International Journal of Pure and Applied Mathematics
Volume 57 No. 1 2009, 87-102

SECRET SHARING SCHEMES BASED ON ALMOST-BENT FUNCTIONS

J.C. Ku-Cauich[1], H. Tapia-Recillas[2] §
[1,2]Departamento de Matemáticas
Universidad Autónoma Metropolitana-Iztapalapa
Col. Vicentina, Del. Iztapalapa, México, D.F., 09340, MEXICO
[1]e-mail: jckc35@hotmail.com
[2]e-mail: htr@xanum.uam.mx

Abstract: A class of linear codes over the finite field $\mathbf{F}_{2^h}$ ($h \geq 1$, an integer) based on almost-bent functions is introduced and the length, dimension and bounds (upper/lower) of the weight of the nonzero codewords of these codes are determined. A secret sharing scheme based on these codes whose secret space is the field $\mathbf{F}_{2^h}$ is given as well as two such schemes whose secret space is of the form $\mathbf{F}_2^m$ which are extensions of a scheme with secret space is $\mathbf{F}_2$.

AMS Subject Classification: 94B05, 94A62
Key Words: almost-bent functions, linear codes, secret sharing schemes

1. Introduction

Since their introduction by G.R. Blakley [3] and A. Shamir [16], secret sharing schemes (SSSch) have attracted the attention of several research groups and a number of such schemes have been proposed. One construction, introduced by J.L. Massey [11] is based on linear error-correcting codes over a finite field, although R.J. McElice and D.V. Sarwate [12] previously pointed out the relation between Shamir's scheme and Reed-Solomon codes. Since the publication of

Received: October 2, 2009

§Correspondence author

these results, several constructions of (SSSch) based on linear error-correcting codes over finite fields have appeared in the literature (see [1], [18], [14], [9], [6], [17]). Any linear code over a finite field can be used to construct a secret sharing scheme but there are several problems that must be resolved, including how to determine the access structure of a (SSSch) based on a linear code, and how to construct linear codes so that the access structure of the corresponding (SSSch) is appropriate. The first problem is related to the covering problem, i.e., determining the minimal codewords of a linear code, which in general is an open question [2]. The second problem is also difficult to solve and depends on the solution to the first. In general terms it seems that only linear codes with suitable properties give appropriate access structures of (SSSch) based on these codes (see [6], [14], [18]).

In [6] a class of linear codes using perfect nonlinear maps over a finite field $\mathbf{F}_q$ where $q = p^r$ and $p \neq 2$ a prime is introduced and those codes are used to determine some (SSSch). Later the same authors determined the weight distribution of these linear codes [19]. In this note we treat the case $p = 2$ and using almost-bent functions over the finite field $\mathbf{F}_{2^n}$ (n an odd integer), a class of linear codes is introduced and their parameters are determined, including upper and lower bounds of the weight of the nonzero codewords. Also, a (SSSch) based on these codes is given where the secret space is a field of the form $\mathbf{F}_{2^h}$ (h a divisor of n). If $h = 1$, the secret space is small and two extended secret sharing schemes (ESSSch) are also presented. The note is organized as follows: in the next section basic results on almost-bent functions are recalled, in Section 3 a class of linear codes based on these functions is introduced and the parameters as well as bounds on the weight of the codewords are determined. General facts concerning (SSSch) associated to linear codes are recalled in Section 4 and a secret sharing scheme based on the introduced linear codes is given in Section 5. Two extended (SSSch) whose secret space is of the form $\mathbf{F}_2^m$ when the code under consideration is a binary linear code are discussed in Section 6. Some results presented in this note were announced with no proofs in [10].

2. Preliminaries

In this section basic definitions and facts about Boolean functions are recalled including nonlinearity and almost-bentness. For further details we refer the reader to [7], [8].

Throughout this note n is an odd integer. Let $\mathcal{A}$ be the group of affine

functions from $\mathbf{F}_{2^n}$ to itself. The *nonlinearity* of a function $f : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^n}$ is defined as:

$$\mathcal{N}_f = \min_{\alpha \in \mathcal{A}} d(f, \alpha),$$

where

$$d(f, g) = |\{x \in \mathbf{F}_{2^n} : \ f(x) \neq g(x)\}|$$

is the Hamming distance between the functions f and g.

Let h be such that $n = hk$ and let $Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}} : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^h}$ be the (relative) trace function. For a given $f : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^n}$ and elements $a, b \in \mathbf{F}_{2^n}$, let

$$\lambda_f(a, b) = \sum_{x \in \mathbf{F}_{2^n}} (-1)^{Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(af(x)+bx)}$$

be the Walsh transform of the function $af(x) + bx$.

A well known fact is that the nonlinearity N_f of a function f is such that

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbf{F}_{2^n}^*, \ b \in \mathbf{F}_{2^n}} |\lambda_f(a, b)|$$

and satisfies the relation (see [7]):

$$\mathcal{N}_f \leq 2^{n-1} - 2^{\frac{n-1}{2}}.$$

A function f is called *almost-bent* if $\mathcal{N}_f$ satisfies the equality of the previous relation. It is easy to see that the Walsh spectrum, Λ_f, of an almost-bent function f is (see [7]):

$$\Lambda_f = \{\lambda_f(a, b); \ a, b \in \mathbf{F}_{2^n}, \ a \neq 0\} = \{0, \pm 2^{\frac{n+1}{2}}\}.$$

Examples of almost-bent functions include those given in the following result (cf. [14], [7]).

Theorem 1. *Let $n = 2t + 1$ be a positive integer and let $f : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^n}$ be the function given by $f(x) = x^{2^r+1}$ where $(n, r) = 1$ and $1 \leq r \leq t$. Then f is an almost-bent function.*

Let $n = hk$ and let $\mathbf{F}_{2^h}$ be the subfield of $\mathbf{F}_{2^n}$ as above. The following result appears in [5].

Lemma 2. *Let $f : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^n}$ be a function and let $(a_i, b_i) \in \mathbf{F}_{2^n} \times \mathbf{F}_{2^n}$, $i = 1, 2, ..., l$, $1 \leq l \leq k$, be linearly independent over $\mathbf{F}_{2^h}$. For $u_1, u_2, ..., u_l \in \mathbf{F}_{2^h}$ let*

$$Z(f; a_1, b_1, \ldots, a_l, b_l; u_1, \ldots, u_l) = |\{x \in \mathbf{F}_{2^n} : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(a_i f(x) + b_i x) = u_i, \ i = 1, \ldots, l\}|.$$

Then, for $l = 1$,

$$|Z(f; a_1, b_1; u_1) - 2^{n-h}| \leq \left(1 - \frac{1}{2^h}\right)(2^n - 2N_f).$$

If $l > 1$ *and* $a_1, a_2, ..., a_l$ *are linearly dependent over* $\mathbf{F}_{2^h}$, *then*

$$|Z(f; a_1, b_1, \ldots, a_l, b_l; u_1, \ldots, u_l) - 2^{n-lh}| \leq \left(1 - \frac{1}{2^h}\right)(2^n - 2N_f).$$

Some consequences of this lemma that will be useful later are the following.

Corollary 3. *Let* n *be an odd integer,* h *a divisor of* n, $f : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$ *a function. Then,*

$$\begin{aligned} & (2^h - 1)\left(2^{n-h} - (1 - \frac{1}{2^h})(2^n - 2N_f)\right) \\ \leq\ & |\{x \in \mathbf{F}_{2^n} : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(af(x) + bx) \in \mathbf{F}_{2^h}^*\}| \\ \leq\ & (2^h - 1)\left(2^{n-h} + (1 - \frac{1}{2^h})(2^n - 2N_f)\right). \end{aligned}$$

Proof. Let $u_1, \ldots, u_{2^h-1}$ be all the elements of $\mathbf{F}_{2^h}^*$ and

$$N_{u_i} = |\{x \in \mathbf{F}_{2^n} : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(af(x) + bx) = u_i\}|, i = 1, \ldots, 2^h - 1.$$

Then

$$\begin{aligned} & \left||\{x \in \mathbf{F}_{2^n} : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(af(x) + bx) \in \mathbf{F}_{2^h}^*\}| - (2^h - 1)(2^{n-h})\right| \\ & \quad = \left|N_{u_1} - 2^{n-h} + N_{u_2} - 2^{n-h} + \cdots + N_{u_{2^h-1}} - 2^{n-h}\right| \\ & \quad \leq |N_{u_1} - 2^{n-h}| + \cdots + |N_{u_{2^h-1}} - 2^{n-h}| \leq (2^h - 1)(1 - \frac{1}{2^h})(2^n - 2N_f), \end{aligned}$$

which implies the claim. □

Corollary 4. *Let* n *be an odd integer,* h *a divisor of* n, $f : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$ *an almost-bent function. Then,*

$$\begin{aligned} & (2^h - 1)\left(2^{n-h} - (1 - \frac{1}{2^h})2^{\frac{n+1}{2}}\right) \\ \leq\ & |\{x \in \mathbf{F}_{2^n} : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(af(x) + bx) \in \mathbf{F}_{2^h}^*\}| \\ \leq\ & (2^h - 1)\left(2^{n-h} + (1 - \frac{1}{2^h})2^{\frac{n+1}{2}}\right). \end{aligned}$$

Proof. Since the functions f is almost-bent, $N_f = 2^{n-1} - 2^{\frac{n-1}{2}}$, and the result follows from Corollary 3. □

If it is also assumed that the function $f : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$ is such that $f(0) = 0$

we have the following,

Corollary 5. *Let n be an odd integer, h a divisor of n, $f : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$ be a function such that $f(0) = 0$. Then,*

$$\begin{aligned} & \frac{2^h - 1}{2^h}(2^n - (2^n - 2N_f)) \\ \leq\ & |\{x \in \mathbf{F}_{2^n}^* : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(af(x) + bx) \in \mathbf{F}_{2^h}^*\}| \\ \leq\ & \frac{2^h - 1}{2^h}(2^n + (2^n - 2N_f)). \end{aligned}$$

Proof. If $(a, b) \neq (0, 0)$, as $f(0) = 0$, from Lemma 2 it follows that

$$\begin{aligned} & 2^{n-h} - \frac{2^h - 1}{2^h}(2^n - 2N_f) - 1 \\ \leq\ & |\{x \in \mathbf{F}_{2^n}^* : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(af(x) + bx) = 0\}| \\ \leq\ & 2^{n-h} + \frac{2^h - 1}{2^h}(2^n - 2N_f) - 1, \end{aligned}$$

which implies the claim. □

Corollary 6. *Let n be an odd integer, h a divisor of n and $f : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$ an almost-bent function such that $f(0) = 0$. Then,*

$$\begin{aligned} & \frac{2^h - 1}{2^h}(2^n - 2^{\frac{n+1}{2}}) \\ \leq\ & |\{x \in \mathbf{F}_{2^n}^* : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(af(x) + bx) \in \mathbf{F}_{2^h}^*\}| \\ \leq\ & \frac{2^h - 1}{2^h}(2^n + 2^{\frac{n+1}{2}}). \end{aligned}$$

Proof. The claim follows from Corollary 5. □

3. The Linear Codes

In this section a class of linear codes associated to an almost-bent function is introduced. The length, dimension, upper and lower bounds for the weight of the nonzero codewords are determined.

Let n be an odd integer and h such that $n = hr$, $h > 1$, as above and let $f : \mathbf{F}_{2^n} \to \mathbf{F}_{2^n}$ be an almost-bent function. For $a, b \in \mathbf{F}_{2^n}$ let

$$F_{a,b}(x) := af(x) + bx,$$

$$C_{a,b} := (Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{a,b}(\gamma))_{\gamma \in \mathbf{F}_{2^n}^*}),$$

and

$$\mathcal{C} := \{C_{a,b} : a, b \in \mathbf{F}_{2^n}\} \subseteq \mathbf{F}_{2^h}^{2^n-1}.$$

Then we have the following,

Theorem 7. *With the notation as above, $\mathcal{C}$ is a $[2^n - 1, 2n/h]$-linear code over the field $\mathbf{F}_{2^h}$ and a basis is given by:*

$$B = \{C_{1,0}, C_{\beta,0}, \ldots, C_{\beta^{r-1},0}, C_{0,1}, C_{0,\beta}, \ldots, C_{0,\beta^{r-1}}\},$$

where β is a primitive element of $\mathbf{F}_{2^n}$ over $\mathbf{F}_{2^h}$.

Proof. Since $\{1, \beta, \ldots, \beta^{r-1}\}$ is a basis for $\mathbf{F}_{2^n}$ over $\mathbf{F}_{2^h}$, from the linearity of the trace function it is easy to see that the set B spans the linear code $\mathcal{C}$. The linear independence of the elements of the set B follows from the transitivity of the trace function and the fact that for an almost-bent function F,

$$|\{x \in \mathbf{F}_{2^n} : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\theta_1 F(x) + \theta_2 x) = 1\}| \in \{2^{n-1}, 2^{n-1} \pm 2^{\frac{n-1}{2}}\},$$

for any $0 \neq \theta_1, \theta_2 \in \mathbf{F}_{2^n}$. □

Observation. The basis of the code $\mathcal{C}$ given above determines a generating matrix for the code. The linear code $\mathcal{C}$ just introduced can be seen as an evaluation code in the following way. The set

$$\mathbf{F} := \{Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{a,b}(x)) : a, b \in \mathbf{F}_{2^n}\},$$

is a $\mathbf{F}_{2^h}$-vector space of dimension $2n/h$ and the evaluation map on $\mathbf{F}$:

$$ev_{\mathbf{F}_{2^n}^*} : \mathbf{F} \to \mathbf{F}_{2^h}^{2^n-1}$$
$$ev_{\mathbf{F}_{2^n}^*}(Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{a,b})) = C_{a,b} = (Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{a,b}(\gamma))_{\gamma \in \mathbf{F}_{2^n}^*})$$

is linear and injective. Then $\mathcal{C} = ev_{\mathbf{F}_{2^n}^*}(\mathbf{F})$ is a linear code over $\mathbf{F}_{2^h}$. A basis is given by the image under the mapping $ev_{\mathbf{F}_{2^n}^*}$ of the elements of the set

$$\Omega = \{Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{1,0}(x)), Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{\beta,0}(x)), \ldots, Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{\beta^{r-1},0}(x)),$$
$$Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{0,1}(x)), Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{0,\beta}(x)), \ldots, Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(F_{0,\beta^{r-1}}(x))\},$$

where β is a primitive element of the field $\mathbf{F}_{2^n}$ and $\{1, \beta, \ldots, \beta^{r-1}\}$ is a basis for $\mathbf{F}_{2^n}$ over $\mathbf{F}_{2^h}$.

Concerning the weight of the nonzero codewords of the code $\mathcal{C}$ introduced above we have the following results.

Corollary 8. *Let n be an odd integer and h a divisor of n. Let $f : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^n}$ be an almost-bent function and $\mathcal{C}$ be the $[2^n - 1, 2n/h] - \mathbf{F}_{2^h}$ linear code introduced above. Then the Hamming weight ω of any nonzero codeword of $\mathcal{C}$*

is such that:

$$(2^h-1)\left(2^{n-h}-(1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right)\leq\omega\leq(2^h-1)\left(2^{n-h}+(1-\frac{1}{2^h})2^{\frac{n+1}{2}}\right).$$

Proof. Since f is almost-bent, $N_f=2^{n-1}-2^{\frac{n-1}{2}}$ and the claim follows from Corollary 4 in the preceding section. □

If, in addition, it is assumed that the function f is such that $f(0)=0$ we have the following,

Corollary 9. *Let n be an odd integer, h a proper divisor of n. Let $f:\mathbf{F}_{2^n}\longrightarrow\mathbf{F}_{2^n}$ be an almost-bent function such that $f(0)=0$ and $\mathcal{C}$ be the $[2^n-1,2n/h]-\mathbf{F}_{2^h}$ linear code introduced above. Then the weight ω of any nonzero codeword of $\mathcal{C}$ is such that:*

$$\frac{2^h-1}{2^h}(2^n-2^{\frac{n+1}{2}})\leq\omega\leq\frac{2^h-1}{2^h}(2^n+2^{\frac{n+1}{2}}).$$

Proof. The result follows from Corollary 6 in the preceding section. □

The following result gives a lower bound of the minimum distance of the dual code of $\mathcal{C}$.

Proposition 10. *Let f be an almost-bent function and let $\mathcal{C}$ be the $[2^n-1,2n/h]$ linear code over the field $\mathbf{F}_{2^h}$ as introduced above. Then the dual code $\mathcal{C}^\perp$ has minimum distance $d^\perp\geq 2$.*

Proof. Let G be the generating matrix of the linear code $\mathcal{C}$ associated to the basis $B=\{C_{1,0},C_{\beta,0},..,C_{\beta^{k-1},0},C_{0,1},C_{0,\beta},...,C_{0,\beta^{k-1}}\}$ given in the proof of Theorem 7. Observe that none of the columns of the matrix G have all its entries equal to zero. Since G is a parity check matrix for the dual code $\mathcal{C}^\perp$, if a codeword of $\mathcal{C}^\perp$ has weight equal to 1, it would imply that G has a zero column, which is not possible and the claim follows. □

In the above discussion an odd integer n was taken, a divisor h of it and a $\mathbf{F}_{2^h}$ linear code $\mathcal{C}$ was defined based on an almost-bent function $f:\mathbf{F}_{2^n}\longrightarrow\mathbf{F}_{2^n}$. If $h=1$ then $\mathcal{C}$ is a binary linear code and in this case the weight distribution of the code can be given.

We begin by determining the possible weights of the nonzero codewords of $\mathcal{C}$.

Proposition 11. *With the notation as introduced above, the weight of any nonzero codeword of $\mathcal{C}$ can take one of the following values: $2^{n-1},2^{n-1}\pm 2^{\frac{n-1}{2}}$. Furthermore, the minimum weight, $d^\perp$, of the dual code $\mathcal{C}^\perp$ is such that $d^\perp\geq 3$.*

Proof. Let $B_1=|\{x\in\mathbf{F}_{2^n}:Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(af(x)+bx)=1,a\neq 0\}|$ and

$B_0 = |\{x \in \mathbf{F}_{2^n} : Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(af(x) + bx) = 0\}|$. We recall that for an almost-bent function f, $\lambda_f(a,b) \in \{0, 2^{\frac{n+1}{2}}, -2^{\frac{n+1}{2}}\}$. If $\lambda_f(a,b) = 2^{\frac{n+1}{2}}$, it follows that $B_0 - B_1 = 2^{\frac{n+1}{2}}$ and hence $B_1 = 2^{n-1} - 2^{\frac{n-1}{2}}$, if $\lambda_f(a,b) = -2^{\frac{n+1}{2}}$ it can be seen that $B_1 = 2^{n-1} + 2^{\frac{n-1}{2}}$ and if $\lambda_f(a,b) = 0$ then $B_1 = B_0 = 2^{n-1}$, and the first claim follows. For the second claim observe that if two columns, say $i+1$, $j+1$, $j = 0, \ldots, 2^n - 2$, of the generating matrix G of the code $\mathcal{C}$ given above, are equal, without loss of generality we may assume that $i < j$, then
$Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\alpha^j - \alpha^i) = Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\beta(\alpha^j - \alpha^i)) = \cdots = Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\beta^{r-1}(\alpha^j - \alpha^i)) = 0$
and therefore for any $x \in \mathbf{F}_{2^n}^*$, $x = e_0 1 + e_1\beta + \cdots + e_{r-1}\beta^{r-1}$,

$$Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}((\alpha^j - \alpha^i)x) = e_0 Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\alpha^j - \alpha^i) + e_1 Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\beta(\alpha^j - \alpha^i))$$
$$+ \cdots + e_{r-1} Tr_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\beta^{r-1}(\alpha^j - \alpha^i)) = 0, \ \forall x$$

which implies that $\alpha^j - \alpha^i = 0$, but since $i \neq j$, this is not possible. If a codeword of $\mathcal{C}$ has weight equal to 2 it would imply that two columns of G are equal, which it is not possible by the above argument. A similar argument as in the proof of Proposition 10 shows that $d^\perp \geq 3$. □

From this result the weight distribution of the code $\mathcal{C}$ (binary case) can be obtained. We first recall the power moments relations introduced by Pless (cf. [15]).

Theorem 12. *Let $\mathcal{C}$ be a $[n,k]$ binary linear code. Let A_i be the number of codewords of $\mathcal{C}$ having weight i and let B_j be the number of codewords of the dual code $\mathcal{C}^\perp$ having weight j. Then,*

$$\sum_{j=0}^{n} j^r A_j = \sum_{j=0}^{n} (-1)^j B_j \left(\sum_{v=0}^{r} v! S(r,v) 2^{k-v} \begin{pmatrix} n-j \\ n-v \end{pmatrix} \right),$$

where

$$S(r,v) = \frac{1}{v!} \sum_{i=0}^{v} (-1)^{v-i} \begin{pmatrix} v \\ i \end{pmatrix} i^r.$$

Observation. From the relations given in Theorem 12 it is easy to see that:

1. $\sum_{j=0}^{n} A_j = 2^k$.
2. $\sum_{j=0}^{n} jA_j = 2^{k-1}(n - B_1)$.
3. $\sum_{j=0}^{n} j^2 A_j = 2^{k-2} n(n+1) - 2^{k-1} n B_1 + 2^{k-1} B_2$.

Lemma 13. *Let $\mathcal{D}$ be a binary $[2^n - 1, 2n]$ linear code such that the possible weights of its codewords are $0, a = 2^{n-1} - 2^{\frac{n-1}{2}}, b = 2^{n-1}, c = 2^{n-1} + 2^{\frac{n-1}{2}}$ and*

the minimum distance of the dual code $\mathcal{D}^\perp$ is ≥ 3. Then:

$$\begin{aligned} A_0 &= 1, \\ A_a &= (2^n-1)(2^{n-2}+2^{\frac{n-3}{2}}), \\ A_b &= (2^n-1)(2^{n-1}+1), \\ A_c &= (2^n-1)(2^{n-2}-2^{\frac{n-3}{2}}). \end{aligned}$$

Proof. Since $B_1 = B_2 = 0$ the result follows by solving for A_a, A_b, A_c in the relations given in the previous observation. □

As an immediate consequence of Proposition 11 and Lemma 13 we have the following,

Corollary 14. *Let $f : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^n}$ be an almost-bent function and let $\mathcal{C}$ be the binary linear code as introduced above (i.e., the case $h = 1$). Then the weight distribution of $\mathcal{C}$ is as given in Lemma 13. In particular, this code has minimum distance $d = 2^{n-1} - 2^{\frac{n-1}{2}}$.*

Observation. Corollary 14 is a particular case of the following more general result due to A. Canteaut et al [4].

Theorem 15. *Let $\mathcal{C}$ be a $[2^n - 1, 2n, d]$ binary linear code such that the all-one vector is not in $\mathcal{C}$. Assume that the minimum distance $d^\perp$ of the dual $\mathcal{C}^\perp$ code is such that $d^\perp \geq 3$ and let ω_0 be the minimum integer such that $0 < \omega_0 < 2^{n-1}$ and that $A_{\omega_0} + A_{2^n-\omega_0} \neq 0$. Then*

$$\omega_0 \leq 2^{n-1} - 2^{\frac{n-1}{2}}.$$

The equality is achieved if and only if the weight of any word of the code is one of the following:

$$\{0, 2^{n-1}, 2^{n-1} - 2^{\frac{n-1}{2}}, 2^{n-1} + 2^{\frac{n-1}{2}}\}.$$

Note that in our linear code $\mathcal{C}$, $\omega_0 = 2^{n-1} - 2^{\frac{n-1}{2}}$ since $A_{\omega_0} + A_{2^n-\omega_0} = 0$ if $\omega_0 < 2^{n-1} - 2^{\frac{n-1}{2}}$. This number is the minimum integer with this property in the code $\mathcal{C}$.

4. Secret Sharing Schemes Based on Linear Codes

In this section general facts about secret sharing schemes (SSSch) based on linear codes that will be used later are recalled. Further details can be found in [6] (see also [11], [2]).

Let $\mathcal{C}$ be a $[n, k, d]$ linear code over the finite field $\mathbf{F}_q$ (q a power of a prime

p) and let $G = (\mathbf{g}_0, \mathbf{g}_1, ..., \mathbf{g}_{n-1})$ be a generating matrix for $\mathcal{C}$, where each $\mathbf{g}_i$ is a non-zero column, and as usual, $\mathcal{C}^\perp$ denotes the dual code of $\mathcal{C}$.

In the (SSSch) based on a linear code $\mathcal{C}$, the secret s is an element of the field $\mathbf{F}_q$ and has an equal probability of being any element of the field. In addition, there is a dealer P_0 and $n-1$ parties $P_1, ..., P_{n-1}$ involved.

In order to compute the shares of a secret s, the dealer chooses an element $\mathbf{u} = (u_0, u_1, ..., u_{k-1}) \in \mathbf{F}_q^k$ at random such that $s = \mathbf{u}\mathbf{g}_0$ (there are q^{k-1} such elements). The dealer takes $\mathbf{u}$ as an information vector, computes the corresponding codeword:

$$\mathbf{v} = \mathbf{u}G = (v_0, v_1, ..., v_{n-1})$$

and gives the share v_i to party P_i for each $i = 1, 2, ..., n-1$.

Since $s = v_0 = \mathbf{u}\mathbf{g}_0$, the recovery of the secret s is given by the following result (see [6], [11]):

Lemma 16. *Let G be a generating matrix for a $[n, k]$ linear code $\mathcal{C}$ over the field $\mathbf{F}_q$. In the secret sharing scheme based on $\mathcal{C}$, a set of shares $\{v_{i_1}, v_{i_2}, ..., v_{i_m}\}$ determines the secret s if and only if there is a codeword*

$$(1, 0, ..., 0, c_{i_1}, 0, ..., 0, c_{i_m}, 0, ..., 0) \in \mathcal{C}^\perp,$$

where $c_{i_j} \neq 0$ for at least one j, $1 \leq i_1 \leq \cdots \leq i_m \leq n-1$ and $1 \leq m \leq n-1$.

If there is such a codeword in $\mathcal{C}^\perp$ then the column $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_{i_1}, ..., \mathbf{g}_{i_m}$, say, $\mathbf{g}_0 = a_1\mathbf{g}_{i_1} + \cdots + a_m\mathbf{g}_{i_m}$, and the secret s is recovered as

$$s = a_1 v_{i_1} + \cdots + a_m v_{i_m}.$$

It is obvious that if a subset of participants can recover the secret from their shares, then any set of participants containing this subset can also recover the secret, so it is important to consider those sets of participants that can recover the secret from their shares in such a way that no proper subsets can do so. These sets of participants are called *minimal access sets*. Thus in the secret sharing scheme based on a linear code one is interested in the minimal access sets, and these sets have a nice interpretation in terms of some codewords of the code. First recall that the support of $\mathbf{c} = (c_0, c_1, ..., c_{n-1}) \in \mathbf{F}_q^n$ is the set $supp(\mathbf{c}) = \{i : 0 \leq i \leq n-1 : c_i \neq 0\}$. A codeword $\mathbf{c}_2$ is said to cover a codeword $\mathbf{c}_1$ if $supp(\mathbf{c}_2) \supseteq supp(\mathbf{c}_1)$. A codeword is called *minimal* if the only codewords it covers are its non-zero multiples (see [6]).

From Lemma 16 it follows that there is a one-to-one correspondence between the minimal access sets of a secret sharing scheme based on a linear code $\mathcal{C}$ and the minimal codewords of the dual code $\mathcal{C}^\perp$ whose first coordinate is equal to 1. Thus in order to determine the access structure of a secret sharing scheme

under consideration, it is enough to determine the subset of minimal codewords with the first coordinate equal to 1, from the set of minimal codewords. The *covering problem* of a linear code is that of determining the set of minimal codewords of the code.

The following result provides, in some cases, a way to determine the minimal codewords of a linear code (see [6]).

Theorem 17. *Let M be the maximum nonzero weight of a $[n, k, d]$ linear code $\mathcal{C}$ over the finite field $\mathbf{F}_q$. Then if*

$$\frac{d}{M} > \frac{q-1}{q}$$

each nonzero codeword of $\mathcal{C}$ is minimal.

A characterization of the minimal access sets of a secret sharing scheme based on the dual code of a given linear code can be determined.

The following result will be useful in the next section (see [6]).

Theorem 18. *Let $\mathcal{C}$ be a $[n, k, d]$ linear code over $\mathbf{F}_q$ with generating matrix*

$$G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1})$$

and let $\mathcal{C}^\perp$ be its dual code with minimum distance $d^\perp$. If each nonzero codeword of $\mathcal{C}$ is minimal, then in the secret sharing scheme based on $\mathcal{C}^\perp$ there are q^{k-1} minimal access sets and:

1. If $d^\perp = 2$,

a) if $\mathbf{g}_i$ is a multiple of $\mathbf{g}_0$, $1 \le i \le n-1$, then participant P_i, must be in every minimal access set,

b) if $\mathbf{g}_i$ is not a multiple of $\mathbf{g}_0$, $1 \le i \le n-1$, then participant P_i must be in $(q-1)q^{k-2}$ minimal access sets.

2. If $d^\perp \ge 3$ and

$$1 \le t \le \min\{k-1, d^\perp - 2\},$$

every group of t participants is involved in

$$(q-1)^t q^{k-(t+1)}$$

minimal access sets.

5. A Secret Sharing Scheme

If $\mathbf{F}_{2^n}$ is the finite field with 2^n elements (n odd), $f : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^n}$ an almost-bent function and h is a divisor of n, for $a, b \in \mathbf{F}_{2^n}$ let $f_{a,b}(x) = af(x) + bx$, $C_{a,b} = (Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}}(f_{a,b}(\gamma))_{\gamma \in \mathbf{F}_{2^n}^*})$, where $Tr_{\mathbf{F}_{2^n}/\mathbf{F}_{2^h}} : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^h}$ is the trace function. Let

$$\mathcal{C} = \{C_{a,b} : \ a, b \in \mathbf{F}_{2^n}\} \subseteq \mathbf{F}_{2^h}^{2^n-1}$$

be the $[2^n - 1, 2n/h]$-linear code over the field $\mathbf{F}_{2^h}$ introduced in Section 3. In this section a secret sharing scheme based on the dual of the linear code $\mathcal{C}$ is given.

Proposition 19. *Let $w_{\min}$ and $w_{\max}$ be the minimum and maximum (Hamming) weight of the non-zero codewords of the linear code $\mathcal{C}$. If $n \geq 5h$ and $h \geq 3$ then,*

$$\frac{w_{\min}}{w_{\max}} > \frac{2^h - 1}{2^h}.$$

Proof. From Corollary 8 it follows that

$$w_{\min} \geq (2^h - 1)\left(2^{n-h} - (1 - \frac{1}{2^h})2^{\frac{n+1}{2}}\right)$$

and

$$w_{\max} \leq (2^h - 1)\left(2^{n-h} + (1 - \frac{1}{2^h})2^{\frac{n+1}{2}}\right)$$

from which it can be seen that

$$\frac{w_{\min}}{w_{\max}} \geq \frac{2^{\frac{n-1}{2}} - (2^h - 1)}{2^{\frac{n-1}{2}} + (2^h - 1)} > \frac{2^h - 1}{2^h}$$

and the claim is proved.

Observe that if $n = 3h$ then

$$2^{2h+1} - 32^h + 1 > 2^{\frac{n-1}{2}}$$

and hence

$$\frac{2^{\frac{n-1}{2}} - (2^h - 1)}{2^{\frac{n-1}{2}} + (2^h - 1)} < \frac{2^h - 1}{2^h}.$$

Therefore the relation stated in the proposition does not hold. □

Proposition 20. *Let $w_{\min}$ and $w_{\max}$ be as above. If $f(0) = 0$, $n \geq 3h$ and $h \geq 3$ then,*

$$\frac{w_{\min}}{w_{\max}} > \frac{2^h - 1}{2^h}.$$

Proof. From Corollary 9 it follows that,

$$\frac{w_{\min}}{w_{\max}} \geq \frac{\frac{2^h-1}{2^h}(2^n - 2^{\frac{n+1}{2}})}{\frac{2^h-1}{2^h}(2^n + 2^{\frac{n+1}{2}})} = \frac{2^{\frac{n+1}{2}}(2^{\frac{n-1}{2}} - 1)}{2^{\frac{n+1}{2}}(2^{\frac{n-1}{2}} + 1)} = \frac{2^{\frac{n-1}{2}} - 1}{2^{\frac{n-1}{2}} + 1}.$$

If $n \geq 3h$, $h \geq 3$,

$$2^{h+1} = 2^h 2 = (2^{2h}2^2)^{1/2} = (\frac{2^{2h}2^3}{2})^{1/2} \leq (\frac{2^{2h}2^h}{2})^{1/2} = (\frac{2^{3h}}{2})^{1/2}$$
$$= 2^{\frac{3h-1}{2}} \leq 2^{\frac{n-1}{2}},$$

then,

$$2^{h+1} - 1 < 2^{\frac{n-1}{2}}.$$

Therefore,

$$2^h 2^{\frac{n-1}{2}} - 2^h > 2^h 2^{\frac{n-1}{2}} + 2^h - 2^{\frac{n-1}{2}} - 1,$$

from which it follows that,

$$2^h \left(2^{\frac{n-1}{2}} - 1\right) > (2^h - 1)\left(2^{\frac{n-1}{2}} + 1\right).$$

Thus,

$$\frac{2^{\frac{n-1}{2}} - 1}{2^{\frac{n-1}{2}} + 1} > \frac{2^h - 1}{2^h},$$

from which the claim of the proposition follows. □

Theorem 21. *Let $w_{\min}$ and $w_{\max}$ be the minimum and maximum (Hamming) weight of the non-zero codewords of the linear code $\mathcal{C}$. If $n > 3$ and $h = 1$, then,*

$$\frac{w_{\min}}{w_{\max}} > \frac{1}{2}.$$

Proof. We know that

$$w_{\min} = 2^{n-1} - 2^{\frac{n-1}{2}} \text{ and } w_{\max} = 2^{n-1} + 2^{\frac{n-1}{2}}.$$

If $n > 3$, then

$$2^{\frac{n+1}{2}} - 3 > 0,$$

so that

$$2 \times 2^{\frac{n+1}{2}} - 2 > 2^{\frac{n-1}{2}} + 1,$$

and hence,

$$\frac{2^{n-1} - 2^{\frac{n-1}{2}}}{2^{n-1} + 2^{\frac{n-1}{2}}} > \frac{1}{2}.$$

□

It follows from Theorem 18 that a characterization of the minimal access

sets from a (SSSch) based on the dual of the linear code $\mathcal{C}$ can be given.

Theorem 22. *Let $n \geq 5h$, $h \geq 3$, or $f(0) = 0$ and $n \geq 3h$, $h \geq 3$. Then all the codewords of the linear code $\mathcal{C}$ are minimal and in the secret sharing scheme based in $\mathcal{C}^{\perp}$, if*

$$G = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1})$$

is a generator matrix, there are 2^{2n-h} minimal access sets and,

— When $d^{\perp} = 2$,

a) if $\mathbf{g}_i$ is multiple of $\mathbf{g}_0$, $1 \leq i \leq n-1$, then participant P_i, must be in every minimal access set.

b) if $\mathbf{g}_i$ is not a multiple of $\mathbf{g}_0$, $1 \leq i \leq n-1$, then participant P_i must be in $(2^h - 1)2^{2(n-h)}$ minimal access sets.

— When $d^{\perp} \geq 3$ and

$$1 \leq t \leq \min\{2n/h - 1, d^{\perp} - 2\},$$

every group of t participants is involved in

$$(2^h - 1)^t \left(2^h\right)^{2n/h-(t+1)}$$

minimal access sets.

6. The Case $h = 1$

In the above discussion the divisor h of n was taken such that $h \neq 1$. For the case $h = 1$ the secret space is the binary field $\mathbf{F}_2$, which is small. However an extension of the (SSSch) can be given. In the following lines two such extensions are considered.

Case 1. In this case a (SSSch) as describes previously is considered in which the secret space is $\mathbf{F}_2$. For a sufficiently large positive integer m the vector space $\mathbf{F}_2^m$ will be considered as the new secret space and the extended secret would be an element $\mathbf{s} = (s_1, s_2, ..., s_m) \in \mathbf{F}_2^m$ which can be obtained by recovering each component s_i, $i = 1, 2, ..., m$. Each component s_i can be taken as a secret in the space $\mathbf{F}_2$, and can be recovered from the (SSSch) whose secret space is $\mathbf{F}_2$. In this extended scheme each participant P_j will receive a share $(t_j^1, t_j^2, ..., t_j^m)$ for $j = 1, 2, ..., 2^n - 2$. Similar arguments as in the proof of Theorem 22 show that results similar to those stated in this theorem also hold in this case.

Case 2. In this case it is assumed that there is a finite set with large cardinality of (SSSch) whose secret space is the binary field $\mathbf{F}_2$. Again, the

new secret space for the extension of the (SSSch) is the vector space $\mathbf{F}_2^m$ for a sufficiently large m. An extended secret is an element $\mathbf{s} = (s_1, s_2, ..., s_m) \in \mathbf{F}_2^m$ which can be obtained by recovering each component s_i, $i = 1, 2, ..., m$ from the shares of the participants of the group of (SSSch) whose secret space is $\mathbf{F}_2$.

7. Concluding Remarks

Given an odd integer n and a divisor h of it, a class of linear codes over the field $\mathbf{F}_{2^h}$ based on almost-bent functions is introduced, its parameters and bounds on the weight of the nonzero codewords are determined. This code is used to give a secret sharing scheme of which the secret space is the field $\mathbf{F}_{2^h}$, with $h \geq 2$. For the case $h = 1$, i.e., where the codes under consideration are binary, the secret space of the scheme is small, but it is used to give two extensions of a secret sharing scheme whose secret space is $\mathbf{F}_2^m$ for a sufficiently large integer m.

References

[1] R.J. Anderson, C. Ding, T. Helleseth, T. Klove, How to build robust shared control systems, *Designs, Codes and Cryptography*, **15** (1998), 111-124.

[2] A. Ashikmin, A. Barg, Minimal vectors in linear codes, *IEEE Trans. on Inf. Theory*, **44**, No. 5 (1998), 2010-2017.

[3] G.R. Blakley, Safeguarding cryptographic keys, In: *Proc. Nat. Computer Conf.*, **48**, New York (1979), 313-317.

[4] A. Canteaut, P. Charpine, H. Dobbertin, Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbf{F}_{2^m}$, and crosscorrelation of maximum-length sequences, *SIAMJ, Discrete Math.*, **13**, No. 1 (2000), 105-138.

[5] C. Carlet, C. Ding, H. Niederreiter, Authentication schemes from highly nonlinear functions, *Designs, Codes and Cryptography*, **40** (2006), 71-79.

[6] C. Carlet, C. Ding, J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, *IEEE Trans. on Inf. Theory*, **51**, No. 6 (2005), 2089-2102.

[7] C. Carlet, P. Chapin, V. Zinoviev, Codes, Bent functions and permutations suitable for des-like cryptosystems, *Designs, Codes and Cryptography*, **15** (1998), 125-156.

[8] F. Chabaud, S. Vaudenay, Links between differential and linear cryptanalysis, In: *Advances in Cryptology-EUROCRYPT'94*, Lecture Notes in Computer Science (Ed. A.D. Santis), New York, Springer-Verlag, **950** (1995), 356-365.

[9] C. Ding, J. Yuan, Covering and secret sharing with linear codes, *Discrete Mathematics and Theoretical Computer Science (Lecture Notes in Computer Science)*, C.S. Calude, M.J. Dinneen, and V. Vajnovszki, Eds., Heidelberg, Germany, Springer-Verlag, **2731** (2003), 11-25.

[10] J.C. Ku, H. Tapia-Recillas, A class of Secret Sharing Schemes, *Anales del IV Congreso Iberoamericano de Seguridad Informática*, J. Castro Lechtaler, Julio César Liporace, Jorge Ramió Aguirre, Compiladores, Mar del Plata, Argentina (2007), 185-193.

[11] J.L. Massey, Minimal codewords and secret sharing, In: *Proc. 6-th Joint Swedish-Russian Workshop on Information Theory*, Mölle, Sweden,(1993), 276-279.

[12] R.J. McElice, D.V. Sarwate, On sharing secrets and Reed-Solomon codes, *Commun. ACM*, **24** (1981), 583-584.

[13] K. Nyberg, Differentially uniform mappings for cryptography, *Advances in Cryptology-EUROCRYPT'93,* LNCS, Springer-Verlag, **765** (1994), 55-64.

[14] J. Pieprzyk, M. Zhang, Ideal secret sharing schemes from MDS codes, In: *Proc. 5-th Int. Conf. Information Security and Cryptography (ICISC 2002)*, Seoul, Korea, November (2002), 269-279.

[15] V. Pless, Power moments identities on weight distributions in error-correcting codes, *Inf. and Control*, **6** (1963), 147-152.

[16] A. Shamir, How to share a secret, *Commun. ACM*, **22** (1979), 612-613.

[17] H. Tapia-Recillas, A secret sharing scheme from a chain ring linear code, *C. Numerantium*, **186** (2007), 33-39.

[18] J. Yuan, C. Ding, Secret sharing schemes from two-weight codes, In: *Proc. The Bose Centenary Symp. Discrete Mathematics and Applications*, Kolkata, India (2002), 1-7.

[19] J. Yuan, C. Carlet, C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, *IEEE Trans. on Inf. Theory*, **52**, No. 2 (2006), 712-717.