Key Preassigned Traceability Schemes for Broadcast Encryption (Extended Abstract)

D. R. Stinson and R. Wei
Department of Combinatorics and Optimization
University of Waterloo
Waterloo Ontario, N2L 3G1
Canada

May 19, 1998

1 Introduction

Most networks can be thought of as broadcast networks, in that any one connected to the network can access to all the information that flows through it. In many situations, such as a pay-per-view television broadcast, the data is only available to authorized users. To prevent an unauthorized user from accessing the data, the trusted authority (TA) will encrypt the data and give the authorized users keys to decrypt it. Some unauthorized users might obtain some decryption keys from a group of one or more authorized users (called *traitors*). Then the unauthorized users can decrypt data that they are not entitled to. To prevent this, Chor, Fiat and Naor [5] devised a traitor tracing scheme, called a *traceability scheme*, which will reveal at least one traitor on the confiscation of a pirate decoder. This scheme was then generalized by Stinson and Wei in [13]. There are some other recent papers discussing this topic (see [7, 8, 9]).

The basic idea of a traceability scheme is as follows. Suppose there are a total of b users. The TA generates a set T of v *base keys* and assigns k keys chosen from T to each user. These k keys comprise a user's *personal key*, and we will denote the personal key for user i by U_i. A *broadcast message*, M, consists of an enabling block, B, and a cipher block, Y. The *cipher block* is the encryption of the actual plaintext data X using a *secret key*,

S. That is, $Y = e_S(X)$, where $e(\cdot)$ is the encryption function for some cryptosystem. The *enabling block* consists of data which is encrypted by some method, using some or all of the v keys in the base set, the decryption of which will allow the recovery of the secret key S. Every authorized user should be able to recover S using his or her personal key, and then decrypt the cipher block using S to obtain the plaintext data, i.e., $X = d_S(Y)$, where $d(\cdot)$ is the decryption function for the cryptosystem.

Some traitors may conspire and give an unauthorized user a *pirate decoder*, E. E will consist of a subset of base keys such that $E \subseteq \cup_{i \in C} U_i$, where C is the coalition of traitors. An unauthorized user may be able to decrypt the enabling block using a pirate decoder. The goal of the TA is to assign keys to the users in such a way that when a pirate decoder is captured and the keys it possesses are examined, it should be possible to detect at least one traitor in the coalition C, provided that $|C| \leq c$ (where c is a predetermined threshold).

In all the traceability schemes discussed in [5, 13, 7, 8] it is assumed that every user can decrypt the enabling block. This means that the data supplier should assign the keys after he or she has determined who the authorized users are. In practice, however, this restriction may be inconvenient, as changes between authorized and unauthorized users may be frequent.

In this paper, we investigate traceability schemes in which the personal keys can be assigned before the authorized users are determined. We will call these schemes *key preassigned schemes*. Key preassigned schemes (for broadcast encryption) have been discussed by several researchers. The first scheme was introduced by Berkovits in [1]. Several recent papers have studied broadcast encryption schemes (see [2, 3, 6, 9, 11, 12], for example). Broadcast schemes enable a TA to broadcast a message to the users in a network so that a certain specified subset of authorized users can decrypt it. However, most of these broadcast schemes have not considered the question of traceability. We will briefly review the traceability of these schemes and then give some key preassigned schemes which have better traceability than the previous schemes. We will use combinatorial methods to describe the schemes and give some explicit constructions. The efficiency of the schemes is measured by considering the information rate and broadcast information rate.

There are two aspects of security in our schemes. One property of the scheme is to prevent unauthorized users from decrypting the enabling block; this is the usual question investigated in broadcast encryption. The second property is the ability of tracing a pirate decoder which is made by a coalition of users (which of course could be authorized users). Although these two properties both protect against coalitions, they have different effects. The first property can prevent the coalition of unauthorized users from decrypting the enabling block, but it does not protect against construction of a pirate decoder. The second property cannot prevent a coalition from decrypting the enabling block, but it enables the TA to trace at least one traitor if the decoder is found.

2 Definitions and notations

In this section, we give basic definitions and the notations used in this paper.

2.1 Broadcast encryption schemes

The definition of a broadcast encryption scheme we use in this paper will be the same as the one given in [11]. As in a traceability scheme, there is a trusted authority (TA) and a set of users $\mathcal{U} = \{1, 2, \cdots, b\}$, and the TA generates a set of v base keys and assigns a subset of the base keys to each user as his or her personal key. At a later time, a *privileged subset*, P, of authorized users is determined. The TA chooses a secret key S and broadcasts an enabling block B_P (which is an encryption of S) that can be decrypted by every authorized user, but which cannot be decrypted by certain *forbidden subsets* disjoint from P.

Let $\mathcal{P}$ denote the collection of possible privileged subsets and let $\mathcal{F}$ denote the collection of possible forbidden subsets. In this paper, we will consider the case when $\mathcal{P} = 2^{\mathcal{U}}$, so $\mathcal{P}$ contains all subsets of users, and $\mathcal{F}$ contains all f-subsets of users, where f is a fixed integer. To make things simpler (and since we want to focus on the traceability first), we will mainly consider the situation when $f = 1$. In the case $\mathcal{P} = 2^{\mathcal{U}}$ and $f = 1$, the privileged subset can be chosen to be any subset of users, and the enabling block cannot be decrypted by individual unauthorized user. (It may be possible for subsets of unauthorized users to jointly decrypt the message, however.)

For $1 \leq i \leq b$, let $\mathbf{U}_i$ denote the set of all possible subsets of base keys that might be distributed to user i by the TA. Thus the personal key $U_i \in \mathbf{U}_i$. Let $\mathbf{S}$ denote the set of possible secret keys, so $S \in \mathbf{S}$. Let $\mathbf{B}_P$ be the set of possible enabling blocks for privileged subset P; thus $B_P \in \mathbf{B}_P$. Usually, U_i, S and B_P consist of tuples from a finite field F_q. We define the *information rate* to be

$$\rho = \min\left\{\frac{\log \mathbf{S}}{\log \mathbf{U}_i} : 1 \le i \le b\right\}.$$

and the *broadcast information rate* to be

$$\rho_B = \min\left\{\frac{\log \mathbf{S}}{\log \mathbf{B}_P} : P \in \mathcal{P}\right\}.$$

In general, to decrease the size of the broadcast, i.e., to increase ρ_B, it is necessary to decrease ρ, and vice versa. Since it is trivial to construct a broadcast encryption scheme with $\rho = 1$ and $\rho_B = 1/b$, we are mainly interested in schemes with $\rho_B > 1/b$.

2.2 Traceability

Suppose a "pirate decoder" E is found. (We assume that the pirate decoder can be used to decrypt some enabling blocks.) If there exists a user i such that $|E \cap U_i| \ge |E \cap U_j|$ for all users $j \ne i$, then i is defined to be an *exposed user*. A c-traceability scheme is defined as follows.

Definition 2.1 Suppose any exposed user i is a member of the coalition $\mathcal{C}$ whenever a pirate decoder E is produced by $\mathcal{C}$ (so $E \subseteq \cup_{i\in C} U_i$) and $|\mathcal{C}| \le c$. Then the scheme is called a *c-traceability scheme.*

When a scheme is c-traceable, $\mathcal{P} = 2^{\mathcal{U}}$, and the forbidden subsets consist of all f-subsets of users, we call it a *(c, f)-key preassigned traceability scheme* and denote it as a (c, f)-KPTS. For the case $f = 1$, we denote the scheme as a c-KPTS.

Remark. The difference between Definition 2.1 and the one in [9] is that the size of the pirate decoder is not specified here. For example, the pirate decoder might be smaller or larger than a legitimate decoder. The only requirement is that a pirate decoder should be able to decode some enabling blocks.

A set system is a pair $(X, \mathcal{A})$, where X is a set of *points* and $\mathcal{A}$ is a collection of subsets of X called *blocks*. We will use set systems with the following property, which is modified from [13, Theorem 2.2].

Definition 2.2 A *traceability scheme system* is a set system $(X, \mathcal{A})$, where every block has size k for some integer k, with the property that for every choice of $c' \le c$ blocks

$A_1, A_2, \cdots, A_{c'} \in \mathcal{A}$, and for any t-subset $E \subseteq \cup_{j=1}^{c'} A_j$, where $t \geq k$, there does not exist a block $A \in \mathcal{A} \backslash \{A_1, A_2, \cdots, A_{c'}\}$ such that $|E \cap A_j| \leq |E \cap A|$ for $1 \leq j \leq c'$. Such a system will be denoted by (c, k)-TSS.

In this definition, the blocks correspond to legitimate decoders and E corresponds to a pirate decoder. We will be able to assume that $|E| \geq k$ due to the encryption scheme we use.

2.3 Secret sharing schemes

Let $\mathcal{U}$ be the set of b users, $\Gamma \subseteq 2^{\mathcal{U}}$ be a set of subsets called *authorized subsets*, and let $\Delta \subseteq 2^{\mathcal{U}}$ be a set of subsets called *unauthorized subsets*. In a (Γ, Δ)-*secret sharing scheme*, the TA has a secret value K. The TA will distribute secret information called *shares* to each user of $\mathcal{U}$ 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 paper [10] contains an introduction to secret sharing schemes.

Let $t \leq b$. A (t, b)-*threshold scheme* is a secret sharing scheme in which the authorized subsets are all the subsets of $\mathcal{U}$ with cardinality at least t and the unauthorized subsets are all the subsets of $\mathcal{U}$ with cardinality at most $t-1$. The Shamir scheme provides a construction of a (t, b)-threshold scheme in which each share is an element of F_q and the secret is also an element of F_q, for any prime power $q \geq b+1$.

2.4 Key predistribution schemes

Fiat-Naor *key predistribution schemes* (or *KPS*) (see [6]) are used in the KIO construction for broadcast encryption schemes given in [11]. Let $f \leq b$ be an integer. The forbidden subsets consist of all subsets of size at most f. In a Fiat-Naor scheme, the TA chooses a secret value x_F for each possible forbidden subset F, and gives that value to each user in $\mathcal{U} \backslash F$. Let $P \subseteq \mathcal{U}$. The value

$$K_P = \sum_{F \cap P = \emptyset} x_F$$

is the *key* for the privileged subset P. K_P can be computed by any member of P, but K_P cannot be computed by any forbidden subset F disjoint from P (where $|F| \leq f$).

3 Traceability of previous broadcast schemes

Since key preassigned broadcast encryption schemes were proposed in [1], several constructions have been given. A summary of these results can be found in Stinson [11]. In [11], the KIO construction is described, and which is further discussed in [12]. We will not review these schemes here — we only wish to indicate that these schemes usually do not have any traceability, or have, at most, 1-traceability. (However, note that if in a scheme, every user has disjoint keys, then the scheme is "totally traceable". Thus the trivial scheme in [11] has b-traceability.)

Staddon first discussed the traceability of key preassigned broadcast schemes in her PhD thesis [9]. She constructed some schemes called "OR protocols" that have higher traceability. We briefly review the OR protocols now. In OR protocols, the size of a forbidden subset is f and the size of the privileged subset is $w = b - f$. These values are fixed ahead of time. The TA produces a key K_t for each subset P_t of $\mathcal{U}$, where $|P_t| = \lceil \frac{w}{n} \rceil$, and gives that key to every user in P_t, where n is a given positive integer. When the TA wants to broadcast an enabling block for a privileged subset P, he uses the n keys in the set

$$\mathcal{L}_P = \{K_t : P_t \subseteq P\}$$

to encrypt it, in such a way that any user who has at least one of these n keys is able to decrypt it.

It is shown in [9] that the OR protocol construction has $\Theta(\sqrt{n})$-traceability for $n > 2$ and b sufficiently large relative to n and f. However, the proof is based on the assumption that the pirate decoder always is the same size as a personal key, i.e., that it always contains

$$\binom{b-1}{\lceil \frac{w}{n} \rceil - 1}$$

keys. This assumption may not be practical. In fact, unauthorized users who possess even one key might be able to decrypt the enabling block if the key happened to belong to the set $\mathcal{L}_P$. Thus the OR protocol has no traceability if we consider the traceability under Definition 2.1, where we allow a pirate decoder to have fewer keys than a personal key.

The traceability schemes in [5, 13] have the desirable property that any possible decoder must consist of the keys from the base key set, otherwise they will be useless for decoding. In some other proposed schemes, an enabling block can be decrypted using keys not in the base set. In such a scheme, the traceability property is defeated. We describe the traceability scheme proposed in [7] to illustrate this point.

In the scheme of [7] (which is not key preassigned), the TA chooses a random polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_c x^c.$$

The TA then computes $f(i)$ and gives it to user i secretly, so that the personal key of user i will be $(i, f(i))$. When TA wants to encrypt the secret key S, he broadcasts the enabling block $(S + a_0, a_1, a_2, \cdots, a_c)$. If a pirate decoder contains a pair $(u, f(u))$, then u will be the exposed user. However, two users i and j can construct a pirate decoder as follows. They choose two random non-zero numbers α and β and compute the following:

$$b_0 = \frac{\alpha f(i) + \beta f(j)}{\alpha + \beta}, b_1 = \frac{\alpha i + \beta j}{\alpha + \beta}, \cdots, b_c = \frac{\alpha i^c + \beta j^c}{\alpha + \beta}.$$

Since

$$a_0 = b_0 - a_1 b_1 - \cdots - a_c b_c,$$

the $(c+1)$-tuple $(b_0, \ldots, b_c)$ can be used as a decoder. In this scenario, the traitors i and j cannot be exposed by the usual traitor tracing method.

4 The new scheme

In this section, we present our traceability schemes which will use a KIO type construction. The basic idea of the KIO construction is that the secret key is split into shares, using a threshold scheme (or a generalization called a ramp scheme), and then the shares are encrypted, thus forming the enabling block. Our scheme is a key preassigned broadcast encryption scheme where $\mathcal{U} = \{1, \ldots, b\}$, $\mathcal{P} = 2^{\mathcal{U}}$ and $\mathcal{F}$ consists of all f-subsets of $\mathcal{U}$. We consider the case $f = 1$ first.

Suppose $(X, \mathcal{A})$ is a (c, k)-TSS, where $X = \{1, 2, \cdots, v\}$ and $\mathcal{A} = \{A_1, A_2, \cdots, A_b\}$. The block A_j determines the personal key given to user j, for $1 \leq j \leq b$. For each $u \in X$, let

$$R_u = \{j \in \mathcal{U} : u \in A_j\}.$$

The main steps in the protocol are as follows:

1. For every set R_u as defined above, the TA constructs a Fiat-Naor key predistribution scheme on user set R_u, with $\mathcal{F}_u = \{\{j\} : j \in R_u\} \cup \{\emptyset\}$ and $\mathcal{P}_u = 2^{R_u}$. Thus, for each

u, $1 \leq u \leq v$, the TA chooses $|R_u| + 1$ secret values, denoted x_{R_u} and $x_{R_u,j}$ $(j \in R_u)$. These values are chosen at random from a finite field F_q. The value x_{R_u} is given to each $i \in R_u$ and $x_{R_u,j}$ is given to each $i \in R_u \backslash \{j\}$. These keys form the personal key for user i.

We will assume the existence of a function Index on the set of base keys such that $\mathsf{Index}(x) = j$ if x is a key from the jth Fiat-Naor scheme. These keys might be stored as pairs, e.g., (x_{R_u}, u) and $(x_{R_u,j}, u)$, so that the users know which keys are from which Fiat-Naor scheme.

2. Suppose the TA wants to encrypt the secret key $S \in \mathsf{F}_q$ for a privileged subset P. For the purposes of illustration, suppose $P = \{1, 2, \cdots, w\}$. The TA first uses a (k, n)-threshold scheme to split S into n shares $y_1, y_2, \cdots, y_n$, where $A_P = \cup_{i=1}^{w} A_i$ and $n = |A_P|$ (note that $n \leq v$, so a (k, v)-threshold scheme can be used here, if desired).

3. For each $j \in A_P$, the TA computes the secret key K_j of Fiat-Naor scheme on R_j for the privileged subset $R_j \cap P$, i.e.,

$$K_j = x_{R_j} + \sum_{\ell \in R_j \backslash P} x_{R_j,\ell}.$$

4. Each share y_j is encrypted using an encryption function $e(\cdot)$ with key K_j. The enabling block consists of the list of encrypted values

$$(e_{K_j}(y_j) : j \in A_P).$$

Since each user in P has k values in A_P, he can compute k keys $K_{i_1}, K_{i_2}, \cdots, K_{i_k}$ and then obtain k shares, $y_{i_1}, y_{i_2}, \cdots, y_{i_k}$. Using the reconstruction function of the threshold scheme, the user is able to recover the value of the secret key, S.

A user not in P cannot compute any of the keys K_i, since the Fiat-Naor scheme is secure against individual unauthorized users. Thus, the user cannot get any information about the n shares.

Now we consider traceability. Suppose a pirate decoder E is found. The TA can compute the Index of the decoder as

$$\mathsf{Index}(E) = \{\mathsf{Index}(x) : x \in E\}.$$

Note that the cardinality of the set $\mathsf{Index}(E)$ is at least k, otherwise the decoder will be useless. The TA can then use this Index to find an exposed user, since the set system $(X, \mathcal{A})$ is a (c, k)-TSS.

The information rate of this scheme is

$$\rho = \frac{1}{k\,r}$$

where r_x is the number of blocks containing x, i.e., $r_x = |R_x|$, and $r = \max\{r_x : x \in X\}$. The broadcast information rate is

$$\rho_B = \frac{1}{n} \geq \frac{1}{v}.$$

The following theorem summarizes the properties of the scheme.

Theorem 4.1 *Suppose $(X, \mathcal{A})$ is a (c, k)-TSS in which $|X| = v$ and $|\mathcal{A}| = b$. Then there is a c-KPTS for a set of b users, having information rate $\rho \geq 1/(k\,r)$ and broadcast information rate $\rho_B \geq 1/v$.*

Remark. For the case $f > 1$, we need only change the construction of the Fiat-Naor scheme on each R_u so that the possible forbidden subsets are all subsets of R_u having size at most f. This will cause the information rate of the scheme to decrease, while the broadcast information rate remains the same.

The following small example will illustrate the scheme.

Example 4.1 *A 2-KPTS with 82 users.*

Let $X = \{0, 1, \cdots, 40\}$ and suppose $\mathcal{A}$ contains the following 82 blocks, where the calculations are in Z_{41}, for $i = 0, 1, 2, \cdots, 40$:

$$\begin{aligned} A_i &= \{1+i, 10+i, 18+i, 16+i, 37+i\} \\ A_{41+i} &= \{36+i, 32+i, 33+i, 2+i, 20+i\} \end{aligned}$$

The set system $(X, \mathcal{A})$ is a $(41, 5, 1)$-balanced incomplete block design (see [4]). This set system has the property that each pair of points appears in exactly one block, and every point appears in exactly 10 blocks. It is in fact a $(2, 5)$-TSS (see Theorem 5.3).

The block A_i is associated with user i. For each $u \in X$, the TA constructs a Fiat-Naor scheme on R_u. For example, for $u = 1$, it can be seen that

$$R_1 = \{0, 32, 24, 26, 5, 47, 51, 50, 81, 63\},$$

so $|R_1| = 11$. The TA will choose 11 secret values in F_q for some prime power q, and every user in R_1 will receive 10 of the 11 values. A Fiat-Naor scheme is implemented in this way on each R_u, and thus every user has 50 values in his or her personal key.

Now, suppose the TA wants to encrypt a secret key $S \in \mathsf{F}_q$, where the privileged subset is $P = \{0, 1, 2, \cdots, 59\}$, so $w = 60$. The TA uses a $(5, 41)$-threshold scheme to split S into 41 shares, $y_0, \ldots, y_{40}$. Then the TA computes the keys K_u, for $0 \le u \le 40$. For example,

$$K_1 = x_{R_1} + x_{R_1,63} + x_{R_1,81}.$$

The enabling block will be the list of encrypted values

$$(e_{K_0}(y_0), \cdots, e_{K_{40}}(y_{40})).$$

Any user in P can decrypt the enabling block. For example, consider user 5. The block $B_5 = \{6, 15, 23, 21, 42\}$. Then user 5 obtains five of the 41 secret keys, namely, K_6, K_{15}, K_{23}, K_{21} and K_{42}, and recovers the five shares y_6, y_{15}, y_{23}, y_{21} and y_{42}. From these five shares S can be obtained.

Any user not in P cannot decrypt the enabling block. For example, let us consider user 63. If $j \notin B_{63}$, then user 63 does not have K_{R_j} and cannot compute K_j. On the other hand, if $j \in B_{63}$, then user 63 does not have $K_{R_j,63}$ and cannot compute K_j either. Thus user 63 cannot compute any of the shares in the threshold scheme.

Finally, let's show that the scheme is 2-traceable. If a pirate decoder E is found, then the TA can compute $\mathsf{Index}(E)$ as described above. $\mathsf{Index}(E)$ must contain at least 5 numbers, otherwise it cannot decode anything. Suppose that the decoder was made by two users, say i and j. Since $\mathsf{Index}(E) \subseteq (B_i \cup B_j)$ it must be the case that $|\mathsf{Index}(E) \cap B_i| \ge 3$ or $|\mathsf{Index}(E) \cap B_j| \ge 3$. Since any two blocks intersect in at most one point, $|\mathsf{Index}(E) \cap B_h| \le 2$ if $h \ne i, j$. Thus user i or user j (or both) will be exposed users.

5 Constructions of traceability set systems

To construct our traceability schemes, we need to find traceability set systems. Some constructions for these types of set systems were given in [13]; they are based on certain types of combinatorial designs. (A comprehensive source for information on combinatorial designs is Colbourn and Dinitz [4].) We present a useful lemma for constructing TSS, and mention some applications of it.

Lemma 5.1 *Suppose there exists a set system $(X, \mathcal{A})$ satisfying the following conditions:*

1. $|A| = k \geq c^2\mu + 1$ *for any* $A \in \mathcal{A}$*;*
2. $|A_i \cap A_j| \leq \mu$ *for any* $A_i, A_j \in \mathcal{A}$*,* $i \neq j$*.*

Then the set system is a (c, k)-TSS.

Proof. Let $E \subseteq \cup_{i=1}^{c} A_i$ with $|E| \geq k$. Since $k \geq c^2\mu + 1$, there is a block A_s, $1 \leq s \leq c$, such that $|E \cap A_s| \geq c\mu + 1$. For any $A \in \mathcal{A} \backslash \{A_1, A_2, \cdots A_c\}$, we have

$$\begin{aligned} |E \cap A| &\leq |A \cap (\cup_{i=1}^{c} A_i)| \\ &\leq c\mu \\ &< c\mu + 1 \\ &\leq |E \cap A_s|. \end{aligned}$$

Hence, the set system is a (c, k)-TSS. ∎

As a first applicaiton of Lemma 5.1, we give a construction using t-designs.

Definition 5.1 *A t-(v, k, λ) design is a set system $(X, \mathcal{A})$, where $|X| = v$ and $|A| = k$ for all $A \in \mathcal{A}$, such that every t-subset of X appears in exactly λ blocks of $\mathcal{A}$.*

Theorem 5.2 *Suppose there exists a t-$(v, k, 1)$ design. Then there exists a (c, k)-TSS, where $c = \lfloor \sqrt{(k-1)/(t-1)} \rfloor$.*

Proof. Any two blocks of a t-$(v, k, 1)$ design intersect in at most $t - 1$ points. Apply Lemma 5.1 with $\mu = t - 1$. ∎

There are many results on t-$(v, k, 1)$ designs for small values of t, i.e., for $2 \leq t \leq 6$. See [4] for a summary of known results. We can construct interesting TSS using designs with $t = 2$. For example, it is known that there is a 2-$(v, 5, 1)$ design for all $v \geq 5$, $v \equiv 1, 5 \bmod 20$. These designs give rise to an infinite family of $(2, 5)$-TSS. Applying Theorem 4.1 we have the following KPTS.

Theorem 5.3 *There exists a 2-KPTS for all $v \geq 5$, $v \equiv 1, 5 \bmod 20$, for a set of $b = v(v-1)/20$ users, having $\rho = \frac{4}{5(v-1)}$ and $\rho_B = \frac{1}{v}$.*

Note that Example 4.1 is the case $v = 41$ of the above theorem.

A 3-$(q^2+1, q+1, 1)$ design, known as an *inversive plane*, exists for any prime power q. The following result concerns the KPTS that can be constructed from inversive planes.

Theorem 5.4 *For any prime power q, there exists a c-KPTS, where $c = \left\lfloor \sqrt{\frac{q}{2}} \right\rfloor$, with information rate $\rho \approx \frac{1}{q^3}$ and $\rho_B \approx \frac{1}{q^2}$.*

Many other constructions of TSS can be given using combinatorial objects such as packing designs, orthogonal arrays and almost strongly universal hash functions. The constructions are similar to those found in [12, 13].

6 Some remarks

We make a couple of final observations in this section.

- The (c, f)-KPTS scheme discussed in this paper is a generalization of the traceability schemes in [5, 13]. The schemes in [5, 13] are in fact the case of $f = 0$ of our main construction. When $f = 0$, there is no protection against an unauthorized user decrypting the enabling block.

- Most broadcast schemes and traceability schemes in the literature are described as unconditionally secure schemes. If the encryption function $e(\cdot)$ used in the scheme in this paper is addition in a finite field F_q, then our scheme is also unconditionally secure. However, the drawback of using the above unconditionally secure encryption scheme is that the resulting KPTS will a one-time scheme. On tho other hand, if we desire only computational security, then we can replace $e(\cdot)$ by any cryptosystem that is computationally secure against a known plaintext attack, and we will obtain a KPTS that can be used for many broadcasts. This simple modification can be applied to other one-time schemes described in previously published papers.

References

[1] S. Berkovits, How to broadcast a secret, *Advances in Cryptology: EUROCRYPT'91, Lecture Notes in Computer Science*, **547**(1992), 536-541.

[2] C. Blundo, and A. Cresti, Space requirement for broadcast encryption, *Advances in Cryptology: EUROCRYPT'94, Lecture Notes in Computer Science*, **950**(1995), 287-298.

[3] C. Blundo, L.A. Frota Mattos and D.R. Stinson, Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution, *Advances in Cryptology: CRYPTO'96, Lecture Notes in Computer Science*, **1109**(1996), 387-400.

[4] C.J. Colbourn and J.H. Dinitz, eds., *CRC Handbook of Combinatorial Designs*, CRC Press, Inc., 1996.

[5] B. Chor, A. Fiat and M. Naor, Tracing traitors, *Advances in Cryptology: CRYPTO'94, Lecture Notes in Computer Science* **839** (1994) 257 - 270.

[6] A. Fiat and M. Naor, Broadcast encryption, *Advances in Cryptology: CRYPTO'93, Lecture Notes in Computer Science*, **773**(1994), 480-491.

[7] K. Kurosawa and Y. Desmedt, Optimum traitor tracing and new direction for asymmetricity, to appear in *Advances in Cryptology: EUROCRYPT'98.*

[8] B. Pfitzmann, Trials of traced traitors, *Information Hiding, Lecture Notes in Computer Science*, **1174**(1996), 49-64.

[9] J.N. Staddon, *A combinatorial study of communication, storage and traceability in broadcast encryption systems*, PhD thesis, University of California at Berkeley, 1997.

[10] D.R. Stinson, An explication of secret sharing schemes, *Designs, Codes and Cryptography*, **2**(1992), 357-390.

[11] D.R. Stinson, On some methods for unconditionally secure key distribution and broadcast encryption, *Designs, Codes and Cryptography*, **12**(1997), 215-243

[12] D.R. Stinson and Tran van Trung, Some new results on key distribution patterns and broadcast encryption, to appear in *Designs, Codes and Cryptography.*

[13] D.R. Stinson and R. Wei, Combinatorial properties and constructions of traceability schemes and frameproof codes, *SIAM J. Discrete Math*, **11**(1998), 41-53.