Improving the trade-off between storage and communication in broadcast encryption schemes

Ignacio Gracia, Sebastià Martín and Carles Padró

Dep. Matemàtica Aplicada IV. Universitat Politècnica de Catalunya
Campus Nord, c/Jordi Girona, 1-3, 08034 Barcelona
e-mail: {ignacio,smartin,matcpl}@mat.upc.es

July 31, 2001

Abstract

The most important point in the design of broadcast encryption schemes (BESs) is obtain a good trade-off between the amount of secret information that must be stored by every user and the length of the broadcast message, which are measured, respectively, by the information rate ρ and the broadcast information rate ρ_B. In this paper we present a simple method to combine two given BESs in order to improve the trade-off between ρ and ρ_B by finding BESs with good information rate ρ for arbitrarily many different values of the broadcast information rate ρ_B. We apply this technique to threshold (R,T)-BESs and we present a method to obtain, for every rational value $1/R \leq \rho_B \leq 1$, a (R,T)-BES with optimal information rate ρ among all (R,T)-BESs that can be obtained by combining two of the (R,T)-BESs proposed by Blundo et al. [7].

Keywords: Cryptography, Key distribution, Broadcast encryption, Key predistribution schemes.

1 Introduction

This paper deals with key distribution methods that are suitable for situations in which some groups of users in a network need to securely and privately communicate between them. This communication can be done efficiently by using a symmetric encryption algorithm. The main problem is that symmetric algorithms require that the users in the group stablish a common key before starting the communication. Usually, an *on-line key distribution center* is used, which provides a common key to every user in a group just before these users need to communicate between them. Other solutions are based on the use of an *off-line key distribution center*, which, in a previous phase, distributes some secret information among all users in the network. Every user will use the information it received to compute the common keys associated with the groups it belongs to. See [13] for an overview on key distribution systems.

Key predistribution schemes (KPSs) and broadcast encryption schemes (BESs) have been introduced as key distribution systems that can be used by an off-line key distribution center.

A *key predistribution scheme* (KPS), which is called a *zero-message broadcast encryption scheme* in [4, 8], is a method by which a trusted authority (TA) distributes secret information among a set of users in such a way that every user is able to compute the keys corresponding to the *privileged groups* it belongs to. Besides, certain coalitions of users (*forbidden subsets*) outside a privileged group must not be able to find any information on the value of the key associated with that group. A *broadcast encryption scheme* (BES) consists of two phases. In the first one, in a similar way as in a KPS, some secret information is sent by the TA to every user. In the second phase, the TA broadcasts through an open channel an encrypted message in such a way that every user in some privileged subset is able to decrypt it. This message will be used by the users in this group as a common key for secure communication. The users in a forbidden subset cannot obtain any information on the message that has been sent by the TA. In general, every user must receive a smaller amount of secret information in a BES that in a KPS. This is due to is less than Broadcasting some public information in a BES makes it possible, in general, to reduce KPS. We are interested here in *unconditionally secure schemes*, that is, schemes whose security does not depend on any computational assumption. The broadcast encryption schemes we consider in this paper are called *one-time broadcast encryption schemes* in [9, 14] because just one single broadcast can be securely made by such schemes. This is due to the fact that the broadcast message can provide to a user in a privileged subset some information about the secret information of the other users in this subset.

Key predistribution schemes were introduced by Blom [3] and have been also considered in [4, 5, 8, 9, 11, 14, 15, 16]. The first broadcast encryption schemes were proposed by Berkovits [2] and Fiat and Naor [8]. Afterwards, several authors have studied these schemes [1, 4, 6, 7, 9, 10, 12, 14, 15]. A good survey on these subjects can be found in [14].

The *specification structure* Γ of a KPS or a BES is the family of all pairs (P, F) of subsets of the set of users $\mathcal{U}$ such that every user in P must be able to compute a common key that will remain unknown to the coalition F. A subset $P \subset \mathcal{U}$ is a *privileged subset* of the specification structure Γ if there exists $F \subset \mathcal{U}$ such that $(P, F) \in \Gamma$. The family of the privileged subsets of Γ is denoted by $\mathcal{P}(\Gamma)$. A Γ-KPS and a Γ-BES are, respectively, a key predistribution scheme and a broadcast encryption scheme with specification structure Γ. The specification structures that have been considered in most previous works about key predistribution and broadcast encryption are in the form $\Gamma = (\mathcal{P}, \mathcal{F}) = \{(P, F) \in \mathcal{P} \times \mathcal{F} \, : \, P \cap F = \emptyset\}$, where $\mathcal{P}, \mathcal{F} \subset 2^{\mathcal{U}}$. *Threshold specification structures*, that is, the specification structures in which $\mathcal{P}$ and $\mathcal{F}$ consist of the subsets of $\mathcal{U}$ with some given number of users have received considerable attention. If $\mathcal{P}$ consists of all subsets of $\mathcal{U}$ with cardinality R and $\mathcal{F}$ is formed by the coalitions of at most T users, a $(\mathcal{P}, \mathcal{F})$-KPS (BES) is called also a (R, T)-KPS (BES). In a $(\leq R, T)$-KPS (BES), the family of privileged subsets consists of all subsets of $\mathcal{U}$ with cardinality at most R.

The information rate and the broadcast information rate are the main parameters to measure the efficiency of a broadcast encryption scheme. The *information rate* of a BES (or a KPS) is the ratio between the length in bits of the secret message (or the common key) and the maximum length of the secret information received by the users. In a BES, one has to consider also the length of the encrypted message to be broadcast by the TA. The ratio between the length of the secret message and the broadcast message is the *broadcast information rate*.

In a BES, the information rate and the broadcast information rate can not be optimized at the same time. In general, the information rate must decrease in order to increase the broadcast information rate.

An easy way to obtain a broadcast encryption scheme is to distribute a random value $u_i \in G$, where G is an Abelian group, to every user $i \in \mathcal{U}$. In order to send a secret message $k_P \in G$ to the users in a privileged subset P, the TA broadcasts the message $m_P = (m_i)_{i \in P}$, where $m_i = k_p + u_i$. In this case, the information rate is maximum, $\rho = 1$, but the broadcast information rate can be very small, $\rho_B = 1/(\max_{P \in \mathcal{P}(\Gamma)} |P|)$.

On the other hand, a Γ-BES with maximum broadcast information rate $\rho_B = 1$ can be constructed from any Γ-KPS such that, for every privileged subset P, the common key u_P is an element of an Abelian group G. In that case, the broadcast message is $m_P = k_P + u_P$, where u_P is the common key that can be computed by the users in P in the Γ-KPS. The information rate of this Γ-BES coincides with the information rate of the Γ-KPS.

One of the problems that have been most considered in previous works about broadcast encryption is obtaining a good trade-off between the information rate and the broadcast information rate. That is, given a specification structure Γ, one is interested in finding a family of Γ-BESs between the two extremal cases above with an optimal relation between their information rate and broadcast information rate. In other words, a family of Γ-BESs whose information rates verify $\rho^* < \rho < 1$ and $1/R < \rho_B < 1$, where ρ^* is the best information rate for a Γ-KPS and $R = \max_{P \in \mathcal{P}(\Gamma)} |P|$, such that it is not possible to improve *simultaneously* both information rates in any of these schemes.

Several bounds have been given for the information rate of a KPS [4, 9]. The optimality of the $(\leq R, T)$-KPSs proposed in [5, 8] is derived from these bounds. Blundo, Frota-Mattos and Stinson present in [6] a family of (R, T)-BESs obtaining a trade-off between the information rate and the broadcast information rate. The BESs in this family have broadcast information rate $\rho_B = \frac{r}{R}$, $r \in \{1, \ldots, R\}$. These BESs are constructed by using the optimal threshold KPSs given in [5]. Nevertheless, no general bounds have been found about the relation between the information rate and the broadcast information rate of a BES in order to prove or disprove the optimality of the BESs in [6].

The general problem that would be interesting to solve is the following: given a specification structure Γ and a value of $\rho_B \in (0, 1)$, to find a Γ-BES with broadcast information rate ρ_B and optimal information rate ρ. In other words, to find a method to determine the values of the function

$$\rho^*(\Gamma, \rho_B) = \sup\{\, \rho \,:\, \text{there exists a } \Gamma\text{-BES with information rates } \rho,\, \rho_B \,\}.$$

At the moment, this is still an open problem, but we present in this work some contributions to the solution of this problem.

The main result of this paper is to obtain (R, T)-BESs with $\rho_B = h$, for any rational value $h \in [1/R, 1]$. This will be attained by applying to the (R, T)-BESs given by Blundo et al. in [7] a simple combination method we present in this paper. We determine, among all possible combinations, the best one in order to to obtain the maximum information rate. In this way, we obtain a function $\rho = g(\rho_B)$, which provides a lower bound on $\rho^*(\Gamma, \rho_B)$, for $\Gamma = (R, T)$ and for every rational value of $\rho_B \in [1/R, 1]$.

The main concepts about broadcast encryption schemes as well as the notation that will be used are presented in Section 2. A simple method to combine two given Γ-BESs is given in Sectioncombi. Section 4 is devoted to construct a family of (R, T)-BESs by applying the combination method provided in the previous section to the BESs given by Blundo et al. in [6].

2 Broadcast encryption schemes

Let Γ be a specification structure on a set of users $\mathcal{U} = \{1, 2, \ldots, N\}$. In a *broadcast encryption scheme* with specification structure Γ, or Γ-BES for short, every user $i \in \mathcal{U}$ receives from the TA some secret information $u_i \in U_i$. Afterwards, for any privileged subset $P \in \mathcal{P}(\Gamma)$ and for any possible value of a secret message (or secret session key) $k_P \in \mathcal{K}$, the TA sends by the broadcast channel some information $m_P \in \mathcal{M}_P$ such that every user $i \in P$ can compute the message k_P from its secret information u_i and the broadcast information m_P. On the other hand, any coalition $F = \{j_1, \ldots, j_s\}$ such that $(P, F) \in \Gamma$ must not obtain any information about k_P from the secret information $(u_{j_1}, \ldots, u_{j_s})$ received by the users in F and the public information m_P. That is,

$$p\,(K_P = k_P \,|\, U_{j_1} = u_{j_1}, \ldots, U_{j_s} = u_{j_s}, M_P = m_P) = p\,(K_P = k_P)$$

where K_P, U_{j_ℓ} and M_P are, respectively, the random variables corresponding to the secret message k_p, the secret information u_{j_ℓ} and the broadcast message m_p.

A more formal definition of broadcast encryption schemes can be given by using the entropy function. See [17] for an introduction to entropy and its properties. For any subset $P = \{i_1, \ldots, i_s\} \subset \mathcal{U}$, let us consider $U_P = U_{i_1} \times \cdots \times U_{i_s}$. We can suppose that the TA chooses a value in $U_{\mathcal{U}}$, according to some probability distribution, in order to distribute the secret information among the users and, afterwards, a value in M_P in order to do the broadcast. A Γ-*broadcast encryption scheme* must satisfy the following conditions:

1. The secret message k_P must be independent from the secret values distributed in the predistribution phase, that is,

$$H(K_P \,|\, U_{\mathcal{U}}) = H(K_P).$$

2. Any participant $i \in P$ in a qualified subset $P \in \mathcal{P}(\Gamma)$ is able to compute the common key k_P from its secret information u_i and the broadcast message m_p:

$$H(K_P \,|\, U_i M_P) = 0.$$

3. Any coalition F such that $(P, F) \in \Gamma$ can not obtain any information on k_P, that is,

$$H(K_P \,|\, U_F M_P) = H(K_P).$$

In this paper we are going to consider only BESs with uniform probability distributions on $\mathcal{K}$, U_i, $\overline{U}_{\mathcal{U}}$ and M_P where $\overline{U}_{\mathcal{U}} \subset U_{\mathcal{U}}$ is the set of all possible combinations $(u_i)_{1 \le i \le N}$ of secret values received by the users in $\mathcal{U}$. In that case, even joining together the secret information $(u_j)_{j \in F}$ of the users in any coalition F, such that $(P, F) \in \Gamma$, and the broadcast message m_P, all values of the secret $k_P \in \mathcal{K}$ are equiprobable.

The *information rate* ρ of a BES is the ratio between the length of the secret message k_P and the maximum length of the secret information received by a user, that is,

$$\rho = \frac{k}{u} \quad \text{, where} \quad k = \log|\mathcal{K}| \quad \text{and} \quad u = \max_{i \in \mathcal{U}} \log|U_i|$$

The *broadcast information rate* ρ_B of a BES is defined as the ratio between the length of the secret message k_P and the maximum length of the broadcast message m_P:

$$\rho_B = \frac{k}{m} \quad \text{, where } m = \max_{P \in \mathcal{P}(\Gamma)} \log|M_P|$$

3 Combination of two different Γ-BESs

We present in this section a method, which is based on a simple combination technique, of designing a family of Γ-BES from two different BESs with the same specification structure Γ.

Let us consider Σ_1 and Σ_2 two Γ-BESs with the following properties:

1. In the Γ-BES Σ_r, where $r = 1, 2$, every user receives the same amount of secret information in the predistribution phase. That is, $\log|U_i^r| = u_r$ for every user $i \in \mathcal{U}$ and for $r = 1, 2$.

2. In both BESs Σ_1 and Σ_2, the broadcast messages corresponding to all qualified subsets have the same length. It will be denoted by m_1 and m_2, respectively.

3. $\rho_{B1} < \rho_{B2}$ and $\rho_1 > \rho_2$, where ρ_1, ρ_{B_1} and ρ_2, ρ_{B_2} are the information rates of the two BESs.

We can design a new Γ-BES combining the previous two Γ-BESs Σ_1 and Σ_2 as follows:

- The secret information of user $i \in \mathcal{U}$ will be (u_i^1, u_i^2), where u_i^1 and u_i^2 are the secret informations of user $i \in \mathcal{U}$ corresponding, respectively, to Σ_1 and Σ_2.
- The encrypted broadcast intended to users in a privileged set $P \in \mathcal{P}$ will be (m_P^1, m_P^2), where m_P^1 and m_P^2 are the broadcast messages in each BES.
- The secret intended to users in a privileged set $P \in \mathcal{P}$ will be (k_P^1, k_P^2), where k_P^1 and k_P^2 are the secrets in each BES.

The information rates of this new Γ-BES are easily computed:

$$\rho_3 = \frac{k_1 + k_2}{u_1 + u_2}, \qquad \rho_{B3} = \frac{k_1 + k_2}{m_1 + m_2},$$

where $k_r = \log |\mathcal{K}_r|$ is the length of the secret message in the BES Σ_r. Since

$$\rho_1 = \frac{k_1}{u_1}, \qquad \rho_{B1} = \frac{k_1}{m_1}$$

and

$$\rho_2 = \frac{k_2}{u_2}, \qquad \rho_{B2} = \frac{k_2}{m_2},$$

we observe that $\rho_{B1} < \rho_{B3} < \rho_{B2}$ and $\rho_1 > \rho_3 > \rho_2$.

Analogously, for any pair of positive integers $\alpha, \beta > 0$, we can consider a more general combination of the two Γ-BESs by combining α copies of the BES Σ_1 with β copies of Σ_2. We obtain in this way a Γ-BES with information rates

$$\rho_3 = \frac{\alpha k_1 + \beta k_2}{\alpha u_1 + \beta u_2} \qquad \rho_{B3} = \frac{\alpha k_1 + \beta k_2}{\alpha m_1 + \beta m_2}$$

The inequalities $\rho_{B1} < \rho_{B3} < \rho_{B2}$ and $\rho_1 > \rho_3 > \rho_2$ still hold. We can construct in this way an infinite family of Γ-BESs with information rate $\rho \in (\rho_2, \rho_1)$ and broadcast information rate $\rho_B \in (\rho_{B1}, \rho_{B2})$.

4 A new family of (R, T)-BESs

In this section, we apply the combination method in section 3 to the family of (R, T)-BESs designed by Blundo et al. in [7].

Theorem 4 in [7] states that, for every integer $r = 1, 2, \ldots, R$, there exists an (R, T)-BES Σ_r such that

$$k = \binom{R-1}{r-1}, \quad u = \binom{R+T-1}{r-1}, \quad m = \binom{R}{r}.$$

Therefore, we have a family of BESs with information rates

$$\rho_{Br} = \frac{r}{R} \text{ and } \rho_r = \binom{R-1}{r-1} \binom{R+T-1}{r-1}^{-1}.$$

From these (R,T)-BESs, we obtain lower bounds on $\rho^*(\Gamma, \rho_B) = \rho^*(R,T,\rho_B)$ for some values of ρ_B. Namely,

$$\rho^*(R,T,r/R) \geq \binom{R-1}{r-1} \binom{R+T-1}{r-1}^{-1} = \binom{T+R(1-(r/R))}{T} \rho(R,T) \quad (1)$$

where $r = 1, 2 \ldots, R$ and $\rho(R,T) = \binom{R+T-1}{R-1}^{-1}$ is the optimal information rate of a (R,T)-KPS.

Observe that this lower bound can be extended to a continous function defined on the interval $[1/R, 1]$:

$$\Phi(x) = \binom{T+R(1-x)}{T} \rho(R,T) = \frac{y(y-1)\cdots(y-T+1)}{T!} \rho(R,T), \qquad (2)$$

where $y = T + R(1-x)$.

Next theorems provided a method to construct (R,T)-BESs whose broadcast information rates achieve any rational value $1/R \leq \rho_B \leq 1$. In this way, we will obtain lower bounds on $\rho^*(R,T,\rho_B)$ for these values of ρ_B.

Theorem 1 *Let us consider two (R,T)-BESs, Σ_{r_1} and Σ_{r_2}, where $1 \leq r_1 < r_2 \leq R$. Then, for every rational value*

$$\rho_B \in \left[\frac{r_1}{R}, \frac{r_2}{R}\right],$$

we can combine Σ_{r_1} and Σ_{r_2} to obtain an (R,T)-BES with broadcast information rate ρ_B and information rate $\rho \in [\rho_{r_2}, \rho_{r_1}]$.

Proof: Let us consider $\rho_{Br_1} = \dfrac{k_1}{m_1}$ and $\rho_{Br_2} = \dfrac{k_2}{m_2}$ and a rational value $\rho_B \in (\rho_{Br_1}, \rho_{Br_2})$. We want to find positive integers α and β such that

$$\rho_B = \frac{\alpha k_1 + \beta k_2}{\alpha m_1 + \beta m_2}.$$

Let us take $\lambda = \dfrac{\alpha}{\beta}$. From the equation $\rho_B = \dfrac{\lambda k_1 + k_2}{\lambda m_1 + m_2}$, we deduce that $\lambda = \dfrac{k_2 - m_2 \rho_B}{m_1 \rho_B - k_1}$. Since $\rho_B \in (\rho_{Br_1}, \rho_{Br_2})$, then $\lambda > 0$. Moreover, since m_1, m_2, k_1 and k_2 are integer numbers, λ is a rational number. If $\rho_B = r_1/R$, we have to take $\alpha = 1$ and $\beta = 0$, and we consider $\alpha = 0$ and $\beta = 1$ if $\rho_B = r_2/R$. ■

For every rational value $\rho_B \in (\rho_{Br_1}, \rho_{Br_2})$, we denote by $\Sigma(r_1, r_2, \rho_B)$ the (R,T)-BES with broadcast information rate that, according to Theorem 1, is obtained by combining Σ_{r_1} and Σ_{r_2}. Next, we are interested in determining, for every rational value $\rho_B \in (1/R, 1)$, the values of r_1 and r_2 that maximize the information rate of the (R,T)-BES $\Sigma(r_1, r_2, \rho_B)$.

Theorem 2 *Let us consider a rational value*

$$\rho_B \in \left[\frac{1}{R}, 1\right].$$

Then, the maximum information rate of the (R,T)*-BESs in the form* $\Sigma(r_1, r_2, \rho_B)$ *is obtained for* $r_1 = \lfloor R\rho_B \rfloor$ *and* $r_2 = r_1 + 1$.

Proof: Let us consider $r \in \{1, 2 \ldots, R-2\}$ and two integers α, β with $1 \leq \alpha < \beta \leq R - r$. Let ρ_B be a rational value in the interval $\left(\frac{r}{R}, \frac{r+\alpha}{R}\right]$. We are going to prove next that the (R,T)-BES $\Sigma(r, r+\alpha, \rho_B)$ has better information rate than the (R,T)-BES $\Sigma(r, r+\beta, \rho_B)$. Let us consider $r_1 = r$, $r_2 = r + \alpha$ and $r_3 = r + \beta$, and let

$$\rho_1 = \frac{k_1}{u_1}, \qquad \rho_{B1} = \frac{k_1}{m_1} = \frac{r_1}{R}$$

and

$$\rho_2 = \frac{k_2}{u_2}, \qquad \rho_{B2} = \frac{k_2}{m_2} = \frac{r_2}{R}$$

be, respectively, the information rates of the (R,T)-BESs Σ_{r_1} and Σ_{r_2}. Since $\rho_B \in \left(\frac{r_1}{R}, \frac{r_2}{R}\right]$, there exists $\lambda \geq 0$ such that $\rho_B = \frac{\lambda k_1 + k_2}{\lambda m_1 + m_2}$. Then, $\rho = \frac{\lambda k_1 + k_2}{\lambda u_1 + u_2}$ is the information rate of $\Sigma(r_1, r_2, \rho_B)$. The previous equalities allow to express ρ as a function of ρ_B. Namely,

$$\rho = f(\rho_B) = \frac{(k_2 m_1 - k_1 m_2)\rho_B}{(u_2 m_1 - u_1 m_2)\rho_B - (u_2 k_1 - u_1 k_2)} = \frac{a_2 \rho_B}{b_2 \rho_B - c_2}.$$

Considering the (R,T)-BESs in the form $\Sigma(r_1, r_3, \rho_B)$ we obtain, analogously,

$$\rho = g(\rho_B) = \frac{(k_3 m_1 - k_1 m_3)\rho_B}{(u_3 m_1 - u_1 m_3)\rho_B - (u_3 k_1 - u_1 k_3)} = \frac{a_3 \rho_B}{b_3 \rho_B - c_3}.$$

Let us observe that $a_2, b_2, c_2, a_3, b_3, c_3 > 0$. It is enough to prove that $f(x) > g(x)$ for all $x \in \left(\frac{r_1}{R}, \frac{r_2}{R}\right]$. Let us consider the function $q(x) = \frac{f(x)}{g(x)}$, derivable in the interval $\left[\frac{r_1}{R}, \frac{r_2}{R}\right]$. The derivative of this function is

$$q'(x) = \frac{a_2(b_2 c_3 - b_3 c_2)}{a_3(b_2 x - c_2)^2}.$$

Then $q'(x)$ has constant sign, and therefore $q(x)$ is a monotone function in the above interval. Since $q(k_1/m_1) = 1$, we only need to find a value $x_0 > k_1/m_1$ such that $q(x_0) > 1$, that is, such that $f(x_0) > g(x_0)$.

Let us consider $x_0 = \frac{r_2}{R} = \frac{k_2}{m_2}$. Then,

$$f\left(\frac{r_2}{R}\right) = \frac{(k_2 m_1 - k_1 m_2) r_2}{u_2 m_1 (r_2 - r_1)} \quad \text{and} \quad g\left(\frac{r_2}{R}\right) = \frac{(k_3 m_1 - k_1 m_3) r_2}{u_3 m_1 (r_2 - r_1) + u_1 m_3 (r_3 - r_2)}.$$

Now,

$$f\left(\frac{r_2}{R}\right) > g\left(\frac{r_2}{R}\right) \Longleftrightarrow (r_3 - r_1)\frac{u_2}{m_2} < (r_2 - r_1)\frac{u_3}{m_3} + (r_3 - r_2)\frac{u_1}{m_1}. \qquad (3)$$

In our case,

$$u_1 = \binom{R+T-1}{r-1}, \qquad u_2 = \binom{R+T-1}{r+\alpha-1}, \qquad u_3 = \binom{R+T-1}{r+\beta-1},$$

$$m_1 = \binom{R}{r}, \qquad m_2 = \binom{R}{r+\alpha}, \qquad m_3 = \binom{R}{r+\beta}.$$

Replacing in (3) and simplifying, we obtain the following inequality:

$$0 < (R-r)\cdots(R-r-\beta+1)(\beta-\alpha)r + (R+T-r)\cdots(R+T-r-\alpha+1)A,$$

where

$$A = \alpha(r+\beta)(R+T-r-\alpha)\cdots(R+T-r-\beta+1) - \beta(r+\alpha)(R-r-\alpha)\cdots(R-r-\beta+1).$$

Equivalently,

$$0 < (R-r-\alpha)\cdots(R-r-\beta+1)(\beta-\alpha)r + \frac{R+T-r}{R-r}\cdots\frac{R+T-r-\alpha+1}{R-r-\alpha+1}A.$$

Since $(R+T-k)/(R-k) > 1$ for every $k \geq 0$, then it suffices to prove the following inequality

$$0 < (R-r-\alpha)\cdots(R-r-\beta+1)(\beta-\alpha)r + A,$$

which is equivalent to

$$0 < r(\beta-\alpha) + \alpha(r+\beta)\frac{R+T-r-\alpha}{R-r-\alpha}\cdots\frac{R+T-r-\beta+1}{R-r-\beta+1} - \beta(r+\alpha).$$

The previous inequality holds if

$$0 \leq r(\beta-\alpha) + \alpha(r+\beta) - \beta(r+\alpha),$$

which is obviously satisfied.

Analogous computations show that, for every $r \in \{3, \ldots, R\}$, for every pair of integers α, β with $1 \leq \alpha < \beta < r$ and for every $\rho_B \in \left[\frac{r-\alpha}{R}, \frac{r}{R}\right)$, the

(R,T)-BES $\Sigma(r-\alpha, r, \rho_B)$ has better information rate than the (R,T)-BES $\Sigma(r-\beta, r, \rho_B)$.

Finally, as a consequence of the partial results previously proved, we can conclude that given a rational value

$$\rho_B \in \left[\frac{1}{R}, 1\right],$$

the maximum information rate of the (R,T)-BESs in the form $\Sigma(r_1, r_2, \rho_B)$ is obtained for $r_1 = \lfloor R\rho_B \rfloor$ and $r_2 = r_1 + 1$. ■

Examples

We are going to show two graphic examples of the optimal value of ρ, obtained by combining two Blundo et al. (R,T)-BESs, for several values of ρ_B.

We represent ρ_B in the x axis and $\log \rho$ in the y axis. Large dots correspond to values of ρ_B for which there exists a Blundo et al. (R,T)-BES, while small dots correspond to the optimal combination of two Blundo et al. (R,T)-BESs given by Theorem 1. The continous curve is the graph of the function $\Phi(x)$ defined in Equation (2).

In Figure 1, we consider $(R,T) = (5,3)$, and $(R,T) = (7,12)$ in Figure 2.

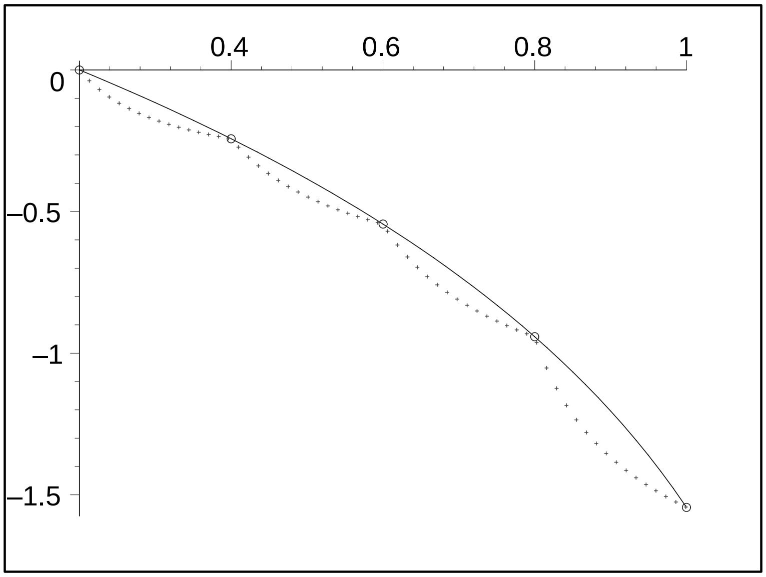

Figure 1: Optimal combination of two Blundo et al. $(5,3)$-BES

5 Conclusions and open problems

In this paper we have obtained the following results:

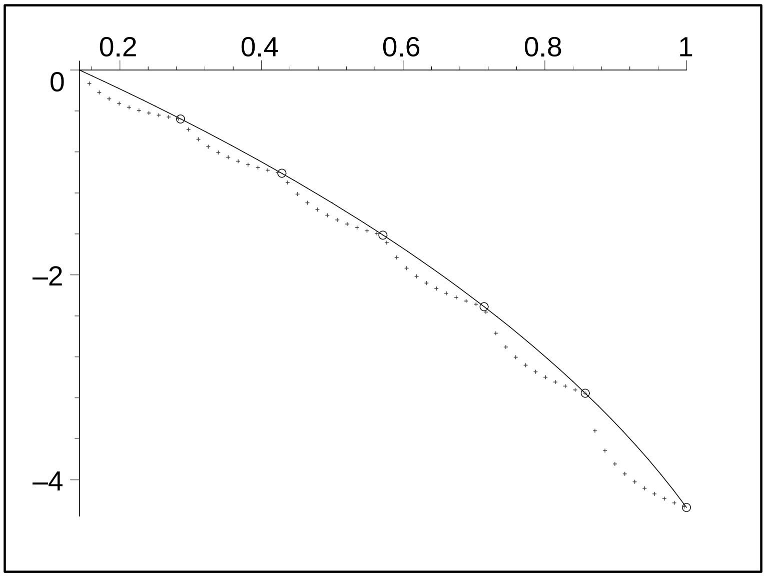

Figure 2: Optimal combination of two Blundo et al. $(7, 12)$-BES

- Given a specification structure Γ and two Γ-BESs with parameters $\rho_{B_1} < \rho_{B_2}$ and $\rho_1 > \rho_2$, we have seen how to obtain a family of Γ-BES with broadcast information rate in the interval (ρ_{B_1}, ρ_{B_2}) and information rate in the interval (ρ_2, ρ_1).
- Given positive integers R and T, we have shown how to obtain a family of different (R, T)-BES with broadcast information rate ρ_B, for any rational value $\rho_B \in [1/R, 1]$, combining two Blundo et al. (R, T)-BESs.
- Given positive integers R, T, and a rational value $\rho_B \in [1/R, 1]$, we have proved that the optimal (R, T)-BESs with broadcast information rate ρ_B designed by combining two Blundo et al. (R, T)-BESs with broadcast information rates $\rho_{B_1} = r_1/R$ and $\rho_{B_2} = r_2/R$ is obtained when $r_1 = \lfloor R\rho_B \rfloor$ and $r_2 = r_1 + 1$.

Some important open problems in the design of broadcast encryption schemes appear from the fact that very few is known about the values of the function $\rho^*(\Gamma, \rho_B)$, which gives the optimal trade-off between ρ and ρ_B.

From the BESs proposed by Blundo et al. in [7] for threshold specification structures $\Gamma = (R, T)$, we obtain the lower bound given in Equation (1). The first open problem we can consider is to determine whether the inequality in equation (1) is an equality or not. If this equality were true, the (R, T)-BESs proposed by Blundo et al. in [7] would have an optimal trade-off between ρ and ρ_B.

Our construction provide a lower bound on $\rho^*(R, T, \rho_B)$ for any rational value $\rho_B \in [1/R, 1]$. This lower bounds are represented by the small points in

Figures 1 and 2. The second open problem is to determine if these lower bound is tight.

On the other hand, we have seen that the lower bound given in Equation (1) can be extended in a natural way to continous function $\Phi(x)$, which is defined by Equation (2) and whose graph is the continous curve in the figures. The last open problem is to determine the relationship between this function and the function $\rho^*(R, T, \rho_B)$. We conjecture that $\rho^*(R, T, \rho_B) \leq \Phi(\rho_B)$ for any $\rho_B \in [1/R, 1]$. The optimality of the (R, T)-BESs proposed by Blundo et al. in [7] would be a direct consequence of this fact.

References

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

[2] S. Berkovits. How to Broadcast a Secret. *Advances in Cryptology–EUROCRYPT '91, Lecture Notes in Computer Science* **547** (1985) 535–541.

[3] R. Blom. An optimal class of symmetric key generation systems. *Advances in Cryptology–EUROCRYPT '84, Lecture Notes in Computer Science* **209** (1985) 335–338.

[4] C. Blundo and A. Cresti. Space requirements for broadcast encryption. *Advances in Cryptology–EUROCRYPT '94, Lecture Notes in Computer Science* **740** (1995) 287–298.

[5] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung. Perfectly secure key distribution for dynamic conferences. *Information and Computation* **146** (1998) 1–23. A previous version appeared in *Advances in Cryptology–CRYPTO '92, Lecture Notes in Computer Science* **740** (1993) 471–486.

[6] C. Blundo, L.A. Frota Mattos and D.R. Stinson. Multiple Key Distribution Mantaining User Anonimity via Broadcast Channels. *J. Computer Security* **3** (1994/5) 309–323.

[7] 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.

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

[9] K. Kurosawa, T. Yoshida, Y. Desmedt and M. Burmester. Some Bounds and a Construction for Secure Broadcast Encryption. *Advances in Cryptology–ASIACRYPT'98, Lecture Notes in Computer Science* **1514** (1998) 420–433.

[10] M. Luby and J. Staddon. Combinatorial bounds for broadcast encryption. *Advances in Cryptology–EUROCRYPT '98, Lecture Notes in Computer Science* **1403** (1998) 512–527.

[11] C. Padró, I. Gracia, S. Martín and P. Morillo. Linear key predistribution schemes. To appear in *Designs, Codes and Cryptography*.

[12] C. Padró, I. Gracia, S. Martín and P. Morillo. Linear Broadcast Encryption Schemes. *International Workshop on Coding and Cryptography WCC 2001, Electronic Notes in Discrete Mathematics* **6**, Paris, France, 2001.

[13] D.R. Stinson. *Cryptography: Theory and Practice*. CRC Press Inc., Boca Raton (1995).

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

[15] D.R. Stinson and T. van Trung. Some new results on key distribution patterns and broadcast encryption. *Designs, Codes and Cryptography* **14** (1998) 261–279.

[16] D.R. Stinson and R. Wei. An application of ramp schemes to broadcast encryption. *Information Processing Letters* **69** (1999) 131–135.

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