On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption

D. R. Stinson*
Department of Computer Science and Engineering
University of Nebraska-Lincoln
Lincoln NE 68588, USA
stinson@bibd.unl.edu
http://bibd.unl.edu/~stinson/

November 21, 1996

Abstract

This paper provides an exposition of methods by which a trusted authority can distribute keys and/or broadcast a message over a network, so that each member of a privileged subset of users can compute a specified key or decrypt the broadcast message. Moreover, this is done in such a way that no coalition is able to recover any information on a key or broadcast message they are not supposed to know. The problems are studied using the tools of information theory, so the security provided is unconditional (i.e., not based on any computational assumption).

We begin by surveying some useful schemes schemes for key distribution that have been presented in the literature, giving background and examples (but not too many proofs). In particular, we look more closely at the attractive concept of key distribution patterns, and present a new method for making these schemes more efficient through the use of resilient functions. Then we present a general approach to the construction of broadcast schemes that combines key predistribution schemes with secret sharing schemes. We discuss the Fiat-Naor Broadcast Scheme, as well as other, new schemes that can be constructing using this approach.

*the author's research is supported by NSF grant CCR-9402141

1 Introduction

Key distribution is one of the major problems in communication and network security. From the point of view of security, most networks can be thought of as broadcast networks, in that anyone connected to the network will have access to all the information that flows through it. This leads to many problems related to the confidentiality and authenticity of information that is transmitted through the network. Encryption is often employed in a network to protect the confidentiality of information. If a conventional private-key cryptosystem, such as DES, is used, then it is necessary to distribute keys to the network users in a secure fashion. Usually, this is done by an on-line key server. (For an overview of key distribution techniques see [39].)

In this paper, we investigate two related problems: key predistribution and broadcast encryption. Key predistribution refers to methods whereby a *trusted authority* (TA) will distribute secret information in such a way that specified privileged subsets of participants will be able to compute certain keys. Broadcast encryption consists of a key predistribution phase, followed at some later time by a broadcast message which is to be decrypted by a specified privileged subset of participants. The decrypted message may be a session (conference) key, for use by the privileged subset, or it may be intended for some other purpose. Such an approach is desirable because the broadcast model provides a realistic model from the standpoint of security since we do not need to assume the existence of secure private channels for on-line key distribution.

In this paper, we look at protocols that provide unconditional security (i.e., they are not based on any computational assumption). In such a scheme, it is desirable to minimize the amount of secret information that needs to be stored by each user. As well, in the case of a broadcast scheme, we would like to minimize the size of the broadcast. These aspects of a scheme are measured by *information rates.* The investigation comprises two goals: establish lower bounds on the information rate (by giving explicit constructions); and establish upper bounds (usually accomplished by entropy arguments).

We confine our attention here almost exclusively to constructions. We begin by surveying some useful schemes schemes for key distribution that have been presented in the literature. In particular, we look more closely at the attractive concept of key distribution patterns, and present a new method for making these schemes more efficient through the use of resilient functions. Then we present a general approach to the construction of broadcast schemes that combines key predistribution schemes with secret sharing schemes. We discuss the Fiat-Naor Broadcast Scheme, as well as other, new schemes that can be constructing using this approach.

2 Key Predistribution

2.1 Definitions

Our model for key distribution and broadcast encryption consists of a trusted authority (TA) and a set of users $\mathcal{U} = \{1, 2, \ldots, n\}$. We assume that the network is a *broadcast channel*, i.e., it is insecure, and any information transmitted by the TA will be received by every user.

In a key pre-distribution scheme, the TA generates and distributes secret information to each user. The information given to user i is denoted by u_i and must be distributed "off-band" (i.e., not using the network) in a secure manner. This secret information will enable various *privileged subsets* to compute keys.

Let $2^{\mathcal{U}}$ denote the set of all subsets of users. $\mathcal{P} \subseteq 2^{\mathcal{U}}$ will denote the collection of all privileged subsets to which the TA is distributing keys. $\mathcal{F} \subseteq 2^{\mathcal{U}}$ will denote the collection of all possible coalitions (called *forbidden subsets*) against which each key is to remain secure.

Once the secret information is distributed, each user i in a privileged set P should be able to compute the key k_P associated with P. On the other hand, no forbidden set $F \in \mathcal{F}$ disjoint from P should be able to compute any information about k_P.

For $1 \leq i \leq n$, let U_i denote the set of all possible secret values that might be distributed to user i by the TA. For any subset of users $X \subseteq \mathcal{U}$, let U_X denote the cartesian product $U_{i_1} \times \ldots \times U_{i_j}$, where $X = \{i_1, \ldots, i_j\}$ and $i_1 < \ldots < i_j$. We assume that there is a probability distribution on $U_{\mathcal{U}}$, and the TA chooses $u_{\mathcal{U}} \in U_{\mathcal{U}}$ according to this probability distribution.

We describe the desired properties mathematically using the entropy function (for an introduction to entropy and its properties, see Welsh [40]). We say that the scheme is a $(\mathcal{P}, \mathcal{F})$-**Key Predistribution Scheme** (or $(\mathcal{P}, \mathcal{F})$-KPS) provided the following conditions are satisfied:

(1) Each user i in any privileged set P can compute k_P:

$$H(K_P|U_i) = 0$$

for all $i \in P \in \mathcal{P}$.

(2) No forbidden subset F disjoint from any privileged subset P has any information on k_P:

$$H(K_P) = H(K_P|U_F)$$

for all $P \in \mathcal{P}$ and $F \in \mathcal{F}$ such that $P \cap F = \emptyset$.

Remark: Our model of a KPS is identical to what Blundo and Cresti [12] call a zero-message broadcast encryption scheme.

We now present some convenient notation. If $\mathcal{P}$ consists of all t-subsets of $\mathcal{U}$, then we will write $(t, \mathcal{F})$-KPS. Similarly, if $\mathcal{P}$ consists of all subsets of $\mathcal{U}$ of size at most t, then we will write $(\leq t, \mathcal{F})$-KPS. An analogous notation will be used for $\mathcal{F}$. Thus, for example, a $(\leq n, 1)$-KPS is a KPS where there is a key associated with any subset of users (i.e., $\mathcal{P} = 2^{\mathcal{U}}$) and no key K_P can be computed by any individual user $i \notin P$.

Note that in any $(\mathcal{P}, \mathcal{F})$-KPS, if $F \in \mathcal{F}$ and $F' \subseteq F$, then $F' \in \mathcal{F}$. Hence, a $(\mathcal{P}, w)$-KPS is the same thing as a $(\mathcal{P}, \leq w)$-KPS.

We will assume that each $k_P \in K$, where $K = GF(q)$ is our key set. Usually, a key k_P is equally likely to be any element of $GF(q)$, in which case $H(K_P) = \log q$ for all $P \in \mathcal{P}$.

We are interested in the efficiency of a KPS, as measured by the amount of secret information that is distributed to each user. The *information rate* of a KPS is thus defined to be

$$\rho = \min \left\{ \frac{\log q}{H(U_i)} : 1 \leq i \leq n \right\}.$$

We might also be interested in the total amount of information distributed to all the users. Hence, we define the *total information rate* of a KPS to be

$$\rho_T = \frac{\log q}{H(U_{\mathcal{U}})}.$$

Remark: The total information rate is the reciprocal of the randomness coefficient, as defined in [14].

The first paper discussing unconditionally secure KPS of the type we are studying in this paper is Blom [11]. Other papers on this topic include [12, 13, 14, 21, 15, 25, 29, 30, 31, 32, 34, 35, 36].

2.2 Constructions

Theorem 2.1 (Trivial Scheme) *For any $t \geq 1$, there is a $(t, \leq n)$-KPS having information rate*

$$\frac{1}{\binom{n-1}{t-1}}$$

and total information rate

$$\frac{1}{\binom{n}{t}}.$$

Proof. For every t-subset $P \subseteq \mathcal{U}$, the TA chooses a random value $k_P \in GF(q)$ and gives k_P to every member of P. □

Theorem 2.2 (Blom Scheme) *[11] For any $w \geq 1$, there is a $(2, \leq w)$-KPS having information rate*

$$\frac{1}{w+1}$$

and total information rate

$$\frac{1}{\binom{w+2}{2}}.$$

Proof. Let $q \geq n$ be a prime power. The TA chooses n distinct random numbers $s_i \in GF(q)$, and gives s_i to user i $(1 \leq i \leq n)$. These values do not need to be secret. Then, the TA constructs a random polynomial

$$f(x, y) = \sum_{i=0}^{w} \sum_{j=0}^{w} a_{ij} x^i y^j$$

having coefficients in $GF(q)$, such that $a_{ij} = a_{ji}$ for all i, j. For $1 \leq i \leq n$, the TA computes the polynomial

$$g_i(x) = f(x, s_i) = \sum_{j=0}^{w} b_{ij} x^j,$$

and gives the $w + 1$ values b_{ij} to user i (note: these values comprise the secret information u_i).

The key associated with the pair of users $P = \{i, j\}$ is

$$k_P = g_i(s_j) = g_j(s_i).$$

□

Remark: The original presentation of the Blom scheme was given in the setting of MDS (maximum distance separable) codes. We have used the formulation from [13] here.

Here is a small example to illustrate. Suppose we take $n = 3$, $q = 17$ and $w = 1$, and the public values are $s_1 = 12$, $s_2 = 7$ and $s_3 = 1$. Now, suppose that the TA chooses the polynomial

$$f(x,y) = 8 + 7(x+y) + 2xy.$$

This gives rise to the polynomials

$$\begin{aligned} g_1(x) &= 7 + 14x \\ g_2(x) &= 6 + 4x \\ g_3(x) &= 15 + 9x. \end{aligned}$$

Thus the secret information distributed to the three users is

$$\begin{aligned} u_1(x) &= (7, 14) \\ u_2(x) &= (6, 4) \\ u_3(x) &= (15, 9). \end{aligned}$$

The three keys determined by this information are

$$\begin{aligned} k_{\{1,2\}} &= 3 \\ k_{\{1,3\}} &= 4 \\ k_{\{2,3\}} &= 10. \end{aligned}$$

Theorem 2.3 (Blundo *et al* **Scheme)** *[13] For any $t \geq 2$, $w \geq 1$, there is a $(t, \leq w)$-KPS having information rate*

$$\frac{1}{\binom{t+w-1}{t-1}}$$

and total information rate

$$\frac{1}{\binom{t+w}{t}}.$$

Proof. The scheme is similar to Blom's scheme, but the TA uses a symmetric polynomial $f(x_1, \ldots, x_t)$ in t variables. □

Remark: When we set $t = 2$ in the Blundo *et al* scheme, the Blom scheme is obtained.

Theorem 2.4 (Fiat-Naor Scheme) *[22] For any $w \geq 1$, there exists a $(\leq n, \leq w)$-KPS having information rate*

$$\frac{1}{\sum_{j=0}^{w} \binom{n-1}{j}}$$

and total information rate

$$\frac{1}{\sum_{j=0}^{w} \binom{n}{j}}.$$

Proof. For every subset $F \subseteq \mathcal{U}$ of cardinality at most w, the TA chooses a random value $s_F \in GF(q)$ and gives s_F to every member of $\mathcal{U} \backslash F$. Then the key associated with a privileged set P is defined to be

$$k_P = \sum_{\{F \in \mathcal{F} : F \cap P = \emptyset\}} s_F.$$

□

Here is a small example to illustrate. Suppose we take $n = 3$, $q = 17$ and $w = 1$, and suppose that the TA chooses the values

$$\begin{aligned} s_\emptyset &= 11 \\ s_{\{1\}} &= 8 \\ s_{\{2\}} &= 3 \\ s_{\{3\}} &= 8. \end{aligned}$$

The eight keys determined by this information are

$$\begin{aligned} k_\emptyset &= 13 \\ k_{\{1\}} &= 5 \\ k_{\{2\}} &= 10 \\ k_{\{3\}} &= 5 \\ k_{\{1,2\}} &= 2 \\ k_{\{1,3\}} &= 14 \\ k_{\{2,3\}} &= 2 \\ k_{\{1,2,3\}} &= 11. \end{aligned}$$

Remark: The information rates of all four of the above schemes are optimal; see [12] for details, for example.

3 Key Distribution Patterns

The elegant idea of a key distribution pattern is due to Mitchell and Piper [34]. Many other papers also use this concept (or variations of it); see, for example, [21, 25, 31, 29, 30, 32]. However, the work of Mitchell and Piper does not seem to be as well-known as it should be.

We begin with a definition, which is essentially the dual formulation of the one given in [34]. Let $\mathcal{B} = \{B_1, \ldots, B_\beta\}$ be a set of subsets of $\mathcal{U}$. We say that $(\mathcal{U}, \mathcal{B})$ is a $(\mathcal{P}, \mathcal{F})$-**Key Distribution Pattern** (or $(\mathcal{P}, \mathcal{F})$-KDP) if

$$\{B_j : P \subseteq B_j \text{ and } F \cap B_j = \emptyset\} \neq \emptyset$$

for all $P \in \mathcal{P}$ and $F \in \mathcal{F}$ such that $P \cap F = \emptyset$.

Note that a KDP can conveniently be represented by an $n \times \beta$ *incidence matrix* $A = (a_{i,j})$ which is defined as follows:

$$a_{i,j} = \begin{cases} 1 & \text{if } i \in B_j \\ 0 & \text{otherwise.} \end{cases}$$

The KDP $(\mathcal{U}, \mathcal{B})$ (or, equivalently, the incidence matrix A) is public knowledge. A KDP can be used to construct a KPS as described in the following theorem, where we define

$$r_i = |\{B_j : i \in B_j\}|$$

for any user $i \in \mathcal{U}$.

Theorem 3.1 *Suppose $(\mathcal{U}, \mathcal{B})$ is a $(\mathcal{P}, \mathcal{F})$-KDP. Then there exists a $(\mathcal{P}, \mathcal{F})$-KPS with information rate*

$$\frac{1}{\max\{r_i : 1 \leq i \leq n\}}$$

and total information rate

$$\frac{1}{\beta}.$$

Proof. For $1 \leq j \leq \beta$, the TA chooses a random value $s_j \in GF(q)$ and gives s_j to every user in B_j. Thus user i receives r_i elements of $GF(q)$ as his or her secret information.

The key k_P for a privileged set P is defined to be

$$k_P = \sum_{\{j:P \subseteq B_j\}} s_j.$$

Note that each member of P can compute k_P. However, if F is a coalition such that $F \cap P = \emptyset$, then there is at least one block B_j such that $P \subseteq B_j$ and $F \cap B_j = \emptyset$. F does not know the value of s_j, and hence has no information about k_P. □

Remark: The trivial KPS and the Fiat-Naor KPS are both in fact KDPs. The trivial KPS is obtained by taking $\mathcal{B}$ to be all t-subsets of $\mathcal{U}$, and the Fiat-Naor KPS is produced by taking $\mathcal{B}$ to be all subsets of $\mathcal{U}$ of cardinality at least $n - w$.

We now give a construction for KDPs that uses combinatorial designs (for results on design theory, see Beth, Jungnickel and Lenz [8]). First, we require a definition. Let Y be a set of v elements (called *points*), and let $\mathcal{A} = \{A_1, \ldots, A_\beta\}$ be a family of k-subsets of Y (called *blocks*). We say that $(Y, \mathcal{A})$ is a t-(v, k, λ) *design* if every subset of t points occurs in exactly λ blocks. It can be shown by elementary counting that a t-(v, k, λ) design is also a t'-(v, k, λ') design for $1 \leq t' \leq t$, where

$$\lambda' = \frac{\lambda\binom{v-t'}{t-t'}}{\binom{k-t'}{t-t'}}.$$

The following result was shown in [34], and a similar result was proved subsequently and independently in [31].

Theorem 3.2 *A 3-(n, k, λ) design, $(\mathcal{U}, \mathcal{B})$, is a $(2, \leq w)$-KDP on a set of n users if*

$$w < \frac{n-2}{k-2}.$$

This KDP has information rate

$$\frac{(k-1)(k-2)}{\lambda(v-1)(v-2)}$$

and total information rate

$$\frac{k(k-1)(k-2)}{\lambda v(v-1)(v-2)}.$$

Proof. Consider two users, i and j. There are exactly

$$\frac{\lambda(n-2)}{k-2}$$

blocks of the design that contain i and j. Now, consider a coalition $F = \{h_1, \ldots, h_w\}$ such that $F \cap \{i, j\} = \emptyset$. For $1 \leq k \leq w$, there are at most λ blocks of the design that contain i, j and h_k. Hence, the number of blocks that contain i, j and at least one member of F is at most λw. Since

$$\lambda w < \frac{\lambda(n-2)}{k-2},$$

the design is a $(2, \leq w)$-KDP. □

Suppose we use inversive planes, as was done in [34]. An *inversive plane* is a 3-$(Q^2+1, Q+1, 1)$ design. Such a design is known to exist whenever Q is a prime power. Applying Theorem 3.2, the following theorem is obtained.

Theorem 3.3 *[34] Suppose Q is a prime power. Then there exists a a $(2, \leq Q)$-KDP with information rate*

$$\frac{1}{Q(Q+1)}$$

and total information rate

$$\frac{1}{Q(Q^2+1)}.$$

As an example, if we take $Q = 3$, then we use a 3-$(10, 4, 1)$ design. The resulting KDP is a $(2, \leq 3)$-KDP with information rate 1/12 and total information rate 1/30.

Theorem 3.2 can be generalized in a straightforward manner to construct $(t, \leq w)$-KDPs with $t \geq 3$. We state the following theorem without proof.

Theorem 3.4 *A $(t+1)$-(n, k, λ) design, $(\mathcal{U}, \mathcal{B})$, is a $(t, \leq w)$-KDP on a set of n users if*

$$w < \frac{n-t}{k-t}.$$

This KDP has information rate

$$\frac{\binom{k-1}{t-1}}{\lambda\binom{v-1}{t-1}}$$

and total information rate

$$\frac{\binom{k}{t}}{\lambda\binom{v}{t}}.$$

We give a small example to illustrate. It is known that there exists a 5-$(12, 6, 1)$ design. Applying Theorem 3.4, we obtain a $(4, \leq 3)$-KPS with information rate $1/66$ and total information rate $1/132$.

3.1 An Efficiency Improvement using Resilient Functions

The idea of a key distribution pattern is very appealing, and there is no computation required on the part of the TA. However, most known examples of KDP have quite low information rates. (The constructions in [21] have very good information rates. However, these constructions are probabilistic, and thus it is still of interest to find good explicit constructions.)

In this section, we present a new technique that will lead to an improvement in the information rate of KDP. This method also allows for trading off the amount of security (i.e., the value of w) against the amount of key computed by a priviliged set.

Suppose we have a $(\mathcal{P}, \mathcal{F})$-KDP, and the members of a privileged set P want to compute a key k_P. Define

$$C_P = |\{B_j : P \subseteq B_j\}|$$

and

$$D_P = \max\{|\{B_j : P \subseteq B_j \text{ and } F \cap B_j \neq \emptyset\}| : F \in \mathcal{F}, F \cap P = \emptyset\}.$$

Each member of P has C_P secret values, of which no forbidden set knows more than D_P. The definition of KDP assures that $D_P \leq C_P - 1$. If it happens that $D_P < C_P - 1$, then it may be possible for P to extract more key from the secret values they hold, by making use of so-called resilient functions.

An (n, m, t, q)-*resilient function* is a function

$$f : [GF(q)]^n \rightarrow [GF(q)]^m$$

which satisfies the property that if the values of t of the n inputs are fixed, and the remaining $n-t$ inputs are chosen independently at random, then every possible output m-tuple is equally likely to occur. Considerable research has been done on resilient functions (see for example, [20, 6, 24, 9, 10, 27]). Most work has concentrated on binary resilient functions (i.e., the case $q = 2$). Here we will be using resilient functions with large q; one paper dealing with the subject is [27].

We can use a publicly known resilient function to improve the efficiency of a KDP in a straightforward manner, as follows.

Theorem 3.5 *Suppose $(\mathcal{U}, \mathcal{B})$ is a $(\mathcal{P}, \mathcal{F})$-KDP and $P \in \mathcal{P}$. Let m and q be integers. Suppose for every $P \in \mathcal{P}$ that there there exists a (C_P, m, D_P, q)-resilient function. Then there exists a $(\mathcal{P}, \mathcal{F})$-KPS having information rate*

$$\frac{m}{\max\{r_i : 1 \leq i \leq n\}}$$

and total information rate m/β.

Proof. The proof is similar to that of Theorem 3.1. For $1 \leq j \leq \beta$, the TA chooses a random value $s_j \in GF(q)$ and gives s_j to every user in B_j. The key $k_P \in [GF(q)]^m$ for a privileged set P is defined to be

$$k_P = f(s_{j_1}, \ldots s_{j_{C_P}}),$$

where

$$\{j : P \subseteq B_j\} = \{j_1, \ldots, j_{C_P}\}$$

and

$$j_1 < \ldots < j_{C_P}.$$

Each member of P can compute k_P since the C_P inputs to the function f are known. However, if F is a coalition such that $F \cap P = \emptyset$, then there are at least $C_P - D_P$ inputs to f that are not known to F. Since f is D_P-resilient, F has no information about k_P. □

Remarks:

1. Theorem 3.1 is in fact a special case of Theorem 3.5. This follows easily from the observation that the function

   $$f : [GF(q)]^n \rightarrow GF(q),$$

   defined as

   $$f(x_1, \ldots, x_n) = x_1 + \ldots + x_n,$$

   is an $(n, 1, n-1, q)$-resilient function.

2. The information rates in Theorem 3.5 have been increased by a factor of m over Theorem 3.1.

In an application of Theorem 3.5, we want an (n, m, t, q)-resilient function where m is as large as possible, given n and t. It can be shown that $m \leq n - t$ in any resilient function. However, it is easy to construct $(n, n-t, t, q)$-resilient functions provided $q \geq n - 1$.

We describe a construction from [26, p. 129] that uses doubly extended Reed-Solomon codes. Let q be a prime power, and let α be a primitive element in $GF(q)$. The doubly extended Reed-Solomon code of dimension k is the code defined over $GF(q)$ having generating matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 0 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} & 0 & 0 \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(q-2)2} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{k-2} & \alpha^{2(k-2)} & \cdots & \alpha^{(q-2)(k-2)} & 0 & 0 \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{(q-2)(k-1)} & 0 & 1 \end{pmatrix}$$

This code is a $[q+1, k, q-k+2]$ q-ary code. The first $n \leq q+1$ columns of G form the generating matrix G_0 of a $[n, k, n-k+1]$ q-ary code. The function $f : [GF(q)]^n \rightarrow [GF(q)]^k$ defined as $f(x) = x(G_0)^T$ is in fact a $(n, k, n-k, q)$-resilient function.

Now, let us illustrate this approach by using the inversive plane KDP described in Theorem 3.3. So we suppose that Q is a prime power, and $w \leq Q$ is fixed. Then it is easy to calculate $C_P = Q + 1$ and $D_P = w$. If we take $q \geq Q$, then there exists a $(Q+1, Q+1-w, w, q)$-resilient function by the discussion above. Applying Theorem 3.5, we have the following result.

Theorem 3.6 *Suppose Q is a prime power and $w \leq Q$. Then there exists a $(2, \leq w)$-KPS having information rate*

$$\frac{Q+1-w}{Q(Q+1)}$$

and total information rate

$$\frac{Q+1-w}{Q(Q^2+1)}.$$

Remark: Note that the value of w does not have to be fixed ahead of time. At the time that a privileged set P actually wants to compute their common key k_P, they can decide on the value of w they wish to use. The key k_P is an element of $(GF(q))^{Q+1-w}$, so they are trading off security (the value of w) against the amount of the key they produce.

As an example, suppose we apply Theorem 3.6 with $Q = 3$. The following 30 blocks of a 3-$(10, 4, 1)$ design comprise the KDP:

$$\begin{array}{lll}
B_1 = \{1,2,3,4\}, & B_2 = \{1,5,6,7\}, & B_3 = \{2,5,8,9\} \\
B_4 = \{3,6,8,10\}, & B_5 = \{4,7,9,10\}, & B_6 = \{6,7,8,9\} \\
B_7 = \{3,4,8,9\}, & B_8 = \{3,4,6,7\}, & B_9 = \{2,4,5,7\} \\
B_{10} = \{2,3,5,6\}, & B_{11} = \{5,7,8,10\}, & B_{12} = \{2,4,8,10\} \\
B_{13} = \{1,4,6,10\}, & B_{14} = \{1,4,5,9\}, & B_{15} = \{1,3,5,8\} \\
B_{16} = \{5,6,9,10\}, & B_{17} = \{2,3,9,10\}, & B_{18} = \{1,3,7,10\} \\
B_{19} = \{1,2,7,9\}, & B_{20} = \{1,2,6,8\}, & B_{21} = \{1,8,9,10\} \\
B_{22} = \{2,6,7,10\}, & B_{23} = \{3,5,7,9\}, & B_{24} = \{4,5,6,8\} \\
B_{25} = \{3,4,5,10\}, & B_{26} = \{2,4,6,9\}, & B_{27} = \{2,3,7,8\} \\
B_{28} = \{1,4,7,8\}, & B_{29} = \{1,3,6,9\}, & B_{30} = \{1,2,5,10\}.
\end{array}$$

Suppose that the scheme is implemented over $GF(13)$, so the TA distributes secret values $s_1, \dots, s_{30} \in GF(13)$ according to this set of blocks. Now, suppose that a privileged set P wishes to compute a key that will be secure against a coalition of size $w = 2$. The resulting $(2, \leq 2)$-KPS has information rate $1/6$ and total information rate $1/15$.

Here is how the key computation could be carried out. Suppose that $P = \{4, 7\}$. Users 4 and 7 both know the values s_5, s_8, s_9, s_{28}. These four values will be the inputs to a $(4, 2, 2, 13)$-resilient function. One such resilient function f, is defined as follows:

$$f(x_1, x_2, x_3, x_4) = (x_1 + x_2 + x_3 + x_4, x_1 + 2x_2 + 4x_3 + 8x_4),$$

where arithmetic is done in $GF(13)$. (This function is obtained by taking $\alpha = 2$ and constructing a $[4, 2, 3]$ code over $GF(13)$ from a Reed-Solomon code, as described above.) If it happened that $s_5 = 10$, $s_8 = 4$, $s_9 = 10$ and $s_{28} = 1$, then the key k_P would be

$$k_P = (10 + 4 + 10 + 1 \bmod 13, 10 + 8 + 40 + 8 \bmod 13) = (12, 1).$$

Let's look at this scheme from the point of view of the coalition $\{3, 8\}$. User 3 knows that $s_8 = 4$ and user 8 knows that $s_{28} = 1$. However, neither of them know the values of s_5 or s_9, and thus they have no information as to the value of the key k_P.

4 One-time Broadcast Encryption

4.1 Definitions

We will use much of the notation from Section 2.1. As before, we have a trusted authority (TA) and a set of users. We assume that network is a *broadcast channel*, i.e., it is insecure, and any information transmitted by the TA will be received by every user.

In a set-up stage, the TA generates and distributes secret information u_i to each user i off-band. At a later time, the TA will want to broadcast a message to a privileged subset P. The particular privileged subset P is, in general, not known ahead of time.

For $1 \leq i \leq n$, let M_i denote the set of possible messages that might be broadcast to user i. In the schemes we discuss, we will assume that all the sets $M_1, \ldots, M_n$ are the same, so $M_1 = \ldots = M_n = M$, say, where $|M| = q$.

$\mathcal{P} \subseteq 2^{\mathcal{U}}$ will denote the collection of all privileged subsets to which the TA might want to broadcast a message. $\mathcal{F} \subseteq 2^{\mathcal{U}}$ will denote the collection of all possible coalitions (forbidden subsets) against which a broadcast is to remain secure.

Now, suppose that the TA wants to broadcast a message to a given privileged set $P \in \mathcal{P}$ at a later time. (The particular privileged set P is not known when the scheme is set up, except for the restriction that $P \in \mathcal{P}$.) We assume that there is a probability distribution on M, and the TA chooses a *message* (i.e., a plaintext) $m_P \in M$ according to this probability distribution. Then the *broadcast* b_P (which is an element of a specified set B_P) is computed as a function of m_P and u_P.

Once b_P is broadcast, each user $i \in P$ should be able to decrypt b_P and obtain m_P. On the other hand, no forbidden set $F \in \mathcal{F}$ disjoint from P should be able to compute any information about m_P.

We discuss the security in terms of a single broadcast, so we call the scheme "one-time". We say that the scheme is a $(\mathcal{P}, \mathcal{F})$**-One-Time Broadcast Encryption Scheme** (or $(\mathcal{P}, \mathcal{F})$-OTBES) provided the following conditions are satisfied:

(0) Without knowing the broadcast, no subset of users has any information about m_P, even given all the secret information $U_{\mathcal{U}}$:

$$H(M_P|U_{\mathcal{U}}) = H(M_P)$$

for all $P \in \mathcal{P}$.

(1) The message for a privileged user is uniquely determined by the broadcast and the user's secret information:

$$H(M_P|U_iB_P) = 0$$

for all $i \in P \in \mathcal{P}$.

(2) After receiving the broadcast, no forbidden subset F disjoint from P has any information on m_P:

$$H(M_P) = H(M_P|U_FB_P)$$

for all $P \in \mathcal{P}$ and $F \in \mathcal{F}$ such that $P \cap F = \emptyset$.

The paper by Berkovitz [7] might be the first on this topic. Other relevant papers include [12, 15, 16, 22, 28].

Remarks:

1. Blundo and Cresti define a slightly different model for broadcast encryption in [12]. They study schemes in which a sequence of broadcasts can be performed without a loss of security. In our model, we study the security with respect to a single broadcast. We observe that, for the various schemes we study, it is usually straightforward to determine conditions under which the schemes remain secure for more than one broadcast. However, we do not pursue this question further in this paper.

2. One practical concern with broadcasting is how the members of the privileged set P know that the broadcast is intended for them. Of course, the broadcast can contain this information explicitly, in unencrypted form. However, this might be undesirable in certain applications since it does not preserve user anonymity. Another question is whether each privileged user needs to know the identities of the other privileged users in order to decrypt the broadcast. We will not dwell on these questions in this paper, but we do note two recent papers that discuss broadcast schemes which do not require addressing and which also maintain user anonymity; namely, Just, Kranakis, Krizanc and van Oorschot [28], and Blundo, Frota Mattos and Stinson [16].

We define the *information rate* of an OTBES exactly as for a KPS:

$$\rho = \min\left\{\frac{\log q}{H(U_i)} : 1 \leq i \leq n\right\}.$$

It is also interesting to look at the size of the broadcast, as compared to the plaintext message. Thus we define the *broadcast information rate* of an OTBES to be

$$\rho_B = \min\left\{\frac{\log q}{H(B_P)} : P \in \mathcal{P}\right\}.$$

In general, there is a trade-off between the amount of secret information held by each user and the size of the broadcast, i.e., to increase ρ_B, ρ must be decreased, and vice versa. This trade-off can be analyzed by looking at the *total information rate*, which we define to be

$$\rho_T = \min\left\{\frac{\log q}{H(U_{\mathcal{U}} B_P)} : P \in \mathcal{P}\right\}.$$

5 Two Simple Constructions

The are many ways to construct OTBES. The simplest method uses a key k_P from a KPS to encrypt a message.

Theorem 5.1 *Suppose there is a $(\mathcal{P}, \mathcal{F})$-KPS having information rate σ and total information rate τ. Then there is a $(\mathcal{P}, \mathcal{F})$-OTBES having information rate σ, broadcast information rate* 1, *and total information rate $\tau/(\tau + 1)$.*

Proof. Suppose the key set for the $(\mathcal{P}, \mathcal{F})$-KPS is $GF(q)$. Then we also take $M = GF(q)$. If the TA wishes to send the message $m_P \in M$ to the privileged set $P \in \mathcal{P}$, then the broadacast is

$$b_P = k_P + m_P.$$

□

This scheme has a very small broadcast ($\rho_B = 1$). Other approaches allow less secret information to be stored by the users, at the expense of a larger broadcast.

Here is a trivial scheme at the other extreme.

Theorem 5.2 *There is an $(\leq n, \leq n)$-OTBES having information rate* 1, *broadcast information rate $1/n$, and total information rate $1/(n + 1)$.*

Proof. In the setup phase, the TA chooses a random element $u_i \in GF(q)$ and gives it to i $(1 \leq i \leq n)$. Later, the TA wishes to send the message $m_P \in GF(q)$ to the privileged set $P \in \mathcal{P}$. Then the broadcast is

$$b_P = (u_i + m_P : i \in P).$$

□

6 A Generalization of the Beimel-Chor Scheme

In this section, we review a recent construction due to Blundo, Frota Mattos and Stinson that is a modification of an interactive key distribution scheme of Beimel and Chor [3, 5].

Theorem 6.1 *[15] Suppose $t \equiv 0 \bmod \ell$, where $\ell \geq 2$ is an integer. Then there is a $(t, \leq w)$-OTBES having information rate*

$$\frac{\binom{t-1}{\ell-1}}{\binom{t+w-1}{\ell-1}},$$

broadcast information rate ℓ/t, and total information rate

$$\frac{\binom{t-1}{\ell-1}}{\binom{t+w}{\ell} + \binom{t-1}{\ell-1}}.$$

We give a brief description of the construction in the case $\ell = 2$. Initially, a $(2, t+w-2)$ Blom scheme in $GF(q)$ is set up. It can be shown (see [13, 3]) that the $\binom{t}{2}$ keys belonging to the $\binom{t}{2}$ pairs within a set P of t users are uniformly distributed random variables from the point of view of a set F of w other users. Thus these keys can be thought of as a big one-time pad which can be used to encrypt a message for broadcast.

Suppose that the privileged set $P = \{i_1, \ldots, i_t\}$. Recall that we are assuming that t is even. Hence, the complete graph K_t on vertex set P and edge set E, say, can be partitioned into one-factors (i.e., perfect matchings). (Each one-factor consists of $t/2$ disjoint edges.) For any edge $e = \{i, j\} \in E$, there is a unique one-factor containing it, and a unique key k_e determined by the Blom scheme.

Suppose that the one-factors are named $F_1, \ldots F_{t-1}$. The message to be broadcast will be a $(t-1)$-tuple $m_P = (m_1, \ldots, m_{t-1}) \in [GF(q)]^{t-1}$. Then the broadcast is

$$b_P = (m_i + k_e : e \in F_i, 1 \leq i \leq t-1).$$

Here is a very small illustrative example. Suppose $t = 4$, and $P = \{i_1, \ldots, i_4\}$. Then we have the following three one-factors:

$$\begin{aligned} F_1 &= \{\{i_1, i_2\}, \{i_3, i_4\}\} \\ F_2 &= \{\{i_1, i_3\}, \{i_2, i_4\}\} \\ F_3 &= \{\{i_1, i_4\}, \{i_2, i_3\}\}. \end{aligned}$$

In this case, the message $m_P = (m_1, m_2, m_3)$ and the broadcast is

$$\begin{aligned} b_P = \; & (m_1 + k_{\{i_1,i_2\}}, m_1 + k_{\{i_3,i_4\}}, m_2 + k_{\{i_1,i_3\}}, \\ & m_2 + k_{\{i_2,i_4\}}, m_3 + k_{\{i_1,i_4\}}, m_3 + k_{\{i_2,i_3\}}). \end{aligned}$$

For further details, proofs and discussion, see [15].

7 A General Construction using Secret Sharing Schemes

In the remainder of this paper, we present a general approach which can be used to construct a broadcast encryption scheme by combining several key predistribution schemes with an ideal secret sharing scheme. Then we will give some applications of this approach.

First, we need to give some definitions and results relating to secret sharing schemes. This is done in the next subsection.

7.1 Secret Sharing Schemes

Let X be a set of n users, and let $\Gamma \subseteq 2^X$ be a set of subsets called *authorized* subsets. In a secret sharing scheme, the TA has one secret value $k \in GF(q)$, called the *key*. The TA will distribute secret information to each user in X, in such a way that any authorized subset can compute k from the shares they jointly hold, but no unauthorized subset has any information about k. The secret information given to user i will be denoted u_i and will be called the *share* of user i.

The two properties of a secret sharing scheme are most easily described using entropy notation. (In the following, the variables U_P and U_F represent the shares held by the sets P and F, respectively, and could be defined formally as in the case of KPS.)

(1) Any authorized subset P can compute k:

$$H(K|U_P) = 0$$

for all $P \in \Gamma$.

(2) No unauthorized subset F has any information on k:

$$H(K) = H(K|U_F)$$

for all $F \not\in \Gamma$.

It is clear that a secret sharing scheme can exist only if Γ is *monotone*; i.e., if $A \in \Gamma$ and $A \subseteq A_0$, then $A_0 \in \Gamma$. Since Γ is monotone, it is determined uniquely given the *basis*, Γ_0, which consists of the minimal subsets of Γ.

If the share given to each user is an element of $GF(q)$, then the scheme is said to be *ideal*. We will denote an ideal secret sharing scheme for an access structure Γ by the abbreviation Γ-ISSS.

There are many classes of access structures Γ for which Γ-ISSS are known to exist. Among these are the so-called threshold access structures. An *(m, n)-threshold access structure*, $\Gamma_{m,n}$, has as its basis all the m-subsets of an n-set. The well-known Shamir threshold scheme [37] is one way to obtain a $\Gamma_{m,n}$-ISSS. Many other classes of ideal schemes have been constructed; see, for example, [17, 18, 4].

We give a short description of the Shamir threshold scheme, since we will be using it later. Let $q \geq n + 1$ be a prime power. Initially, the TA chooses n distinct non-zero random numbers $x_i \in GF(q)$, and gives x_i to user i $(1 \leq i \leq n)$. These values do not need to be secret. Then, the TA the constructs a random polynomial of degree at most $t - 1$

$$f(x) = \sum_{i=0}^{t-1} a_i x^i,$$

having coefficients in $GF(q)$. The key is the constant term, a_0. For $1 \leq i \leq n$, the TA computes the polynomial

$$y_i = f(x_i)$$

and gives y_i to user i (note: the value y_i is the share of user i).

At a later time, if t users pool their information, then they have t pairs (x_i, y_i) on the unknown polynomial f. They can determine f by Lagrange interpolation, for example, and then extract the constant term, which is the key. On the other hand, no $t-1$ users have any information as to the value of the key.

Here is a small example to illustrate. Suppose we wish to construct a $\Gamma_{3,5}$-ISSS in $GF(17)$, and the public values are $x_i = i$, $1 \le i \le 5$. Suppose that the TA chooses the polynomial

$$f(x) = 13 + 10x + 2x^2,$$

so the key is 13. The shares that are distributed are

$$\begin{aligned} y_1 &= 8 \\ y_2 &= 7 \\ y_3 &= 10 \\ y_4 &= 0 \\ y_5 &= 11. \end{aligned}$$

Any three of the ordered pairs $(1,8)$, $(2,7)$, $(3,10)$, $(4,0)$ and $(5,11)$ can be used to reconstruct the polynomial f.

For more information on secret sharing schemes, the reader is referred to [38, 39].

7.2 The KIO Construction

We now describe our general construction, which for lack of a better acronym, we call the *KIO construction*, (since it uses **K**PS together with **I**SSS to construct **O**TBES).

Suppose that $\mathcal{B} = \{B_1, \ldots, B_\beta\}$ is a family of subsets of $\mathcal{U}$. $\mathcal{B}$ is public knowledge, as in the case of a KDP. Let $\theta \ge 0$ be an integer. For each B_j, $1 \le j \le \beta$, suppose a Fiat-Naor $(\le |B_j|, \le \theta)$-KPS is constructed with respect to user set B_j. The secret values associated with the jth scheme will be denoted s_{jC}, $C \subseteq B_j$, $|C| \le \theta$. (The value s_{jC} is given to every user in $B_j \backslash C$.)

Next, suppose that $\Gamma \subseteq 2^{\mathcal{B}}$, and there exists a Γ-ISSS (defined on $\mathcal{B}$ and having key set $GF(q)$). Let $\mathcal{F} \subseteq 2^{\mathcal{U}}$, and suppose that the following two properties are satisfied:

(1) $\{B_j \in \mathcal{B} : i \in B_j\} \in \Gamma$ for every $i \in \mathcal{U}$.

(2) $\{B_j \in \mathcal{B} : |F \cap B_j| \geq \theta + 1\} \notin \Gamma$ for every $F \in \mathcal{F}$.

Then we can construct a $(\leq n, \mathcal{F})$-OTBES. Let $P \subseteq \mathcal{U}$. The TA can broadcast a message $m_P \in GF(q)$ to P using the following algorithm:

1. For each $B_j \in \mathcal{B}$, the TA computes a share $y_j \in GF(q)$ corresponding to the secret m_P.
2. For each $B_j \in \mathcal{B}$, the TA computes the key k_j corresponding to the set $P \cap B_j$ in the Fiat-Naor KPS implemented on B_j:
$$k_j = \sum_{\{C \subseteq B_j : C \cap P = \emptyset, |C| \leq \theta\}} s_{jC}.$$
3. For each $B_j \in \mathcal{B}$, the TA computes
$$b_j = y_j + k_j.$$
4. The broadcast is
$$b_P = (b_j : B_j \in \mathcal{B}).$$

The basic idea of the KIO construction is very simple. First, consider a user $i \in P$. Define
$$A_i = \{j : i \in B_j\}.$$
User i can compute k_j for every $j \in A_i$. Then, for each $j \in A_i$, i can compute
$$y_j = b_j - k_j.$$
Finally, since $A_i \in \Gamma$, i can compute the message m_P from the shares y_j $(j \in A_i)$.

On the other hand, suppose $F \in \mathcal{F}$, $F \cap P = \emptyset$. Define
$$A_F = \{j : |F \cap B_j| \geq \theta + 1\}.$$
The coalition F can compute k_j, and hence y_j, for every $j \in A_F$. However, they can obtain no information about the shares y_j, $j \notin A_F$. Since $A_F \notin \Gamma$, F has no information about the value of m_P.

8 An OTBES Using Threshold Access Structures

We illustrate the KIO construction by delevoping a $(\leq n, \leq w)$-OTBES from a suitable BIBD (balanced incomplete block design) with a threshold access structure defined on it (recall that any threshold access structure is ideal). First, we need to give the definition of BIBD: a *balanced incomplete block design* is in fact just a 2-(v, k, λ) design. A BIBD has five parameters, and it is written as $(v, \beta, r, k, \lambda)$-BIBD. The parameter β denotes the total number of blocks, and the parameter r denotes the number of blocks containing each point. These two parameters can be computed from v, k and λ by using the simple equations $vr = \beta k$ and $\lambda(v-1) = r(k-1)$.

Suppose $(\mathcal{U}, \mathcal{B})$ is an $(n, \beta, r, k, \lambda)$-BIBD such that $r > \lambda\binom{w}{2}$. We will apply the KIO construction with $\theta = 1$.

Every point occurs in r blocks of the design. Further, any set of w points intersect at most $\lambda\binom{w}{2}$ blocks in at least two points. Hence the KIO construction can be applied if we define Γ to be a $(\lambda\binom{w}{2}+1, \beta)$ threshold access structure.

It is not hard to compute the information rates of the resulting OTBES. We have the following:

$$\begin{aligned}
H(B_P) &= \beta \log q \\
H(M_P) &= \log q \\
H(U_i) &= rk \log q \\
H(U_{\mathcal{U}}) &= \beta(k+1) \log q \\
H(B_P|U_{\mathcal{U}}) &= \left(\lambda\binom{w}{2}+1\right) \log q \\
H(U_{\mathcal{U}} B_P) &= \left(\lambda\binom{w}{2}+1+\beta(k+1)\right) \log q.
\end{aligned}$$

All of these calculations are straightforward. Note that the value of $H(B_P|U_{\mathcal{U}})$ follows easily from the description of Shamir scheme we gave earlier. The Shamir scheme is implemented by choosing the $\lambda\binom{w}{2}+1$ coefficients of a polynomial of degree $\lambda\binom{w}{2}$; this determines the values of all the shares.

We record this application of the KIO construction in the following theorem.

Theorem 8.1 *Suppose there is an $(n, \beta, r, k, \lambda)$-BIBD such that $r > \lambda\binom{w}{2}$. Then there exists a $(\leq n, \leq w)$-OTBES having information rate $1/(rk)$,* *broadcast information rate* $1/\beta$, *and total information rate*

$$\frac{1}{\lambda\binom{w}{2} + 1 + \beta(k+1)}.$$

We will work out a simple example now. We will construct a $(\leq 7, \leq 2)$-OTBES from a $(7,7,3,3,1)$-BIBD. The blocks of the BIBD are:

$$\begin{aligned} B_1 &= \{1,2,4\} \\ B_2 &= \{2,3,5\} \\ B_3 &= \{3,4,6\} \\ B_4 &= \{4,5,7\} \\ B_5 &= \{1,5,6\} \\ B_6 &= \{2,6,7\} \\ B_7 &= \{1,3,7\} \end{aligned}$$

A total of nine values from $GF(q)$ will be given to each user, as indicated below:

1	2	3	4	5	6	7
$s_{1,\emptyset}$	$s_{1,\emptyset}$	$s_{2,\emptyset}$	$s_{1,\emptyset}$	$s_{2,\emptyset}$	$s_{3,\emptyset}$	$s_{4,\emptyset}$
$s_{1,2}$	$s_{1,1}$	$s_{2,2}$	$s_{1,1}$	$s_{2,2}$	$s_{3,3}$	$s_{4,4}$
$s_{1,4}$	$s_{1,4}$	$s_{2,5}$	$s_{1,2}$	$s_{2,3}$	$s_{3,4}$	$s_{4,5}$
$s_{5,\emptyset}$	$s_{2,\emptyset}$	$s_{3,\emptyset}$	$s_{3,\emptyset}$	$s_{4,\emptyset}$	$s_{5,\emptyset}$	$s_{6,\emptyset}$
$s_{5,5}$	$s_{2,3}$	$s_{3,4}$	$s_{3,3}$	$s_{4,4}$	$s_{5,1}$	$s_{6,2}$
$s_{5,6}$	$s_{2,5}$	$s_{3,6}$	$s_{3,6}$	$s_{4,7}$	$s_{5,5}$	$s_{6,6}$
$s_{7,\emptyset}$	$s_{6,\emptyset}$	$s_{7,\emptyset}$	$s_{4,\emptyset}$	$s_{5,\emptyset}$	$s_{6\emptyset,}$	$s_{7,\emptyset}$
$s_{7,3}$	$s_{6,6}$	$s_{7,1}$	$s_{4,5}$	$s_{5,1}$	$s_{6,2}$	$s_{7,1}$
$s_{7,7}$	$s_{6,7}$	$s_{7,7}$	$s_{4,7}$	$s_{5,6}$	$s_{6,7}$	$s_{7,3}$

Now, suppose that the TA wants to broadcast a message to the set $P = \{1,2,3\}$. The following will be the keys used in the seven Fiat-Naor schemes:

$$\begin{aligned} k_1 &= s_{1,\emptyset} + s_{1,4} \\ k_2 &= s_{2,\emptyset} + s_{2,5} \\ k_3 &= s_{3,\emptyset} + s_{3,4} + s_{3,6} \\ k_4 & \quad \text{not used} \\ k_5 &= s_{5,\emptyset} + s_{5,5} + s_{5,6} \\ k_6 &= s_{6,\emptyset} + s_{6,6} + s_{6,7} \\ k_7 &= s_{7,\emptyset} + s_{7,7}. \end{aligned}$$

A Shamir $(2,7)$-threshold scheme is set up on the seven blocks of the BIBD. Suppose that the public value associated with block B_j is $x_j = j$, $1 \leq j \leq 7$. Now, suppose that the TA wants to broadcast the message m_P. The TA will construct a linear polynomial

$$f(x) = a_0 + a_1 x,$$

where $a_0 = m_P$. Then the TA will compute $y_j = a_0 + a_1 x_j$, for $1 \leq j \leq 7$. Finally, $b_j = k_j + y_j$ $(1 \leq j \leq 7)$, so the broadcast b_P consists of the following six values (recalling that k_4 is not used):

$$\begin{aligned} b_1 &= s_{1,\emptyset} + s_{1,4} + a_0 + a_1 x_1 \\ b_2 &= s_{2,\emptyset} + s_{2,5} + a_0 + a_1 x_2 \\ b_3 &= s_{3,\emptyset} + s_{3,4} + s_{3,6} + a_0 + a_1 x_3 \\ b_5 &= s_{5,\emptyset} + s_{5,5} + s_{5,6} + a_0 + a_1 x_5 \\ b_6 &= s_{6,\emptyset} + s_{6,6} + s_{6,7} + a_0 + a_1 x_6 \\ b_7 &= s_{7,\emptyset} + s_{7,7} + a_0 + a_1 x_7. \end{aligned}$$

8.1 An Improvement in the Case $w = 2$

Using BIBDs does not turn out to be an efficient method in practice. The well-known Fisher's Inequality (see, for example, [19, p. 261]) states that $\beta \geq n$ in any $(n, \beta, r, k, \lambda)$-BIBD. Hence, the broadcast rate of the scheme is at most $1/n$, which is no improvement over the trivial scheme.

However, we do not need all the properties of a BIBD in order to carry out the construction. For example, it is not necessary that every pair of points occurs in exactly λ blocks. The method works just as well provided that every pair of points occurs in *at most* λ blocks, and every point occurs in *at least* r blocks, where $r > \lambda\binom{w}{2}$, as before.

We look more closely at the case $w = 2$, which provides a nice example. In this case, we want a "design" $(\mathcal{U}, \mathcal{B})$ such that, for every two points x, y, there exists a block B_x with $x \in B_x$ and $y \notin B_x$, and a block B_y with $y \in B_y$ and $x \notin B_y$.

Consider the so-called *dual design* $(\mathcal{B}, \mathcal{V})$, in which

$$\mathcal{V} = \{V_i : 1 \leq i \leq n\},$$

where

$$V_i = \{B_x \in \mathcal{B} : i \in B_x\},$$

$1 \leq i \leq n$. It is easy to see that there do not exist two distinct blocks V_i, V_j such that $V_i \subseteq V_j$. In other words, the dual design $(\mathcal{B}, \mathcal{V})$ is a *Sperner family.*

Now, it is well-known that there exists a Sperner family consisting of n subsets of a β-set if and only if

$$n \leq \binom{\beta}{\left\lfloor \frac{\beta}{2} \right\rfloor}.$$

Further, the case of equality can be realized by taking all $\left\lfloor \frac{\beta}{2} \right\rfloor$-subsets of a β-set. (See, for example, Cameron [19, p. 101].)

For example, suppose β is even, and let $\beta = 2\alpha$. Using an obvious notation, we obtain a design with parameters

$$\left(\binom{2\alpha}{\alpha}, 2\alpha, \alpha, \binom{2\alpha - 1}{\alpha - 1}, \leq \alpha - 1 \right).$$

(Notice that r turns out to be constant; it is only λ that varies.) This design has n exponentially large compared to β, which represents an enormous improvement over using a BIBD.

Theorem 8.2 *Suppose that α is an integer and $n = \binom{2\alpha}{\alpha}$. Then there exists a $(\leq n, \leq 2)$-OTBES having information rate*

$$\frac{1}{\alpha\binom{2\alpha-1}{\alpha-1}}$$

and broadcast information rate $1/(2\alpha)$.

From Stirling's Formula, we see that

$$\log_2 n \approx 2\alpha - \frac{1}{2}\log_2(\pi\alpha).$$

Hence,

$$2\alpha \approx \log_2 n.$$

In the resulting scheme, the broadcast information rate is about $1/\log_2 n$, as compared to $1/n$, which is the best that can be obtained from Theorem 8.1. The information rate is approximately

$$\frac{4}{n \log n.}$$

As a small example, if we take $\alpha = 3$, then we get a $(\leq 20, \leq 2)$-OTBES having information rate $1/30$ and broadcast information rate $1/6$. The set $\mathcal{B}$ consists of the following six blocks:

$$\begin{array}{l}
\{1,\ldots,10\} \\
\{1,2,3,4,11,12,13,14,15,16\} \\
\{1,5,6,7,11,12,13,17,18,19\} \\
\{2,5,8,9,11,14,15,17,18,20\} \\
\{3,6,8,10,12,14,16,17,19,20\} \\
\{4,7,9,10,13,15,16,18,19,20\}.
\end{array}$$

The access structure Γ in the KIO construction in this case will be a $(3,6)$-threshold access structure.

9 The Fiat-Naor Broadcast Scheme

One of the first constructions of OTBES was due to Fiat and Naor [22]. It uses perfect hash families, which we now define. A (n, m, w)-*perfect hash family* is a set of functions $\mathcal{H}$ such that

$$f : \{1,\ldots,n\} \rightarrow \{1,\ldots,m\}$$

for each $f \in \mathcal{H}$, and for any $X \subseteq \{1,\ldots,n\}$ such that $|X| = w$, there exists at least one $f \in \mathcal{H}$ such that $f|_X$ is one-to-one. We will use the notation $\mathrm{PHF}(N; n, m, w)$ for a (n, m, w)-perfect hash family with $|\mathcal{H}| = N$.

The motivation for the terminology "perfect hash family" is that we have a family of hash functions with the property that if at most w elements are to be hashed, then at least one function in the family yields no collisions when applied to the given w inputs.

We will typically depict a $\mathrm{PHF}(N; n, m, w)$ in the form of a $N \times n$ array of m symbols, where each row of the array corresponds to one of the functions in the family. This array has the property that, for any subset of w columns, there exists at least one row such that the entries in the w given columns of that row are distinct.

Perfect hash families have undergone considerable study in the last fifteen years. Some results can be found in the following papers (as well as in many other papers): [1, 2, 23, 33]. We will not discuss perfect hash families in detail here. However, we note that very efficient (i.e., small) families are known to exist via probabilistic arguments, but explicit constructions seem to be more difficult.

To construct a broadcast scheme, we first reformulate the concept of a perfect hashing family. A *resolvable block design* is a pair (X, Π), where the following properties are satisfied:

1. X is a finite set of elements called *points*
2. $\mathcal{P}$ is a finite set of *parallel classes*, each of which is a partition of X (the members of the parallel classes are called *blocks*)

A *w-separating resolvable block design* is a resolvable block design in which the following propertiy is satisfied: For any subset Y of w points, there exists a parallel class $\pi \in \Pi$ such that the w points in Y occur in w different blocks in π. (Note the we do not require constant block size.)

We will use the notation w-SRBD(v, β, r, m) to denote such a design, where

$$\begin{aligned} v &= |X|, \\ r &= |\Pi|, \\ \beta &= \sum_{\pi \in \Pi} |\pi|, \text{and} \\ m &= \max\{|\pi| : \pi \in \Pi\}. \end{aligned}$$

PHF are related to SRBD as follows:

Theorem 9.1 *If there exists a PHF$(N; n, m, w)$, then a w-SRBD(n, β, N, m) exists for some $\beta \leq Nm$. Conversely, if there exists a w-SRBD(v, β, r, m), then there exists a PHF$(r; v, m, w)$.*

Here now is the Fiat-Naor OTBES.

Theorem 9.2 (Fiat-Naor Scheme) *[22] Suppose there is a PHF$(N; n, m, w)$. Then there is a $(\leq n, \leq w)$-OTBES having information rate at least $1/(nN)$, broadcast information rate $1/(mN)$, and total information rate at least*

$$\frac{1}{(n + m + 1)N}.$$

Proof. From the given PHF, construct a w-SRBD(n, β, N), $(\mathcal{U}, \Pi)$, where $\beta \leq Nm$. Define $\mathcal{B}$ to consist of all the blocks in the SRBD, and define the access structure Γ (on the set $\mathcal{B}$) to have basis

$$\Gamma_0 = \pi_1 \times \ldots \times \pi_N,$$

where

$$\Pi = \{\pi_1, \ldots, \pi_N\}.$$

It is easy to see that there exists a Γ-ISSS: let $k \in GF(q)$ be the key, and let $y_i, \ldots, y_N$ be chosen in $GF(q)$ so that

$$y_i + \ldots + y_N = k.$$

Then the share y_i is given to each block in π_i, $1 \leq i \leq N$.

Now, define $\theta = 1$ and apply the KIO construction. The information rates of the resulting scheme can be computed using the following entropies:

$$\begin{aligned} H(B_P) &\leq mN \log q \\ H(M_P) &= \log q \\ H(U_i) &\leq nN \log q \\ H(U_{\mathcal{U}}) &\leq (n+m)N \log q \\ H(B_P|U_{\mathcal{U}}) &= N \log q \\ H(U_{\mathcal{U}} B_P) &\leq (n+m+1)N \log q. \end{aligned}$$

□

Remark: If we have a resolvable block design and define Γ as in the above proof, we obtain a $(\leq n, \leq w)$-OTBES from the KIO construction if and only if the design is w-separating.

9.1 The Case $w = 2$

We will illustrate the Fiat-Naor scheme by examining the simple case $w = 2$. Suitable perfect hashing families are easy to construct in this case, as follows.

Theorem 9.3 *There is a PHF$(N; n, m, 2)$ if and only if*

$$n \leq m^N.$$

Proof. An $N \times n$ array of m symbols is a PHF$(N; n, m, 2)$ if and only if no two columns of the array are identical. □

Thus we have the following corollary of Theorem 9.2.

Theorem 9.4 *Suppose $m \geq 2$ is an integer and n is an integral power of m. Then there is an $(\leq n, \leq 2)$-OTBES having information rate at least*

$$\frac{\log m}{n \log n}$$

and broadcast information rate

$$\frac{\log m}{m \log n}.$$

Note that the broadcast information rate is maximized by taking $m = 3$. As m increases, the information rate increases and the broadcast information rate decreases.

It is also interesting to compare Theorem 9.4 to Theorem 8.2:

	Theorem 8.2	Theorem 9.4
information rate	$\frac{4}{n \log n}$	$\frac{\log m}{n \log n}$
broadcast information rate	$\frac{1}{\log n}$	$\frac{\log m}{m \log n}$.

Hence, Theorem 8.2 always has yields a higher broadcast information rate than Theorem 9.4. Theorem 9.4 yields a higher information rate than Theorem 8.2 provided that $m \geq 16$, but then the information rate becomes quite small.

Let's work out a small example to illustrate the construction of an OTBES with $w = 2$ by this method. Suppose we take $n = 5$ and $m = 2$. Since 5 is not an integral power of 2, the best we can do is to use a PHF of size

$$\left\lceil \frac{\log 5}{\log 2} \right\rceil = 3.$$

Suppose we begin with the following PHF$(3; 5, 2, 2)$:

$$\begin{array}{|ccccc|}
\hline
1 & 1 & 1 & 2 & 2 \\
1 & 1 & 2 & 1 & 2 \\
1 & 2 & 1 & 1 & 2 \\
\hline
\end{array}$$

The corresponding 2-SRBD$(5, 6, 3, 2)$ is as follows:

$$\begin{array}{cc}
\{1,2,3\} & \{4,5\} \\
\{1,2,4\} & \{3,5\} \\
\{1,3,4\} & \{2,5\}
\end{array}$$

We will end up with an OTBES having information rate 1/9 and broadcast information rate 1/6. The following information (from $GF(q)$) will be given out in setting up a Fiat-Naor KPS on each block of the above SRBD:

1	2	3	4	5
$s_{1,\emptyset}$	$s_{1,\emptyset}$	$s_{1,\emptyset}$	$s_{2,\emptyset}$	$s_{2,\emptyset}$
$s_{1,2}$	$s_{1,1}$	$s_{1,1}$	$s_{2,5}$	$s_{2,4}$
$s_{1,3}$	$s_{1,3}$	$s_{1,2}$		
$s_{3,\emptyset}$	$s_{3,\emptyset}$	$s_{4,\emptyset}$	$s_{3,\emptyset}$	$s_{4,\emptyset}$
$s_{3,2}$	$s_{3,1}$	$s_{4,5}$	$s_{3,1}$	$s_{4,3}$
$s_{3,4}$	$s_{3,4}$		$s_{3,2}$	
$s_{5,\emptyset}$	$s_{6,\emptyset}$	$s_{5,\emptyset}$	$s_{5,\emptyset}$	$s_{6,\emptyset}$
$s_{5,3}$	$s_{6,5}$	$s_{5,1}$	$s_{5,1}$	$s_{6,2}$
$s_{5,4}$		$s_{5,4}$	$s_{5,3}$	

Now, suppose the privileged set is $P = \{3, 4, 5\}$. The following will be the keys used in the six Fiat-Naor KPS:

$$\begin{aligned}
k_1 &= s_{1,\emptyset} + s_{1,1} + s_{1,2} \\
k_2 &= s_{2,\emptyset} \\
k_3 &= s_{3,\emptyset} + s_{3,1} + s_{3,2} \\
k_4 &= s_{4,\emptyset} \\
k_5 &= s_{5,\emptyset} + s_{5,1} \\
k_6 &= s_{6,\emptyset} + s_{6,2}.
\end{aligned}$$

Now, suppose that the TA wants to broadcast the message m_P. The TA will choose three values y_1, y_2, y_3 such that $m_P = y_1 + y_2 + y_3$. Then the broadcast b_P consists of the following six values:

$$\begin{aligned}
b_1 &= s_{1,\emptyset} + s_{1,1} + s_{1,2} + y_1 \\
b_2 &= s_{2,\emptyset} + y_1 \\
b_3 &= s_{3,\emptyset} + s_{3,1} + s_{3,2} + y_2 \\
b_4 &= s_{4,\emptyset} + y_2 \\
b_5 &= s_{5,\emptyset} + s_{5,1} + y_3 \\
b_6 &= s_{6,\emptyset} + s_{6,2} + y_3.
\end{aligned}$$

10 Summary

We have surveyed some known constructions for key predistribution schemes and broadcast schemes. We have also introduced some new directions for future research. One contribution is the use of resilient functions in making key distribution patterns more efficient. This allows the construction of key predistribution schemes that permit a trade-off between security and the size of the key that is computed. One novel feature is that this trade-off is accomplished at the time the key is computed.

The second contribution is the general approach to broadcast encryption using secret sharing schemes and key predistribution schemes. This approach was illustrated by using balanced incomplete block designs (BIBDs) together with threshold schemes to construct a new broadcast encryption scheme. Although the resulting scheme is not efficient, a variation of the scheme was described when $w = 2$ that is very efficient. By using a suitable generalization of a BIBD, it may be possible to construct new efficient schemes for larger w.

Acknowledgements

I would like to thank Bert den Boer, K. Gopalakrishnan, Wen-ai Jackson and the referees for many helpful comments.

References

[1] N. Alon and M. Naor. Derandomization, Witnesses for Boolean Matrix Multiplication and Constructions of Perfect Hash Functions. Technical Report CS94-11, Weizmann Institute of Science.

[2] M. Atici, S. S. Magliveras, D. R. Stinson and W.-D. Wei. Some Recursive Constructions for Perfect Hash Families. *Journal of Combinatorial Designs* 4 (1996), 353–363.

[3] A. Beimel and B. Chor. Interaction in Key Distribution Schemes. *Lecture Notes in Computer Science* **773** (1994), 444–455 (Advances in Cryptology – CRYPTO '93).

[4] A. Beimel and B. Chor. Universally Ideal Secret Sharing Schemes. *IEEE Transactions on Information Theory* **40** (1994), 786–794.

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

[6] C. H. Bennett, G. Brassard and J.-M. Robert. Privacy Amplification by Public Discussion. *SIAM J. Comput.* **17** (1988), 210–229.

[7] S. Berkovits. How to Broadcast a Secret. *Lecture Notes in Computer Science* **547** (1992), 536–541 (Advances in Cryptology — EUROCRYPT '91).

[8] Th. Beth, D. Jungnickel and H. Lenz. *Design Theory.* Bibliographisches Institut, Zurich, 1985.

[9] J. Bierbrauer, K. Gopalakrishnan and D. R. Stinson. Bounds for Resilient Functions and Orthogonal Arrays. *Lecture Notes in Computer Science* **839** (1994), 247–256 (Advances in Cryptology – CRYPTO '94).

[10] J. Bierbrauer, K. Gopalakrishnan and D. R. Stinson. Orthogonal Arrays, Resilient Functions, Error-correcting Codes and Linear Programming Bounds. *SIAM J. Discrete Math* **9** (1996), 424–452.

[11] R. Blom. An Optimal Class of Symmetric Key Generation Systems. *Lecture Notes in Computer Science* **209** (1985), 335–338 (Advances in Cryptology — EUROCRYPT '84).

[12] C. Blundo and A. Cresti. Space Requirements for Broadcast Encryption. *Lecture Notes in Computer Science* **950** (1995), 287–298 (Advances in Cryptology — EUROCRYPT '94).

[13] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung. Perfectly Secure Key Distribution for Dynamic Conferences. *Lecture Notes in Computer Science* **740** (1993), 471–486 (Advances in Cryptology — CRYPTO '92).

[14] C. Blundo, A. De Santis and U. Vaccaro. Randomness in Distribution Protocols. *Lecture Notes in Computer Science* **820** (1994), 568–579. (Automata, Languages and Programming — ICALP '94).

[15] C. Blundo, L. A. Frota Mattos and D. R. Stinson. Tradeoffs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution. *Lecture Notes in Computer Science* **1109** (1996), 387–400 (Advances in Cryptology — CRYPTO '96).

[16] C. Blundo, L. A. Frota Mattos and D. R. Stinson. Multiple Key Distribution Maintaining User Anonymity via Broadcast Channels. *J. Computer Security* **3** (1994/95), 309–323.

[17] E. F. Brickell. Some Ideal Secret Sharing Schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing* **9** (1989), 105–113.

[18] E. F. Brickell and D. M. Davenport. On the Classification of Ideal Secret Sharing Schemes. *Journal of Cryptology* **4** (1991), 123–134.

[19] P. J. Cameron. *Combinatorics: Topics, Techniques, Algorithms.* Cambridge University Press, 1994.

[20] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich and R. Smolensky. The Bit Extraction Problem or t-resilient Functions. *Proc. 26th IEEE Symposium on Foundations of Computer Science* (1985), 396–407.

[21] M. Dyer, T. Fenner, A. Frieze and A. Thomason. On Key Storage in Secure Networks. *Journal of Cryptology* **8** (1995), 189–200.

[22] A. Fiat and M. Naor. Broadcast Encryption. *Lecture Notes in Computer Science* **773** (1994), 480–491 (Advances in Cryptology — CRYPTO '93).

[23] M. L. Fredman and J. Komlos. On the Size of Separating Systems and Families of Perfect Hash Functions. *SIAM Journal of Algebraic and Discrete Methods* **5** (1984), 61–68.

[24] J. Friedman. On the Bit Extraction Problem. *Proc. 33rd IEEE Symposium on Foundations of Computer Science* (1992), 314–319.

[25] L. Gong and D. L. Wheeler. A Matrix Key-distribution Scheme. *Journal of Cryptology* **2** (1990), 51–59.

[26] K. Gopalakrishnan. *A Study of Correlation-immune, Resilient and Related Cryptographic Functions.* PhD Thesis, University of Nebraska-Lincoln, 1994.

[27] K. Gopalakrishnan and D. R. Stinson. Three Characterizations of Non-binary Correlation-immune and Resilient Functions. *Designs, Codes and Cryptography* **5** (1995), 241-251.

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

[29] V. Korjik, M. Ivkov, Y. Merinovitch, A. Barg and H. van Tilborg. A Broadcast Key Distribution Scheme Based on Block Designs. *Lecture Notes in Computer Science* **1025** (1995), 12–21 (Cryptography and Coding, V).

[30] K. Kurosawa, K. Okada and K. Sakano. Security of the Center in Key Distribution Schemes. *Lecture Notes in Computer Science* **917** (1995), (Advances in Cryptology — ASIACRYPT '94).

[31] T. Leighton and S. Micali. Secret-key Agreement without Public-key Cryptography. *Lecture Notes in Computer Science* **773** (1994), 456–479 (Advances in Cryptology — CRYPTO '93).

[32] T. Matsumoto. Incidence Structures for Key Sharing. *Lecture Notes in Computer Science* **917** (1995), 342–353 (Advances in Cryptology — ASIACRYPT '94).

[33] K. Mehlhorn. On the Program Size of Perfect and Universal Hash Functions. *Proc. 23rd Annual IEEE Symposium on Foundations of Computer Science*, 1982, pp. 170–175.

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

[35] C. M. O'Keefe. Applications of Finite Geometries to Information Security. *Australasian J. Combinatorics* **7** (1993), 195–212.

[36] K. A. S. Quinn. Some Constructions for Key Distribution Patterns. *Designs, Codes and Cryptography* **4** (1994), 177–191.

[37] A. Shamir. How to Share a Secret. *Communications of the ACM* **22** (1979), 612–613.

[38] D. R. Stinson. An Explication of Secret Sharing Schemes. *Designs, Codes and Cryptography* **2** (1992), 357–390.

[39] D. R. Stinson. *Cryptography Theory and Practice.* CRC Press, Inc., Boca Raton, 1995.

[40] D. Welsh. *Codes and Cryptography.* Oxford University Press, 1988.