An Application of Ramp Schemes to Broadcast Encryption

D. R. Stinson
Department of Computer Science and Engineering
University of Nebraska-Lincoln
Lincoln, NE 68588
stinson@bibd.unl.edu

R. Wei
Department of Mathematics and Statistics
University of Nebraska-Lincoln
Lincoln, NE 68588
rwei@cse.unl.edu

November 25, 1997

1 Introduction and definitions

Broadcast encryption schemes were first introduced in [1] and since then have been studied by several authors (see the bibliography of [5]). In [3], Fiat and Naor presented a very efficient broadcast encryption scheme. This scheme was generalized in [5], where the so-called "KIO construction" was proposed. The KIO construction was further considered in [6], where several applications using combinatorial designs were given. In [6], a threshold scheme is used to divide the secret into pieces called shares. In this note, we instead use a ramp scheme, which allows the information rates of the broadcast encryption scheme to be improved significantly.

1.1 One-time broadcast encryption scheme

We give an informal description of a *one-time broadcast encryption scheme* (or OTBES; for formal definitions, see [5, 6]). The participants in the scheme include a *trusted authority* (TA) and a set of n *users*, say $\mathcal{U} = \{1, 2, \cdots, n\}$. Let w be an integer such that $1 \leq w \leq n$. In a set-up stage, the TA generates and distributes secret information u_i to each user $i \in \mathcal{U}$. At a later time, the TA chooses a *privileged subset* $P \subseteq \mathcal{U}$, and then transmits an encrypted message, b_P, over a broadcast channel. We require that any user in P can decrypt b_P to obtain the (plaintext) message m_P, but no disjoint *forbidden subset* of size at most w can obtain any information on m_P. The privileged set P is assumed to be publicly known. Such a scheme will be called a *w-secure OTBES*.

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 a privileged set $P \subseteq \mathcal{U}$, let M_P denote the set of possible (plaintext) messages that might be broadcasted to P, and let B_P denote the set of possible broadcast messages (i.e., ciphertexts) for the set P.

For a given OTBES, we define the *information rate* to be

$$\rho = \min\left\{\frac{\log M_P}{\log U_i} : i \in P, P \subseteq \mathcal{U}\right\}.$$

and the *broadcast information rate* to be

$$\rho_B = \min\left\{\frac{\log M_P}{\log B_P} : P \subseteq \mathcal{U}\right\}.$$

(Note that all logarithms in this paper are defined to the base 2.)

In general, to decrease the size of the broadcast, i.e., to increase ρ_B, it is necessary to decrease ρ, and vice versa.

1.2 Orthogonal arrays

An *orthogonal array* OA(t,k,v) is a $v^t \times k$ array, $A = (a_{i,j})$, with entries from a v-set, Y, such that for any t-tuple $(u_1, u_2, \cdots, u_t) \in Y^t$ and for any t columns of A, say $\gamma_1, \gamma_2, \cdots, \gamma_t$, there is exactly one row of A in which the entry u_i occurs in column γ_i for all i, $1 \le i \le t$. Orthogonal arrays are well-studied combinatorial objects. A recent summary of existence results can be found in [2]. We will use the following well-known class of orthogonal arrays that can be constructed from Reed-Solomon codes.

Lemma 1.1 *For any prime power q, there exists an $OA(t,k,q)$ for all integers t and k such that $2 \le t \le q$ and $t \le k \le q+1$.*

1.3 Threshold schemes and ramp schemes

Let $\mathcal{X}$ be a set of b users, $\Gamma \subseteq 2^{\mathcal{X}}$ be a set of subsets of $\mathcal{X}$ called *authorized subsets*, and let $\Delta \subseteq 2^{\mathcal{X}}$ be a set of subsets of $\mathcal{X}$ called *unauthorized sets* such that $\Gamma \cap \Delta = \emptyset$. In a *secret sharing scheme*, the TA has a secret value denoted by K. The TA will distribute secret information (*shares*) to each user in $\mathcal{X}$ in such a way that any authorized subset can compute K from the shares they jointly hold, but no unauthorized subset can compute any information about K.

Let $0 < c < r \le b$. A (c,r,b)-*ramp scheme* is a secret sharing scheme in which the authorized subsets are all the subsets of $\mathcal{X}$ with cardinality at least r, and the unauthorized subsets are all the subsets of $\mathcal{X}$ with cardinality at most c. When $c = r-1$, the ramp scheme is a *threshold scheme.*

It is straightforward to construct a ramp scheme from an orthogonal array. We present the construction from [4]. Suppose $A = (a_{i,j})$ is an OA$(r, b+r-c, q)$ which is public knowledge. The secret information is $K \in (GF(q))^{r-c}$. The shares are computed as follows: The TA chooses a row h of A such that the restriction of A to the last $r-c$ columns holds the $(r-c)$-tuple K in row h (given any $K \in (GF(q))^{r-c}$, it is easy to see that there are exactly q^c such rows). The TA then gives user i the share $s_i = a_{h,i}$ (for $1 \le i \le b$). Since any r of the shares determine a unique row of A, it follows that any r users can compute K. However, no c shares provide any information about K, since these c values occur in exactly one row of A together with any possible secret $(r-c)$-tuple in the last $r-c$ columns. Thus we have a (c,r,b)-ramp scheme.

The following result is an immediate consequence of this construction and Lemma 1.1.

Theorem 1.2 *[4] Suppose $0 < c < r < b$, and suppose that q is a prime power such that $q \geq b + r - c - 1$. Then there exists a (c, r, b)-ramp scheme in $GF(q)$.*

2 The broadcast encryption scheme

In this section, we introduce our modification of the KIO construction. The strategy employed in the KIO construction ([5, 6]) and in the earlier Fiat-Naor scheme ([3]) is that the secret message is divided into shares, and then each share is encrypted. Each member in a privileged set P can decrypt an authorized set of shares, which then allow the secret to be computed. However, a disjoint forbidden set of size at most $w - 1$ can only decrypt an unauthorized set of shares.

We will use a certain type of set system, which was defined in [6] as follows. An (n, b, r, λ)-*design* is a pair $(X, \mathcal{B})$ which satisfies the following properties:

1. X is a set of *points* with $|X| = n$;
2. $\mathcal{B}$ is a set of b subsets of X called *blocks*;
3. every point of X occurs in exactly r blocks;
4. every pair of points occurs in at most λ blocks.

An (n, b, r, λ)-design is called a *w-threshold* design provided that, for all $F \subseteq X$ such that $|F| \leq w$, we have:

$$|\{B \in \mathcal{B} : |F \cap B| \geq 2\}| \leq r - 1.$$

Now we state our main result, which is similar to [6, Theorem 4.2], the main difference being that the threshold scheme is replaced by a ramp scheme. The resulting information rates are increased by a factor of $r - c$.

Theorem 2.1 *Suppose $(X, \mathcal{B})$ is a (n, b, r, λ)-design which is w-threshold. Let*

$$c = \max\{|\{B \in \mathcal{B} : |F \cap B| \geq 2\}| : F \subseteq X, |F| \leq w\}.$$

If $1 \leq c \leq r-1$, then there exists a w-secure OTBES for a set $\mathcal{U}$ of n users, with information rate at least

$$\frac{r - c}{r + \lambda(n - 1)}$$

and broadcast information rate

$$\frac{r - c}{b.}$$

Remarks

1. When $c = r - 1$, Theorem 2.1 reduces to [6, Theorem 4.2]. However, in many applications it is the case that $c < r - 1$, so our construction often allows improved information rates.

2. The value c computed above satisfies the following inequality:

$$c \leq \lambda \binom{w}{2}. \tag{1}$$

We briefly outline the construction as follows.

1. Let q be a prime power, $q \geq b + r - c - 1$. The TA constructs a Fiat-Naor key predistribution scheme (see [3]) with respect to every block $B \in \mathcal{B}$. Thus, for each B, the TA chooses $|B| + 1$ secret values, denoted u_B and $u_{B,x}$ ($x \in B$). These are all elements of $GF(q)$. The value u_B is given to every user in B, and the value $u_{B,x}$ is given to each user in $B \backslash \{x\}$.

2. The TA uses a (c, r, b)-ramp scheme implemented over $GF(q)$ to constuct shares for a secret message $m_P \in (GF(q))^{r-c}$. (This is where we require $q \geq b + r - c - 1$; see Theorem 1.2.) The shares are denoted s_B ($B \in \mathcal{B}$).

3. For each $B \in \mathcal{B}$, the TA computes a key

$$k_B = u_B + \sum_{x \in B \backslash P} u_{B,x},$$

where addition is performed in $GF(q)$. The k_B's have the property that an individual user i can compute k_B if and only if $i \in P \cap B$, and any two or more users in B can compute k_B (see [3]).

4. For every $B \in \mathcal{B}$, the key k_B is used to encrypt s_B, as follows:

$$b_B = s_B + k_B,$$

where addition is performed in $GF(q)$.

5. The broadcast for the privileged set P is:

$$b_P = (b_B : B \in \mathcal{B}).$$

Each user $x \in P$ can compute r keys, namely those in the set $\{k_B : x \in B\}$. Thus x can decrypt r shares, from which the secret message can be determined. However, a disjoint forbidden set, F can determine only the keys k_B such that $|F \cap B| \geq 2$. There are at most c such keys, and thus the shares that can be decrypted by F are an unauthorized set of shares. Thus F cannot obtain any information about the secret message m_P.

Now we look at the information rates of this scheme. Suppose the blocks containing x are $B_1, B_2, \cdots, B_r$. Then x needs to store $\sum_{i=1}^{r} |B_i|$ secret values (elements of $GF(q)$). Since every pair of points occurs in at most λ blocks, we have that

$$\sum_{i=1}^{r} (|B_i| - 1) \leq \lambda(n - 1).$$

Hence

$$\sum_{i=1}^{r} |B_i| \leq r + \lambda(n-1).$$

Thus we have

$$\rho \geq \frac{r-c}{r+\lambda(n-1).}$$

The broadcast consists of b elements from $GF(q)$ and the message is an $(r-c)$-tuple of elements from $GF(q)$. Hence, we see that

$$\rho_B = \frac{r-c}{b}.$$

3 An application

In [5, 6], various combinatorial designs, such as Steiner systems, universal hash families and orthogonal arrays, have been used to construct w-secure OTBES. Simple computations show that $r-c>1$ in all these constructions. Hence, using Theorem 2.1, both the information rate and broadcast information rate of the OTBES will increase from the rates obtained in [5, 6].

As an example, we modify a construction from [6] that uses threshold designs derived from orthogonal arrays.

Lemma 3.1 *Suppose that Q is a prime power and $t \leq Q$ is a positive integer. Suppose also that $n \leq Q^t$ and $Q > (t-1)\binom{w}{2}$. Then there exists a $(n, Q^2, Q, t-1)$ w-threshold design.*

Proof. Let $A = (a_{i,j})$ be an $\mathrm{OA}(t, Q, Q)$ defined on $GF(Q)$, which exists by Lemma 1.1. Define a set system $(X, \mathcal{B})$, where $X = GF(Q) \times \{1, \cdots, Q\}$ and

$$\mathcal{B} = \{\{(a_{i,1}, 1), \cdots, (a_{i,Q}, Q)\} : 1 \leq i \leq Q^t\}.$$

(The design $(X, \mathcal{B})$ is a *transversal design.*) It is easy to see that $|X| = Q^2$, $|\mathcal{B}| = Q^t$, every block in $\mathcal{B}$ has size Q, and any two blocks intersect in at most $t-1$ points. Therefore, the dual incidence structure, $(\mathcal{B}, X)$, forms the desired $(n, Q^2, Q, t-1)$-design. □

Since we have $c \leq \binom{w}{2}(t-1)$ (see Eq. (1)), we obtain the following result by applying Theorem 2.1.

Theorem 3.2 *Suppose that Q is a prime power and $t \leq Q$ is a positive integer. Suppose also that $n \leq Q^t$ and $Q > (t-1)\binom{w}{2}$. Then there exists a w-secure OTBES for a set of n users, with information rate at least*

$$\frac{Q - \binom{w}{2}(t-1)}{Q + (t-1)(n-1)}$$

and broadcast information rate at least

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

We illustrate the application of Theorem 3.2. For given integers n and w, we construct a w-secure OTBES for n users by choosing a Q and t appropriately. Suppose we take

$$Q \approx w^2 \log n \quad \text{and} \quad t \approx \log n.$$

It is easy to check that $Q^t > n$ and $Q > t$. The (n, b, r, λ) design that is constructed by application of Lemma 3.1 is a w-threshold design in which

$$\begin{aligned} b &\approx w^4 (\log n)^2, \\ r &\approx w^2 \log n, \\ \lambda &\approx \log n, \quad \text{and} \\ c &\approx \binom{w}{2} \log n. \end{aligned}$$

Apply Theorem 3.2 to construct a w-secure OTBES. The information rate and broadcast information rates are as follows:

$$\rho \approx \frac{w^2}{2(w^2+n)} \quad \text{and} \quad \rho_B \approx \frac{1}{2w^2 \log n}.$$

This is a significant improvement of the scheme in [6, Section 5.4] in which ρ and ρ_B are both smaller by a factor of

$$r - c \approx \frac{w^2}{2} \log n.$$

It is also a considerable improvement compared to the scheme of Fiat and Naor ([3, Theorem 5]), in which

$$\rho \approx \frac{1}{wn \log n} \quad \text{and} \quad \rho_B \approx \frac{1}{w^3 \log n}.$$

Acknowledgment

This research is supported by NSF grant CCR-9610138.

References

[1] S. Berkovits. How to broadcast a secret, in "Advances in Cryptology – EUROCRYPT '91", Springer-Verlag, Berlin, 1992, pp. 536-541.

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

[3] A. Fiat and M. Naor. Broadcast encryption, in "Advances in Cryptology – CRYPTO '93", Springer-Verlag, Berlin, 1994, pp. 480-491.

[4] W.-A. Jackson and K. M. Martin. A combinatorial interpretation of ramp schemes, *Austral. J. Combinatorics* **14** (1996), 51-60.

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

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