Linear broadcast encryption schemes

Carles Padró [a], Ignacio Gracia [a], Sebastià Martín [b] and Paz Morillo [a]

[a] *Departament de Matemàtica Aplicada i Telemàtica, Universitat Politècnica de Catalunya, C. Jordi Girona 1–3, 08034 Barcelona, Spain*

[b] *Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, C. Colom 11, 08122 Terrassa, Spain*

Abstract

A new family of broadcast encryption schemes (BESs), which will be called linear broadcast encryption schemes (LBESs), is presented in this paper by using linear algebraic techniques. This family generalizes most previous proposals and provide a general framework to the study of broadcast encryption schemes. We present a method to construct LBESs for a general specification structure in order to find schemes that fit in situations that have not been considered before.

Key words: Distributed 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 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 [25] for an overview on key distribution systems.

We consider here key distribution systems that can be used by an off-line key distribution center. More concretely, broadcast encryption schemes (BESs) are the main subject of this paper. Key predistribution schemes (KPSs), which are very useful in the construction of BESs, are also considered in this work.

A *key predistribution scheme* (KPS), which is called a *zero-message broadcast encryption scheme* in [5,11], 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) broadcast encryption scheme 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. Broadcasting some public information in a BES makes it possible, in general, to reduce the amount of secret information that every user receives in the predistribution phase. 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 [16,26] 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 [4] and have been also considered in [5–7,10–12,14–17,19–24,26,27]. The first broadcast encryption schemes were proposed by Berkovits [3] and Fiat and Naor [11]. Afterwards, several authors have studied these schemes [1,2,5,8,9,13,16,18,26,27]. A good survey on these subjects can be found in [26].

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 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 $(r, \leq t)$-KPS (BES). In a

$(\leq r, \leq t)$-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 that has to be broadcasted 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 $m_P \in G$ to the users in a privileged subset P, the TA broadcasts the message $b_P = (b_i)_{i \in P}$, where $b_i = m_p + u_i$. 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 k_P is an element of an Abelian group G. In that case, the broadcast message is $b_P = m_P + k_P$, where k_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 [5,7,16]. The optimality of the $(\leq r, \leq t)$-KPSs proposed in [6,11] is derived from these bounds. Blundo, Frota-Mattos and Stinson present in [8] a family of $(r, \leq t)$-BESs obtaining a trade-off between the information rate and the broadcast information rate. These BESs are constructed by using the optimal threshold KPSs given in [6]. 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 [8].

The authors present in [22] a new approach to the design of key predistribution schemes, the *linear key predistribution schemes* (LKPSs). This model, which is based on linear algebraic techniques, unifies all previous proposals and provides a common mathematical formulation and a better understanding of key predistribution schemes. Besides, we present in [22] some methods to construct LKPSs that fit in situations that had not been considered before. For instance, specification structures in which different families of forbidden subsets correspond to different privileged subsets are considered.

In this paper, we apply the ideas in [22] to the design of broadcast encryption schemes. We present the family of *linear broadcast encryption schemes* (LBESs), which includes, as far as we know, all previously proposed BESs. Analogously to the case of key predistribution, this new model provides a general framework to future works on broadcast encryption.

By using this approach, we present a method to construct families of LBESs, for specification structures that are not threshold, in order to obtain a trade-off between the information rate and the broadcast information rate. Concretely, given a specification structure Γ, we consider several coverings of the privileged subsets. For each one of these coverings $\mathcal{B}$, a specification structure Γ_B is defined and a Γ-LBES is constructed from any $\Gamma_{\mathcal{B}}$-LKPS.

The main concepts about key predistribution schemes and broadcast encryption schemes as well as the notation that will be used are presented in Section 2. We recall the definition and some facts about linear key predistribution schemes in Section 3. Linear broadcast encryption schemes are introduced in Section 4. Section 5 is devoted to present a method to construct LBESs from LKPSs. By using this method, we obtain LBESs for specification structures different from the threshold ones.

2 Preliminaries

A *specification structure* Γ on a set of users $\mathcal{U}$ is a subset of $\{(P,F) \in 2^{\mathcal{U}} \times 2^{\mathcal{U}} : P \cap F = \emptyset\}$. 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 will be denoted by $\mathcal{P}(\Gamma)$. For any $P \in \mathcal{P}(\Gamma)$, let us consider $\mathcal{F}_P = \{F \subset \mathcal{U} : (P,F) \in \Gamma\}$. The elements of $\mathcal{F}_P$ will be called the *P-forbidden subsets* of Γ. We are going to consider only specification structures such that, for any $P \in \mathcal{P}(\Gamma)$, the family of P-forbidden subsets $\mathcal{F}_P$ is monotone decreasing, that is, if $F_1 \in \mathcal{F}_P$ and $F_2 \subset F_1$, then $F_2 \in \mathcal{F}_P$.

In a *broadcast encryption scheme* with specification structure Γ, or Γ-BES for short, every user $i \in \mathcal{U}$ receives also 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 $m_P \in \mathcal{M}$, the TA sends by the broadcast channel some information $b_P \in B_P$ such that every user $i \in P$ can compute the message m_P from its secret information u_i and the broadcast information b_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 m_P from the secret information $(u_{j_1}, \ldots, u_{j_s})$ received by the users in F and the public information b_P. That is,

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

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

A more formal definition of broadcast encryption schemes can be given by using the entropy function. See [29] 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 B_P in order to do the broadcast. A Γ-*key predistribution scheme* must satisfy the following conditions:

(1) The secret message m_P must be independent from the secret values distributed in the predistribution phase, that is,

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

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

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

(3) The participants in a P-forbidden subset $F \in \mathcal{F}_P$ can not obtain any information on m_P, that is,

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

In this paper we are going to consider only BESs with uniform probability distributions on $\mathcal{M}$, U_i, $\overline{U}_{\mathcal{U}}$ and B_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, the third condition of the definition of a BES means that, regarding to the secret information $(u_j)_{j \in F}$ of the users in any coalition $F \in \mathcal{F}_P$ and the broadcast message b_P, all values of the secret $m_P \in \mathcal{M}$ are equiprobable.

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

$$\rho = \frac{\log |\mathcal{M}|}{\max_{i \in \mathcal{U}} \log |U_i|}$$

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

$$\rho_B = \frac{\log |\mathcal{M}|}{\max_{P \in \mathcal{P}(\Gamma)} \log |B_P|}$$

Next lemmas are a key point in the definition of linear key predistribution schemes and linear broadcast encryption schemes.

Lemma 1 *Let E and E_0 be vector spaces over a finite field $\mathbf{F}_q$ and let $V \subset E$ be a vector subspace. Let $\varphi_0 : E \to E_0$ be a surjective linear mapping. Then, $\varphi_0(V) = E_0$ if and only if $V + \ker \varphi_0 = E$.*

PROOF. Let us suppose that $\varphi_0(V) = E_0$. Then, for any $x \in E$, there exists $y \in V$ such that $\varphi_0(x) = \varphi_0(y)$. Therefore, $x = y + (x - y)$, where $y \in V$ and $x - y \in \ker \varphi_0$. Reciprocally, if $V + \ker \varphi_0 = E$, then $E_0 = \varphi_0(E) = \varphi_0(V + \ker \varphi_0) = \varphi_0(V)$. $\square$

Lemma 2 *Let E, E_0 and E_1 be vector spaces over a finite field $\mathbf{F}_q$. Let us consider two linear mappings, $\varphi_0 : E \to E_0$ and $\varphi_1 : E \to E_1$, where φ_0 is surjective. Let us suppose that a vector $x \in E$ is chosen uniformly at random. Then,*

(1) the value of $x_0 = \varphi_0(x)$ can be uniquely determined from $x_1 = \varphi_1(x)$ if and only if $\ker \varphi_1 \subset \ker \varphi_0$,
(2) the value of x_1 provides no information about the value of x_0 if and only if $\ker \varphi_1 + \ker \varphi_0 = E$.

PROOF. If we know the value of $x_1 = \varphi_1(x)$, then, we know that $x_0 \in \varphi_0(x') + \varphi_0(\ker \varphi_1)$, where $x' \in E$ is any vector with $\varphi_1(x') = x_1$. Besides, all values in $\varphi_0(x') + \varphi_0(\ker \varphi_1)$ are equiprobable.

Then, x_0 can be uniquely determined from x_1 if and only if $\varphi_0(\ker \varphi_1) = \{0\}$, that is, if and only if $\ker \varphi_1 \subset \ker \varphi_0$.

The value of x_1 does not provide any information on the value of x_0 if and only if $\varphi_0(\ker \varphi_1) = E_0$. In any other case, the value of x_1 provides partial information about the value of x_0. Finally, by Lemma 1, we have that $\varphi_0(\ker \varphi_1) = E_0$ if and only if $\ker \varphi_1 + \ker \varphi_0 = E$. $\square$

3 Linear key predistribution schemes

We recall in this section the definition of linear key predistribution schemes, that were introduced by the authors in [22].

Theorem 3 *Let Γ be a specification structure on the set of users $\mathcal{U} = \{1, 2, \ldots, N\}$. Let E and $E_i \neq \{0\}$, where $i = 0, 1, \ldots, N$, be vector spaces over a finite field $\mathbf{F}_q$. Let us suppose that there exist a surjective linear mapping $\pi_i : E \to E_i$ for every user $i \in \mathcal{U}$ and a surjective linear mapping $\pi_P : E \to E_0$ for every privileged subset $P \in \mathcal{P}(\Gamma)$ satisfying:*

(1) $\ker \pi_i \subset \ker \pi_P$ *for any* $i \in P$,
(2) $\bigcap_{j \in F} \ker \pi_j + \ker \pi_P = E$ *for any* $F \in \mathcal{F}_P$.

Then, there exists a Γ-KPS with information rate and total information rate

$$\rho = \frac{\dim E_0}{\max_{i \in \mathcal{U}} \dim E_i} \quad \textit{and} \quad \rho_T = \frac{\dim E_0}{\dim E}$$

PROOF. We are going to describe a Γ-KPS with set of keys $\mathcal{K} = E_0$. We suppose that the vector spaces E, E_0, $E_1 \cdots, E_N$, as well as the mappings π_i and π_P are publicly known. In the initialization phase, the TA randomly chooses a vector $x \in E$ and sends privately the vector $u_i = \pi_i(x) \in E_i$ to every user $i \in \mathcal{U}$.

Let $P \in \mathcal{P}(\Gamma)$ be a privileged subset. The key associated with P will be $k_P = \pi_P(x) \in E_0$. By considering $\varphi_0 = \pi_P$ and $\varphi_1 = \pi_i$ in Lemma 2, every user $i \in P$ can compute the key k_P. On the other hand, in order to prove that any coalition $F \in \mathcal{F}_P$ cannot obtain any information about the key k_P, we consider the linear mappings $\varphi_0 = \pi_P$ and $\varphi_1 : E \to \prod_{j \in F} E_j$ defined by $\varphi_1(x) = (\pi_j(x))_{j \in F}$. Observe that $\varphi_1(x)$ corresponds to the secret information known by the users in F. Since $\ker \varphi_1 = \bigcap_{j \in F} \ker \pi_j$, we have that $\ker \varphi_0 + \ker \varphi_1 = E$ and, applying Lemma 2, we conclude that the users in F cannot obtain any information on $k_P = \varphi_0(x)$. $\square$

Definition 4 A key predistribution scheme with specification structure Γ that can be defined as in the proof of Theorem 3 will be called a Γ-*linear* *key predistribution scheme* (Γ-LKPS).

We proved in [22] that the best known KPSs, that is, the trivial scheme [26], the Fiat-Naor scheme [11] and the KPS proposed by Blundo et al. [6], are linear.

4 Linear broadcast encryption schemes

We present in this section the definition of linear broadcast encryption schemes and some basic examples.

Theorem 5 *Let Γ be a specification structure on a set of users $\mathcal{U} = \{1, 2, \ldots, N\}$. Let E, V_0, and E_i, for any $i \in \mathcal{U}$ be vector spaces over a finite field $\mathbf{F}_q$. Let us suppose that there exist a surjective linear mapping $\pi_i : E \to E_i$ for every user $i \in \mathcal{U}$. Let us suppose that, for any $P \in \mathcal{P}(\Gamma)$, there exist vector spaces E_P and V_P over $\mathbf{F}_q$ and surjective linear mappings $\Phi_P : E_P \to E$, $\Psi_P : E_P \to V_P$ and $\Pi_P : E_P \to V_0$ such that*

(1) $\ker \Phi_P + \ker \Pi_P = E_P$,
(2) $\ker(\pi_i \circ \Phi_P) \cap \ker \Psi_P \subset \ker \Pi_P$ *for any* $i \in P$,
(3) if $F \in \mathcal{F}_P$, *then* $\left(\bigcap_{j \in F} \ker(\pi_j \circ \Phi_P) \cap \ker \Psi_P \right) + \ker \Pi_P = E_P$.

Then, there exists a Γ-BES with information rate and broadcast information rate

$$\rho = \frac{\dim V_0}{\max_{i \in \mathcal{U}} \dim E_i} \qquad \text{and} \qquad \rho_B = \frac{\dim V_0}{\max_{P \in \mathcal{P}(\Gamma)} \dim V_P},$$

respectively.

PROOF. For any $x \in E$ and for any $m_P \in V_0$, there exists a vector $y \in E_P$ such that $\Phi_P(y) = x$ and $\Pi_P(y) = m_P$. In effect, let $y' \in E_P$ be a vector such that $\Phi_P(y') = x$. Since $\ker \Phi_P + \ker \Pi_P = E_P$, by Lemma 1, $\Pi_P(y' + \ker \Phi_P) = V_0$. Then, there exists a vector $y'' \in \ker \Phi_P$ such that $\Pi_P(y' + y'') = m_P$ and $\Phi_P(y' + y'') = x$.

We describe next a Γ-BES with the required information rates. In the predistribution phase, the TA chooses at random a vector $x \in E$ and distributes privately to every participant $i \in \mathcal{U}$ the secret information $u_i = \pi_i(x) \in E_i$. At a latter moment, if it is necessary to send a secret message $m_P \in V_0$ to a privileged subset P, the TA chooses at random a vector $y \in E_P$ such that $\Phi_P(y) = x$ and $\Pi_P(y) = m_P$ and broadcasts the message $b_P = \Psi_P(y) \in V_P$.

The secret information received by the users in the predistribution phase is determined by the value of $x = \Phi_P(y) \in E$. Since $\ker \Phi_P + \ker \Pi_P = E_P$, the value of the secret message, $m_P = \Pi_P(y)$, is independent from the secret information distributed among the users.

Let $i \in P$ be a user in a privileged subset $P \in \mathcal{P}(\Gamma)$. Let us consider the linear mappings $\varphi_0 : E_P \to V_0$ and $\varphi_1 : E_P \to E_i \times V_P$ defined by $\varphi_0 = \Pi_P$ and $\varphi_1(y) = ((\pi_i \circ \Phi_P)(y), \Psi_P(y))$. Observe that $\varphi_1(y)$ consists of the secret information received in the predistribution phase by user i and the broadcast message. Since $\ker \varphi_1 = \ker(\pi_i \circ \Phi_P) \cap \ker \Psi_P$, we can apply Lemma 2 in order to prove that user i can compute the secret message m_P from its secret information and the broadcast message.

On the other hand, if $F = \{j_1, \dots j_s\} \in \mathcal{F}_P$, we consider

$$\varphi_1 : E_P \to E_{j_1} \times \cdots \times E_{j_s} \times V_P$$

defined by $\varphi_1(y) = ((\pi_{j_1} \circ \Phi_P)(y), \dots, (\pi_{j_s} \circ \Phi_P)(y), \Psi_P(y))$. Observe that $\varphi_1(y)$ consists of the secret information received by the users in F and the broadcast message. If, as before, we consider $\varphi_0 = \Pi_P$, taking into account that

$$\ker \varphi_1 + \ker \varphi_0 = \left(\bigcap_{j \in F} \ker(\pi_j \circ \Phi_P) \cap \ker \Psi_P \right) + \ker \Pi_P = E_P,$$

we can apply Lemma 2 in order to prove that the users in F do not obtain any information on the secret message m_P from their secret information and the broadcast message. $\square$

Definition 6 A broadcast encryption scheme with specification structure Γ that can be defined as in the proof of Theorem 5 will be called a Γ-*linear broadcast encryption scheme* (Γ-LBES).

We show next two basic examples of linear broadcast encryption schemes, that correspond to the extremal cases that were considered in Section 2.

Example 7 Let Γ be a specification structure on a set of users $\mathcal{U} = \{1, 2, \dots, N\}$ We present first a Γ-LBES with maximum information rate $\rho = 1$ and broadcast information rate $\rho_B = 1/r$, where $r = \max_{P \in \mathcal{P}(\Gamma)} |P|$. Let us consider the vector spaces $E = \mathbf{F}_q^N$ and $V_0 = \mathbf{F}_q$, and, for any $i = 1, \dots, N$, the surjective linear mapping $\pi_i : E \to \mathbf{F}_q$ defined by $\pi_i(u_1, \dots, u_N) = u_i$. For any privileged subset $P \in \mathcal{P}(\Gamma)$, we consider $E_P = E \times \mathbf{F}_q$, $V_P = \mathbf{F}_q^r$, where $r = |P|$, and the mappings

- $\Phi_P : E_P \to E$, defined by $\Phi_P(\mathbf{u}, y) = \mathbf{u}$,
- $\Psi_P : E_P \to V_P$, defined by $\Psi_P((u_1, \ldots, u_N), y) = (u_i + y)_{i \in P}$,
- $\Pi_P : E_P \to V_0$, defined by $\Pi_P(\mathbf{u}, y) = y$.

It is easy to check that these linear mappings satisfy conditions 1 and 2 in Theorem 5. Let us prove that the third condition is also satisfied. Let us consider a pair $(P, F) \in \Gamma$ and a vector $(\mathbf{u}, y) \in E_P$. Let $(\mathbf{v}, y) = ((v_1, \ldots, v_N), y) \in E_P$ be such that $v_i = -y$ if $i \in P$ and $v_j = 0$ if $j \in F$. Then $(\mathbf{u}, y) = (\mathbf{v}, y) + (\mathbf{u} - \mathbf{v}, 0)$, where $(\mathbf{v}, y) \in \bigcap_{j \in F} \ker(\pi_j \circ \Phi_P) \cap \ker \Psi_P$ and $(\mathbf{u} - \mathbf{v}, 0) \in \ker \Pi_P$. Therefore, by Theorem 5, we obtain a Γ-LBES with the required information rates.

Example 8 This example consists in an easy method to obtain a Γ-LBES with maximum broadcast information rate $\rho_B = 1$ from any Γ-linear key predistribution scheme. Let E, $E_1, \ldots, E_N$, E_0 be vector spaces over a finite field $\mathbf{F}_q$. Let us consider surjective linear mappings $\pi_i : E \to E_i$, where $i = 1, \ldots N$, and $\pi_P : E \longrightarrow E_0$, where $P \in \mathcal{P}(\Gamma)$, that define a Γ-LKPS. Let us take $V_0 = E_0$ and, for any $P \in P(\Gamma)$, we consider $E_P = E \times E_0$, $V_P = E_0$ and the mappings

- $\Phi_P : E_P \to E$, defined by $\Phi_P(x, y) = x$,
- $\Psi_P : E_P \to V_P$, defined by $\Psi_P(x, y) = \pi_P(x) + y$,
- $\Pi_P : E_P \to V_0$, defined by $\Pi_P(x, y) = y$.

It is obvious that these liner mappings verify the first condition in Theorem 5. In order to prove that condition 2 is also satisfied take into account that, by the definition of a Γ-LKPS, $\ker \pi_i \subset \ker \pi_P$ if $i \in P$ is a user in the privileged subset $P \in \mathcal{P}(\Gamma)$. If $(P, F) \in \Gamma$ and $(x, y) \in E_P$, we consider $x' \in E$ such that $\pi_P(x') = -y$. By the definition of the Γ-LKPS, we have that $x' = x'_1 + x'_2$ with $x'_1 \in \bigcap_{j \in F} \ker \pi_j$ and $x'_2 \in \ker \pi_P$. Finally, observe that

$$(x, y) = (x'_1, -\pi_P(x'_1)) + (x - x'_1, 0) \in \left(\bigcap_{j \in F} \ker(\pi_j \circ \Phi_P) \cap \ker \Psi_P \right) + \ker \Pi_P,$$

which implies that the third condition in Theorem 5 is also satisfied.

5 Constructing LBES from LKPS

In this section, we are going to present a method to construct a family of Γ-LBESs for any specification structure Γ, in order to obtain a trade-off between the information rate and broadcast information rate. First, we define a family of specification structures associated with a given structure Γ.

Definition 9 Let Γ be a specification structure on $\mathcal{U} = \{1, 2, \ldots, N\}$. Let us consider, for every $P \in \mathcal{P}(\Gamma)$, a family of subsets $\mathcal{B}_P \subset 2^{\mathcal{U}}$ such that $\bigcup_{Q \in \mathcal{B}_P} Q = P$ and $Q \not\subset Q'$ for any pair of different subsets $Q, Q' \in \mathcal{B}_P$. Let us take $\mathcal{B} = \{\mathcal{B}_P : P \in \mathcal{P}(\Gamma)\}$. We define $\Gamma_{\mathcal{B}}$ as the specification structure on $\mathcal{U}$ that is formed by the pairs $(Q, F_1) \in 2^{\mathcal{U}} \times 2^{\mathcal{U}}$ such that $Q \in \mathcal{B}_P$ and $F_1 = F \cup (P \setminus Q)$ for some $(P, F) \in \Gamma$. Observe that we obtain a different specification structure $\Gamma_{\mathcal{B}}$ for every choice of $\mathcal{B}$.

The family of Γ-LBESs we introduce in this section is obtained by considering the family of specification structures defined above. Namely, we present a method to construct a Γ-LBES from any given $\Gamma_{\mathcal{B}}$-LKPS.

Lemma 10 *Let Γ be specification structures on $\mathcal{U}$ and let $\Gamma_{\mathcal{B}}$ be a specification structure in the above family. Let us consider surjective linear mappings $\pi_i : E \to E_i$, where $i \in \{1, \ldots, N\}$, and $\pi_Q : E \to \mathbf{F}_q$, where $Q \in \mathcal{P}(\Gamma_{\mathcal{B}})$, defining a $\Gamma_{\mathcal{B}}$-LKPS. Let $P \in \mathcal{P}(\Gamma)$ be a privileged subset of Γ and let us suppose that $\mathcal{B}_P = \{Q_1, \ldots, Q_M\}$. Let us consider the linear mapping $\Theta_P : E \to \mathbf{F}_q^M$ defined by $\Theta_P(x) = (\pi_{Q_1}(x), \ldots, \pi_{Q_M}(x))$. Then,*

(1) Θ_P is surjective and
(2) $\ker \Theta_P + \bigcap_{j \in F} \ker \pi_j = E$ if $(P, F) \in \Gamma$.

PROOF. Let us suppose that Θ_P is not surjective. Then, there exists a subspace $G \subset \mathbf{F}_q^M$, with $\dim G = M - 1$, such that $\Theta_P(E) \subset G$. The subspace G will be defined by an equation in the form $\sum_{k=1}^{M} \lambda_k x_k = 0$, where $\lambda_k \in \mathbf{F}_q$. We can assume without loss of generality that $\lambda_M \neq 0$. Therefore, $\sum_{k=1}^{M} \lambda_k \pi_{Q_k}(x) = 0$ for any $x \in E$. Let us suppose that every user $i \in \mathcal{U}$ has received the secret information $\pi_i(x)$, where $x \in E$, corresponding to the $\Gamma_{\mathcal{B}}$-LKPS we are considering. If the users in $P \setminus Q_M$ join together, they can compute $\pi_{Q_1}(x), \cdots, \pi_{Q_{M-1}}(x)$ from their secret information, and, hence, they can obtain the value of $\pi_{Q_M}(x)$. That is a contradiction because $(Q_M, P \setminus Q_M) \in \Gamma_{\mathcal{B}}$.

Let us suppose now that $\ker \Theta_P + \bigcap_{j \in F} \ker \pi_j \neq E$ for some $(P, F) \in \Gamma$. Then, by taking $\varphi_0 = \Theta_P$ in Lemma 1, $\Theta_P(\bigcap_{j \in F} \ker \pi_j) \neq \mathbf{F}_q^M$. Therefore, there exists a subspace $G \subset \mathbf{F}_q^M$, with $\dim G = M - 1$, such that $\Theta_P(\bigcap_{j \in F} \ker \pi_j) \subset G$. Let us consider the equation $\sum_{k=1}^{M} \lambda_k x_k = 0$ that define the subspace G, where $\lambda_k \in \mathbf{F}_q$. We can assume without loss of generality that $\lambda_M \neq 0$. Let us consider the linear mappings $\varphi_0 : E \to \mathbf{F}_q$ and $\varphi_1 : E \to \prod_{j \in F} E_j$ defined by $\varphi_0(x) = \sum_{k=1}^{M} \lambda_k \pi_{Q_k}(x)$ and $\varphi_1(x) = (\pi_j(x))_{j \in F}$ Observe that $\ker \varphi_1 = \bigcap_{j \in F} \ker \pi_j \subset \ker \varphi_0$. Let us suppose that the vector $x \in E$ has been used by the TA in order to distribute among the users the secret information corresponding to the $\Gamma_{\mathcal{B}}$-LKPS. By Lemma 2, if the users in F put together their secret information, they will be able to compute $\sum_{k=1}^{M} \lambda_k \pi_{Q_k}(x)$. Therefore, the coalition $F \cup (P \setminus Q_M)$ can find some information about the value of the common key $\pi_{Q_M}(x)$ corresponding to the set Q_M, a contradiction. $\square$

Last lemma implies that there is no relation between the common keys $\pi_{Q_1}(x), \ldots, \pi_{Q_M}(x)$ corresponding to the privileged subsets $Q_1, \ldots, Q_M$ in the $\Gamma_{\mathcal{B}}$-LKPS because the vector $(\pi_{Q_1}(x), \ldots, \pi_{Q_M}(x))$ can take any value in $\mathbf{F}_q^M$. Besides, a coalition of users F such that $(P, F) \in \Gamma$ cannot obtain any information about the value of this vector, that is, they are not able to obtain any information about these keys nor any relation between them. Both facts will be used in the proof of next theorem, which provides a construction of a Γ-LBES from a $\Gamma_{\mathcal{B}}$-LKPS.

Theorem 11 *Let Γ be a specification structure on $\mathcal{U} = \{1, \ldots, N\}$ and let $\Gamma_{\mathcal{B}}$ be a specification structure in the form described in Definition 9. For every $P \in \mathcal{P}(\Gamma)$, we consider $M_P = |\mathcal{B}_P|$ and $\mu_P = \min_{i \in P} |\{Q \in \mathcal{B}_P \,:\, i \in Q\}|$. Let us consider $M = \max_{P \in \mathcal{P}(\Gamma)} M_P$ and $\mu = \min_{P \in \mathcal{P}(\Gamma)} \mu_P$. Let $\pi_i : E \to E_i$, where $i \in \mathcal{U}$, and $\pi_Q : E \to \mathbf{F}_q$, where $Q \in \mathcal{P}(\Gamma_{\mathcal{B}})$, be surjective linear mappings defining a Γ_B-LKPS with information rate ρ'. Then, there exists a Γ-LBES with information rate $\rho = \mu\rho'$ and broadcast information rate $\rho_B = \mu/M$.*

PROOF. We consider, for every $P \in \mathcal{P}(\Gamma)$, a set of publicly known vectors $\{v_1, \ldots v_{M_P}\} \subset \mathbf{F}_q^\mu$ such that any subset with cardinality μ is a basis of $\mathbf{F}_q^\mu$. For instance, we can consider $v_j = (1, x_j, x_j^2, \ldots, x_j^{\mu-1})$, where $x_1, \ldots, x_{M_P}$ are distinct elements of the field $\mathbf{F}_q$. Let us take the vector spaces $E_P = E \times \mathbf{F}_q^\mu$, $V_P = \mathbf{F}_q^{M_P}$, where $P \in \mathcal{P}(\Gamma)$, and $V_0 = \mathbf{F}_q^\mu$. For every $P \in \mathcal{P}(\Gamma)$, we consider the linear mappings $\Pi_P : E_P \to V_0$, $\Phi_P : E_P \to E$ and $\Psi_P : E_P \to V_P$, which are defined, respectively, by $\Pi_P(x, v) = v$, $\Phi_P(x, v) = x$ and

$$\Psi_P(x, v) = (v \cdot v_1 + \pi_{Q_1}(x), \ldots, v \cdot v_{M_P} + \pi_{Q_{M_P}}(x)).$$

Observe that Ψ_P is surjective because, by Lemma 10, the linear mapping $\Theta_p(x) = (\pi_{Q_1}(x), \ldots, \pi_{Q_{M_P}}(x))$ is surjective. We are going to prove that these linear mappings fulfill the conditions in Theorem 5 and, then, define a Γ-LBES. That is, we have to prove that:

(1) $\ker \Phi_P + \ker \Pi_P = E_P$,
(2) $\ker(\pi_i \circ \Phi_P) \cap \ker \Psi_P \subset \ker \Pi_P$ for any $i \in P$,
(3) if $F \in \mathcal{F}_P$, then $\left(\bigcap_{j \in F} \ker(\pi_j \circ \Phi_P) \cap \ker \Psi_P \right) + \ker \Pi_P = E_P$.

First condition is obviously satisfied.

Let $i \in P$ be a user in a privileged subset $P \in \mathcal{P}(\Gamma)$. Let us consider $(x, v) \in \ker(\pi_i \circ \Phi_P) \cap \ker \Psi_P$. Then, since $\ker \pi_i \subset \ker \pi_Q$ for any $Q \in \mathcal{P}(\Gamma_B)$ such that $i \in Q$, there exist at least μ distinct subsets $Q_{h_1}, \ldots, Q_{h_\mu} \in \mathcal{B}_P$ such that $\pi_{Q_{h_j}}(x) = 0$. Then, $v \cdot v_{h_j} = 0$ for any $j = 1, \ldots, \mu$ because $\Psi_P(x, v) = 0$. Since $v_{h_1}, \ldots, v_{h_\mu}$ are linearly independent vectors in $\mathbf{F}_q^\mu$, we have that $\Pi_P(x, v) = v = 0$.

Let us consider now a forbidden subset $F \in \mathcal{F}_P$. Since, by Lemma 10, Θ_P is surjective, for any $v \in V_0$, there exists a vector $x_v \in E$ such that $\Theta_P(x_v) = -(v \cdot v_1, \ldots, v \cdot v_{M_P})$. By Lemma 10, $\ker \Theta_P + \bigcap_{j \in F} \ker \pi_j = E$. Then $x_v = y_v + z_v$, where $y_v \in \ker \Theta_P$ and $z_v \in \bigcap_{j \in F} \ker \pi_j$. Observe that

$$\Psi_P(z_v, v) = (v \cdot v_1, \ldots, v \cdot v_{M_P}) + \Theta_P(z_v) = (v \cdot v_1, \ldots, v \cdot v_{M_P}) + \Theta_P(x_v) = 0.$$

Therefore, for any $(x, v) \in E_P$, we have that $(x, v) = (z_v, v) + (x - z_v, 0)$, where $(z_v, v) \in \bigcap_{j \in F} \ker(\pi_j \circ \Phi_P) \cap \ker \Psi_P$ and $(x - z_v, 0) \in \ker \Pi_P$.

Since the linear mappings above satisfy the three conditions in Theorem 5, we have obtained a Γ-LBES with information rate

$$\rho = \frac{\dim V_0}{\max_{i \in \mathcal{U}} \dim E_i} = \frac{\mu}{\max_{i \in \mathcal{U}} \dim E_i} = \mu \rho'$$

and broadcast information rate

$$\rho_B = \frac{\dim V_0}{\max_{P \in \mathcal{P}(\Gamma)} \dim V_P} = \frac{\mu}{\max_{P \in \mathcal{P}(\Gamma)} M_P} = \frac{\mu}{M}.$$

□

We obtain in this way several LBES for the access structure Γ, namely, one for each choice of the family $\mathcal{B}$ and a $\Gamma_\mathcal{B}$-LKPS. At this point, the problem of finding Γ-LBES with a good trade-off between the information rate ρ and the broadcast information rate ρ_B can be reduced to make a good choice of the families $\mathcal{B}$.

For instance, if the specification structure Γ is such that $|P| = r$ for any $P \in \mathcal{P}(\Gamma)$, we can consider, for any $\ell = 1, \ldots, r$ the family $\mathcal{B}^\ell = \{\mathcal{B}_P^\ell : P \in \mathcal{P}(\Gamma)\}$ such that $\mathcal{B}_P^\ell = \{Q \subset P : |Q| = \ell\}$ for any $P \in \mathcal{P}(\Gamma)$. Observe that, in this case, $M_P = \binom{r}{\ell}$ and $\mu_P = \binom{r-1}{\ell-1}$ for any $P \in \mathcal{P}(\Gamma)$. Therefore, for any $\ell = 1, \ldots, r$, there exists a Γ-LBES with information rate $\rho_\ell = \binom{r-1}{\ell-1}\rho'_\ell$, where ρ'_ℓ is the information rate of a $\Gamma_{\mathcal{B}^\ell}$-LKPS, and broadcast information rate $\rho_{B\ell} = \mu/M = \ell/r$.

Example 12 In particular, we can consider the threshold specification structure $\Gamma = (r, \leq t)$. Then $\Gamma_{\mathcal{B}^\ell} = (\ell, \leq t + r - \ell)$ for any $\ell = 1, \dots, r$. In this case, since there exists a $\Gamma_{\mathcal{B}^\ell}$-LKPS with information rate $\rho'_\ell = \binom{t+r-1}{\ell-1}^{-1}$ [6,22], we obtain, for any $\ell = 1, \dots, r$, a $(r, \leq t)$-LBES with information rate $\rho_\ell = \binom{r-1}{\ell-1} / \binom{t+r-1}{\ell-1}$ and broadcast information rate $\rho_{B\ell} = \ell/r$. These $(r, \leq t)$-LBESs are equivalent to the BESs proposed in [9].

Our construction can be also applied to other specification structures different from the threshold ones, as can be seen in the following example.

Example 13 Let us suppose that the set of users is divided into two parts, $\mathcal{U} = \mathcal{U}_1 \cup \mathcal{U}_2$. Let r, t_1 and t_2 be positive integers and let Γ^{r,t_1,t_2} be the specification structure on $\mathcal{U}$ defined by: $(P, F) \in \Gamma^{r,t_1,t_2}$ if and only if $|P| = r$ and $|F \cap \mathcal{U}_i| \leq t_i$ if $P \cap \mathcal{U}_i \neq \emptyset$. Observe that, if, for instance, $P \subset \mathcal{U}_1$, then $\mathcal{U}_2 \cup F \in \mathcal{F}_P$ for any $F \subset \mathcal{U}_1$ with $|F| \leq t_1$. That is, any coalition of users in $\mathcal{U}_2$ can not obtain any information about the secret key associated to a privileged subset $P \subset \mathcal{U}_1$ and vice versa. Observe that privileged groups with users in both $\mathcal{U}_1$ and $\mathcal{U}_2$ are also considered.

A Γ^{r,t_1,t_2}-LKPS with information rate $\rho = \binom{t+r}{r-1}^{-1}$, where $t = t_1 + t_2$, is constructed in [22]. It is easy to check that $\Gamma^{r,t_1,t_2}_{\mathcal{B}^\ell} = \Gamma^{\ell, t_1+r-\ell, t_2+r-\ell}$ for any $\ell = 1, 2, \dots, r$. Therefore, for any $\ell = 1, 2, \dots, r$, there exists a Γ^{r,t_1,t_2}-LBES with information rate $\rho_\ell = \binom{r-1}{\ell-1} / \binom{t+2r-\ell}{\ell-1}$ and broadcast information rate $\rho_{B\ell} = \ell/r$.

6 Conclusions and open problems

Following some ideas in [22], in the present work we have provided a new general approach to the construction of broadcast encryption schemes based on linear algebraic techniques. We introduce a class of BESs, called linear broadcast encryption schemes (LBESs), containing, as far as we know, all previous proposals of BESs.

Given a specification structure Γ, we present some techniques to construct Γ-LBESs from several linear key predistribution schemes whose specification structures $\Gamma_{\mathcal{B}}$ are constructed from a family of coverings of the privileged subsets of Γ. The good trade-off between the information rates, ρ and ρ_B, depends on the choice of the specification structures $\Gamma_{\mathcal{B}}$, and the $\Gamma_{\mathcal{B}}$-LKPSs that are used. We present as well a family of Γ-LBESs, where Γ is not a threshold specification structure.

Observe that the construction we have presented in Section 5 works only for specification structures in which all privileged subsets have the same number of users. The construction of LBESs for other specification structures, for instance, for threshold specification structures in the form $\Gamma = (\leq r, \leq t)$, is still an open problem.

It is shown in [9] how to design a family of BESs with specification structure $\Gamma = (r, \leq t)$, and information rates $\rho = \binom{r-1}{\ell-1}/\binom{t+r-1}{\ell-1}$ and $\rho_B = \ell/r$, for every $\ell \in \{1, \cdots, r\}$. In this way, a trade-off between ρ and ρ_B is obtained. Nevertheless, it has not been possible until now to prove or disprove the optimality of these BESs. Another open problem appears at this point: to find bounds on the information rate ρ in terms of the broadcast information rate ρ_B, or vice versa. We feel that the optimality of the BESs in [9] could be derived from such bounds.

On the other side, it would be also interesting to design $(r, \leq t)$-LBESs whose values of ρ and ρ_B are not achieved in the construction in [9] and, if possible, to prove their optimality.

Finally, the model we present in this paper could be applied to study the design of unconditionally secure *multiple use broadcast encryption schemes* (MBESs) [16], that is, schemes in which several broadcasts can be made without loss of security. The MBESs proposed in [5,16] are based on computational assumptions.

References

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

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

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

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

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

[6] 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.

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

[8] 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.

[9] 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.

[10] M. Dyer, T. Fenner, A. Frieze and A. Thomason. On key storage in secure networks. *J. Cryptology* **8** (1995) 189–200.

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

[12] L. Gong and D.L. Wheeler. A matrix key-distribution scheme. *J. Cryptology* **2** (1990) 51–59.

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

[14] V. Korjik, M. Ivkov, Y. Merinovitch, A. Barg and H. van Tilborg. A broadcast key distribution scheme based on block designs. *Cryptography and Coding V, Lecture Notes in Computer Science* **1025** (1995) 12–21.

[15] K. Kurosawa, K. Okada and K. Sakano. Security of the center in Key Distribution Schemes. *Advances in Cryptology–ASIACRYPT'94, Lecture Notes in Computer Science* **917** (1995) 333–341.

[16] 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.

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

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

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

[20] C.J. Mitchell and F.C. Piper. Key Storage in Secure Networks. *Discrete Applied Mathematics* **21** (1998) 215–228.

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

[22] C. Padró, I. Gracia, S. Martín and P. Morillo. Linear key predistribution schemes. *Designs, Codes and Cryptography* (submitted).

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

[24] G. Sáez. Generation of Key Predistribution Schemes using Secret Sharing Schemes. *Proceedings of the International Workshop on Coding and Cryptography WCC 2001*, 435–444, Paris, France, 2001.

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

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

[27] 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.

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

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