A Simplified Combinatorial Treatment of Constructions and Threshold Gaps of Ramp Schemes

Maura B. Paterson
Department of Economics, Mathematics and Statistics
Birkbeck, University of London
Malet Street, London WC1E 7HX, UK

Douglas R. Stinson*
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada

September 10, 2012

Abstract

We give easy proofs of some recent results concerning threshold gaps in ramp schemes. We then give a simplified and unified treatment of construction methods for ramp schemes using error-correcting codes. Finally, as an immediate consequence of these results, we provide a new explicit bound on the the minimum length of a code having a specified distance and dual distance.

1 Introduction

Suppose that t_1, t_2 and n are positive integers such that $t_1 < t_2 \leq n$. Informally, a (t_1, t_2, n)-*ramp scheme* is a method whereby a *dealer* distributes a *share* to each of n *players* such that the following two properties are satisfied:

reconstruction Any subset of t_2 players can compute a unique *secret* from the shares that they collectively hold

secrecy No subset of t_1 players can determine any information about the secret.

When $t_2 = t_1 + 1$, the ramp scheme is known as a (t_2, n)-*threshold scheme*. Ramp schemes were introduced by Blakley and Meadows [2] and much basic information about ramp schemes can be found in [3, 10, 19]. Ramp schemes have found numerous applications over the years, including broadcast encryption [20], secure multiparty computation [5] and error decodable secret sharing [15].

Cascudo, Cramer and Xing [4] proved the interesting result that $n - t_1 + 1 \leq q(t_2 - t_1)$ in any (t_1, t_2, n)-ramp scheme having a share space of cardinality q. This inequality (the "threshold gap

*D. Stinson's research is supported by NSERC discovery grant 203114-11

bound") provides an upper bound on the number of participants in a ramp scheme having given thresholds and a share space of a given size. The proof in [4] is rather complex, and builds on a related unpublished result due to Kilian and Nisan concerning threshold schemes. In this paper, we give an easy combinatorial proof of this bound and we also discuss connections with some classical bounds for orthogonal arrays. Then, we provide a simplified, general treatment of construction methods for ramp schemes using both linear and nonlinear codes. We also construct some new ramp schemes that are optimal with respect to the threshold gap bound. Finally, as an immediate consequence of these results, we provide a new explicit bound on the the minimum length of a code having a specified distance and dual distance. We also show that there are infinite classes of codes that are optimal with respect to this bound.

2 The Threshold Gap Bound

Suppose we have a $(1, t, n)$-ramp scheme where the *share space* $\mathcal{S} = \{1, \ldots, q\}$. A *distribution rule* $\mathbf{r}$ is written as an n-tuple with entries from $\mathcal{S}$, i.e., $\mathbf{r} = (r_1, \ldots, r_n)$, where r_i is the share given to player P_i. Let the *secret space* be $\mathcal{K} = \{1, \ldots, q'\}$ where $q' > 1$. For any $K \in \mathcal{K}$, let $\mathcal{F}_K$ denote the collection of distribution rules corresponding to the secret having the value K. We do not require that all the n-tuples in $\mathcal{F}_K$ are distinct. Denote $\mathcal{F} = \cup_{K \in \mathcal{K}} \mathcal{F}_K$.

Given any share S, the secrecy condition of a $(1, t, n)$-ramp scheme requires that $\mathbf{Pr}[K|S] = \mathbf{Pr}[K]$ for all $K \in \mathcal{K}$. By Bayes' Theorem, this is equivalent to $\mathbf{Pr}[S|K] = \mathbf{Pr}[S]$, so $\mathbf{Pr}[S|K]$ is independent of K. Note that taking multiple copies of each distribution rule in any $\mathcal{F}_K$ does not change $\mathbf{Pr}[S|K]$. Suppose that $|\mathcal{F}_{K_1}| = L_1$ and $|\mathcal{F}_{K_2}| = L_2$ where $L_2 \neq L_1$. Let $L = \mathrm{lcm}(L_1, L_2)$. If we take L/L_1 copies of every distribution rule in $\mathcal{F}_{K_1}$ and L/L_2 copies of every rule in $\mathcal{F}_{K_2}$, then we have $|\mathcal{F}_{K_1}| = |\mathcal{F}_{K_2}| = L$.

Now we can rephrase the secrecy condition in a combinatorial form: there exist non-negative integers $\lambda_{i,j}$ for $1 \leq i \leq n$, $1 \leq j \leq q$, such that

$$|\{\mathbf{r} \in \mathcal{F}_K : r_i = j\}| = \lambda_{i,j}$$

for $K = K_1, K_2$. Observe that

$$\sum_{j=1}^{q} \lambda_{i,j} = L$$

for any i, $1 \leq i \leq n$.

Suppose we define

$$\mu(\mathbf{r}, \mathbf{s}) = |\{i : r_i = s_i\}|$$

for any $\mathbf{r}, \mathbf{s} \in \mathcal{F}$. By the reconstruction condition, it is required that t shares determine a unique value of the secret. Therefore, it follows that $\mu(\mathbf{r}, \mathbf{s}) \leq t - 1$ if $\mathbf{r} \in \mathcal{F}_{K_1}$ and $\mathbf{s} \in \mathcal{F}_{K_2}$.

For any $\mathbf{r} \in \mathcal{F}$, define

$$f(\mathbf{r}) = \sum_{i=1}^{n} \lambda_{i,r_i}.$$

Lemma 2.1. *If $\mathbf{r} \in \mathcal{F}$, then $f(\mathbf{r}) \leq L(t-1)$.*

Proof. Suppose $\mathbf{r} \in \mathcal{F}_{K_1}$. We have that

$$\begin{aligned}\sum_{\mathbf{s}\in\mathcal{F}_{K_2}} \mu(\mathbf{r},\mathbf{s}) &= \sum_{i=1}^{n} |\{\mathbf{s} \in \mathcal{F}_{K_2} : r_i = s_i\}| \\ &= \sum_{i=1}^{n} \lambda_{i,r_i} \\ &= f(\mathbf{r}).\end{aligned}$$

However, $\mu(\mathbf{r},\mathbf{s}) \leq t-1$ for all $\mathbf{s} \in \mathcal{F}_{K_2}$, so we have that $f(\mathbf{r}) \leq |\mathcal{F}_{K_2}|(t-1) = L(t-1)$. □

Theorem 2.2. *If a $(1,t,n)$-ramp scheme has a share space of cardinality q, then $n \leq q(t-1)$.*

Proof. We compute upper and lower bounds on the sum $\sum_{\mathbf{r}\in\mathcal{F}_{K_1}} f(\mathbf{r})$. First, we have

$$\begin{aligned}\sum_{\mathbf{r}\in\mathcal{F}_{K_1}} f(\mathbf{r}) &= \sum_{\mathbf{r}\in\mathcal{F}_{K_1}} \sum_{i=1}^{n} \lambda_{i,r_i} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{q} \sum_{\mathbf{r}\in\mathcal{F}_{K_1}:r_i=j} \lambda_{i,j} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{q} (\lambda_{i,j})^2 \\ &\geq \frac{\sum_{i=1}^{n}\left(\sum_{j=1}^{q}\lambda_{i,j}\right)^2}{q} \\ &= \frac{nL^2}{q}.\end{aligned}$$

Second, from Lemma 2.1, we have that

$$\sum_{\mathbf{r}\in\mathcal{F}_{K_1}} f(\mathbf{r}) \leq L^2(t-1).$$

Combining the upper and lower bounds, we have

$$\frac{nL^2}{q} \leq L^2(t-1),$$

which simplifies to yield the desired result. □

Before proving the main theorem, we need a preliminary lemma.

Lemma 2.3. *If there exists a (t_1,t_2,n)-ramp scheme having a share space of cardinality q, then there exists a $(t_1-1,t_2-1,n-1)$-ramp scheme having a share space of cardinality q.*

Proof. Let $\mathcal{F}_x$ consist of all the distribution rules $\mathbf{r} \in \mathcal{F}$ for which $r_n = x$ for some fixed share x where $\lambda_{n,x} > 0$. Then define

$$\mathcal{G} = \{(r_1, \ldots, r_{n-1}) : \mathbf{r} = (r_1, \ldots, r_n) \in \mathcal{F}_x\}.$$

It is easy to see that $\mathcal{G}$ comprises a set of distribution rules for a $(t_1 - 1, t_2 - 1, n - 1)$-ramp scheme having a share space of cardinality q. □

We can now prove the main result from [4].

Theorem 2.4. *If a (t_1, t_2, n)-ramp scheme has a share space of cardinality q, then $n - t_1 + 1 \leq q(t_2 - t_1)$.*

Proof. The proof is by induction on t_1, applying Lemma 2.3 and Theorem 2.2. □

A ramp scheme that meets the bound of Theorem 2.4 with equality will be termed *gap-optimal*. We observe that it is easy to find examples of gap-optimal ramp schemes with $t_1 = 1$.

Theorem 2.5. *For all integers $t, q \geq 2$, there exists a gap-optimal $(1, t, n)$-ramp scheme having a share space of cardinality q.*

Proof. Let $n = q(t - 1)$, $\mathcal{S} = \mathbb{Z}_q$ and $\mathcal{K} = \{K_1, K_2\}$. For any integer m, define $v(i, m) \in \mathcal{S}^m$ to be the m-tuple all of whose entries are equal to i. Now let

$$\mathcal{F}_1 = \{v(i, n) : i \in \mathcal{S}\}$$

and let

$$\mathcal{F}_2 = \{v(i, t-1) \parallel v(i + 1 \bmod q, t-1) \parallel \cdots \parallel v(i - 1 \bmod q, t-1) : i \in \mathcal{S}\}.$$

For example, if $q = t = 3$, then

$$\mathcal{F}_{K_1} = \{(1,1,1,1,1,1), (2,2,2,2,2,2), (0,0,0,0,0,0)\}$$

and

$$\mathcal{F}_{K_2} = \{(1,1,2,2,0,0), (2,2,0,0,1,1), (0,0,1,1,2,2)\}.$$

It can be verified that $\mathcal{F}_{K_1}$ and $\mathcal{F}_{K_2}$ comprise distribution rules for a $(1, t, q(t-1))$-ramp scheme having a share space of cardinality q and a secret space of cardinality two. □

It is more difficult to find examples of gap-optimal ramp schemes when $t_1 \geq 2$; however, we will give some examples with $t_1 = 2$ in Section 3.

2.1 Orthogonal Array Bounds

An *orthogonal array* $\mathrm{OA}_\lambda(t, m, q)$ is a $\lambda q^t \times m$ array A of symbols chosen from a set X of cardinality q, such that, within any t columns of A, every ordered t-tuple of symbols occurs in exactly λ rows of A. The parameter t is often called the *strength* of the orthogonal array. Orthogonal arrays have been studied extensively for over 60 years; for an extensive treatment of these objects, see Hedayat, Sloane and Stufken [9].

An *ideal threshold scheme* is one in which the share space and secret space have the same cardinality. It is well-known (see, for example, [6]) that an ideal (t, n)-threshold scheme with a share space of cardinality q is equivalent to an $\mathrm{OA}_1(t, n+1, q)$. In this case, Theorem 2.4 tells us that $n \leq q + t - 1$. It may be of interest to note that this special case of Theorem 2.4 is a classical orthogonal array bound (from 1952) known as the "Bush Bound". The standard proof of the Bush bound consists of two parts:

1. A proof that an $\mathrm{OA}_1(2, n, q)$ exists only if $n \leq q + 1$.
2. A proof that an $\mathrm{OA}_1(t, n, q)$ implies the existence of an $\mathrm{OA}_1(t-1, n-1, q)$.

The proof of 1. is in fact similar to, but even simpler than the proof of Theorem 2.2. It is interesting to note that the bound in 1. also follows immediately from the more complicated "Rao Bound", which was first proven in 1947. Finally, the proof of 2. is basically identical to that of Lemma 2.3. For details of the proofs of these and related bounds, see [9].

3 Codes and Ramp Schemes

We give a simple construction for ramp schemes from codes having specified distance and dual distance. This idea is not new: Chen and Cramer observed in [5, p. 529] that it is possible to "study privacy and reconstruction in terms of properties of the underlying linear codes and their duals ... their respective minimum distances imply bounds on the parameters of a ramp scheme". Here, we explicitly state how a code with specified distance and dual distance immediately yields a ramp scheme; this generalises a similar theorem given in [17]. We note that our generalisation does not require the use of linear codes: it works equally well for nonlinear codes by utilising the concept of *dual distance* as introduced by Delsarte [7, 8].

Here are some basic definitions relating to codes: A code $\mathcal{C}$ of *length* n over an alphabet Γ of cardinality q is a subset of Γ^n. The n-tuples in $\mathcal{C}$ are termed *codewords*. The *distance* of $\mathcal{C}$, denoted by d, is the minimum hamming distance between any two distinct codewords. The code $\mathcal{C}$ is a *linear* code if Γ is a finite field and $\mathcal{C}$ is a vector subspace of Γ^n. The code is a *binary* code if $q = 2$. Much information about codes can be found in standard textbooks, such as [1, 13, 18]. All the codes we require in this paper can be found in one or more of these textbooks, unless otherwise noted.

Here is the definition of dual distance of a code: suppose $A(\mathcal{C})$ is the distance distribution of a code $\mathcal{C}$ and $A'(\mathcal{C})$ is the MacWilliams transform of $A(\mathcal{C})$ (for more details, see [8]). Then the dual distance of $\mathcal{C}$ is the smallest positive integer d' such that $A'_{d'}(\mathcal{C}) \neq 0$. This definition applies to nonlinear as well as linear codes. It is well-known that the dual distance of a linear code is in fact equal to the distance of the dual code. Delsarte proved the following fundamental result:

Lemma 3.1. *[7, 8] Suppose $\mathcal{C}$ is a code of length n, on an alphabet of size q, having dual distance d^*. Then the $|\mathcal{C}| \times n$ array consisting of all the codewords in $\mathcal{C}$ is an $OA_\lambda(t, n, q)$, where $t = d^* - 1$ and $\lambda = |\mathcal{C}|/q^t$.*

Our next theorem was explicitly stated and proven for linear codes in the case $s = 1$ by Mirandola [17]. The proof we provide holds for nonlinear as well as linear codes; it is simplified by making use of the concept of dual distance.

Theorem 3.2. *Suppose $\mathcal{C}$ is a code of length n having distance d and dual distance d^*. Let $1 \leq s \leq d^* - 2$. Then there is a $(t_1, t_2, n-s)$-ramp scheme having information rate s, where $t_1 = d^* - s - 1$ and $t_2 = n - d + 1$.*

Proof. By Lemma 3.1, it follows that the $|\mathcal{C}| \times n$ array consisting of all the codewords in $\mathcal{C}$ is an orthogonal array of strength $t = d^* - 1$. Suppose the last s co-ordinates of each codeword define the secret and the remaining $n - s$ coordinates specify shares for $n - s$ participants. Therefore, we define

$$\mathcal{F}_{(r_{n-s+1},\ldots,r_n)} = \{(r_1, \ldots, r_{n-s}) : (r_1, \ldots, r_n) \in \mathcal{C}\}$$

for all $(r_{n-s+1}, \ldots, r_n) \in \mathcal{S}^s$. Given any $t - s$ shares and any $\mathcal{K}$, there are exactly $\lambda = |\mathcal{C}|/q^t$ distribution rules in $\mathcal{F}_K$ having the specified $t - s$ shares; this follows immediately because $\mathcal{C}$ is an orthogonal array of strength t. On the other hand, given any $n - d + 1$ shares, it is easy to show that there is at most one distribution rule containing the specified shares. For, if there existed two distribution rules containing $n - d + 1$ given shares, then the distance between the corresponding codewords would be at most $d - 1$, which is a contradiction. □

The above construction will serve to unify several constructions that can be found in the literature. It also allows us to easily find ramp schemes for a wide variety of parameter situations by using "off-the-shelf" codes. First we give a "classic" construction using Reed-Solomon codes (see, for example [10]).

Theorem 3.3. *Suppose that q is a prime power and $1 \leq s < t \leq n \leq q + 1$. Then there exists a $(t_1, t_2, n - s)$-ramp scheme over $\mathbb{F}_q$ having information rate s, where $t_1 = t - s$ and $t_2 = t$.*

Proof. If q is a prime power and $1 \leq t \leq n \leq q + 1$, then there is a Reed-Solomon code defined over $\mathbb{F}_q$, having length n, dimension t, distance $n - t + 1$ and dual distance $t + 1$. Let $s \leq t - 1$ and apply Theorem 3.2. We obtain a $(t_1, t_2, n - s)$-ramp scheme, where $t_1 = t - s$ and $t_2 = t$. □

Remark. In the above-constructed ramp scheme, the share space has cardinality q^s, which yields the optimal information rate (e.g., see [10]). When $s = 1$, we obtain the Shamir threshold scheme.

Another way that Theorem 3.2 can be applied makes use of algebraic geometry codes (AG codes); this approach was first described in [5]. We base our presentation on the simplified treatment of AG codes given in [14]. The starting point is an irreducible nonsingular projective curve of genus g having $n + 1$ rational points (i.e., points whose coordinates are in $\mathbb{F}_q$). Take m to be an integer such that $2g - 2 < m < n$. Under these assumptions, there is an AG code of length n, dimension $m - g + 1$, distance $d \geq n - m$ and dual distance $d^* \geq m - 2g + 2$. Then an application of Theorem 3.2 immediately yields the ramp schemes constructed in [5].[1]

Next, we give a new construction for ramp schemes that makes use of Reed-Muller codes. For $0 \leq r \leq m$, an *r-th order Reed-Muller code*, denoted $\mathcal{R}(r, m)$, is a binary linear code having length $n = 2^m$ and distance $d = 2^{m-r}$. For $0 \leq r < m$, the dual code of $\mathcal{R}(r, m)$ is $\mathcal{R}(m - r - 1, m)$, and so the dual distance of $\mathcal{R}(r, m)$ is $d^* = 2^{r+1}$. Setting $s = 1$ in Theorem 3.2, we obtain the following.

Theorem 3.4. *For $0 \leq r < m$, there exists a $(2^{r+1} - 2, 2^m - 2^{m-r} + 1, 2^m - 1)$-ramp scheme over a binary alphabet, having information rate 1.*

[1] However, we should note that [5] requires additional "multiplicative" properties of the constructed ramp schemes, which necessitate a more detailed examination of the algebraic structure of the underlying AG codes.

The above construction is of particular interest because it yields an infinite class of gap-optimal ramp schemes with $t_1 = 2$.

Corollary 3.5. *For $m \geq 2$, there exists a gap-optimal $(2, 2^{m-1}+1, 2^m - 1)$-ramp scheme over a binary alphabet, having information rate 1.*

Proof. Setting $r = 1$ in Theorem 3.4, the result is a (t_1, t_2, n)-ramp scheme over a binary alphabet, where $t_1 = 2$, $t_2 = 2^{m-1} + 1$ and $n = 2^m - 1$. Since

$$q(t_2 - t_1) = 2^m - 2 = n - t_1 + 1,$$

the scheme is gap-optimal. □

We finish this section by presenting a simple application of Theorem 3.2 that makes use of nonlinear codes. Let $r \geq 3$ be odd. The *Kerdock code* $\mathcal{K}(r+1)$ is a nonlinear binary code of length $n = 2^{r+1}$ having distance $d = 2^r - 2^{(r-1)/2}$ and dual distance $d^* = 6$.

Theorem 3.6. *Suppose $r \geq 3$ is odd and $1 \leq s \leq 4$. Then there exists a $(t_1, t_2, n-s)$-ramp scheme over a binary alphabet, having information rate s, where $t_1 = 5 - s$ and $t_2 = 2^r + 2^{(r-1)/2}$.*

4 A New Bound on Codes with Specified Distance and Dual Distance

We combine two previously discussed results in order to obtain a new bound on codes having specified distance and dual distance:

Theorem 4.1. *Suppose $\mathcal{C}$ is a code of length n, on an alphabet of size q, having distance d and dual distance d^* Then*

$$d \leq \frac{q-1}{q}(n - d^* + 2) + 1. \tag{1}$$

Proof. From the hypothesized code, we get a $(t_1, t_2, n-1)$-ramp scheme having a share space of cardinality q, where $t_1 = d^* - 2$ and $t_2 = n - d + 1$, by applying Theorem 3.2. Now we apply Theorem 2.4, which yields

$$(n-1) - (d^* - 2) + 1 \leq q((n - 1 - d + 2) - (d^* - 2)),$$

or

$$n - d^* + 2 \leq q(n - d - d^* + 3).$$

This simplifies to give the desired result. □

We also note that a bound having a similar flavour was proven much earlier (in 1973) by Delsarte [8], namely,

$$d \leq n - d^* + 2. \tag{2}$$

Matsumoto *et al.* [16] studied the function $N(d, d^*)$, which denotes the minimum length n of a linear binary code having distance d and dual distance d^*. (Their motivation was an application to the construction of certain boolean functions; see [12].) Several lower bounds for $N(d, d^*)$ were proven in [16], and constructions for small codes meeting some of these bounds were given. Additional work along this line can be found in [11].

If we set $q = 2$ in (1), then we obtain the following new bound on $N(d, d^*)$:

Corollary 4.2.

$$N(d, d^*) \geq 2d + d^* - 4. \tag{3}$$

The bound (3) is apparently unrelated to the bounds proven in [16]. The strongest bounds in [16] are linear programming bounds. As such, they cannot be considered to be explicit bounds, becuase a different LP has to be solved for every new parameter case in order to evaluate the bound. The bound (3) is, in general, not as strong as the linear programming bounds, but it is a very simple explicit bound which is often fairly close to the LP bounds.

We also note that the bound (3) holds for nonlinear as well as linear codes. The work in [16, 11] only considers linear codes, though some of the bounds proven in those papers also hold for nonlinear codes.

4.1 Examples

In this section, we give some examples of infinite classes of codes for which the bounds we proved above are tight. The allows the exact determination of $N(d, 3)$ and $N(d, 4)$ for infinitely many values of d.

A *simplex code* is a linear code of dimension k over the alphabet $\mathbb{F}_q$ (it is in fact the dual of the hamming code). Its length is $n = (q^k - 1)/(q - 1)$, it has distance $d = q^{k-1}$ and its dual distance $d^* = 3$. It is easy to verify that a simplex code meets the bound (1) with equality, because

$$\frac{q-1}{q}(n - d^* + 2) + 1 = \frac{q-1}{q}\left(\frac{q^k - 1}{q - 1} - 3 + 2\right) + 1 = q^{k-1}.$$

Setting $q = 2$, we immediately obtain the following theorem.

Theorem 4.3. *$N(2^m, 3) = 2^{m+1} - 1$ for all integers $m \geq 1$.*

Analogously, from a first-order Reed-Muller code (see Section 3), we obtain the following.

Theorem 4.4. *$N(2^m, 4) = 2^{m+1}$ for all integers $m \geq 1$.*

We refer again to the Kerdock codes as an interesting example involving nonlinear codes. As mentioned in Section 3, the Kerdock code $\mathcal{K}(r + 1)$ has length $n = 2^{r+1}$, distance $d = 2^r - 2^{(r-1)/2}$ and dual distance $d^* = 6$, where r is odd. Here we have

$$2d + d^* - 4 = 2^{r+1} - 2^{(r+1)/2} + 2 = n - \sqrt{n} + 2,$$

so the parameters of these codes are fairly close to the bound given in (3).

5 Summary

The main contributions of this paper are:

- a simplified proof of the threshold gap bound for ramp schemes,
- a simple, general construction of ramp schemes from nonlinear as well as linear codes, and
- a new bound on the length of codes having specified distance and dual distance.

One main topic for additional research is to find additional examples of ramp schemes and codes that meet the proven bounds with equality.

Acknowledgement

We would like to thank Ruizhong Wei for helpful comments.

References

[1] J. Bierbrauer. *Introduction to Coding Theory*, Chapman & Hall/ CRC, 2005.

[2] G.R. Blakley and C. Meadows. Security of ramp schemes. *LNCS* **196** (1985), 242–268 (CRYPTO 1984).

[3] C. Blundo, A. De Santis and U. Vaccaro. Efficient sharing of many secrets. *LNCS* **665** (1993), 692–703 (STACS '93).

[4] I. Cascudo, R. Cramer and C. Xing. Bounds on the threshold gap in secret sharing over small fields. Cryptology ePrint Archive: Report 2012/319, `http://eprint.iacr.org/2012/319`.

[5] H. Chen and R. Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. *LNCS* **4117** (2006), 521–536 (CRYPTO 2006).

[6] E. Dawson and E.S. Mahmoodian. Orthogonal arrays and ordered threshold schemes. *Australasian Journal of Combinatorics* **8** (1993), 27–44.

[7] P. Delsarte. *An Algebraic Approach to the Association Schemes of Coding Theory.* Philips Research Reports Supplements, 1973.

[8] P. Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Information and Control* **23** (1973), 407–438.

[9] A.S. Hedayat, N.J.A. Sloane and J. Stufken. *Orthogonal Arrays, Theory and Applications*, Springer, 1999.

[10] W.-A. Jackson and K.M. Martin. A combinatorial interpretation of ramp schemes. *Australasian Journal of Combinatorics* **14** (1996), 51–60.

[11] A. Kohnert. Construction of linear codes having prescribed primal-dual minimum distance with applications in cryptography. *Albanian Journal Math.* **2** (2008), 221–227.

[12] K. Kurosawa and T. Satoh. Design of SAC/PC(ℓ) of order k boolean functions and three other cryptographic criteria. *LNCS* **1233** (1997), 434–449 (EUROCRYPT 1997).

[13] J.H. van Lint. *Introduction to Coding Theory, Third Edition*, Springer, 1998.

[14] J.H. van Lint and T.A. Springer. Generalized Reed-Solomon codes from algebraic geometry. *IEEE Transactions on Information Theory* **33** (1987), 305–309.

[15] K.M. Martin, M.B. Paterson and D.R. Stinson. Error decodable secret sharing and one-round perfectly secure message transmission for general adversary structures. *Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences* **3** (2011), 65–86.

[16] R. Matsumoto, K. Kurosawa, T. Itoh, T. Konno, and T. Uyematsu. Primal-dual distance bounds of linear codes with application to cryptography. *IEEE Transactions on Information Theory* **52** (2006), 4251–4256.

[17] D. Mirandola. *Schur Products of Linear Codes: A Study of Parameters*. Master Thesis, Université de Bordeaux 1 / Stellenbosch University, 2012.

[18] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-correcting Codes*, North-Holland, 1977.

[19] W. Ogata and K. Kurosawa. Some basic properties of general nonperfect secret sharing schemes. *Journal of Universal Computer Science* **4** (1998), 690–704.

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