Information and Computation **146**, 1–23 (1998)
Article No. IC982717

Perfectlv Secure Kev Distribution for

Carlo Blundo* and Alfredo De Santis*

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

Amir Herzberg and Shay Kutten

IBM T.J. Watson Research Center, Yorktown Heights, New York 10598

Ugo Vaccaro*

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

and

Moti Yung

CertCo, New York, New York 10004

In this paper we analyze perfectly secure key distribution schemes for dynamic conferences. In this setting, *any* member of a group of t users can compute a common key using only his private initial piece of information and the *identities* of the other $t-1$ users in the group. Keys are secure against coalitions of up to k users; that is, even if k users pool together their pieces they cannot compute anything about a key of any conference comprised of t other users. First we consider a noninteractive model where users compute the common key without any interaction. We prove the tight bound on the size of each user's piece of information of $\binom{k+t-1}{t-1}$ times the size of the common key. Then, we consider the model where interaction is allowed in the common key computation phase and show a *gap* between the models by exhibiting a one-round interactive scheme in which the user's information is only $k+t-1$ times the size of the common key. Finally, we present its adaptation to network topologies with neighbourhood constraints and to asymmetric (e.g., client-server) communication models.

* Partially supported by Italian Ministry of University and Research (MURST) and by National Council for Research (CNR).

0890-5401/98 $25.00

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. The increase in bandwidth, size, usage, and applications of such systems is likely to pose new challenges and to require novel ideas. A growing application area in networking is "conferencing" where a group of entities (or network locations) collaborate privately in an interactive procedure. In this work we consider the basic case of perfectly secure key distribution for conferences. Note that key distribution for two-party communication is a special case of conferences of size two.

If users of a group (which we call a conference) wish to communicate using symmetric encryption, they must share a common key. A key distribution scheme (denoted KDS for short) is a method to distribute off-line initial private pieces of information among a set of users, so that each group of a given size (or up to a given size) can compute a common key for secure conference. This information is generated and distributed by a trusted server which is active only at the distribution phase (like in a set-up phase of a public-key (PK) system suggested by Diffie and Hellman [7] and in contrast to on-line server-based key distribution schemes suggested by Needham and Schroeder, where the server is on-line active at all times [21]).

Various key distribution schemes have been proposed so far, mainly to serve pairs of users. A basic and straightforward perfectly secure scheme (which is useful in small systems) consists of distributing initial keys to users in such a way that each potential group of users shares a common key. In the case of common keys for pairs of users, if n is the number of users, the server has to generate $n(n-1)/2$ keys and each user holds $n-1$ keys, one for each possible communication. When n gets large it becomes problematic or even impossible to manage all keys. This is known as the n^2 scheme. For conferences, when we allow all possible subsets of a given size to join together (what we call the dynamic conference setting), the number of keys becomes prohibitively large.

Given the high complexity of such a distribution mechanism, a natural step is to trade complexity for security. We may still require that keys are perfectly secure, but only with respect to an adversary controlling coalitions of a limited size. This novel approach was initiated by Blom [3] for the case of conference of cardinality two (other related schemes are given in [9, 11, 17]). We are motivated by Blom's (somewhat forgotten) pioneering work. We study key distribution for dynamic conferences. Our scheme has two parameters: t, the size of the conference (group), and k, the size of adversary coalitions. Another characteristic of such schemes is whether they are interactive (users exchange messages during common-key establishment phase) or noninteractive. Note that interactive key distribution involves only the users of the particular conference and is a one-time operation, in contrast to practical schemes which involve a trusted server during repeatable conferences.

1.1. The Results

We give a precise model of our setting and then we analyze and design perfectly-secure key distribution schemes for dynamic conferences. We show the following:

1. *Lower bound*: We consider the noninteractive model and prove that the size of the piece of a user's information is at least $\binom{k+t-1}{t-1}$ times the size of the common key.

2. *Matching upper bound*: We propose a concrete scheme and show that it indeed gives pieces of this size, thus establishing the optimality of the bound.

3. *Gap*: We compare the interactive to the noninteractive settings. We show a one-round interactive scheme for distributing one conference key where the user's information is only $t+k-1$ times the size of the common key, proving a separation between the interactive and the noninteractive cases.

4. *Constrained communication-graph conferencing*: We present modifications of the schemes to systems in which conferences are generated according to neighbourhood constraints (of the network communication graph).

5. *Asymmetric communication model*: We extend our results to an asymmetric model where there are two types of users with one type having higher "rank" than the other.

Our analysis deals with the generation of one key and it applies information theory and its basic notions of entropy and mutual information, as well as their conditional versions. In the Appendix we review these notions and present basic equations that we use.

1.2. Related Work

The two common approaches to key distribution (different from the one in this paper), which were taken in order to reduce the inherent complexity of the basic straightforward n^2 scheme, are schemes based on public-key cryptography (using PK-cryptosystems or key-exchange protocols) [7] or on an on-line authentication server [21]. Numerous suggestions for key distribution schemes based on computational assumptions in the above settings are known (e.g., [10, 13, 18, 20, 22, 25–27]), as well as a number of suggestions for conference keys (e.g., [5, 14, 24]). We remark that our approach is information theoretic (a one-time perfectly secure distribution) and indeed differs from the above computational (more practical) approaches. Yet, our bounds serve as foundations for the key distribution problem in general and in particular formally prove the necessity of n^2 keys (if an on-line server is not employed and we allow any size of user set to collude against a pair of users).

In [12] it has been proved that two parties cannot establish a common key from scratch using only one-way permutation based on black-box reductions unless P can be separated from NP.

Blom's innovative method is a key distribution for pairs of users which are ID-based that predated the formal definition of this notion by Shamir [23]. Blom's technical tool was MDS linear codes. Later, Matsumoto and Imai [17] extended the work of [3] to general symmetric functions; they further systematically defined key distribution schemes based on general functions (our scheme as well as the basic n^2 scheme can actually be viewed as a special case of their general system).

Inspired by the preliminary version of this work [+], Beimel and Chor [1] proved that in key distribution schemes where many key are generated, the interaction cannot help in decreasing the size of the pieces of information given to the users. They also proposed a t-round interactive protocol for k-secure t-conference key distribution schemes to establish a single conference key: At the expense of an increase in the round complexity, the user's information is only $2(t+k-1)/t$ times the size of the common key.

Fiat and Naor [8] considered a new scenario for key distribution in which a center gives some predefined keys to users. Later, the center wants to enable a *privileged* subset of users to recover a common key in such a way that coalitions of users that are not in the privileged class have no information on this common key. The center enables the privileged users to share a key by broadcasting a message. Leighton and Micali [15] described various approaches to unconditional secure key distribution schemes which are not based on public-key cryptography or polynomial/integer arithmetic.

Finally, Blundo and Cresti [4] modelled the problem of unconditionally secure broadcast encryption schemes with an information theoretic framework giving tight limitations both on the number of private keys associated with each user and on the number of keys generated by the server, proving that the unconditional scheme presented in [8] is optimal.

Organization. In Section 2 we formally define a KDS in terms of the entropy. In Section 3 we prove the lower bound on the entropy of each user in a k-secure t-conference KDS. In Section 4 we then describe and analyse an actual optimal scheme for k-secure t-conference KDS. In Section 5 we show how interaction can be used to dramatically decrease the amount of information held by each user. In Section 6 we present an optimal protocol to realize a conference KDS when not all pairs of users are able to communicate. In Section 7 we present results for the asymmetric models where the system is comprised of more-trusted users (e.g., servers) and less-trusted users. In the Appendix we recall the definition of entropy and some of its properties.

2. THE MODEL

In this section we present the key distribution problem and model. A key distribution scheme distributes some information among a set of users, so that any t of them can join and generate a secure key. We assume a trusted off-line server active only at initiation (unlike an on-line server approach put forth in [21] which we call server-based KDS). As we said, the system is k-secure if any k users, pooling together their pieces, have no information on keys they should not know. These schemes can be further classified into two categories: interactive (where users are engaged in a protocol, prior to usage of the common key) and noninteractive (where keys are generated privately by the individuals). Next, we formally define non-interactive key distribution schemes. Our definition of security is based on the notion of entropy and is thus unconditional.

A key distribution scheme for a set of users $\mathcal{U} = \{\mathsf{User}_1, ..., \mathsf{User}_n\}$ consists of a triple: a matrix M whose columns are indexed by the members of $\mathcal{U}$, a probability distribution Π on the rows of M, and a function f. When the server wants to set up a scheme he randomly chooses according to Π a row of the matrix M. If the server chooses the jth row, then he gives the value $u_i = M(j, i)$ to user User_i. The *reconstruction function* f is a publicly known three-argument function which is used to noninteractively compute a common conference key. If User_i wants to compute the common key of the set $X \subseteq \{1, ..., n\}$, $i \in X$, then he computes $s_X = f(u_i, i, X)$, where u_i is the piece of information received by the server. The function f satisfies $f(u_i, i, X) = f(u_j, j, X)$ if $i, j \in X$.

Let U_i be the set of all possible pieces given to User_i. Given a set $X = \{i_1, i_2, ..., i_r\}$, where $i_1 < i_2 < \cdots < i_r$, of elements in $\{1, 2, ..., n\}$, denote by U_X the set $U_{i_1} \times \cdots \times U_{i_r}$. The server's algorithm defines a probability distribution on $U_1 \times \cdots \times U_n$, that, in turn, naturally induces a probability distribution $\{p_{U_X}(u)\}_{u \in U_X}$ on U_X, for any set $X \subseteq \{1, 2, ..., n\}$. Let $H(U_X) = H(U_{i_1} \cdots U_{i_r})$ be the entropy of the probability distribution on $U_X = U_{i_1} \times \cdots \times U_{i_r}$.

We denote by S_X the set of all possible values of the common key s_X. Hence, $S_X = \{f(u, i, X): u \in U_i\}$, for any $i \in X$. For any set $X \subseteq \{1, 2, ..., n\}$, the probability distribution on $U_1 \times \cdots \times U_n$ naturally induces a probability distribution on S_X, since each User_i deterministically computes the conference key s_X from the information u_i received by the server. Let $\{p_{S_X}(s)\}_{s \in S_X}$ be the probability that $s_X = s$ and let $H(S_X)$ be its entropy.

The maximum value that the security parameter k can take in any t-conference KDS for n users is $n - t$, since any adversary coalition can contain at most $n - t$ users. Formally, we define a noninteractive k-secure t-conference key distribution scheme for n users as follows.

DEFINITION 2.1. Let $\mathcal{U}$ be a set of n users and let t and k be nonnegative integers with $k + t \leqslant n$. A noninteractive k-secure t-conference key distribution scheme for $\mathcal{U}$ is a scheme such that

1. *Each group of t users can noninteractively compute the common key.* Formally, for all $X \subseteq \{1, 2, ..., n\}$ with $|X| = t$, for all $u_X \in U_X$ with $p_{U_X}(u_X) > 0$, a unique secret-key s_X exists such that for each user, User_i, $i \in X$, it holds that $p(s_X | u_i) = 1$.

2. *Any group of k users have no information on any key they should not know.* Formally, for all $Y, X \subseteq \{1, 2, ..., n\}$, with $|Y| = k$, $|X| = t$, and $X \cap Y = \varnothing$, for all $u_X \in U_X$ and $u_Y \in U_Y$, *with* $p_{U_Y}(u_Y) > 0$, and for all $s_X \in S_X$, it holds that $p(s_X | u_Y) = p_{S_X}(s_X)$.

Property 1 means that given the value held by the User_{i_l}, $l = 1, 2, ..., t$, and the identity of the other $t - 1$ users, a unique value of the common key exists. Property 2 means that the probability that the common key among users $\mathsf{User}_{i_1}, ..., \mathsf{User}_{i_t}$ is s_X, where $X = \{i_1, ..., i_t\}$, given the information held by users $\mathsf{User}_{j_1}, ..., \mathsf{User}_{j_k}$, where $Y = \{j_1, ..., j_k\}$, and $X \cap Y = \varnothing$, is equal to the *a priori* probability that the common

key is s_X. This means that random variables S_X and U_Y are statistically independent and, thus, the values $u_{j_1}, ..., u_{j_k}$ reveal no information on the common key s_X.

By using the entropy function it is possible to give an equivalent definition of a noninteractive k-secure t-conference KDS.

DEFINITION 2.2. Let $\mathcal{U}$ be a set of n users and let t and k be nonnegative integers with $k + t \leqslant n$. A noninteractive k-secure t-conference key distribution scheme for $\mathcal{U}$ is a scheme such that

1′. *Each t user can noninteractively compute the common key.* Formally, for all $X \subseteq \{1, 2, ..., n\}$ with $|X| = t$, and for each User_i, $i \in X$, it holds that $H(S_X | U_i) = 0$.

2′. *Any group of k users have no information on any key they should not know.* Formally, for all Y, $X \subseteq \{1, 2, ..., n\}$, *with* $|Y| = k$, $|X| = t$, and $X \cap Y = \varnothing$, it holds that $H(S_X | U_Y) = H(S_X)$.

Notice that $H(S_X | U_i) = 0$ for each User_i, $i \in X$, means that each set of values held by the User_i corresponds to a unique value of the common key. In fact, by definition, $H(S_X | U_i) = 0$ is equivalent to the fact that for all $u_i \in U_i$, with $p_{U_i}(u_i) > 0$, a unique value $s_X \in S_X$ such that $p(s_X | u_i) = 1$ exists. Moreover, $H(S_X | U_Y) = H(S_X)$ is equivalent to saying that S_X and U_Y are statistically independent; i.e., for all $u_Y \in U_Y$, with $p_{U_Y}(u_Y) > 0$, we have $p(s_X | u_Y) = p(s_X)$. Hence the two definitions of noninteractive KDS are equivalent.

Definition 2.2 does not say anything on the entropies of random variables S_X and $S_{X'}$, for different $X, X' \subseteq \{1, 2, ..., n\}$, with $|X| = |X'| = t$. For example, we could have either $H(S_X) > H(S_{X'})$ or $H(S_X) \leqslant H(S_{X'})$. Our results apply to the general case of arbitrary entropies on keys, but for clarity we state our results for the simpler case that all entropies on keys are equal, i.e., $H(S_X) = H(S_{X'})$. We denote this common entropy by $H(S)$.

The next simple lemma proves that if a t-conference KDS is k-secure then it is k'-secure for all integers $k' < k$.

LEMMA 2.3. *Let $\mathcal{U}$ be a set of n users and let t and k be nonnegative integers with $k + t \leqslant n$. In any noninteractive k-secure t-conference key distribution scheme for $\mathcal{U}$, for any nonnegative integer $k' < k$ and for all sets $X, Y \subseteq \{1, 2, ..., n\}$ with $|X| = t$, $|Y| = k'$, and $X \cap Y = \varnothing$, it holds that*

$$H(S_X | U_Y) = H(S_X).$$

Proof. Let $X' \subseteq \{1, 2, ..., n\}$ be a set such that $|X'| = k$, $X' \cap X = \varnothing$, and $Y \subset X'$. From 2′ of Definition 2.2 we have $H(S_X) = H(S_X | U_{X'})$. From Eq. (14) in the Appendix, one gets

$$H(S_X | U_{X'}) \leqslant H(S_X | U_Y) \leqslant H(S_X).$$

Thus, $H(S_X | U_Y) = H(S_X)$. ∎

From Lemma 2.3 one has that Property 2′ of Definition 2.2 can be equivalently written as

2″. *Any group of $k' \leqslant k$ users have no information on any key they should not know.* Formally, for all Y, $X \subseteq \{1, 2, ..., n\}$, with $|Y| = k'$, $|X| = t$, and $X \cap Y = \varnothing$, it holds that $H(S_X | U_Y) = H(S_X)$.

3. LOWER BOUND: CONFERENCE KEY DISTRIBUTION

In this section we prove a lower bound on the size of the user's information for a k-secure t-conference KDS.

In a k-secure t-conference KDS the knowledge of k keys does not convey any information on any other key. This is formalized by the next lemma.

LEMMA 3.1. *Let $\mathcal{U}$ be a set of n users and let r, k, and t be integers with $k + t \leqslant n$. Let $X, Y_1, ..., Y_r$, $Z \subseteq \{1, 2, ..., n\}$ such that $|Z| = k$, $Z \cap X = \varnothing$, $Z \cap Y_i \neq \varnothing$ and $|X| = |Y_i| = t$, for $i = 1, ..., r$. Then, in any noninteractive k-secure t-conference key distribution scheme for $\mathcal{U}$ it holds that*

$$H(S_X | S_{Y_1} \cdots S_{Y_r}) = H(S_X).$$

Proof. From Eq. (12) in the Appendix we have $H(S_X) \geqslant H(S_X | S_{Y_1} \cdots S_{Y_r})$. To prove the lemma it is enough to prove that $H(S_X | S_{Y_1} \cdots S_{Y_r}) \geqslant H(S_X)$. Since $Z \cap Y_i \neq \varnothing$, from 1′ of Definition 2.2 we obtain $0 \leqslant H(S_{Y_1} \cdots S_{Y_r} | U_Z) \leqslant \sum_{i=1}^{r} H(S_{Y_i} | U_Z) = 0$. Hence, $H(S_{Y_1} \cdots S_{Y_r} | U_Z) = 0$. From Eq. (15) in the Appendix we get $H(S_X | S_{Y_1} \cdots S_{Y_r}) \geqslant H(S_X | U_Z)$. Moreover, since $Z \cap X = \varnothing$ and $|Z| = k$, from 2′ of Definition 2.2 we obtain $H(S_X | U_Z) = H(S_X)$. Therefore, $H(S_X | S_{Y_1} \cdots S_{Y_r}) \geqslant H(S_X)$ which proves the lemma. ∎

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

THEOREM 3.2. *Let $\mathcal{U}$ be a set of n users and let k and t be integers with $k + t \leqslant n$. In any noninteractive k-secure t-conference key distribution scheme, if all entropies on keys are equal, i.e., $H(S) = H(S_X)$ for all $X \subseteq \{1, 2, ..., n\}$ and $|X| = t$, then the entropy $H(U_i)$ satisfies*

$$H(U_i) \geqslant \binom{k+t-1}{t-1} H(S). \tag{1}$$

Moreover, if all keys are chosen in sets of the same cardinality, i.e., $|S| = |S_X|$ for all $X \subseteq \{1, 2, ..., n\}$ and $|X| = t$, then, for any user User_i it holds that

$$\log |U_i| \geqslant \binom{k+t-1}{t-1} \log |S|. \tag{2}$$

Proof. Consider the set of indices $I=\{j_1, ..., j_{k+t-1}\}$ and an index i such that $i \notin I$. Define set C as $C=\{j_1, ..., j_k\}$ and set A as $A=\{i, j_{k+1}, ..., j_{k+t-1}\}$. Let m be the number of different sets B_l constructed by taking the element i along with any $(t-1)$ elements from the set I, with the exception of $\{j_{k+1}, ..., j_{k+t-1}\}$. It is easy to see that there are exactly $m=\binom{k+t-1}{t-1}-1$ such sets, denoted $B_1, ..., B_m$. Namely,

$$B_l \in \{\{i, x_1, ..., x_{t-1}\} \mid x_1, ..., x_{t-1} \in I, \{x_1, ..., x_{t-1}\} \neq \{j_{k+1}, ..., j_{k+t-1}\}\}.$$

We have

$$\begin{aligned}
H(U_i) &= H(S_{B_1} \cdots S_{B_m} S_A) - H(S_{B_1} \cdots S_{B_m} S_A \mid U_i) + H(U_i \mid S_{B_1} \cdots S_{B_m} S_A) \\
&\qquad \text{(from Eqs. (10) and (11) in the Appendix)} \\
&\geqslant H(S_{B_1} \cdots S_{B_m} S_A) - \sum_{l=1}^{m} H(S_{B_l} \mid U_i) - H(S_A \mid U_i) + H(U_i \mid S_{B_1} \cdots S_{B_m} S_A) \\
&\qquad \text{(from Eqs. (9) and (14) in the Appendix)} \\
&= H(S_{B_1} \cdots S_{B_m} S_A) + H(U_i \mid S_{B_1} \cdots S_{B_m} S_A) \qquad \text{(from 1$'$ of Definition 2.2)} \\
&\geqslant H(S_{B_1} \cdots S_{B_m} S_A) \qquad \text{(from Eq. (8) in the Appendix)} \\
&= H(S_{B_1}) + H(S_{B_2} \mid S_{B_1}) + \cdots + H(S_{B_m} \mid S_{B_1} \cdots S_{B_{m-1}}) + H(S_A \mid S_{B_1} \cdots S_{B_m}) \\
&\qquad \text{(from Eq. (9) in the Appendix)}
\end{aligned}$$

Sets $X=A$, $Z=C$, and $Y_i=B_i$ for $i=1, ..., m$ satisfy the hypothesis of Lemma 3.1. Thus, we have $H(S_A \mid S_{B_1} \cdots S_{B_m}) = H(S_A)$. Moreover, for each h, $1 \leqslant h \leqslant m$, sets $X=B_h$, $Z=I \backslash B_h$, and $Y_i=B_i$, for $i=1, ..., h-1$ satisfy the hypothesis of Lemma 3.1. Thus, $H(S_{B_h} \mid S_{B_1} \cdots S_{B_{h-1}}) = H(S_{B_h})$ and

$$\begin{aligned}
H(U_i) &\geqslant H(S_{B_1}) + H(S_{B_2}) + \cdots + H(S_{B_m}) + H(S_A) \\
&= (m+1)\, H(S) \\
&= \binom{k+t-1}{t-1} H(S).
\end{aligned}$$

To prove the bound (2) notice that the index i belongs to sets $B_1, ..., B_m$, and A; hence, User_i has to compute at least $m+1=\binom{k+t-1}{t-1}$ keys. From Lemma 3.1, the keys of these conferences are independent. Therefore, supposing that all keys are chosen in sets of the same cardinality $|S|$, there are at least $|S|^{\binom{k+t-1}{t-1}}$ possible vectors of keys. Each of these vectors of keys can be a possible vector to be reconstructed by User_i. Hence, $|U_i| \geqslant |S|^{\binom{k+t-1}{t-1}}$ which proves the bound (2). ∎

Beimel and Chor [1] proved that the lower bound (2) of Theorem 3.2 holds under weaker assumptions. However, the bound (1) of Theorem 3.2 on the entropy of each user does not hold in Beimel and Chor's weaker model. Indeed, consider the following 1-secure 2-conference key distribution scheme.

TABLE I

1-Secure 2-Conference KDS

$s_{1,2}$	$s_{1,3}$	$s_{2,3}$	Prob.
0	0	0	$1-7\varepsilon$
0	0	1	ε
0	1	0	ε
0	1	1	ε
1	0	0	ε
1	0	1	ε
1	1	0	ε
1	1	1	ε

The server chooses a row in Table I, according to the probability distribution in the last column. The first row is chosen with probalility $1-7\varepsilon$, where $0<\varepsilon\leqslant 1/7$ and $\varepsilon\neq 1/8$; whereas each other row is chosen with probability ε. The server distributes the key $s_{i,j}$ to users User_i and User_j. This scheme satisfies the condition of the weaker model in [1] and meets the bound (2) of Theorem 3.2. One can easily compute that $H(S) \triangleq H(S_{1,2})=H(S_{1,3})=H(S_{2,3})=h(4\varepsilon)$ (where $h(p)=-p\log p-(1-p)\log(1-p)$ is the binary entropy). We have that $H(U_i)=h(4\varepsilon)+4\varepsilon+(1-4\varepsilon)\,h(2\varepsilon/(1-4\varepsilon))$, for $i=1,2,3$. It results that $H(U_i)<2h(4\varepsilon)=2H(S)$ for $0<\varepsilon\leqslant 0.12$. Therefore, in the weaker model of Beimel and Chor [1] the bound (1) of Theorem 3.2 on the entropy of each user does not hold. This is essentially due to the fact that Lemma 3.1 under their weaker assumption does not hold.

A particular case of Theorem 3.2 is when $t=2$ and $k=n-2$. In this case the key of a pair of users cannot be computed (even one of its bits cannot be computed) by an adversary coalition comprised of the other $n-2$ users. Each user holds at least $n-1$ pieces of information of a size equal to the size of the common key. The total number of pieces of information held by all users is at least $n(n-1)$. This is the well-known problem of n^2 keys. The bound (2) is achieved by the protocol we propose in Section 4.

4. PROTOCOLS FOR KEY DISTRIBUTION

In this section we design and analyze protocols for k-secure t-conference key distribution which are applicable to hierarchical KDS as well (as will be later explained). The scheme we propose when applied to 2-party KDS is a particular case of Blom's scheme [3] based on MDS linear codes, and, in particular based on polynomials.

Blom's protocol for a k-secure (2-conference) KDS for n users is as follows. Let G be a (publicly known) generator matrix of a $(n, k+1)$ MDS linear code over $GF(q)$ (see [16] for definitions and analysis of such codes) and let D be a secret random matrix with elements in $GF(q)$. From the matrices G and D, construct a $n\times n$ symmetric matrix K whose entries will be the users' keys. The matrix K is equal to $K=(DG)^T G$. The information given to User_i consists of the row i of $(DG)^T$.

If User_i wants to communicate with User_j then he computes the inner product of the held vector with the column j of G and he obtains the common key $s_{i,j} = K(i, j)$.

We propose the following protocol (to be extended to various other applications in the following) for a noninteractive k-secure t-conference KDS based on symmetric polynomials. A polynomial $P(x_1, ..., x_t) = \sum_{0 \leq j_1, ..., j_t \leq k} a_{j_1, ..., j_t} (x_1)^{j_1} (x_2)^{j_2} \cdots (x_t)^{j_t}$ of degree k, where $a_{j_1, ..., j_t} \in GF(q)$, is said to be symmetric if $P(x_1, ..., x_t) = P(x_{\sigma(1)}, ..., x_{\sigma(t)})$ for any permutation $\sigma: \{1, 2, ..., t\} \to \{1, 2, ..., t\}$. We define an equivalence relation $\sim$ on the coefficients of the polynomial P as follows. Two coefficients $a_{i_1, ..., i_t}$ and $a_{j_1, ..., j_t}$ are $\sim$ equivalent if $i_1, ..., i_t$ is a permutation of $j_1, ..., j_t$. In a symmetric polynomial $P(x_1, ..., x_t)$ all pairs of $\sim$ equivalent coefficients are equal. That is, the coefficient $a_{i_1, ..., i_t}$ is equal to $a_{\sigma(i_1), ..., \sigma(i_t)}$, for any permutation $\sigma: \{i_1, i_2, ..., i_t\} \to \{i_1, i_2, ..., i_t\}$. Note that in a symmetric polynomial in t variables of degree k the number of all coefficients that are not pairwise $\sim$ equivalent is equal to the number of possible ways of choosing with repetitions t elements (corresponding to indices $i_1, ..., i_t$) from a set of $k+1$ elements (each i_j can assume $k+1$ values). This number is equal to $\binom{k+t}{t}$. Thus, to randomly choose a symmetric polynomial in t variables of degree k with coefficients in $GF(q)$ it is enough to randomly select only $\binom{k+t}{t}$ values from $GF(q)$.

The protocol to realize a noninteractive k-secure t-conference key distribution scheme can be found in Fig. 1.

As we mentioned above, when $t = 2$ our scheme is a particular case of Blom's scheme. Indeed, the generator matrix G of the MDS code is constructed by setting the entry $G(i, j)$ to j^{i-1}.

To prove that the protocol proposed in Fig. 1 realizes a noninteractive k-secure t-conference key distribution scheme, we need the following technical lemma.

LEMMA 4.1. *Let $R_1(x_1, ..., x_l), ..., R_{k+1}(x_1, ..., x_l)$ be polynomials in l variables of degree k with coefficients in $GF(q)$ and let $y_1, ..., y_{k+1}$ be $k+1$ different values in $GF(q)$. There exists an unique polynomial $Q(x_1, ..., x_{l+1})$ in $l+1$ variables of degree k with coefficients in $GF(q)$ such that, for $i = 1, 2, ..., k+1$, it holds that $Q(x_1, ..., x_l, y_i) = R_i(x_1, ..., x_l)$.*

Protocol 1

1. The server randomly chooses a symmetric polynomial $P(x_1, \ldots, x_t)$ in t variables of degree k with coefficients over $GF(q)$, $q > n$.
2. To each User_i the server gives the polynomial $f_i(x_2, \ldots, x_t) = P(i, x_2 \ldots, x_t)$, that is the polynomial obtained by evaluating $P(x_1, \ldots, x_t)$ at $x_1 = i$.
3. If the users $\mathsf{User}_{j_1}, \ldots, \mathsf{User}_{j_t}$ want to set up a conference key then each User_{j_i} evaluates $f_{j_i}(x_2, \ldots, x_t)$ at $(x_2, \ldots, x_t) = (j_1, \ldots, j_{i-1}, j_{i+1}, \ldots, j_t)$.
4. The conference key for users $\mathsf{User}_{j_1}, \ldots, \mathsf{User}_{j_t}$ is equal to $s_{j_1, \ldots, j_t} = P(j_1, \ldots, j_t)$.

FIG. 1. Protocol for noninteractive k-secure t-conferences KDS.

Proof. It is simple to show that there exists a polynomial satisfying the hypothesis of the lemma. Indeed, consider the polynomial $Q(x_1, ..., x_{l+1}) = \sum_{i=1}^{k+1} (\prod_{j=1, j\neq i}^{k+1} ((x_{l+1} - y_j)/(y_i - y_j)))\, R_i(x_1, ..., x_l)$. Clearly, for $i = 1, 2, ..., k+1$, it holds that $Q(x_1, ..., x_l, y_i) = R_i(x_1, ..., x_l)$. Now, we prove that the polynomial satisfying the hypothesis is unique. The polynomial Q can be rewritten as $Q(x_1, ..., x_{l+1}) = \sum_{0 \leqslant j_1, ..., j_{l+1} \leqslant k} a_{j_1, ..., j_{l+1}} (x_1)^{j_1} \cdots (x_{l+1})^{j_{l+1}}$. We have that $R_i(x_1, ..., x_l) = Q(x_1, ..., x_l, y_i) = \sum_{0 \leqslant j_1, ..., j_l \leqslant k} A_{j_1, ..., j_l, i} (x_1)^{j_1} \cdots (x_l)^{j_l}$ where, for any $0 \leqslant j_1, ..., j_l \leqslant k$ and $i = 1, 2, ..., k+1$,

$$A_{j_1, ..., j_l, i} = \sum_{j_{l+1}=0}^{k} a_{j_1, ..., j_l, j_{l+1}} (y_i)^{j_{l+1}}. \tag{3}$$

If we consider (3) for fixed $j_1, ..., j_l$ we have the following linear system of $k+1$ unknowns (the coefficients $a_{j_1, ..., j_l}$) and $k+1$ equations

$$\begin{cases} a_{j_1, ..., j_l, 0} + a_{j_1, ..., j_l, 1}\, y_1 + a_{j_1, ..., j_l, 2} (y_1)^2 + \cdots + a_{j_1, ..., j_l, k} (y_1)^k = A_{j_1, ..., j_l, 1} \\ a_{j_1, ..., j_l, 0} + a_{j_1, ..., j_l, 1} y_2 + a_{j_1, ..., j_l, 2} (y_2)^2 + \cdots + a_{j_1, ..., j_l, k} (y_2)^k = A_{j_1, ..., j_l, 2} \\ \qquad\qquad \vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ a_{j_1, ..., j_l, 0} + a_{j_1, ..., j_l, 1} y_{k+1} + a_{j_1, ..., j_l, 2} (y_{k+1})^2 + \cdots + a_{j_1, ..., j_l, k} (y_{k+1})^k = A_{j_1, ..., j_l, k+1}. \end{cases}$$

This can be written in matrix form as follows:

$$\begin{pmatrix} 1 & y_1 & (y_1)^2 & \cdots & (y_1)^k \\ 1 & y_2 & (y_2)^2 & \cdots & (y_2)^k \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & y_{k+1} & (y_{k+1})^2 & \cdots & (y_{k+1})^k \end{pmatrix} \begin{pmatrix} a_{j_1, ..., j_l, 0} \\ a_{j_1, ..., j_l, 1} \\ \vdots \\ a_{j_1, ..., j_l, k} \end{pmatrix} = \begin{pmatrix} A_{j_1, ..., j_l, 1} \\ A_{j_1, ..., j_l, 2} \\ \vdots \\ A_{j_1, ..., j_l, k+1} \end{pmatrix}.$$

The matrix Y on the left side is a Vandermonde matrix, and its determinant is

$$\det Y = \prod_{1 \leqslant m < r \leqslant k+1} (y_m - y_r).$$

The y_i's are all distinct, so no term $y_m - y_r$ is equal to 0, and $\det Y \neq 0$. Therefore, the system has an unique solution over $GF(q)$. By resolving this system, we can compute the unique coefficients $a_{j_1, ..., j_l, 0}, a_{j_1, ..., j_l, 1}, ..., a_{j_1, ..., j_l, k}$. Thus, for $0 \leqslant j_1, ..., j_l \leqslant k$, resolving $(k+1)^l$ linear systems represented by (3) (a system for each choice of $0 \leqslant j_1, ..., j_l \leqslant k$) we can compute all coefficients $a_{j_1, ..., j_{l+1}}$ where $0 \leqslant j_1, ..., j_{l+1} \leqslant k$. This proves the lemma. ∎

The following theorem proves that the protocol proposed in Fig. 1 realizes a noninteractive k-secure t-conference key distribution scheme.

THEOREM 4.2. Protocol 1 *is a noninteractive k-secure t-conference key distribution scheme.*

Proof. It is easy to see that in **Protocol 1** any group of t users, say $\mathsf{User}_{j_1}, ..., \mathsf{User}_{j_t}$, can compute the same conference key $s_{j_1, ..., j_t} = P(j_1, ..., j_t)$. Thus, Property 1 of Definition 2.2 is satisfied. We prove that the scheme realized by **Protocol 1** is k-secure. From Lemma 4.1, any $k+1$ users can compute all coefficients of the polynomial $P(x_1, ..., x_t)$. We will prove that any k users, say $\mathsf{User}_{z_1}, ..., \mathsf{User}_{z_k}$, knowing the polynomials $f_{z_1}, ..., f_{z_k}$ and guessing a conference key $s \in GF(q)$ of other t users, say $\mathsf{User}_{z_1'}, ..., \mathsf{User}_{z_t'}$, where $\{z_1', ..., z_t'\} \cap \{z_1, ..., z_k\} = \varnothing$, can compute the unique polynomial $P'(x_1, ..., x_t)$ such that, for $i = 1, 2, ..., k$, $P'(z_i, x_2, ..., x_t) = f_{z_i}(x_2, ..., x_t)$ and $P'(z_1', ..., z_t') = s$. Since the key s can be an arbitrary value in $GF(q)$, the users $\mathsf{User}_{z_1}, ..., \mathsf{User}_{z_k}$ can construct q different polynomials. Since the polynomial P was uniformly chosen, the q polynomials the users $\mathsf{User}_{z_1}, ..., \mathsf{User}_{z_k}$ can construct are equally likely to be the polynomial P used by the center to set up the scheme. That is, $Pr(S_{z_1, ..., z_k} = s \mid U_{z_1} = u_{z_1} \cdots U_{z_k} = u_{z_k}) = Pr(S_{z_1, ..., z_k} = s)$, and therefore $H(S_{z_1, ..., z_k} \mid U_{z_1} \cdots U_{z_k}) = H(S_{z_1, ..., z_k})$.

Suppose users $\mathsf{User}_{z_1}, ..., \mathsf{User}_{z_k}$ guess a value $s \in GF(q)$ for the common key among $\mathsf{User}_{z_1'}, ..., \mathsf{User}_{z_t'}$, that is, they know $P(z_1', ..., z_t') = s$. For $i = 1, 2, ..., k$, User_{z_i} evaluates the polynomial $f_{z_i}(x_2, ..., x_t)$ at $(x_2, ..., x_t) = (z_1', ..., z_{t-1}')$ obtaining $P(z_i, z_1', ..., z_{t-1}') = y_i$. Since the polynomial $P(x_1, x_2, ..., x_t)$ is symmetric, we have that $P(z_1', ..., z_{t-1}', z_i) = P(z_i, z_1', ..., z_{t-1}') = y_i$. Hence, the users $\mathsf{User}_{z_1}, ..., \mathsf{User}_{z_k}$ know $P(z_1', ..., z_{t-1}', z_t') = s$ and $P(z_1', ..., z_{t-1}', z_i) = y_i$, for $i = 1, 2, ..., k$. Therefore, using Lagrange's interpolation, they can compute the unique polynomial $P(z_1', ..., z_{t-1}', x_t)$ of degree k in the variable x_t.

Now, for $i = 1, 2, ..., k$, the user User_{z_i} evaluates the polynomial $f_{z_i}(x_2, ..., x_t)$ at $(x_2, ..., x_{t-1}) = (z_1', ..., z_{t-2}')$ obtaining the polynomial $P(z_i, z_1', ..., z_{t-2}', x_t)$. Using the symmetry of $P(x_1, x_2, ..., x_t)$, we have $P(z_i, z_1', ..., z_{t-2}', x_t) = P(z_1', ..., z_{t-2}', z_i, x_t)$. Hence, using the polynomial $P(z_1', ..., z_{t-2}', z_{t-1}', x_t)$ previously computed and the polynomials $P(z_1', ..., z_{t-2}', z_i, x_t)$, the users $\mathsf{User}_{z_1}, ..., \mathsf{User}_{z_k}$ can compute the polynomial $P(z_1', ..., z_{t-2}', x_{t-1}, x_t)$ of degree k in the variables x_{t-1} and $x - t$ as shown in Lemma 4.1. Iterating the previous argument $t-3$ times, the users $\mathsf{User}_{z_1}, ..., \mathsf{User}_{z_k}$ can compute the polynomial $P(z_1', x_2, ..., x_t)$ which is the polynomial $f_{z_1'}(x_2, ..., x_t)$ known by the user $\mathsf{User}_{z_1'}$. At this point users $\mathsf{User}_{z_1}, ..., \mathsf{User}_{z_k}$ know the $k+1$ polynomials $f_{z_1}, ..., f_{z_k}, f_{z_1'}$ and from Lemma 4.1, they can construct the unique polynomial $P'(x_1, ..., x_t)$ such that, for $i = 1, 2, ..., k$, $P'(z_i, x_2, ..., x_t) = f_{z_i}(x_2, ..., x_t)$, $P'(z_1', x_2, ..., x_t) = f_{z_1'}(x_2, ..., x_t)$, and $P(z_1', ..., z_t') = s$. ∎

The scheme proposed meets the bound provided by Theorem 3.2, when all coefficients are uniformly chosen. Indeed, in a symmetric polynomial $P(x_1, ..., x_r)$ the coefficient $a_{i_1, ..., i_r}$ is equal to $a_{\sigma(i_1), ..., \sigma(i_r)}$, for all permutations $\sigma: \{i_1, i_2, ..., i_r\} \to \{i_1, i_2, ..., i_r\}$. Thus, the number of coefficients of a symmetric polynomial in r variables of degree k is equal to the number of possible ways of choosing with repetitions r elements (corresponding to indices $i_1, ..., i_r$) from a set of $k+1$ elements (each i_j can assume $k+1$ values). This is equal to $\binom{k+r}{r}$.

5. NONINTERACTIVE VERSUS INTERACTIVE SCHEMES

In Section 3 we proved that in a noninteractive k-secure t-conference KDS, for each User_i it holds that $H(U_i) \geqslant \binom{k+t-1}{t-1} H(S)$. In this section we prove that if we allow interaction among users (not with the server!) to set up a common key, then the lower bound can be beaten! We extend the definitions of Section 2 to interactive key distribution schemes and present a protocol that realizes an interactive k-secure t-conference KDS. A non-interactive scheme is an interactive scheme in which there is no interaction among the users.

In fact, for our purposes it suffices to define schemes with very little interaction, which we call *one-round interactive KDS*. In one-round interactive KDS, each user User_i gets/sends a single message γ_i from/to other users, based on the users' keys. Let Γ_i be the set of all possible values of γ_i. Given a set $X = \{i_1, i_2, ..., i_r\}$, where $i_1 < i_2 < \cdots < i_r$, of elements in $\{1, 2, ..., n\}$, denote by Γ_X the set $\Gamma_{i_1} \times \cdots \times \Gamma_{i_r}$. The server's algorithm and the users' algorithms define a probability distribution on $\Gamma_1 \times \cdots \times \Gamma_n$, that, in turn, naturally induces a probability distribution $\{p_{\Gamma_X}(\gamma)\}_{\gamma \in \Gamma_X}$ on Γ_X, for any set $X \subseteq \{1, 2, ..., n\}$. Let $H(\Gamma_X) = H(\Gamma_{i_1} \cdots \Gamma_{i_r})$ be the entropy of the probability distribution on $\Gamma_X = \Gamma_{i_1} \times \cdots \times \Gamma_{i_r}$.

Formally, following the information theoretical approach of Section 2, we define an interactive k-secure t-conference key distribution scheme for n users as follows.

DEFINITION 5.1. Let $\mathscr{U}$ be a set of n users and let t and k be nonnegative integers with $k + t \leqslant n$. A one-round interactive k-secure t-conference key distribution scheme for $\mathscr{U}$ is a scheme such that

1. *Each t user can interactively (after one-round exchange of messages among the t users) compute the common key.* Formally, for all $X \subseteq \{1, 2, ..., n\}$ with $|X| = t$, and for each User_i, $i \in X$, it holds that $H(S_X | U_i \Gamma_i) = 0$.

2. *Any group of k users have no information on any key they should not know.* Formally, for all Y, $X \subseteq \{1, 2, ..., n\}$, with $|Y| = k$, $|X| = t$, and $X \cap Y = \varnothing$, it holds that $H(S_X | U_Y \Gamma_X) = H(S_X)$.

It is easy to see that the noninteractive model is a particular case of the interactive one. However, note a few issues of practical nature which are not covered by the definition. Since we now allow interaction, there are new "active" attacks on this interactive stage; e.g., an attacker may send forged messages to some users. Our definition does not preclude such active attacks (similar to an active attack on the system when in use for, say, message exchange). Allowing authentication codes (which may double the message size) may solve such attacks by outsiders. Furthermore, note that the definition does not permit the users to repeat the computation of the common key (interactively) twice. Namely, once computed, a conference key has to be remembered by the conference. We do not consider a system where forgetting a key and allowing recomputation are allowed. Another immediate possible extension is to allow many rounds in the interactive key computation.

Now we illustrate a protocol realizing a one-round interactive k-secure t-conference KDS. First, we construct a noninteractive $(k + t - 2)$-secure 2-conference KDS using the protocol presented in Section 4. For any pair of users, the common key will be a randomly chosen element of $GF(q)$. Then, given a group of t users that want to

compute a conference key, the user with the largest identity in the group chooses as conference key a random value in $GF(q)$. Finally, the user with the largest identity in the group sends this value to the other $t-1$ users by using the noninteractive $(k+t-2)$-secure 2-conference KDS. Recall that γ_i denotes the message *received/sent* by User_i.

More formally protocol 2 for parties $\mathsf{User}_1, \ldots \mathsf{User}_n$ can be seen in Fig. 2 (based on the scheme presented above). To simplify the notation, in case of noninteractive k-secure 2-conference KDS for n users, for any set $X \subseteq \{1, 2, \ldots, n\}$ consisting of two elements, $X = \{i, j\}$, $i < j$, we denote the key s_X either with $s_{i,j}$ or with $s_{j,i}$, and the set of common keys S_X either with $S_{i,j}$ or with $S_{j,i}$ (i.e., $S_X = S_{i,j} = S_{j,i}$).

Protocol 2 realizes an interactive k-secure t-conference KDS since the KDS that is established is $(k+t-2)$-secure, as we prove in the next theorem.

In this protocol only $t+k-1$ elements of $GF(q)$ are distributed by the server and kept by each user. This proves a separation between the interactive and the noninteractive case for information–theoretically key distribution schemes for dynamic conferences.

In protocol 2, the message γ_i, for $i = 1, 2, \ldots, t-1$, used by User_i, to set up the common key s, is equal to $\gamma_i = s_{t,i} \oplus s$. Let S be the set of all possible secret keys. The next theorem holds.

THEOREM 5.2. Protocol 2 *realises a one-round interactive k-secure t-conference key distribution scheme.*

Proof. Without loss of generality let $\mathsf{User}_1, \ldots, \mathsf{User}_t$ be the users that want to set up a common key. Let $X = \{1, 2, \ldots, t\}$ be a set in $\subseteq \{1, 2, \ldots, n\}$. Let Y be a set

Protocol 2

1. The server chooses a symmetric polynomial $P(x, y)$ of degree $(k+t-2)$ with coefficients over $GF(q)$, $q > n$, by randomly choosing its coefficients in $GF(q)$.
2. To each User_i the server gives the polynomial $f_i(y) = P(i, y)$ that is the polynomial obtained by evaluating $P(x, y)$ at $x = i$.
3. If parties $\mathsf{User}_{i_1}, \ldots, \mathsf{User}_{i_t}$, where $i_1 < i_2 < \cdots < i_t$, want to set up a conference key, then:
   - 3.1 User_{i_t} randomly chooses a secret key s in $GF(q)$ (the value s is the conference key).
   - 3.2 User_{i_t} evaluates the polynomial $f_{i_t}(y)$ at $y = i_l$, for $l = 1, \ldots, t-1$, and, then, he computes temporary keys $s_{i_t,i_l} = f_{i_t}(i_l)$ (which is equal to $P(i_t, i_l)$).
   - 3.3 User_{i_t} sends to User_{i_l} the value $\gamma_l = s_{i_t,i_l} \oplus s$, for $l = 1, \ldots, t-1$, where $\oplus$ is addition modulo q.
   - 3.4 For $l = 1, \ldots, t-1$: User_{i_l}, first computes $s_{i_t,i_l} = s_{i_l,i_t} = f_{i_l}(i_t)$ (which is equal to $P(i_l, i_t) = P(i_t, i_l)$). Then, User_{i_l} computes s by subtracting modulo q s_{i_t,i_l} from the value γ_l received by User_{i_t}.

FIG. 2. Protocol for one-time interactive k-secure t-conference KDS.

in $\subseteq \{1, 2, ..., n\}$, with $|Y| = k$, such that $Y \cap \{1, 2, ..., t\} = \varnothing$. It is easy to see that the scheme realized by Protocol 2 satisfies Property 1 of Definition 5.1. Thus, to prove that the scheme realized by Protocol 2 is k-secure we have to prove that

$$H(S_X | U_Y \Gamma_1 \cdots \Gamma_t) = H(S_X).$$

Since the secret key $s \in S_X$ is independently chosen from $u_Y \in U_Y$, then $H(S_X | U_Y) = H(S_X)$. Therefore, it is sufficient to prove that

$$H(S_X | U_Y \Gamma_1 \cdots \Gamma_t) = H(S_X | U_Y).$$

Note that in Protocol 2 we have $H(S_X | U_Y \Gamma_1 \cdots \Gamma_t) = H(S_X | U_Y \Gamma_1 \cdots \Gamma_{t-1})$. In fact, it is easy to see that the set of all possible communication Γ_t of User_t is determined by the union of the sets $\Gamma_1, ..., \Gamma_{t-1}$, since the message sent by User_t consists of all the messages received by participants $\mathsf{User}_1, ..., \mathsf{User}_{t-1}$. Thus, to prove the theorem is sufficient to show that $H(S_X | U_Y \Gamma_1 \cdots \Gamma_{t-1}) = H(S_X | U_Y)$. One way of showing that $H(S_X | U_Y \Gamma_1 \cdots \Gamma_{t-1}) = H(S_X | U_Y)$ is to prove that $I(S_X; \Gamma_1 \cdots \Gamma_{t-1} | U_Y) = 0$.

First, we prove that

$$H(S_{t,1} ... S_{t,t-1} | U_Y) = \sum_{j=1}^{t-1} H(S_{t,j}). \tag{4}$$

Indeed, by Eq. (9) in the Appendix we have

$$H(S_{t,1} \cdots S_{t,t-1} | U_Y) = H(S_{t,1} | U_Y) + \sum_{j=2}^{t-1} H(S_{t,j} | U_Y S_{t,1} \cdots S_{t,j-1}).$$

By Definition 2.2 we have $H(S_{i,j} | U_i) = 0$. Thus, from Eq. (15) in the Appendix, one has

$$H(S_{t,1} \cdots S_{t,t-1} | U_Y) \geqslant H(S_{t,1} | U_Y) + \sum_{j=2}^{t-1} H(S_{t,j} | U_Y U_1 \cdots U_{j-1}) = \sum_{j=1}^{t-1} H(S_{t,j}).$$

The last equality holds since $|Y| \leqslant k$ and Protocol 2 uses a polynomial of degree $k+t-2$. Therefore, $k+t-2$ users have no information on keys they should not know. On the other hand, by Eqs. (9) and (12) in the Appendix one finds

$$H(S_{t,1} \cdots S_{t,t-1} | U_Y) \leqslant \sum_{j=1}^{t-1} H(S_{t,j}).$$

Hence, Eq. (4) is proved. From Eqs. (9) and (12) in the Appendix one has

$$H(\Gamma_1 \cdots \Gamma_{t-1} | U_Y) \leqslant \sum_{j=1}^{t-1} H(\Gamma_j).$$

Since $s_{i,j} \in S_{i,j}$ and $s \in S_X$ are independent and uniformly chosen and since adding S to the keys in $GF(q)$ preserves the entropy of the $t-1$ keys (after addition), we have

$$H(\Gamma_1, ..., \Gamma_{t-1} \mid S_X) = H(S_{t,1} \cdots S_{t,t-1}) \tag{5}$$

and $H(\Gamma_j) = H(S_{t,j})$, and thus

$$H(\Gamma_1 \cdots \Gamma_{t-1} \mid U_Y) \leqslant \sum_{j=1}^{t-1} H(S_{t,j}). \tag{6}$$

From Eq. (13) in the Appendix it follows that

$$\begin{aligned} I(\Gamma_1 \cdots \Gamma_{t-1}; S_X \mid U_Y) &= H(\Gamma_1 \cdots \Gamma_{t-1} \mid U_Y) - H(\Gamma_1 \cdots \Gamma_{t-1} \mid U_Y S_X) \\ &\leqslant \sum_{j=1}^{t-1} H(S_{t,j}) - H(S_{t,1} \cdots S_{t,t-1} \mid U_Y) \qquad \text{(from (5) and (6))} \\ &= \sum_{j=1}^{t-1} H(S_{t,j}) - \sum_{j=1}^{t-1} H(S_{t,j}) \qquad \text{(from (4))} \\ &= 0. \end{aligned}$$

Since the mutual information is nonnegative, from Eq. (11) in the Appendix we have that $I(S_X; \Gamma_1 \cdots \Gamma_{t-1} \mid U_Y) = 0$. Hence the theorem is proved. ∎

6. CONFERENCE KEY DISTRIBUTION AND COMMUNICATION GRAPH

In a noninteractive 2-conference KDS for n users each pair of users is able to compute a common key. It can be the case that some pairs of users will never need to compute a common key. In this section we explore the possibility of using smaller pieces of information for users by exploiting such known structures of the possible conferences. Note that our goal here is to improve efficiency rather than security.

This situation can arise when a computer network has a topology which is not the complete graph; here each computer takes the place of a user in a KDS, and two computers can communicate if and only if there is a link between them. As an example, consider a ring of n computers $\mathscr{R} = \{C_0, C_1, ..., C_{n-1}\}$: computer C_i can communicate directly with only two computers, C_{i-1} and C_{i+1} (arithmetic on indices is modulo n) so it will never need to compute a common key with C_{i+2}, for example. We do not allow communication via other computers in the above example; in many situations the communication is restricted *a priori* as in this example. In this section we analyse this case.

Let $\mathscr{U} = \{\mathsf{User}_1, ..., \mathsf{User}_n\}$ be a set of participants (users). A *communication structure* $\mathscr{C}$ is a subset of $\mathscr{U}\&\mathscr{U}$. The communication structure contains all pairs of users for which the server has to provide a common key. A convenient way to represent a communication structure is by a graph G, in which each vertex User_i corresponds to User_i, and there is an edge $\{\mathsf{User}_i, \mathsf{User}_j\}$ if and only if $(\mathsf{User}_i, \mathsf{User}_j)$ or $(\mathsf{User}_j, \mathsf{User}_i)$ belongs

to $\mathscr{C}$. We call the graph associated to a communication structure the *communication graph.*

Definition 2.2 can be extended to a key distribution scheme for any communication structure $\mathscr{C}$, as follows.

DEFINITION 6.1. Let $\mathscr{U}$ be a set of n users, let k be a nonnegative integer with $k+2 \leqslant n$, and let $\mathscr{C} \subseteq \mathscr{U}\&\mathscr{U}$ be a communication structure. A noninteractive k-secure 2-conference key distribution scheme for $\mathscr{C}$ is a scheme such that

1. *Each pair of users in $\mathscr{C}$ can noninteractively compute the common key.* For all $(\mathsf{User}_i, \mathsf{User}_j) \in \mathscr{C}$ it holds that $H(S_{i,j} | U_i) = H(S_{i,j} | U_j) = 0$.

2. *Any group of k users have no information on any key they should not know.* For all sets $Y \subseteq \{1, 2, ..., n\}$ with $|Y| = k$ and indices $i, j \in \{1, 2..., n\} \setminus Y$ it holds that $H(S_{i,j} | U_Y) = H(S_{i,j})$.

Now we describe a k-secure (2-conference) KDS for a communication structure $\mathscr{C}$. First, we do not take into account the communication structure and construct a k-secure KDS for all users as if each pair has to compute a common key. User_i could receive more information than needed. If the degree of vertex User_i in the communication graph is less than k, then the piece of information given to User_i could consist of only the actual keys he needs for communicating.

In Fig. 3 we describe a noninteractive k-secure key distribution scheme (Protocol 3) for a communication structure $\mathscr{C}$, where $\deg(\mathsf{User}_i)$ denotes the cardinality of the set $\{\mathsf{User}_j | (\mathsf{User}_i, \mathsf{User}_j) \in \mathscr{C}\}$.

THEOREM 6.2. Protocol 3 *realizes a noninteractive k-secure 2-conference key distribution for any communication structure $\mathscr{C}$.*

It is easy to see that in Protocol 3 each User_i receives $\min\{k+1, \deg(\mathsf{User}_i)\}$ pieces of information; that is, the size of the information he has is $\min\{k+1, \deg(\mathsf{User}_i)\}$ the size of the common key. The following theorem proves that Protocol 3 is optimal with respect to the size of the information held by each user. In the following theorem we suppose that all keys have the same entropy; i.e., $H(S_{i,j}) = H(S)$ for all i and j.

Protocol 3

1. The server chooses a symmetric polynomial $P(x, y)$ of degree k with coefficients over $GF(q)$, $q > n$, by randomly choosing its coefficients.

2. To each User_i, the server gives the following pieces of information:

   2.1 If $\deg(\mathsf{User}_i) > k$ then the server gives to User_i the polynomial $f_i(y) = P(i, y)$, that is the polynomial obtained by evaluating $P(x, y)$ at $x = i$.

   2.2 If $\deg(\mathsf{User}_i) \leq k$ and $\mathsf{User}_{i_1}, \ldots, \mathsf{User}_{i_m}$, where $m = \deg(\mathsf{User}_i)$, are the adjacent vertices of User_i in the communication graph G, then the server gives to User_i the pieces $\alpha_j = P(i, i_j)$, where $j = 1, \ldots, m$.

FIG. 3. Protocol for noninteractive k-secure KDS for a communication structure $\mathscr{C}$.

THEOREM 6.3. *Let $\mathcal{U}$ be a set of users n, let k be a known integer with $k+2 \leqslant n$, and let G be a communication graph on $\mathcal{U}$. In any noninteractive k-secure 2-conference key distribution scheme for G, the entropy $H(U_i)$ satisfies*

$$H(U_i) \geqslant \mu \cdot H(S),$$

where $\mu = \min\{k+1, \deg(u_i)\}$.

Proof. Let $\{\mathsf{User}_i, \mathsf{User}_{j_1}\}$, ..., $\{\mathsf{User}_i, \mathsf{User}_{j_\mu}\}$ be elements of the communication structure described by graph G. That is, the server has to provide a common key for such pairs of users. Since $0 \leqslant H(S_{i,j_1} \cdots S_{i,j_\mu} | U_i) \leqslant \sum_{l=1}^{\mu} H(S_{i,j_l} | U_i) = 0$, from Eq. (16) in the Appendix one has

$$\begin{aligned} H(U_i) &\geqslant H(S_{i,j_1} \cdots S_{i,j_\mu}) \\ &= H(S_{i,j_1}) + H(S_{i,j_2} | S_{i,j_1}) + \cdots + H(S_{i,j_\mu} | S_{i,j_1} \cdots S_{i,j_{\mu-1}}) \\ &\qquad \text{(from Eq. (9) in the Appendix)} \\ &= H(S_{i,j_1}) + H(S_{i,j_2}) + \cdots + H(S_{i,j_\mu}) \qquad \text{(from Lemma 3.1)} \\ &= \mu H(S). \quad \blacksquare \end{aligned}$$

Analogously to KDSs, in t-conference KDS we can consider the case when not all the t-tuples of users need to set up a common key. Let $\mathcal{U} = \{\mathsf{User}_1, ..., \mathsf{User}_n\}$ be a set of users. A *t-communication structure* $\mathcal{C}_t$ is a subset of $\mathcal{U}^t$. The communication structure contains all t-tuples of users for which the protocol has to provide a conference key. A convenient way to represent a t-communication structure is by an hypergraph H in which each vertex User_i corresponds to User_i and there is a hyperedge $(\mathsf{User}_{i_1}, ..., \mathsf{User}_{i_t})$ if and only if $(\mathsf{User}_{i_1}, ..., \mathsf{User}_{i_t}) \in \mathcal{C}_t$. We will call the hypergraph associated with a t-communications tructure the *communication hypergraph.* Definition 6.1, Protocol 3, and Theorem 6.3 can be easily extended to a key distribution scheme for any t-communication structure $\mathcal{C}_t$.

7. THE ASYMMETRIC MODEL

In this section we consider the case when two parties in a network must be considered to be of a different type (e.g., one party is a server, the other is a client). We show how this case can be considered as a particular case of the symmetric model, from the point of view of the efficiency of the result. Note that there may be security objectives also to the classification of users to different kinds; e.g., we may trust servers more than we trust users—these aspects are not considered here.

Let $\mathcal{U} = \{\mathsf{User}_1, ..., \mathsf{User}_{n+m}\}$ be a set of users. These users are divided into two sets: the set $\mathcal{A} = \{\mathsf{User}_1, ..., \mathsf{User}_n\}$ of system-servers and the set $\mathcal{B} = \{\mathsf{User}_{n+1}, ..., \mathsf{User}_{n+m}\}$ of clients. An asymmetric key distribution scheme distributes some information among system-servers and clients in such a way that any pair consisting of a client and a system-server can generate a common secure key. This is called the asymmetric KDS for n system-servers and m clients. In an asymmetric KDS a

system-server is not able to claim to be a client nor is a client able to claim to be a system-server. We say that the scheme is k-secure if any k entities (clients, system-servers, or both), pooling together their pieces, have no information on keys they should not know. When we want to distinguish between a system-server and a client we denote with A_i the information received by $\mathsf{User}_i \in \mathscr{A}$, for $i = 1, 2, ..., n$, while with B_j we denote the information received by $\mathsf{User}_j \in \mathscr{B}$, for $j = n+1$, $n+2, ..., n+m$. The maximum value that the security parameter k can take is $n+m-2$ since any adversary coalition can contain at most $n+m-2$ entities.

The asymmetric model can be viewed as a particular case of the symmetric model, since it can be represented by a communication graph G for a 2-conference key distribution scheme. In this case the graph G is a complete bipartite graph where each vertex in the graph G is an entity in the scheme, and each edge of G joins a system-server and a client. The set of vertices of G is equal to $V(G) = \mathscr{A} \cup \mathscr{B}$, the sets $\mathscr{A}$ and $\mathscr{B}$ are the parts of the complete bipartite graph. The set of edges is equal to $E(G) = \{(\mathsf{User}_i, \mathsf{User}_j) \mid \mathsf{User}_i \in \mathscr{A},\ \mathsf{User}_j \in \mathscr{B}\}$. We can apply to this case the analysis for the communication graph (see Section 6). In addition, the protocol shown in Section 6 can be used for the asymmetric case.

The next corollary gives a lower bound on the size of user's information in the asymmetric model. Its proof is very similar to the proof of Theorem 6.3, so it is omitted.

CROLLARY 7.1. *Let $\mathscr{A}$ be a set of n system-servers, let $\mathscr{B}$ be a set of m clients, and let k be an integer with $k+2 \leqslant n+m$. In any asymmetric k-secure key distribution scheme for $\mathscr{A}$ and $\mathscr{B}$, the entropy $H(A_i)$ satisfies*

$$H(A_i) \geqslant \mu \cdot H(S),$$

where $\mu = \min\{m, k+1\}$, while the entropy $H(B_i)$ satisfies

$$H(B_i) \geqslant \eta \cdot H(S), \qquad \text{where} \quad \eta = \min\{n, k+1\}.$$

8. OPEN PROBLEMS

In this paper we have presented a protocol for one-round interactive KDS to establish a single conference key in which the user's information is only $t+k-1$ times the size of the common key. An open problem is whether the size of the user's information can be decreased in a one-round key distribution scheme.

Beimel and Chor [1] proposed a t-round interactive KDS in which the user's information is only $2(t+k-1)/t$ times the size of the common key. An interesting area for further research is to analyse the trade-off between round complexity and user's space requirements.

The interactive KDSs we constructed is good only for a single conference key. To construct an interactive KDS in which it is possible to establish ℓ conference keys we can simply use ℓ independent copies of an interactive KDS for a single conference. Can we do better?

APPENDIX

In this appendix we review the information theoretic concepts we used in this paper. For a complete treatment of the subject the reader is advised to consult [6].

Given a probability distribution $\{p(x)\}_{x \varepsilon X}$ on a finite set X, we define the *entropy* of X, $H(X)$, as

$$H(X) = -\sum_{x \varepsilon X} p(x) \log p(x)$$

(all logarithms in this paper are of base 2). The entropy $H(X)$ is a measure of the average information content of the elements in X or, equivalently, a measure of the average uncertainty one has about which element of the set X has been chosen when the choices of the elements from X are made according to the probability distribution $\{p(x)\}_{x \varepsilon X}$. The entropy enjoys the following property

$$0 \leqslant H(X) \leqslant \log |X|, \tag{7}$$

where $H(X) = 0$ if and only if there exists $x_0 \in X$ such that $p(x_0) = 1$; $H(X) = \log |X|$ if and only if $p(x) = 1/|X|$, $\forall x \in X$.

Given two finite sets X and Y and a joint probability distribution $\{p(x, y)\}_{x \in X,\, y \in Y}$ on their cartesian product, the *conditional entropy* $H(X|Y)$, also called the equivocation of X given Y, is defined as

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

where $p(x|y)$ is the conditional probability of x given y. The conditional entropy can be written as $H(X|Y) = \sum_{y \varepsilon Y} p(y)\, H(X|Y = y)$, where $H(X|Y = y) = -\sum_{x \varepsilon X} p(x|y) \log p(x|y)$ can be interpreted as the average uncertainty one has about which element of X has been chosen when the choices are made according to the probability distribution $\{p(x|y)\}_{x \in X}$, that is, when it is known that the value chosen from the set Y is y. From the definition of conditional entropy it is easy to see that

$$H(X|Y) \geqslant 0. \tag{8}$$

If we have $n+1$ sets $X_1, ..., X_n$, Y and a probability distribution on their cartesian product, the conditional entropy $H(X_1 X_2 \cdots X_n | Y)$ of the joint space $X_1 X_2 \cdots X_n$ given Y is defined as

$$H(X_1 X_2 \cdots X_n | Y) = H(X_1 | Y) + H(X_2 | X_1 Y) + \cdots + H(X_n | X_1 X_2 \cdots X_{n-1} Y). \tag{9}$$

The *mutual information* $I(X; Y)$ between X and Y is defined by

$$I(X; Y) = H(X) - H(X|Y) \tag{10}$$

and enjoys the properties

$$I(X;\ Y) = I(Y;\ X), \tag{11}$$

and

$$I(X;\ Y) \geqslant 0,$$

from which one gets

$$H(X) \geqslant H(X|Y), \tag{12}$$

with equality if and only if X and Y are independent. Given sets X, Y, Z and a joint probability distribution on their cartesian product, the *conditional mutual information* $I(X;\ Y|Z)$ between X and Y given Z can be written as

$$I(X;\ Y|Z) = H(X|Z) - H(X|ZY) = H(Y|Z) - H(Y|ZX). \tag{13}$$

Since the conditional mutual information $I(X;\ Y|Z)$ is always nonnegative we get

$$H(X|Z) \geqslant H(X|ZY). \tag{14}$$

Let X, Y, and Z be three random variables. If $H(Y|Z) = 0$ then from (13) and (14) it follows that

$$H(X|Z) \leqslant H(X|\ Y) \tag{15}$$

and

$$H(Z) \geqslant H(Y). \tag{16}$$

ACKNOWLEDGMENTS

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

Received July 8, 1994; final manuscript received December 4, 1997

REFERENCES

1. Beimel, A., and Chor, B. (1994), Interaction in key distribution schemes, *in* "Advances in Cryptology—CRYPTO 93" (D. R. Stinson, Ed.), Lecture Notes in Computer Science, Vol. 773, pp. 444–457, Springer-Verlag, Berlin/New York.
2. Bird, R., Gopal, I., Herzberg, A., Jansen, P., Kutten, S., Molva, R., and Yung, M. (1991), Systematic design of two-party authentication protocols, *in* "Advances in Cryptology: Proceedings of Crypto 91," Lecture Notes in Computer Science, Vol. 576, pp. 44–61, Springer-Verlag, Berlin.

3. Blom, R. (1984), An optimal class of symmetric key generation systems, *in* "Advances in Cryptology: Proceedings of Eurocrypt 84," Lecture Notes in Computer Science, Vol. 209, pp. 335–338, Springer-Verlag, Berlin.
4. Blundo, C., and Cresti, A. (1994), Space requirements for broadcast encryption, *in* "Advances in Cryptology—EUROCRYPT '94" (A. De Santis, Ed.), Lecture Notes in Computer Science, Springer-Verlag, Berlin.
[+] Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., and Yung, M. (1992), Perfectly secure key distribution for dynamic conferences, *in* "Advances in Cryptology—Crypto 92."
5. Brickell, E., Lee, P. J., and Yacobi, Y. (1987), Secure audio conferencing, *in* "Advances in Cryptology: Proceedings of Crypto 87," Lecture Notes in Computer Science, Vol. 239, pp. 418–426, Springer-Verlag, Berlin.
6. Cover, T. M., and Thomas, J. A. (1991), "Elements of Information Theory," Wiley, New York.
7. Diffie, W., and Hellman, M. E. (1976), New direction in cryptography, *IEEE Trans. Inform. Theory* **22**(6), 644–654.
8. Fiat, A., and Naor, M. (1994), Broadcast encryption, *in* "Advances in Cryptology—CRYPTO 93" (D. R. Stinson, Ed.), Lecture Notes in Computer Science, Vol. 773, pp. 480–491, Springer-Verlag, Berlin.
9. Fischer, M. J., and Wright, R. N. (1991), Multiparty secret key exchange using a random deal of cards, *in* "Advances in Cryptology: Proceedings of Crypto 91," Lecture Notes in Computer Science, Vol. 576, pp. 141–155, Springer-Verlag, Berlin.
10. Fumy, W., and Munzert, M. (1990), A modular approach to key distribution, *in* "Advances in Cryptology: Proceedings of Crypto 90," Lecture Notes in Computer Science, Vol. 537, pp. 274–283, Springer-Verlag, Berlin.
11. Gong, L., and Wheeler, D. J. (1990), A matrix-key distribution scheme, *J. Cryptology* **2**, 51–59.
12. Impagliazzo, R., and Rudich, S. (1989), Limits on the provable consequences of one-way permutations, *in* "Proceedings, 21st STOC," pp. 44–61.
13. Ingemarsson, I., Wang, D. T., and Wong, C. K. (1978), A conference key distribution system, *IEEE Trans. Inform. Theory* **28**(5), pp. 714–720.
14. Koyama, K., and Ohta, K. (1987), Identity-based conference key distribution, *in* "Advances in Cryptology: Proceedings of Crypto 87," Lecture Notes in Computer Science, Vol. 239, pp. 175–184, Springer-Verlag, Berlin.
15. Leighton, T., and Micali, S. (1994), Sectret-key agreement without public-key cryptography, *in* "Advances in Cryptology—CRYPTO 93" (D. R. Stinson, Ed.), Lecture Notes in Computer Science, Vol. 773, pp. 456–479, Springer-Verlag, Berlin.
16. MacWilliams, F. J., and Sloane, N. J. A. (1988), "The Theory of Error Correcting Codes," North-Holland, New York.
17. Matsumoto, T., and Imai, H. (1987), On the key predistribution system: A practical solution to the key distribution problem, *in* "Advances in Cryptology: Proceedings of Crypto 87," Lecture Notes in Computer Science, Vol. 239, pp. 185–193, Springer-Verlag, Berlin.
18. McCurley, K. S. (1988), A key distribution system equivalent to factoring, *J. Cryptology* **1**, 95–105.
19. Maurer, U., and Yacobi, Y. (1991), Non-interactive public-key cryptography, *in* "Advances in Cryptology: Proceedings of Eurocrypt 91," Lecture Notes in Computer Science, Vol. 547, pp. 498–507, Springer-Verlag, Berlin.
20. Merkle, R. C. (1978), Secure communication over insecure channels, *Commun. Assoc. Comput. Mach.* **21**, 294–299.
21. Needham, R. M., and Schroeder, M. D. (1978), Using encryption for authentication in large networks of computers, *Commun. Assoc. Comput. Mach.* **21**, 993–999.
22. Okamoto, E., and Tanaka, K. (1989), Key distribution system based on identification information, *IEEE J. Selected Areas Commun.* **7**(4), 481–485.

23. Shamir, A. (1984), Identity-based cryptosystems and signature scheme, "Proceedings of Crypto 84," pp. 47–53.
24. Steer, D. G., Strawczynsji, L., Diffie, W., and Wiener, M. (1990), A secure audio teleconferencing system, *in* "Advances in Cryptology: Proceedings of Crypto 89," Lecture Notes in Computer Science, Vol. 403, pp. 518–528, Springer-Verlag, Berlin.
25. Tsujii, S., and Chao, J. (1991), A new ID-based key sharing scheme, *in* "Advances in Cryptology: Proceedings of Crypto 91," Lecture Notes in Computer Science, Vol. 576, pp. 288–299, Springer-Verlag, Berlin.
26. Yacobi, Y. (1990), A key distribution paradox, *in* "Advances in Cryptology: Proceedings of Crypto 90," Lecture Notes in Computer Science, Vol. 537, pp. 268–273, Springer-Verlag, Berlin.
27. Yacobi, Y., and Shmuely, Z. (1989), On key distribution systems, *in* "Advances in Cryptology: Proceedings of Crypto 89," Lecture Notes in Computer Science, Vol. 435, pp. 344–355, Springer-Verlag, Berlin.