|S| = q^g$ for some positive number $q \geq 2$ (not necessary a prime power). For every pair of users the server chooses two independent random strings from $\{0,\ldots,q-1\}$ denoted $s'_{i,j}, s''_{i,j}$. The piece of each user is the $2(n-1)$ random strings corresponding to the pairs that contain the user. When the users of a conference G want to generate a conference key, every user $i \in G$ picks at random $s_i \in \{0,\ldots,q-1\}$. The conference key s of the set G is the concatenation of these random s_i's, namely $s = s_1 \circ s_2 \circ \ldots \circ s_g$. Every user $i \in G$ should send s_i to every user $j \in G$. User i can send messages only on a broadcast channel, so, he uses the common random string of i and j as a one time pad. Since user i has to send the sub-secret s_i to user j and user j has to send s_j to user i, they have to use different random strings. That is, user i broadcasts $s_i + s'_{i,j} \pmod q$ if $i < j$, and $s_i + s''_{i,j} \pmod q$ if $i > j$. Therefore, every random string is used only once. Hence, the messages that are sent are all uniformly distributed and independent of the conference key of G and the pieces of any coalition B with b users (provided $G \cap B = \emptyset$). This implies that the scheme is secure.

We now describe our communicating one-time (g,b)-scheme for every $n \geq g+b$. The scheme is similar to the case $n = g+b$, with one change. To guarantee that the scheme is secure, we make sure that from the point of view of every coalition of size at most b the pads used in the generation of a key are uniformly distributed and independent of each other. On the other hand, we do not require that all $2\binom{n}{2}$ strings that are given to the users are totally independent. It suffices that the server deals vectors of pieces according to the non-communicating $(2, g+b-2)$ scheme of Blom [1] for n users, with keys taken from a domain of cardinality $|S|^{2/g} = q^2$. The pads used in the generation of a key are the keys of this scheme. Before we discuss the security of the scheme, we consider its efficiency. In Blom's scheme the cardinality of the domain of keys has to be at least n – the number of users. Hence, we require that $q^2 \geq n$. Furthermore, in Blom's scheme the domain is a finite field, so q has to be a prime-power. We use the non-communicating $(2, g+b-2)$-scheme with domain of keys of cardinality $q^2 = |S|^{2/g}$. So the cardinality of the domain of pieces of each user is

$$(|S|^{2/g})^{g+b-1} = |S|^{2+2\cdot(b-1)/g} .$$

To prove the security of the scheme we show in Claim 7.2 that the collection of keys of all pairs of users in a set G of g users in a non-communicating $(2, g+b-2)$ scheme is uniformly distributed and independent of the pieces of coalition B of b users. Since these keys are used as one-time pads, it follows that no information is leaked on the generated key, and therefore the scheme is secure. The formal proof that Claim 7.2 implies the security property of the one time scheme appears in Claim A.1 in Appendix A.

Claim 7.2: Let $\mathcal{U}$ be a non-communicating $(2, g+b-2)$-scheme with a-priori distribution $\mathcal{P}$ on a key domain S. Let G and B be sets of g and b users respectively, such that $G \cap B = \emptyset$, $G_1, G_2, \ldots, G_{\binom{g}{2}}$ be all the subsets of G of cardinality 2, $s_1, \ldots, s_{\binom{g}{2}}$ be any combination of $\binom{g}{2}$ keys from S, and $\langle u_1, \ldots, u_n \rangle$ be a vector of pieces that is distributed with positive probability. Then:

$$\Pr[\bigwedge_{1\le i\le\binom{g}{2}} s_{G_i}(r)=s_i | \bigwedge_{j\in B}\mathcal{U}_j(r)=u_j] = \prod_{1\le i\le\binom{g}{2}} \mathcal{P}(s_i)\ . \tag{1}$$

Proof: To simplify the notations, we denote $t=\binom{g}{2}$, and denote the key of the set G_i, i.e. $s_{G_i}(r)$, by $s_i(r)$. Notice that

$$\Pr[\bigwedge_{1\le i\le t} s_i(r)=s_i | \bigwedge_{j\in B}\mathcal{U}_j(r)=u_j] = \prod_{1\le k\le t} \Pr[s_k(r)=s_k | \bigwedge_{k+1\le i\le t} s_i(r)=s_i \wedge \bigwedge_{j\in B}\mathcal{U}_j(r)=u_j]$$

Therefore, to prove Equation (1) (and therefore the lemma) it is enough to prove that for every k, where $1\le k\le t$, it holds that:

$$\Pr[s_k(r)=s_k | \bigwedge_{k+1\le i\le t} s_i(r)=s_i \wedge \bigwedge_{j\in B}\mathcal{U}_j(r)=u_j] = \mathcal{P}(s_k)\ . \tag{2}$$

That is, the key $s_k(r)$ is independent of the other keys and the pieces of the users in B. To prove Equation (2), we partition the conditional probability space into disjoint subspaces, and prove this equality for every subspace. Thus, Equation (2) will hold for the original conditional space. The partition of the conditional space is according to the pieces of the $g-2$ users in $G\setminus G_k$. These pieces determine the keys of all the G_i except G_k. Without loss of generality $G_k=\{1,2\}$. Let $\vec{v}=\langle v_3,\ldots,v_{g+b}\rangle$, be any vector of pieces that is distributed with positive probability, such that:

- For every $j\in B$ it holds that $u_j=v_j$.
- For every i, such that $k+1\le i\le t$, it holds that the key of G_i reconstructed according to the pieces of $\vec{v}$ is s_i.

Since the cardinality of $B\cup G\setminus G_k$ is $g+b-2$ then the security property of the $(2,g+b-2)$ scheme guarantees that

$$\Pr[s_k(r)=s_k | \bigwedge_{j\in G\setminus G_k}\mathcal{U}_j(r)=v_j \wedge \bigwedge_{j\in B}\mathcal{U}_j(r)=v_j] = \mathcal{P}(s_k)\ . \qquad \square$$

We have constructed a one time scheme with the desired parameters, and have proven its security. Hence Lemma 7.1 follows. $\square$

One property of our communicating scheme is that it uses only one-way communication. The messages of different members of G do not depend on other messages. Another property of our scheme is that for a fixed b, the cardinality of the domain of pieces of each user is a monotonically *decreasing* function of g. This feature stands in contrast to unrestricted (g,b) schemes, where the cardinality of the domain of pieces of each user is a monotonically *increasing* function of g.

In the proof of Lemma 7.1, the conference key of G (i.e. $s = s_1 \circ s_2 \circ \ldots \circ s_j$) is distributed uniformly in S. It is possible to change this a-priori probability distribution on the keys. One way to achieve this goal is to first generate a key s as in the previous way. Then an arbitrary user chooses the real key k for the conference according to any desired distribution. The user sends the message $(k + s) \bmod q$.

We remark that the one time scheme cannot be reused. For example, if users $\{1, 2\}$ are members of two conferences G_1, G_2 then the part of the keys generated by them in the two conferences will be known to all the users in $G_1 \cup G_2$. To extend our scheme to a τ-secure one, we use τ independent copies of the one time scheme. The generation of a key for each conference is done using a different copy of the one time scheme. Since the copies are independent, each conference does not add any information to other conferences. Hence, the security of the one-time scheme implies the security of the τ-restricted scheme. We summarize this construction in the next theorem.

Theorem 7.3: Let S be a domain of keys, such that $|S| = q^g$ for some prime-power $q \geq \sqrt{n}$. There exists a τ-restricted (g, b)-scheme with n users and domain of keys S (with any a-priori probability distribution), in which the domain of pieces of each user has cardinality $|S|^{2\tau(1+(b-1)/g)}$.

This τ-restricted communicating schemes requires that the users hold a counter, which is incremented each time a conference key is generated. Given such a reliable counter, *active attack* by users sending messages deviating from the protocol, do not reveal information on different conferences. Such attack could only prevent the generation of the present conference key. Our scheme does not work in the absence of a reliable counter. It is an open question to construct an efficient τ-restricted scheme (for $\tau > 1$) in which the keys and messages do not depend on a counter or any other history of previous conferences.

Acknowledgments We thank Amir Herzberg and Moty Yung for helpful discussions on these topics. We would also like to thank Eyal Kushilevitz for his useful comments on earlier drafts of this paper.

References

[1] R. Blom. An optimal class of symmetric key generation systems. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology – Eurocrypt '84*, volume 209 of *Lecture Notes in Computer Science*, pages 335–338. Springer-Verlag, 1985.

[2] T. Matsumoto and H. Imai. On the key predistribution systems: a practical solution to the key distribution problem. In C. Pomerance, editor, *Advances in Cryptology*

– *CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 185–193. Springer-Verlag, 1988.

[3] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In E. F. Brickell, editor, *Advances in Cryptology - CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 471–486. Springer-Verlag, 1993.

[4] C. J. Mitchell and F. C. Piper. Key storage in secure networks. *Discrete Applied Mathematics*, 21(3):215–228, 1988.

[5] E. Okamoto and K. Tanaka. Key distribution system based on identification information. *IEEE Journal on Selected Areas in Communications*, 7(4):481–485, 1989.

[6] L. Gong and D. J. Wheeler. A matrix key-distribution scheme. *Journal of Cryptology*, 2(1):51–59, 1990.

[7] K. A. S. Quinn. Some constructions for key distribution patterns. *Designs, Codes and Cryptography*, 4(2):177–191, 1994.

[8] M. J. Fischer, M. S. Paterson, and C. Rackoff. Secure bit exchange using a random deal of cards. In *Distributed Computing and Cryptography*, pages 173–181. AMS, 1991.

[9] M. J. Fischer and R. N. Wright. Multiparty secret key exchange using a random deal of cards. In J. Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 141–155. Springer-Verlag, 1992.

[10] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[11] A. Fiat and M. Naor. Broadcast encryption. In D.R. Stinson, editor, *Advances in Cryptology - CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 480–491. Springer-Verlag, 1994.

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

[13] R. G. Gallanger. *Information Theory and Reliable Communications.* John Wiley & Sons, New York, 1968.

[14] I. Csiszar and J. Körner. *Information Theory. Coding Theorems for Discrete Memoryless Systems.* Academic press, 1986.

[15] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[16] R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography – part I: secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993.

A Formal Proof of Security of the One-time Scheme

In this appendix, we prove that Claim 7.2 implies the security requirement of our one-time key distribution scheme.

Claim A.1: The one-time (g, b) scheme presented in the proof of Lemma 7.1 has the 1-restricted security property.

Proof: Since in our scheme the generated key is only a function of the local random inputs of the users (and not their pieces), we denote this key by $s_G(\vec{r}_G)$. We have to prove that for every vector of pieces $\langle u_1, \ldots, u_n \rangle$ which is dealt with positive probability, every conference G of g users, every coalition B of b users, such that $G \cap B = \emptyset$, every possible key $s = s_1 \circ s_2 \circ \ldots \circ s_g \in S$, and every possible consistent messages $\{m_{i,j} \ : i, j \in G\}$ (where $m_{i,j}$ is the message sent by user i to help user j)

$$\Pr[s_G(\vec{r}_G) = s_1 \circ \ldots \circ s_g \mid \bigwedge_{\ell \in B} (\mathcal{U}_\ell(r) = u_\ell) \wedge \bigwedge_{i<j} r_i + s'_{i,j} = m_{i,j} \wedge \bigwedge_{i>j} r_j + s''_{i,j} = m_{j,i} \,] = \frac{1}{|S|} \quad (3)$$

Where the probability is taken over r – the random input of the server and $\vec{r}_G = \langle r_i : i \in G \rangle$ – the random inputs of the users of the conference G. Let S' be a domain of keys of cardinality $|S|^{2/g}$ (the domain of keys of the non-communicating scheme). We first claim that for every fixed key $\vec{r}_G = \langle r_1, r_2, \ldots, r_g \rangle \in S$ it holds that

$$\begin{aligned}
&\Pr[\bigwedge_{\ell \in B} (\mathcal{U}_\ell(r) = u_\ell) \wedge \bigwedge_{i<j} r_i + s'_{i,j} = m_{i,j} \wedge \bigwedge_{i>j} r_j + s''_{i,j} = m_{j,i} \,] \\
&= \Pr[\bigwedge_{i,j \in G} s_{i,j} = (m_{i,j} - r_i) \circ (m_{j,i} - r_j) \mid \bigwedge_{\ell \in B} (\mathcal{U}_\ell(r) = u_\ell) \,] \cdot \Pr[\bigwedge_{\ell \in B} (\mathcal{U}_\ell(r) = u_\ell) \,] \\
&= \frac{\Pr[\bigwedge_{\ell \in B} (\mathcal{U}_\ell(r) = u_\ell) \,]}{|S'|^t} \,. \qquad (4)
\end{aligned}$$

Equation (4) follows from Lemma 7.2, and the fact that the keys of the non-communicating scheme are distributed uniformly (recall that $t = \binom{g}{2}$). We return to prove Equation (3).

$$\Pr[s_G(\vec{r}_G) = s \mid \bigwedge_{\ell \in B} (\mathcal{U}_\ell(r) = u_\ell) \wedge \bigwedge_{i<j} r_i + s'_{i,j} = m_{i,j} \wedge \bigwedge_{i>j} r_j + s''_{i,j} = m_{j,i} \,]$$

$$
\begin{aligned}
&= \frac{\Pr[s_G(\vec{r}_G) = s \wedge \bigwedge_{\ell\in B}(\mathcal{U}_\ell(r) = u_\ell) \wedge \bigwedge_{i<j} r_i + s'_{i,j} = m_{i,j} \wedge \bigwedge_{i>j} r_j + s''_{i,j} = m_{j,i}]}{\Pr[\ \bigwedge_{\ell\in B}(\mathcal{U}_\ell(r) = u_\ell) \wedge \bigwedge_{i<j} s_i + s'_{i,j} = m_{i,j} \wedge \bigwedge_{i>j} s_j + s''_{i,j} = m_{j,i}\ ]} \\
&= \frac{\Pr[\bigwedge_{\ell\in B}(\mathcal{U}_\ell(r) = u_\ell) \wedge \bigwedge_{i<j} r_i + s'_{i,j} = m_{i,j} \wedge \bigwedge_{i>j} r_j + s''_{i,j} = m_{j,i}\ ]}{\sum_{\vec{r}_G\in S} \Pr[\ \bigwedge_{\ell\in B}(\mathcal{U}_\ell(r) = u_\ell) \wedge \bigwedge_{i<j} r_i + s'_{i,j} = m_{i,j} \wedge \bigwedge_{i>j} r_j + s''_{i,j} = m_{j,i}\ ]} \\
&= \frac{1/|S'|^t}{|S|\cdot 1/|S'|^t} = \frac{1}{|S|}\ . \qquad \square
\end{aligned}
$$