Interaction in Key Distribution Schemes[*] (Extended Abstract)

Amos Beimel[**] and 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, so that disjoint coalitions of b users cannot gain any information on the key (in the information theoretic sense). In this work we study the relationships between interaction and space efficiency of key distribution schemes. We prove that interaction does not help in the context of *unrestricted schemes*. On the other hand, we show that for restricted schemes, which are secure for a limited number of conferences, interaction can substantially improve the space efficiency.

1 Introduction

A non-interactive key distribution scheme for conferences of size g which is secure against b "bad" users (denoted (g, b)-scheme) is a method in which an off-line server initially distributes private individual pieces of information to n users such that:

1. The pieces of every "good" conference G of g users determine a key, such that every user in G can reconstruct the key from his piece. This reconstruction requires no interaction (either among users or with the server).
2. Every "bad" coalition B of b users does not gain any information on the key of any disjoint conference G.

It is clear that non-interactive schemes require initial distribution of pieces of information to the users. The (space) efficiency of the 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, $|S|$, of the number of users, n, of the size of conferences g, and of the size of coalitions b.

Blom [1] was the first to consider non-interactive schemes for conference of size 2 and coalitions of size b. He presented an efficient $(2, b)$ scheme, based on MDS codes. Other works dealing with non-interactive schemes in our setting are [7, 9]. Matsumoto and Imai [8] suggest the use of symmetric linear functions for (g, b) schemes. Blundo, De Santis, Herzberg, Kutten, Vaccaro and Yung [2]

[*] Supported by the Fund for the Promotion of Research at the Technion.

[**] email: beimel@cs.technion.ac.il

[***] email: benny@cs.technion.ac.il

D.R. Stinson (Ed.): Advances in Cryptology - CRYPTO '93, LNCS 773, pp. 444-455, 1994.

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 $|S|^{\binom{g+b-1}{g-1}}$ (where S is the domain of keys). For large values of g and b, this expression is quite large. However, using entropy arguments, Blundo et. al. [2] prove a tight lower bound on the cardinality of the domain of pieces. Therefore, their scheme is spacc-optimal. We use direct arguments (no entropy) to prove the same lower bound. Our proof has two advantages. First, it seems 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 interactive schemes which is described in the next paragraph.

The large lower bound (for big conferences or coalitions) raises the question whether interaction could be of help in reducing the size of pieces. Interaction has some subtle implications on the security requirement (see section 5 for details). Just like the non-interactive schemes, we require that even if all conferences interact 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, interaction 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 interactive schemes. We prove that, regrettably, such unrestricted interactive schemes require pieces from a domain as large as non-interactive schemes.

This negative result motivates the introduction of *restricted* interactive 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 interactive scheme of [2]. (The fact that this scheme is only one-time secure was not mentioned in [2]). Other, less efficient, one time secure interactive schemes are presented in [5, 6].

We contrast our results with known results in the computational model, where users are restricted to probabilistic polynomial time computations. Diffie and Hellman [3], in their pioneering work on public key cryptography, introduced an interactive scheme of key generation for conferences of size two[4]. This interactive 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 party to compute the key from the communication (of course, in our setting this information enables other users to find the conference key). On the other hand, even in the computational model, a non-interactive scheme requires

[4] Let p be a prime number, and let α be a primitive element in the field 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 $m_j^{r_i} = \alpha^{r_i \cdot r_j}$.

pieces taken from a domain which is at least as large as the domain of keys. So in the computational model, interaction does reduce the size of pieces, up to complete elimination. Fiat and Naor [4] present a non-interactive $(n,1)$-scheme in the computational model. In their scheme, which is based on the assumed intractability of extracting root modulo composites, the domain of pieces has the same cardinality as the domain of keys. Recall that in the computationally unbounded model a non interactive $(n,1)$-scheme requires that the domain of pieces is at least of cardinality $|S|^n$.

The remaining of this extended abstract is organized as follows. In section 2 we give formal definition of interactive and non-interactive schemes. Section 3 contains our proof of the lower bound for weak non-interactive schemes. In section 4 we use this result to prove a lower bound to unrestricted interactive schemes. In section 5 we introduce restricted interactive schemes, present an efficient construction, and prove some weak lower bounds.

2 Definition of Key Distribution Schemes

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

Definition 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 interactive* (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 input). 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 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.

unrestricted security requirement Every coalition B of b (bad) users, having their pieces and knowing the conversations of *all* possible conferences, does not gain any information on the key of every subset G_0 such that $G_0 \cap B = \emptyset$. 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 possible consistent conversations $C_1, \ldots, C_{\binom{n}{g}}$ of all sets of cardinality g:

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

Where 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. We denote by $\vec{r_A}$ the restriction of $\vec{r}$ to a set $A \subseteq \{1, \ldots, n\}$.

The security property implies that for every conference G of cardinality g, it holds that $\Pr\,[\ s_G(r, \vec{r_G}) = s\ ] \ = \ \mathcal{P}(s)$, 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 possible to prove that every $b+1$ keys are independent. 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-interactive schemes, which are a special case of interactive schemes.

Definition 2. A *non interactive (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 has 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.

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 set 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-interactive weak schemes.

Definition 3. A *weak non-interactive (g, b) key distribution scheme* is a non-interactive (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, can not rule out any key of G. That is, for every vector of pieces $\vec{u} = \langle u_1, \ldots, u_n \rangle$ that 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-interactive schemes are a special case of weak non-interactive schemes. Therefore, every lower bound for weak schemes, implies the same lower bound for unrestricted non-interactive schemes.

3 Lower Bound for Non-Interactive Schemes

Blundo et. al. [2] prove a tight lower bound on the size of the pieces in every non-interactive key distribution scheme. Their proof is based on the entropy function, and does not seems to reveal the intuition behind this lower bound. We present a simpler proof of this lower bound, which is not based on entropy. Furthermore, this proof gives a stronger result, which we use in the sequel.

Theorem 4. [2] *Let $\mathcal{U}$ be a weak non-interactive (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 $\vec{u} = \langle u_1, \ldots, u_{g+b} \rangle$ (that is dealt with positive probability), such that for every $1 \leq i \leq \ell$ the key of the set G_i reconstructed from $\vec{u}$ equals s_i. Otherwise, let i be a maximal index such that there exist keys $s'_i, \ldots, s'_\ell \in S$ for which the vector $\vec{s'} = \langle s_1, \ldots, s_{i-1}, s'_i, \ldots, s'_\ell \rangle$ is the vector of keys for some possible vector of pieces $\vec{u}$. Such index $i \geq 1$ exists, since given any b pieces, each key is distributed according to the a-priori distribution. Consider the set $B = \{1, \ldots, g + b\} \setminus G_i$, which contains exactly b users. Since the set B intersects every G_j for $j \neq i$, then the users in B can compute the keys of the sets $G_1, \ldots, G_{i-1}, G_{i+1}, \ldots, G_\ell$. Therefore, the pieces from $\vec{u}$ of the users of B determine that the keys of $G_1, \ldots, G_{i-1}$ are $s_1, \ldots, s_{i-1}$ respectively. By the maximality of i it follows that:

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

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 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. □

In this proof we use the weak security requirement. That is, even weak (g,b) schemes must have large domain of pieces. Thus, our proof yields a stronger result than the lower bound of [2]. 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 5. *Let $\mathcal{U}$ be a (weak) non-interactive (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 [2] have constructed an unrestricted non-interactive (g,b) scheme with domains of pieces $|U_i| = |S|^{\binom{g+b-1}{g-1}}$. 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 Interaction from Unrestricted Schemes

In this section we show how to transform an unrestricted interactive scheme into a unrestricted (weak) non-interactive key distribution scheme, without changing the domain of pieces. This means that the lower bound on the cardinality of the domain of pieces applies to unrestricted interactive schemes.

Theorem 6. *Let $\mathcal{U}$ be an interactive (g,b)-KDS 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 u. Then for every user i:*

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

Proof. The high level 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 interacts in order to generate a conference key). 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 interaction is required. In the proof, we show first how to choose communications for different conferences such that they are consistent among themselves. Therefore there are vectors of pieces that are consistent with all the communications. Once this is done, it is clear that the non-interactive scheme has the reconstruction property. We then prove that the resulting non-interactive scheme has the weak security property. Therefore it is a weak non-interactive (g, b) scheme.[5] By Theorem 4 the cardinality of the domain of pieces of every user in the resulting non-interactive scheme is at least $|S|^{\binom{g+b-1}{g-1}}$. But the domain of the pieces in the non-interactive scheme is not larger than that of the interactive scheme. Therefore, the lower bound on the size of the pieces applies to the original interactive scheme as well.

To complete this 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 $\vec{u}$, that the server deals 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 chooses at random a vector of pieces that is consistent with the communications. That is, the server chooses from all the vectors of pieces $\vec{v}$ for which there exists a vector of random inputs $\vec{r}$, such that every set G of g users, holding the pieces of $\vec{v}$, and having the random inputs $\vec{r_G}$, communicate C_G.

We next prove the weak security property of the non-interactive scheme. Let G be any set of cardinality g, and B be a disjoint set of cardinality b. By the security property of the interactive 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 in which the pieces of the users in B are the same, but the key of the conference G is s. That is, the non-interactive scheme has the weak security property, as claimed. □

We can define the notion of weak security for unrestricted interactive schemes as well. The lower bound of Theorem 6 is also applicable to such weak unrestricted interactive schemes.

5 Restricted Interactive Key Distribution Schemes

5.1 Motivation and Definition

By Theorem 6, interaction 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

[5] 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.

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 6). First, we state the exact definition of τ-restricted key distribution scheme, and then prove upper and lower bounds on the size of the pieces in such schemes. There is still a gap between our upper and lower bounds.

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 interactive schemes. For non-interactive schemes, the generation of a conference key does not add any information with respect to any user (either in the conference, or not in the conference). Therefore a one-time secure non-interactive scheme would also be secure in the unrestricted sense, and no saving can be expected. On the other hand, in interactive schemes the interaction, heard by all users (not only conference members), could reduce the secrecy of the remaining pieces. Finally, after sufficiently many interactions take place, no uncertainty is left, and the pieces become useless for additional conferences. This means that the amount of initial secrecy in restricted interactive schemes can be smaller than in unrestricted schemes. The proof that unrestricted interactive schemes can not be more space efficient than unrestricted non-interactive schemes (Theorem 6) can not be used for restricted schemes. For example, one could transform a one-time secure interactive scheme into a non-interactive scheme, using the technique of Theorem 6. However, this would yield a non-interactive scheme which is secure with respect to a single *fixed* conference, depending one initiating the interaction.

Definition 7. A τ-restricted (g, b)-scheme is an interactive (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 knowing the conversations sent in any τ conferences, do not have any information on the key of any disjoint set G_0. 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 $G_0, \ldots, G_{\tau-1}$ respectably:

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

Where 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, where the restriction of $\vec{r}$ to the coalition B equals $r_{\vec{B}}$.

We denote 1-restricted scheme by *one-time scheme.*

5.2 Upper Bound

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

Lemma 8. *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 $|S|$ in which the cardinality of the domain of pieces of every user is $|S|^{2+2\cdot(b-1)/g}$.*

Proof Sketch. We construct our interactive one-time (g, b)-scheme as following: The server deals vectors of pieces according to the non-interactive $(2, g + b - 2)$ scheme of Blom [1] for n users, with keys taken from a domain of cardinality $|S|^{2/g} = q^2$ (this is where we need $q \geq \sqrt{n}$). When the users of a set 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. That is

$$s = s_1 \circ s_2 \circ \ldots \circ s_g$$

We will show how every user $i \in G$ sends a message on a broadcast channel, such that every user in G will be able to reconstruct s_i, and every user not in G does not learn anything from these messages. Every user $i \in G$ will send a message to every user $j \in G$, that will be meaningful only to user j. The idea is to use the keys of the non-interactive scheme as a one-time pad. More formally, every pair of users $i, j \in G$ reconstruct the joint key $s_{i,j} \in \{0, \ldots, q^2 - 1\}$ according to the pieces from the non-interactive scheme. Now we view this joint key as consisting of two sub-keys $s'_{i,j}, s''_{i,j}$, both in $\{0, \ldots, q - 1\}$. In order to inform user j of s_i, user i broadcasts $s_i + s'_{i,j} \pmod q$, in the case $i < j$, and $s_i + s''_{i,j} \pmod q$, in the case $i > j$. Notice that every sub-key is used only once.

To prove that the interactive scheme has the 1-restricted security property, it is enough to show that the messages 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 fact, in turn, follows the next claim from [2] about unrestricted non-interactive $(2, g + b - 2)$ schemes. The claim states that the vector of keys of all pairs of users in G in the non-interactive scheme is uniformly distributed and independent of the pieces of the users in B. Formally,

Lemma 9. *(Lemma 4.1 of [2]) Let $\mathcal{U}$ be a non-interactive unrestricted $(2, g+b-2)$-scheme with the uniform a-priori distribution on the key domain S. Let G and B be sets of g and b users respectably, such that $G \cap B = \emptyset$. Let $G_1, G_2, \ldots, G_{\binom{g}{2}}$ be all the subsets of G of cardinality 2. Let $s_1, \ldots, s_{\binom{g}{2}}$ 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:*

$$\Pr[\bigwedge_{1 \leq i \leq \binom{g}{2}} s_{G_i}(r) = s_i | \bigwedge_{j \in B} \mathcal{U}_j(r) = u_j] = \frac{1}{|S|^{\binom{g}{2}}}$$

We used the non-interactive $(2, g+b-2)$-scheme with domain of keys of cardinality $|S|^{2/g}$. So the cardinality of the domain of pieces of each user is

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

as claimed. □

Notice that the conference key of G ($s = s_1 \circ s_2 \circ \ldots \circ s_j$) is distributed uniformly in S. It is possible to change this probability distribution on the keys. One way to achieve this goal is to first generate a key s as in the previous way. Then user 1 chooses the real key k for the conference according to any desired distribution. User 1 sends the message $(k+s) \bmod q$.

One property of our interactive scheme is that it uses only one-way interaction. 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.

We remark that the 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 $G_1 \cup G_2$. We use τ independent copies of the one time scheme in order to extend our scheme to a τ-secure one. Since the copies are independent, each conference does not add any information on other conferences. Hence the security of the one-time scheme, implies the security of the τ-restricted scheme.

Theorem 10. *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, in which the domain of pieces is of each user is of cardinality $|S|^{2\tau(1+(b-1)/g)}$.*

This τ-restricted interactive 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 prevent the generation of the present conference key. Our scheme does not work in the absence of a reliable counter.

5.3 Lower Bound

The cardinality of the domain of pieces in the τ-restricted scheme depends on τ. We show that if $\tau \leq \binom{g+b-1}{g-1}$, then this dependency on τ cannot be avoided. We conclude, that for $\tau \geq \binom{g+b-1}{g-1}$, the unrestricted scheme of [2] are space optimal even for τ-restricted schemes.

Theorem 11. *Let $\ell = \min\left\{\tau, \binom{g+b-1}{g-1}\right\}$. 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 $|S|^{\ell}$.*

Proof Sketch. Again, we limit the number of users to $g+b$. Using the same ideas as in the proof of Theorem 6, we transform a τ-restricted (g,b)-scheme into a a non-interactive (g,b)-scheme in which ℓ pre-defined sets can reconstruct a key. That is, we fix consistent conversations of the ℓ sets, and the server generates vectors of pieces consistent with these conversations. The original scheme is secure for τ conferences, therefore by fixing $\ell \leq \tau$ conversations,we get a secure scheme in which these ℓ sets can reconstruct a key without any interaction. Since $\ell \leq \binom{g+b-1}{g-1}$, then there are ℓ sets that contain user i. Choosing ℓ such sets, we can apply Lemma 5 to the transformed scheme. So, by Lemma 5. the cardinality of the domain of pieces of user i in the transformed scheme at least $|S|^{\ell}$. 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 $|S|^{\ell}$. □

This lower bound is not tight. For example, we can prove that for a one-time $(2,1)$-scheme, the domain of pieces has to be bigger than $|S|$. We believe that for $(2,1)$-schemes the lower bound can be improved to $|S|^2$ (which is the upper bound).

Acknowledgement Thanks to Amir Herzberg for helpful discussions on these topics.

References

1. R. Blom. An Optimal Class of Symmetric Key Generation Systems. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology – proceeding of Eurocrypt 84*, volume 209 of *Lecture notes in computer Science*, pages 335–338. Springer-Verlag, 1984.
2. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-Secure Key Distribution for Dynamic Conferences. In *Advances in Cryptology - CRYPTO '92 proceeding*, 1992.
3. W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
4. A. Fiat and M. Naor. Broadcast Encryption. In *Advances in Cryptology - CRYPTO '93 proceeding*, 1993.

5. 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.
6. M. J. Fischer and R. N. Wright. Multiparty Secret Key Exchange Using a Random Deal of Cards. In J. Feigenbaum, editor, *Advances in Cryptology - proceeding of CRYPTO 91*, volume 576 of *Lecture notes in computer Science*, pages 141–155. Springer-Verlag, 1992.
7. L. Gong and D. J. Wheeler. A matrix Key-Distribution Scheme. *Journal of Cryptology*, 2:51–59, 1990.
8. T. Matsumoto and I. Imai. On the Key Predistribution Systems: A Practical Solution to the key Distribution Problem. In C. Pomerance, editor, *Advances in Cryptology - proceeding of CRYPTO 87*, volume 293 of *Lecture notes in computer Science*, pages 185–193. Springer-Verlag, 1988.
9. E. Okamoto and K. Tanaka. Key Distribution System Based on Identification Information. *IEEE Journal on Selected Areas in Communications*, 7(4):481–485, 1989.