Linear Codes From Perfect Nonlinear Mappings and Their Secret Sharing Schemes

Claude Carlet, Cunsheng Ding, *Senior Member, IEEE*, and Jin Yuan

***Abstract*—In this paper, error-correcting codes from perfect nonlinear mappings are constructed, and then employed to construct secret sharing schemes. The error-correcting codes obtained in this paper are very good in general, and many of them are optimal or almost optimal. The secret sharing schemes obtained in this paper have two types of access structures. The first type is democratic in the sense that every participant is involved in the same number of minimal-access sets. In the second type of access structures, there are a few dictators who are in every minimal access set, while each of the remaining participants is in the same number of minimal-access sets.**

***Index Terms*—Cryptography, linear codes, perfect nonlinear functions, planar functions, secret sharing schemes.**

I. Introduction

SECRET sharing schemes were introduced by Blakley [2] and Shamir [22] in 1979. Since then, a number of constructions have been proposed. The relationship between Shamir's secret sharing scheme and the Reed–Solomon codes was pointed out by McEliece and Sarwate in 1981 [19]. Massey described another construction of secret sharing schemes using error-correcting codes in 1993 [17], [18]. Later, several authors have considered the construction of secret sharing schemes using linear error correcting codes [1], [11], [12], [20], [21], [23]. In principle, every linear code gives a secret sharing scheme. However, the following problems are essential.

1. How do we determine the access structure of the secret sharing scheme based on a linear code?
2. How do we construct the underlying linear code so that the corresponding secret sharing scheme has a prescribed access structure, while minimizing the information rate?

Attacking the first problem is more or less equivalent to determining the set of all minimal codewords of the underlying linear code, which is called the covering problem of the linear code. This is a very hard problem for general linear codes, and has been solved only for a few classes of special linear codes.

Manuscript received February 29, 2004; revised January 19, 2005. The work of C. Ding was supported by the Research Grants Council of the Hong Kong Special Administrative Region, Project HKUST6183/04E, China.

C. Carlet is with the INRIA Project Codes, Domaine de Voluceau, BP 105, 78153 Le Chesnay Cedex, France. He is also with the University of Paris 8, Paris, France (e-mail: Claude.Carlet@inria.fr).

C. Ding and J. Yuan are with the Department of Computer Science, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China (e-mail: cding@cs.ust.hk; jyuan@cs.ust.hk).

Communicated by K. A. S. Abdel-Ghaffar, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2005.847722

The second problem depends on solutions to the first problem, and is also a very hard problem in general. So far, no general solution is known. Intuitively, only well structured linear codes give secret sharing schemes with nice access structures. Thus, constructing linear codes with certain properties is one interesting direction in the study of secret sharing schemes.

Highly nonlinear functions are useful in constructing stream ciphers, block ciphers, hash functions, and authentication codes. In this paper, we use perfect nonlinear functions to construct several classes of linear codes and develop tight lower bounds on the minimum distance of the codes. We determine the minimum distance of their dual codes, and analyze the access structures of the secret sharing schemes based on the dual codes. We show that the secret sharing schemes have nice access structures. The error-correcting codes constructed in this paper are very good in general, and many of them are optimal or almost optimal.

II. Perfect Nonlinear Functions and Their Properties

Let f be a function from an Abelian group $(A,+)$ of order n to another Abelian group $(B,+)$ of order m. f is *linear* if and only if $f(x+y)=f(x)+f(y)$ for all $x,y\in A$. A function g is *affine* if and only if $g=f+b$, where f is linear and b is a constant. Clearly, the zero function is linear. If f is a nonzero linear function from A to B, let $H=\{x\in A \mid f(x)=0\}$. Then H is a subgroup of A, $f(A)$ is a subgroup of B, and, denoting by $|S|$ the size of a set S, $|f(A)|\times|H|=n$. In the case that n is odd and m is a power of 2, the only linear function from A to B is the zero function, since if $f\neq 0$, then $|f(A)|$ is even, a contradiction with the fact that n is odd; thus, all affine functions are constant functions.

The (Hamming) distance between two functions f and g from A to B, denoted by $d(f,g)$, is defined to be

$$d(f,g)=|\{x\in A|f(x)-g(x)\neq 0\}|.$$

One way of measuring the nonlinearity of a function f from $(A,+)$ to $(B,+)$ is to use the minimum distance between f and all affine functions from $(A,+)$ to $(B,+)$. With this approach the nonlinearity of f is defined to be

$$N_f=\min_{l\in L} d(f,l) \tag{1}$$

where L denotes the set of all affine functions from $(A,+)$ to $(B,+)$. This measure of nonlinearity is related to linear cryptanalysis, but it is not useful in some general cases. For example, as pointed out earlier, in the case $|A|$ is odd and $|B|$ is a power of 2, this measure makes little sense as there are no nonconstant affine functions from $(A,+)$ to $(B,+)$.

A robust measure of the nonlinearity of functions is related to differential cryptanalysis and uses the derivatives $D_a f(x) = f(x+a) - f(x)$. It may be defined by

$$P_f = \max_{0 \neq a \in A} \max_{b \in B} \frac{\left| D_a f^{-1}(b) \right|}{|A|}. \tag{2}$$

The smaller the value of P_f, the higher the corresponding nonlinearity of f (if f is linear, then $P_f = 1$). In some cases, it is possible to find the exact relation between the two measures on nonlinearity.

It is easily seen that

$$P_f \geq \frac{1}{|B|}. \tag{3}$$

This lower bound can be considered as an upper bound for the nonlinearity of f. For applications in coding theory and cryptography, we wish to find functions with the smallest possible P_f. A function $f : A \to B$ has perfect nonlinearity if $P_f = \frac{1}{|B|}$.

The following lemma and theorem about perfect nonlinear functions were proved in [6].

Lemma 1: [6] Let $(A, +)$ and $(B, +)$ be Abelian groups of orders n and m, respectively, where m divides n. If f is a perfect nonlinear mapping from A to B, then for any nonzero $b \in B$

$$\begin{cases} \sum_{z \in B} k_z^2 = \frac{n^2 + (m-1)n}{m} \\ \sum_{z \in b} k_z k_{z+b} = \frac{n(n-1)}{m} \\ \sum_{z \in B} k_z = n \end{cases} \tag{4}$$

where $k_z = |\{x \in A : f(x) = z\}|$ for each $z \in B$.

Theorem 2: [6] Let $(A, +)$ and $(B, +)$ be Abelian groups of orders n and m, respectively, where n is a multiple of m. If f is a function from A to B with perfect nonlinearity $P_f = \frac{1}{m}$, then for any $b \in B$

$$\frac{n}{m} - \sqrt{\frac{(m-1)n}{m}} \leq k_b \leq \frac{n}{m} + \sqrt{\frac{(m-1)n}{m}}$$

where $k_z = |\{x \in A | f(x) = z\}|$. Furthermore

$$\frac{(m-1)n}{m} - \sqrt{\frac{m-1}{m}}\sqrt{n} \leq N_f \leq \frac{(m-1)n}{m} + \sqrt{\frac{m-1}{m}}\sqrt{n}.$$

If B has exponent 2, i.e., $2b = 0$ for any $b \in B$, then for any $b \in B$

$$\frac{n}{m} - \frac{m-1}{m}\sqrt{n} \leq k_b \leq \frac{n}{m} + \frac{m-1}{m}\sqrt{n}$$

where $k_z = |\{x \in A | f(x) = z\}|$. Furthermore

$$\frac{(m-1)n}{m} - \frac{m-1}{m}\sqrt{n} \leq N_f \leq \frac{(m-1)n}{m} + \frac{m-1}{m}\sqrt{n}.$$

The bounds of Theorem 2 are tight only when B has exponent 2. For the case that the exponent of B is not 2, we can improve the bounds as follows.

Theorem 3: Let $(A, +)$ and $(B, +)$ be Abelian groups of orders n and m, respectively, where n is a multiple of m. If f is a function from A to B with perfect nonlinearity $P_f = \frac{1}{m}$, then for any $b \in B$

$$\frac{n}{m} - \frac{m-1}{m}\sqrt{n} \leq k_b \leq \frac{n}{m} + \frac{m-1}{m}\sqrt{n}$$

where $k_z = |\{x \in A | f(x) = z\}|$. Furthermore

$$\frac{m-1}{m}\left(n - \sqrt{n}\right) \leq N_f \leq \frac{m-1}{m}\left(n + \sqrt{n}\right).$$

Proof: Let $b_1, b_2, \ldots, b_m$ denote the elements of B. We now prove the bounds for k_{b_m}. The bounds for other k_{b_i} can be similarly proved.

First of all, note that

$$\begin{aligned} 0 &\leq \sum_{i \neq j, 1 \leq i,\ j \leq m-1} (k_{b_i} - k_{b_j})^2 \\ &= 2(m-2) \sum_{i=1}^{m-1} k_{b_i}^2 - 2 \sum_{i \neq j, 1 \leq i,\ j \leq m-1} k_{b_i} k_{b_j}. \end{aligned}$$

Then we have

$$(m-2) \sum_{i=1}^{m-1} k_{b_i}^2 \geq \sum_{i \neq j, 1 \leq i,\ j \leq m-1} k_{b_i} k_{b_j} \tag{5}$$

where the equality holds if and only if all k_{b_i} are equal.

Combining the first and third equations in (4), we have

$$\sum_{i=1}^{m-1} k_{b_i}^2 + \left(n - \sum_{j=1}^{m-1} k_{b_j} \right)^2 = \frac{n^2 + (m-1)n}{m}$$

which can be reformulated as

$$2 \sum_{i=1}^{m-1} k_{b_i}^2 + n^2 - 2n \sum_{j=1}^{m-1} k_{b_j} + \sum_{i \neq j, 1 \leq i,\ j \leq m-1} k_{b_i} k_{b_j} = \frac{n^2 + (m-1)n}{m}.$$

Combining this equation and (5) yields

$$2 \sum_{i=1}^{m-1} k_{b_i}^2 + n^2 - 2n \sum_{j=1}^{m-1} k_{b_j} + (m-2) \sum_{i=1}^{m-1} k_{b_i}^2 \geq \frac{n^2 + (m-1)n}{m}.$$

This inequality and the first and third equations of (4) together give

$$m \left(\frac{n^2 + (m-1)n}{m} - k_{b_m}^2 \right) + n^2 - 2n(n - k_{b_m}) \geq \frac{n^2 + (m-1)n}{m}$$

which can be easily written as

$$\left(k_{b_m} - \frac{n}{m} \right)^2 \leq \frac{(m-1)^2}{m^2} n.$$

This proves the lower and upper bounds on k_{b_m}. As mentioned before, the bounds are proved similarly for other k_{b_i}.

The bounds on N_f follow from those on k_b and the fact that the sum of a function with perfect nonlinearity and any affine function gives another function with perfect nonlinearity.

It will be seen later that the bounds of Theorem 3 can be achieved, and are the basis of the main results of this paper.

III. The Constructions of Linear Codes

Let $\Pi(x)$ be any perfect nonlinear mapping from GF(p^m) to itself. This implies that p is an odd prime. For any $a, b \in$ GF(p^m), define

$$f_{a,b}(x) = \mathrm{Tr}_{p^m/p^h}(a\Pi(x) + bx)$$

where h is a positive divisor of m.

An $[n, k, d; q]$ linear code $\mathcal{C}$ is a linear subspace of GF$(q)^n$ with dimension k and minimum nonzero Hamming weight d. We now define a linear code over GF(p^h) as

$$\mathcal{C}_\Pi = \{\boldsymbol{c}_{a,b} = (f_{a,b}(\gamma_1), \ldots, f_{a,b}(\gamma_{p^m-1}))|a, b \in \mathrm{GF}(p^m)\} \tag{6}$$

where $\gamma_1, \ldots, \gamma_{p^m-1}$ are all the nonzero elements of GF(p^m).

For any $a, b, c \in$ GF(p^m), define

$$g_{a,b,c}(x) = \mathrm{Tr}_{p^m/p^h}(a\Pi(x) + bx + c).$$

We define another linear code over GF(p^h) as

$$\overline{\mathcal{C}}_\Pi = \{\boldsymbol{c}_{a,b,c}|a, b, c \in \mathrm{GF}(p^m)\} \tag{7}$$

where

$$\boldsymbol{c}_{a,b,c} = (g_{a,b,c}(\gamma_0), \ldots, g_{a,b,c}(\gamma_{p^m-1}))$$

and $\gamma_0, \ldots, \gamma_{p^m-1}$ are all the elements of GF(p^m).

The code $\overline{\mathcal{C}}_\Pi$ is closely related to $\mathcal{C}_\Pi$. We shall use $\mathcal{C}_\Pi$ to construct secret sharing schemes in the sequel. Before doing this, we prove some properties of these codes.

Theorem 4: If Π has perfect nonlinearity and $\Pi(0) = 0$, the code $\mathcal{C}_\Pi$ of (6) has parameters $[p^m - 1, 2m/h, d; p^h]$ with

$$d \geq \frac{p^h - 1}{p^h}\left(p^m - p^{m/2}\right).$$

Furthermore, for every nonzero weight w in $\mathcal{C}_\Pi$, we have

$$\frac{p^h - 1}{p^h}\left(p^m - p^{m/2}\right) \leq w \leq \frac{p^h - 1}{p^h}\left(p^m + p^{m/2}\right).$$

Proof: $f_{0,b}(x)$ is a linear function. Hence, the Hamming weight of $\boldsymbol{c}_{0,b}$ is $p^m - p^{m-h}$ if $b \neq 0$.

If $a \neq 0$, then $f_{a,b}(x)$ is perfect nonlinear. This is because a perfect nonlinear function plus a linear function yields another perfect nonlinear function. Since $\Pi(0) = 0$, by Theorem 3 the number of times 0 occurs in $\boldsymbol{c}_{a,b}$ is at most

$$p^{m-h} + \frac{p^h - 1}{p^h}p^{m/2} - 1$$

and at least

$$p^{m-h} - \frac{p^h - 1}{p^h}p^{m/2} - 1.$$

Hence the Hamming weight of $\boldsymbol{c}_{a,b}$ satisfies

$$\mathrm{HW}(\boldsymbol{c}_{a,b}) \geq p^m - p^{m-h} - \frac{p^h - 1}{p^h}p^{m/2}$$
$$\mathrm{HW}(\boldsymbol{c}_{a,b}) \leq p^m - p^{m-h} + \frac{p^h - 1}{p^h}p^{m/2}.$$

This proves all the bounds.

Since $\Pi(x)$ has perfect nonlinearity, $\Pi(x) \neq ux$ for all $u \in$ GF(p^m). Thus, $\boldsymbol{c}_{a,b}$ is the zero codeword if and only if $(a, b) = (0, 0)$. Hence, $\mathcal{C}_\Pi$ has exactly p^{2m} distinct codewords. Since $\mathcal{C}_\Pi$ is obviously linear, its dimension is $2m/h$.

The lower bound on the minimum distance d of the code $\mathcal{C}_\Pi$ is very tight. Later we shall see that it can be met in many cases. On the other hand, numerical data shows that the codes $\mathcal{C}$ are among the best codes known in many cases.

Similarly, we can prove the following.

Theorem 5: If Π has perfect nonlinearity, the code $\overline{\mathcal{C}}_\Pi$ of (7) has parameters $[p^m, 1 + 2m/h, d; p^h]$ with

$$d \geq \frac{p^h - 1}{p^h}\left(p^m - p^{m/2}\right).$$

Furthermore, for every nonzero weight w in $\overline{\mathcal{C}}_\Pi$, we have

$$\frac{p^h - 1}{p^h}\left(p^m - p^{m/2}\right) \leq w \leq \frac{p^h - 1}{p^h}\left(p^m + p^{m/2}\right).$$

The code $\overline{\mathcal{C}}_\Pi$ may give optimal and almost optimal codes. For example, when $(p, m, h) = (3, 2, 1)$, it is a $[9, 5, 4; 3]$ code which is optimal [3]. When $(p, m, h) = (3, 3, 1)$, it is a $[27, 7, 15; 3]$ code which is optimal [3]. When $(p, m, h) = (3, 4, 1)$, it is an $[81, 9, d \geq 48; 3]$ code which is either optimal or almost optimal because the minimum distance of any ternary code with length 81 and dimension 9 is at most 49 [3]. When $(p, m, h) = (5, 2, 1)$, it is a $[25, 5, d \geq 16; 5]$ code which is either optimal or almost optimal because the minimum distance of any code over GF(5) with length 25 and dimension 5 is at most 17 [3].

The dual code $\mathcal{C}_\Pi^\perp$ has length $p^m - 1$ and dimension $p^m - 1 - 2m/h$. For our applications, we are interested in the minimum distance of the dual code $\mathcal{C}_\Pi^\perp$. We have the following conclusion.

Theorem 6: Let $m > 1$, and let $d^\perp$ denote the minimum distance of the dual code $\mathcal{C}_\Pi^\perp$ of the code $\mathcal{C}_\Pi$ described in Theorem 4. Then $2 \leq d^\perp \leq 4$. In addition, $d^\perp = 2$ if and only if there are

$$x \in \mathrm{GF}(p^m)^* \quad \text{and} \quad c \in \mathrm{GF}(p^h) \setminus \{0, 1\}$$

such that $\Pi(cx) = c\Pi(x)$.

Furthermore, in the special case that $p = 3$ and $h = 1$, if

1. $\Pi(x) = \Pi(-x)$ for all $x \in$ GF(p^m) and
2. $\Pi(x) = 0$ if and only if $x = 0$

then $d^\perp = 4$.

Proof: Clearly, $d^\perp \geq 2$. We now prove that $d^\perp \leq 4$, which is true for any linear code over GF(p^h) with the same

length and dimension as $\mathcal{C}_\Pi$. Suppose that $d^\perp \geq 5$. Note that $p \geq 3$ and $m > 1$. We would then have

$$\begin{aligned}
&\sum_{i=0}^{2} \binom{p^m-1}{i} (p^h-1)^i \\
&\quad = \frac{2+2(p^m-1)(p^h-1)+(p^{2m}-3p^m+2)(p^h-1)^2}{2} \\
&\quad \geq \frac{2+4(p^m-1)+4(p^{2m}-3p^m+2)}{2} \\
&\quad = \frac{2p^{2m}+2p^m(p^m-4)+6}{2} \\
&\quad \geq \frac{2p^{2m}+2\times 3^2(3^2-4)+6}{2} \\
&\quad > p^{2m} = (p^h)^{2m/h}
\end{aligned}$$

which is contrary to the sphere-packing bound. Hence, $d^\perp \leq 4$.

By definition, $d^\perp = 2$ if and only if there are two distinct elements x_1 and x_2 in GF$(p^m)^*$ and an element $c \in$ GF$(p^h)^*$ such that

$$\mathrm{Tr}_{p^m/p^h}[a\Pi(x_1)+bx_1] = c\mathrm{Tr}_{p^m/p^h}[a\Pi(x_2)+bx_2]$$

for all $(a,b) \in$ GF$(p^m)^2$. This is equivalent to

$$a\Pi(x_1)+bx_1 = ac\Pi(x_2)+bcx_2, \quad \forall\,(a,b) \in \mathrm{GF}(p^m)^2$$

which is further equivalent to

$$x_1 = cx_2, \qquad \Pi(x_1) = c\Pi(x_2).$$

Since $x_1 \neq x_2$, $c \neq 1$. This completes the proof of the conclusion in the first part of this theorem.

Consider now the special case that $p = 3$ and $h = 1$. By assumption, $\Pi(x) = \Pi(-x)$ for all $x \in$ GF(p^m). Hence, $\mathcal{C}_\Pi^\perp$ has no codeword of weight 2. Then it suffices to prove that the code has no codeword of weight three either. Clearly, $\mathcal{C}_\Pi^\perp$ has a codeword of weight three if and only if there are three pairwise distinct elements $x_1, x_2, x_3 \in$ GF$(3^m)^*$ and three elements $c_1, c_2, c_3 \in$ GF$(3)^*$ such that

$$\begin{cases} c_1x_1+c_2x_2+c_3x_3 = 0 \\ c_1\Pi(x_1)+c_2\Pi(x_2)+c_3\Pi(x_3) = 0. \end{cases} \tag{8}$$

Without loss of generality, we only need to consider the following two subcases.

- $c_1 = c_2 = 1, c_3 = -1$: In this subcase we have

  $$\begin{cases} x_1 - 0 = x_3 - x_2 \\ \Pi(x_1) - \Pi(0) = \Pi(x_3) - \Pi(x_2). \end{cases}$$

  By the perfect nonlinearity of Π we have $x_1 = x_3$, which is a contradiction.
- $c_1 = c_2 = c_3 = 1$: In this case

  $$\Pi(-x_2-x_3)+\Pi(x_2)+\Pi(x_3) = 0.$$

  Since $\Pi(x_2) = \Pi(-x_2)$, we have

  $$\Pi(-x_2-x_3)+\Pi(-x_2)+\Pi(x_3) = 0, \tag{9}$$

  which is the same as

  $$\Pi(x_2+x_3)-\Pi(-x_2) = \Pi(-x_2)-\Pi(-x_3). \tag{10}$$

  This implies that $x_2 = x_3$ by the perfect nonlinearity of Π, and is contrary to our assumption that $x_2 \neq x_3$. The proof of this theorem is now complete.

Remark: If $p = 2$ and $h = 1$, $d^\perp = 5$ is possible when Π is almost perfect nonlinear (see [5] for details).

Theorem 7: Let $m \geq 2$, and let $\overline{d}^\perp$ denote the minimum distance of the dual code $\overline{\mathcal{C}}_\Pi^\perp$ of the code $\overline{\mathcal{C}}_\Pi$ described in Theorem 5. Then $\overline{\mathcal{C}}_\Pi^\perp$ is a $[p^m, p^m - 2m/h - 1, \overline{d}^\perp; p^h]$ code. Furthermore

1. if $(p,h) = (3,1)$, then $\overline{d}^\perp = 5$
2. otherwise, $3 \leq \overline{d}^\perp \leq 4$.

Proof: Similar to the discussion on $d^\perp$ in the proof of Theorem 6 we can prove $\overline{d}^\perp > 2$.

1. Suppose $(p,h) = (3,1)$. First we prove $\overline{\mathcal{C}}_\Pi^\perp$ has no codeword of weight 3. Otherwise, there exist pairwise distinct elements $x_1, x_2, x_3 \in$ GF(p^m) and $c_2, c_3 \in$ GF$(p)^*$ such that

$$\begin{cases} x_1+c_2x_2+c_3x_3 = 0 \\ \Pi(x_1)+c_2\Pi(x_2)+c_3\Pi(x_3) = 0 \\ 1+c_2+c_3 = 0. \end{cases} \tag{11}$$

Note that $p = 3$ and $c_2c_3 \neq 0$. It then follows from the last equation of (11) that $c_2 = c_3 = 1$. By (11) we have $x_3 = -x_1 - x_2$ and

$$\Pi(x_1)+\Pi(x_2)+\Pi(-x_1-x_2) = 0.$$

Since $-\Pi(-x_1-x_2) = 2\Pi(-x_1-x_2)$ we get

$$\Pi(x_1)-\Pi(-x_1-x_2) = \Pi(-x_1-x_2)-\Pi(x_2).$$

Note that $(-x_1-x_2)-x_1 = x_2-(-x_1-x_2)$. Applying the perfect nonlinearity of Π, we have $x_1 = -x_1-x_2$. This is equivalent to $x_1 = x_2$, which is contradictory to our assumption.

Next we prove $\overline{\mathcal{C}}_\Pi^\perp$ has no codeword of weight 4. Otherwise, there exist pairwise distinct elements $x_1, x_2, x_3, x_4 \in$ GF(p^m) and $c_2, c_3, c_4 \in$ GF$(p)^*$ such that

$$\begin{cases} x_1+c_2x_2+c_3x_3+c_4x_4 = 0 \\ \Pi(x_1)+c_2\Pi(x_2)+c_3\Pi(x_3)+c_4\Pi(x_4) = 0 \\ 1+c_2+c_3+c_4 = 0. \end{cases} \tag{12}$$

Note that $p = 3$ and $c_2c_3c_4 \neq 0$. It then follows from the last equation of (12) that two of c_2, c_3, and c_4 must be -1 and the other must be 1. Hence, without loss of generality, we assume $c_2 = c_3 = -1$, and $c_4 = 1$. Then (12) becomes

$$\begin{cases} x_1-x_2 = x_3-x_4 \\ \Pi(x_1)-\Pi(x_2) = \Pi(x_3)-\Pi(x_4). \end{cases} \tag{13}$$

Since Π is a perfect nonlinear mapping, we obtain that $x_1 = x_3$. This is contradictory to the assumption that these x_i's are pairwise distinct.

Finally, we prove that $\overline{\mathcal{C}}_\Pi^\perp$ has a codeword of weight 5. We first claim that there exist three pairwise distinct elements $x_3, x_4, x_5 \in$ GF(3^m) such that $x_3+x_4+x_5 \neq 0$. To prove this claim, we consider all possible sets $\{x_3, x_4, x_5\}$, where x_3, x_4, x_5 are pairwise distinct elements of GF(3^m). The total number of such sets $\{x_3, x_4, x_5\}$ is $\binom{3^m}{3}$. The total number of

such sets $\{x_3, x_4, x_5\}$ satisfying $x_3 + x_4 + x_5 = 0$ is at most $3^m(3^m - 1)$. Note that

$$\binom{3^m}{3} > 3^m(3^m - 1)$$

because $m \geq 2$. Hence, there must exist such a set $\{x_3, x_4, x_5\}$ with $x_3 + x_4 + x_5 \neq 0$. This completes the proof of the claim above.

Let $\{x_3, x_4, x_5\}$ be such a set with $x_3 + x_4 + x_5 \neq 0$. Define

$$\begin{aligned} a &= x_3 + x_4 + x_5 \neq 0 \\ b &= \Pi(x_3) + \Pi(x_4) + \Pi(x_5). \end{aligned}$$

Since $a \neq 0$ and $\Pi(x)$ has perfect nonlinearity, the equation

$$\Pi(x + a) - \Pi(x) = b$$

has a unique solution x_2. Define

$$x_1 = x_2 + a = x_2 + x_3 + x_4 + x_5.$$

Then we have

$$\begin{cases} x_1 - x_2 - x_3 - x_4 - x_5 = 0 \\ \Pi(x_1) - \Pi(x_2) - \Pi(x_3) - \Pi(x_4) - \Pi(x_5) = 0. \end{cases} \tag{14}$$

We now prove that x_1, x_2, x_3, x_4, x_5 are pairwise distinct. Note that x_3, x_4, x_5 are pairwise distinct. We need only to prove that $x_2 \notin \{x_3, x_4, x_5\}$ and $x_1 \notin \{x_2, x_3, x_4, x_5\}$.

(A) We now prove that $x_2 \notin \{x_3, x_4, x_5\}$.

Since x_3, x_4 and x_5 are symmetric, we need only to prove that $x_2 \neq x_3$. Suppose $x_2 = x_3$. Then (14) becomes

$$\begin{cases} x_1 = -x_3 + x_4 + x_5 \\ \Pi(x_1) = -\Pi(x_3) + \Pi(x_4) + \Pi(x_5) \end{cases}$$

which is equivalent to

$$\begin{cases} x_1 - x_4 = x_5 - x_3 \\ \Pi(x_1) - \Pi(x_4) = \Pi(x_5) - \Pi(x_3). \end{cases} \tag{15}$$

It then follows from the perfect nonlinearity of Π that $x_4 = x_3$. This is contrary to the fact that $x_3 \neq x_4$. Hence, $x_2 \neq x_3$.

(B) We then prove that $x_1 \notin \{x_2, x_3, x_4, x_5\}$.

Since $x_1 = x_2 + a$ and $a \neq 0$, $x_1 \neq x_2$. Due to symmetry, it remains to prove that $x_1 \neq x_3$.

Suppose $x_1 = x_3$. Then (14) becomes

$$\begin{cases} x_2 + x_4 + x_5 = 0 \\ \Pi(x_2) + \Pi(x_4) + \Pi(x_5) = 0. \end{cases} \tag{16}$$

We proved earlier that x_2, x_4, x_5 are pairwise distinct. By (16) and the equality $1+1+1 = 0$, we know that $\overline{\mathcal{C}}_\Pi^\perp$ has a codeword of weight 3. This is contrary to the fact we proved earlier that $\overline{\mathcal{C}}_\Pi^\perp$ has no codeword of weight 3. Hence, $x_1 \neq x_3$.

In summary, we proved that x_1, x_2, x_3, x_4, x_5 are pairwise distinct. Now it follows from the equation $1-1-1-1-1 = 0$ and (14) that $\overline{\mathcal{C}}_\Pi^\perp$ has a codeword of weight 5. Hence, $\overline{d}^\perp = 5$.

2. We now prove that $3 \leq \overline{d}^\perp \leq 4$ if $(p, h) \neq (3, 1)$.

Because $p \geq 5$ or $h \geq 2$, it can be verified that

$$\sum_{i=0}^{2} \binom{p^m}{i} (p^h - 1)^i - p^{2m+h} > 0.$$

It then follows from the sphere-packing bound that $\overline{d}^\perp < 5$. Hence, $3 \leq \overline{d}^\perp \leq 4$. This completes the proof of this theorem.

A. Connection Between Some Codes $\mathcal{C}_\Pi$ and Cyclic Codes With Two Zeros

Let us choose $\gamma_i = \alpha^{i-1}$ for all i. Then the code $\mathcal{C}_\Pi$ defined in (6) is cyclic when $\Pi(x)$ is a power function, and is, in general, noncyclic otherwise. In this subsection, we point out that the code $\mathcal{C}_\Pi$ defined in (6) is the dual of a cyclic code with two zeros when $\Pi(x)$ is a power function.

Define $l = m/h$ and $q = p^h$. We now consider any integer t with $2 \leq t \leq q^l - 2$ and $t \neq q^j$ for any $j > 0$. We use $m_\alpha(x)$ and $m_{\alpha^t}(x)$ to denote the minimal polynomials over GF(q) of α and α^t, respectively. Since $t \neq q^j$ for any $j > 0$, α^t is not a Galois conjugate of α. Hence, the two polynomials $m_\alpha(x)$ and $m_{\alpha^t}(x)$ are not equal.

Let $\mathcal{C}_{1,t}$ denote the cyclic code generated by $m_\alpha(x)m_{\alpha^t}(x)$, which is an ideal of the ring GF$(q)[x]/(x^{q^l-1} - 1)$. Our task now is to determine the dual code $\mathcal{C}_{1,t}^\perp$. To this end, we need the following lemma, which is referred to as Delsarte's theorem [9].

Lemma 8: Let $\mathcal{C}$ be a linear code of length n over GF(q^l). Then

$$\mathrm{Trace}(\mathcal{C})^\perp = \mathrm{Res}(\mathcal{C}^\perp),$$

where $\mathrm{Res}(\mathcal{C}^\perp) = \mathcal{C}^\perp \cap \mathrm{GF}(q)^n$ is the restriction of $\mathcal{C}^\perp$ to GF(q), and $\mathrm{Trace}(\mathcal{C})$ is the GF(q)-code given by

$$\mathrm{Trace}(\mathcal{C}) = \{\mathrm{Tr}_{q^l/q}(\boldsymbol{c}) : \boldsymbol{c} \in \mathcal{C}\}.$$

We deduce the following result which may be familiar to some people. For completeness, we also include a proof here.

Lemma 9: Let symbols and notations be as before. Then

$$\mathcal{C}_{1,t}^\perp = \mathcal{C}_\Pi$$

where $\Pi(x) = x^t$ and $\gamma_i = \alpha^{i-1}$ for all i with $1 \leq i \leq q^l - 1$.

Proof: We first prove that $\mathcal{C}_{1,t}$ is the restriction of the ideal

$$(x - \alpha)(x - \alpha^t) \subset \mathrm{GF}(q^l)[x]/(x^{q^l-1} - 1).$$

Note that α generates GF$(q^l)^*$ and α^t is not a Galois conjugate of α. Since the codewords in the ideal $(x - \alpha)(x - \alpha^t)$ are precisely those that vanish in α and α^t, the code $\mathcal{C}_{1,t}$ is the restriction of the ideal $(x - \alpha)(x - \alpha^t)$ to GF$(q)[x]/(x^{q^l-1} - 1)$.

We then prove that

$$\begin{aligned} &(x - \alpha)(x - \alpha^t)^\perp \\ &= \{(h_{a,b}(1), h_{a,b}(\alpha), \ldots, h_{a,b}(\alpha^{q^l-2}) : a, b \in \mathrm{GF}(q^l)\} \end{aligned} \tag{17}$$

where $h_{a,b}(x) = ax^t + bx$. Indeed, the polynomials in the ideal $(x-\alpha)(x-\alpha^t)$ are the vectors $(a_0, a_1, \ldots, a_{q^l-2})$ that are orthogonal to

$$(1, \alpha, \alpha^2, \ldots, \alpha^{q^l-2})$$

and

$$(1, \alpha^t, \alpha^{2t}, \ldots, \alpha^{(q^l-2)t}).$$

Since α generates GF $(q^l)^*$, the vector $(1, \alpha, \alpha^2, \ldots, \alpha^{q^l-2})$ has precisely all elements of GF $(q^l)^*$ as its coordinates. Hence, (17) follows.

Finally, the conclusion of Lemma 9 follows from Lemma 8. This completes the proof.

Lemma 9 says that our code $\mathcal{C}_\Pi$ is equivalent to the dual code of a cyclic code with two zeros when Π is a power function. It will be shown in the sequel that some perfect nonlinear functions are power functions and some are not power functions. Therefore, some of the codes $\mathcal{C}_\Pi$ of (6) obtained from perfect nonlinear functions are certainly noncyclic and thus new.

B. The Codes From $\Pi(x) = x^2$

It is straightforward to show that $\Pi(x) = x^2$ is a perfect nonlinear mapping from GF (p^m) to itself, where p is odd. In this case, the minimum distance and all weights can be determined. The case $h = 1$ is treated in [10].

Theorem 10: Let $h = 1$ and $\Pi(x) = x^2$. If m is even, the code $\mathcal{C}_\Pi$ of (6) has parameters

$$[p^m - 1, 2m, d = (p-1)p^{m-1} - (p-1)p^{m/2-1}; p]$$

and has the following five nonzero weights:

$$(p-1)(p^{m-1} \pm p^{m/2-1}), \quad (p-1)p^{m-1} \pm p^{m/2-1}, \quad (p-1)p^{m-1}.$$

If m is odd, the code $\mathcal{C}_\Pi$ of (6) has parameters

$$[p^m - 1, 2m, d = (p-1)p^{m-1} - p^{(m-1)/2}]$$

and has the following three nonzero weights:

$$(p-1)p^{m-1} \pm p^{(m-1)/2}, \quad (p-1)p^{m-1}.$$

This theorem shows that the lower bound on the minimum distance d of the code $\mathcal{C}_\Pi$ given in Theorem 4 can be met, and is thus tight when m is even.

Theorem 11: Let $h = 1$ and $\Pi(x) = x^2$. Then $\mathcal{C}_\Pi^\perp$ is a $[p^m - 1, p^m - 2m - 1, d^\perp; p]$ code, where $d^\perp = 3$ if $p > 3$, and $d^\perp = 4$ if $p = 3$.

Proof: Using Theorem 6, it is straightforward to prove that $d^\perp \neq 2$. We now give a necessary and sufficient condition for $\mathcal{C}_\Pi^\perp$ to have a codeword of weight 3. Clearly, this condition is that there are two nonzero elements c_2 and c_3 in GF (p) and three pairwise distinct elements x_1, x_2, x_3 in GF $(p^m)^*$ such that

$$a[\Pi(x_1) + c_2\Pi(x_2) + c_3\Pi(x_3)] + b(x_1 + c_2x_2 + c_3x_3) = 0 \quad (18)$$

for all pairs $(a, b) \in \text{GF}(p^m)^2$. Equation (18) is equivalent to

$$\begin{cases} x_1 = -c_2x_2 - c_3x_3 \\ \left(c_2^2 + c_2\right)x_2^2 + \left(c_3^2 + c_3\right)x_3^2 + 2c_2c_3x_2x_3 = 0. \end{cases} \quad (19)$$

We now consider the case $p \geq 5$ and show that $d^\perp = 3$. In this case, we put $c_2 = -1$. Since $p \geq 5$, we can choose one $c_3 \in \text{GF}(p) \setminus \{0, 1, -1\}$, and define x_3 to be any nonzero element of GF (p^m). Then $(x_3(1-c_3)/2, x_3(c_3+1)/2, x_3)$ is a solution to (18) and the three coordinates of this vector are pairwise distinct and nonzero. Thus, in the case $p \geq 5$, $\mathcal{C}_\Pi^\perp$ has a codeword of weight 3, and thus minimum distance 3.

In the case that $p = 3$, it follows from the second part of Theorem 6 that $d^\perp = 4$.

Remark: The first part of the conclusion in Theorem 11 may be proved by combining Lemma 9 of this paper and [7, Theorem 3]. But the second part (i.e., $d^\perp = 4$ if $p = 3$) cannot be derived from Lemma 9 and [7].

Theorem 12: Let $\Pi(x) = x^2$, and $h = 1$. $\overline{\mathcal{C}}_\Pi^\perp$ is a

$$[p^m, p^m - 2m - 1, \overline{d}^\perp] \text{ code}$$

where $\overline{d}^\perp = 5$ when $p = 3$, and $\overline{d}^\perp = 4$ when $p > 3$.

Proof: When $p = 3$, the conclusion follows from Theorem 7. When $p > 3$, suppose $\overline{\mathcal{C}}_\Pi^\perp$ has a codeword of weight 3. Then there exist pairwise distinct $x_1, x_2, x_3 \in \text{GF}(p^m)$ and $s, t \in \text{GF}(p)^*$ such that

$$\text{Tr}\left(ax_1^2 + bx_1 + c\right) + s\text{Tr}\left(ax_2^2 + bx_2 + c\right) + t\text{Tr}(ax_3^2 + bx_3 + c) = 0$$

for all $a, b, c \in \text{GF}(p^m)$. Hence,

$$\begin{cases} 1 + s + t = 0 \\ x_1 + sx_2 + tx_3 = 0 \\ x_1^2 + sx_2^2 + tx_3^2 = 0 \end{cases} \quad (20)$$

i.e.,

$$\begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{pmatrix} \begin{pmatrix} 1 \\ s \\ t \end{pmatrix} = 0.$$

Since x_1, x_2, x_3 are pairwise distinct, the coefficient matrix is nonsingular and there do not exist s, t such that (20) holds. It then follows from Theorem 7 that $\overline{d}^\perp = 4$.

The four classes of codes $\mathcal{C}_\Pi$, $\overline{\mathcal{C}}_\Pi$, $\mathcal{C}_\Pi^\perp$, $\overline{\mathcal{C}}_\Pi^\perp$ contain the following optimal codes:

$$[8, 4, 4; 3],\ [26, 6, 15; 3],\ [26, 20, 4; 3],\ [80, 72, 4; 3],$$
$$[242, 232, 4; 3],\ [4, 2, 3; 5],\ [124, 6, 95; 5],\ [9, 4, 5; 3],$$
$$[27, 20, 5; 3],\ [81, 72, 5; 3],\ [243, 232, 5; 3],\ [5, 2, 4; 5]$$

and the following best codes known:

$$[80, 8, 48; 3] \text{ and } [242, 10, 153; 3]$$

according to [3].

C. The Ternary Codes From $\Pi(x) = x^{(3^k+1)/2}$ and $\Pi(x) = x^{10} + x^6 - x^2$

Theorem 13: Let $p = 3$, $h = 1$, k be odd, and $\gcd(m, k) = 1$. Let $\Pi(x) = x^{\frac{3^k+1}{2}}$, which is a perfect nonlinear mapping from GF(p^m) to GF(p^m) [6]. If $m \geq 2$, then we have the following:

a) $\mathcal{C}_\Pi$ is a $[3^m - 1, 2m, d; 3]$ code with $d \geq \frac{2}{3}(3^m - 3^{m/2})$;
b) $\mathcal{C}_\Pi^\perp$ is a $[3^m - 1, 3^m - 2m - 1, 4; 3]$ code;
c) $\overline{\mathcal{C}}_\Pi$ is a $[3^m, 2m + 1, \overline{d}; 3]$ code with $\overline{d} \geq \frac{2}{3}(3^m - 3^{m/2})$;
d) $\overline{\mathcal{C}}_\Pi^\perp$ is a $[3^m, 3^m - 2m - 1, 5; 3]$ code.

Proof: a), c), and d) follow from Theorems 4, 5, and 7, respectively. Part b) follows from the second part of Theorem 6.

Remark: The conclusion of Part b) in Theorem 13 cannot be proved by combining Lemma 9 of this paper and [7], because it only proves $3 \leq d^\perp \leq 4$.

The ternary codes $\mathcal{C}_\Pi$, $\overline{\mathcal{C}}_\Pi$, $\mathcal{C}_\Pi^\perp$, $\overline{\mathcal{C}}_\Pi^\perp$ described in Theorem 13 contain a number of optimal codes and are very good in general according to [3].

Let m be odd. It is known that $\Pi(x) = x^{10} + x^6 - x^2$ is a planar function from GF(3^m) to itself [8], and has thus perfect nonlinearity. This perfect nonlinear function also gives several classes of ternary codes described in the following theorem.

Theorem 14: Let m be odd, and let $\Pi(x) = x^{10} + x^6 - x^2$ be the perfect nonlinear mapping from GF(p^m) to GF(p^m). Then we have the following:

a) $\mathcal{C}_\Pi$ is a $[3^m - 1, 2m, d; 3]$ code with $d \geq \frac{2}{3}(3^m - 3^{m/2})$;
b) $\mathcal{C}_\Pi^\perp$ is a $[3^m - 1, 3^m - 2m - 1, 4; 3]$ code;
c) $\overline{\mathcal{C}}_\Pi$ is a $[3^m, 2m + 1, \overline{d}; 3]$ code with $\overline{d} \geq \frac{2}{3}(3^m - 3^{m/2})$;
d) $\overline{\mathcal{C}}_\Pi^\perp$ is a $[3^m, 3^m - 2m - 1, 5; 3]$ code.

Proof: a), c), and d) follow from Theorems 4, 5, and 7, respectively. The conclusion of b) follows from Theorem 6.

Example 1: Let $m = 3$ and $\Pi(x) = x^{10} + x^6 - x^2$. Then $\mathcal{C}_\Pi$ is a $[26, 6, 15; 3]$ code with weight distribution

$$1 + 312x^{15} + 260x^{18} + 156x^{21}.$$

$\mathcal{C}_\Pi^\perp$ is a $[26, 20, 4; 3]$ code with weight distribution

$$\begin{aligned} 1 &+ 260x^4 + 3380x^5 + 20384x^6 + 112840x^7 \\ &+ 549640x^8 + 2198560x^9 + 7464912x^{10} \\ &+ 21702408x^{11} + 54206880x^{12} \\ &+ 116955440x^{13} + 217157720x^{14} + 346953464x^{15} \\ &+ 477691552x^{16} + 562088020x^{17} + 561273700x^{18} \\ &+ 473318040x^{19} + 331250556x^{20} + 189090876x^{21} \\ &+ 86045960x^{22} + 29949920x^{23} + 7454720x^{24} \\ &+ 1203904x^{25} + 91264x^{26}. \end{aligned}$$

Both $\mathcal{C}_\Pi$ and $\mathcal{C}_\Pi^\perp$ are optimal ternary codes.

Remarks: The codes described in Theorem 14 are noncyclic because the perfect nonlinear function $\Pi(x) = x^{10} + x^6 - x^2$ is not a power function.

Note that the conditions of (4) reduce to

$$\begin{cases} k_0^2 + k_1^2 + k_2^2 = \frac{n^2+2n}{3} \\ k_0 + k_1 + k_2 = n \end{cases} \tag{21}$$

since these two equations imply $k_0k_1 + k_1k_2 + k_2k_0 = \frac{n^2-n}{3}$. For example

$$(k_0, k_1, k_2) = \left(\frac{n + \sqrt{n}}{3}, \frac{n + \sqrt{n}}{3}, \frac{n - 2\sqrt{n}}{3}\right)$$

and

$$(k_0, k_1, k_2) = \left(\frac{n - \sqrt{n}}{3}, \frac{n - \sqrt{n}}{3}, \frac{n + 2\sqrt{n}}{3}\right)$$

are solutions to the two equations of (21). This means that both the lower and upper bounds on k_b given in Theorem 3 may be obtained. We have seen again that the lower and upper bounds on k_b of Theorem 3 are very tight. The following problem is open.

Open Problem 1: Determine all possible integral solutions (k_0, k_1, k_2) to (21).

If this open problem can be solved, then it is possible to determine the weight distribution of the four classes of ternary codes constructed from the perfect nonlinear functions $\Pi(x) = x^{(3^k+1)/2}$ and $\Pi(x) = x^{10} + x^6 - x^2$. Of course it is possible to determine the weight distribution of the codes directly without solving the open problem above.

Open Problem 2: Find the weight distribution of the four classes of ternary codes $\mathcal{C}_\Pi$ and $\overline{\mathcal{C}}_\Pi$ obtained from the perfect nonlinear function $\Pi(x) = x^{(3^k+1)/2}$ and $\Pi(x) = x^{10} + x^6 - x^2$.

D. The Codes From $\Pi(x) = x^{p^k+1}$

Theorem 15: Let $m > 1$, $h = 1$, and $m/\gcd(m, k)$ be odd. Let $\Pi(x) = x^{p^k+1}$, which is a perfect nonlinear mapping from GF(p^m) to GF(p^m) [6]. Then

a) $\mathcal{C}_\Pi$ is a $[p^m - 1, 2m, d; p]$ code with $d \geq \frac{p-1}{p}(p^m - p^{m/2})$;
b) $\mathcal{C}_\Pi^\perp$ is a $[p^m - 1, p^m - 2m - 1, d^\perp; p]$ code with $d^\perp = 4$ if $p = 3$, and $d^\perp = 3$ if $p > 3$;
c) $\overline{\mathcal{C}}_\Pi$ is a $[p^m, 2m+1, \overline{d}; p]$ code with $\overline{d} \geq \frac{p-1}{p}(p^m - p^{m/2})$;
d) $\overline{\mathcal{C}}_\Pi^\perp$ is a $[p^m, p^m - 2m - 1, \overline{d}^\perp; p]$ code with $\overline{d}^\perp = 5$ if $p = 3$, and $\overline{d}^\perp = 4$ if $p > 3$.

Proof: a) and c) follow from Theorems 4 and 5, respectively. Part b) follows from Theorem 6. We now prove d). When $p = 3$ the conclusion follows from Theorem 7.

We now prove that $\overline{\mathcal{C}}_\Pi^\perp$ has no codeword of weight 3. Otherwise, there exist three pairwise distinct elements $x_1, x_2, x_3 \in$ GF(p^m) and two elements $c_2, c_3 \in$ GF$(p)^*$ such that

$$\begin{cases} x_1 = -c_2x_2 + c_3x_3 \\ (c_2x_2 + c_3x_3)^{p^k+1} + c_2x_2^{p^k+1} + c_3x_3^{p^k+1} = 0 \\ 1 + c_2 + c_3 = 0. \end{cases} \tag{22}$$

Without loss of generality, suppose $x_3 \neq 0$. Let $y = x_2/x_3$. From the second equation of (22) it follows that

$$\left(c_2^2 + c_2\right) y^{p^k+1} + c_2c_3y^{p^k} + c_2c_3y + \left(c_3^2 + c_3\right) = 0. \tag{23}$$

From the last equation of (22) we get

$$c_2^2 + c_2 = c_3^2 + c_3 = -c_2c_3.$$

Thus, the second equation of (22) becomes

$$-c_2c_3y^{p^k+1} + c_2c_3y^{p^k} + c_2c_3y - c_2c_3 = 0$$

which is equivalent to

$$y^{p^k+1} - y^{p^k} - y + 1 = 0.$$

Note that $y^{p^k+1} - y^{p^k} - y + 1 = (y^{p^k} - 1)(y-1) = (y-1)^{p^k+1}$, so $y = 1, x_2 = x_3$. This is contrary to our assumption. Thus, $\overline{\mathcal{C}}_{\Pi}^{\perp}$ has no codeword of weight 3. It then follows from Theorem 7 that $\overline{d}^{\perp} = 4$.

Remark: The conclusion of Part b) in Theorem 15 may be proved by combining Lemma 9 of this paper, [7, Proposition 2 and Theorem 3].

Open Problem 3: Determine the minimum distance and weight distribution of the two classes of codes $\mathcal{C}_{\Pi}$ and $\overline{\mathcal{C}}_{\Pi}$ obtained from the perfect nonlinear function $\Pi(x) = x^{p^k+1}$.

The ternary codes $\mathcal{C}_{\Pi}, \overline{\mathcal{C}}_{\Pi}, \mathcal{C}_{\Pi}^{\perp}, \overline{\mathcal{C}}_{\Pi}^{\perp}$ described in Theorem 15 contain a number of optimal codes and are very good in general according to [3].

IV. Secret Sharing Schemes From the Linear Codes

In this section, we analyze the access structure of the secret sharing schemes based on the duals of the class of linear codes from perfect nonlinear functions constructed earlier.

A. A General Construction of Secret Sharing Schemes From Linear Codes

Let $G = [\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{n-1}]$ be a generator matrix of an $[n, k, d; q]$ code $\mathcal{C}$, i.e., the row vectors of G generate the linear subspace $\mathcal{C}$. For all the linear codes in this paper no column vector of any generator matrix is the zero vector. There are several ways to use linear codes to construct secret sharing schemes [17], [19]–[21]. One of them is the following described by Massey [17].

In the secret sharing scheme based on $\mathcal{C}$, the secret is an element of $\mathrm{GF}(q)$ and is equally likely to be any element of $\mathrm{GF}(q)$, which is called the *secret space*, and $n-1$ parties $P_1, P_2, \ldots, P_{n-1}$ and a dealer are involved.

To compute the shares with respect to a secret s, the dealer chooses randomly a vector $\boldsymbol{u} = (u_0, \ldots, u_{k-1}) \in \mathrm{GF}(q)^k$ such that $s = \boldsymbol{u}\boldsymbol{g}_0$. There are altogether q^{k-1} such vectors $\boldsymbol{u} \in \mathrm{GF}(q)^k$. The dealer then treats $\boldsymbol{u}$ as an information vector and computes the corresponding codeword

$$\boldsymbol{t} = (t_0, t_1, \ldots, t_{n-1}) = \boldsymbol{u}G.$$

He then gives t_i to party P_i as share for each $i \geq 1$.

The secret is recovered as follows. Note that $t_0 = \boldsymbol{u}\boldsymbol{g}_0 = s$. It is easily seen that a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determines the secret if and only if $\boldsymbol{g}_0$ is a linear combination of $\boldsymbol{g}_{i_1}, \ldots, \boldsymbol{g}_{i_m}$.

So we have the following lemma [17].

Lemma 16: Let G be a generator matrix of an $[n, k; q]$ code $\mathcal{C}$. In the secret sharing scheme based on $\mathcal{C}$, a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determine the secret if and only if there is a codeword

$$(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0) \tag{24}$$

in the dual code $\mathcal{C}^{\perp}$, where $c_{i_j} \neq 0$ for at least one j, $1 \leq i_2 < \cdots < i_m \leq n-1$, and $1 \leq m \leq n-1$.

If there is a codeword of form (24) in $\mathcal{C}^{\perp}$, then the vector $\boldsymbol{g}_0$ is a linear combination of $\boldsymbol{g}_{i_1}, \ldots, \boldsymbol{g}_{i_m}$, say

$$\boldsymbol{g}_0 = \sum_{j=1}^{m} x_j \boldsymbol{g}_{i_j}.$$

Then the secret s is recovered by computing

$$s = \sum_{j=1}^{m} x_j t_{i_j}.$$

If a group of participants can recover the secret by combining their shares, then any group of participants containing this group can also recover the secret. A group of participants is called a *minimal access set* if they can recover the secret with their shares, any of its proper subgroups cannot do so. Here a proper subgroup has fewer members than this group. Due to these facts, we are only interested in the set of all minimal-access sets. To determine this set, we need the notion of minimal codewords.

The *support* of a vector $\boldsymbol{c} \in \mathrm{GF}(q)^n$ is defined to be

$$\{0 \leq i \leq n-1 : c_i \neq 0\}.$$

A codeword $\boldsymbol{c}_2$ *covers* a codeword $\boldsymbol{c}_1$ if the support of $\boldsymbol{c}_2$ contains that of $\boldsymbol{c}_1$.

If a nonzero codeword $\boldsymbol{c}$ covers only its multiples, but no other nonzero codewords, then it is called a *minimal codeword*.

From Proposition 16 and the preceding discussions, it is clear that there is a one-to-one correspondence between the set of minimal-access sets and the set of minimal codewords of the dual code $\mathcal{C}^{\perp}$ whose first coordinate is 1. In the sequel, we shall consider the secret sharing schemes based on the dual codes of these linear codes from perfect nonlinear functions.

It should be noticed that to determine the access structure of the secret sharing scheme, we need to determine only the set of minimal codewords whose first coordinate is 1, i.e., a subset of the set of all minimal codewords. However, in almost every case we should be able to determine the set of all minimal codewords as long as we can determine the set of minimal codewords whose first coordinate is 1. The *covering problem* of a linear code is to determine the set of all its minimal codewords.

The shares for the participants depend on the the selection of the generator matrix G of the code $\mathcal{C}$. However, by Proposition 16, the selection of G does not affect the access structure of the secret sharing scheme. Hence, in the sequel we will call it the secret sharing scheme based on $\mathcal{C}$, without mentioning the generator matrix used to compute the shares.

B. The Access Structure of the Secret Sharing Schemes

We described the general construction of secret sharing schemes based on a linear code $\mathcal{C}$. Clearly, we have also a secret sharing scheme based on the dual code $\mathcal{C}^{\perp}$. Thus, for every given linear code $\mathcal{C}$ we have two secret sharing schemes. In this and later sections, we consider only the secret sharing schemes based on the dual code of a given linear code. The reader should not be confused about the two secret sharing schemes based on $\mathcal{C}$ and $\mathcal{C}^{\perp}$.

The following describes the access structure of the secret sharing scheme based on the dual code of a given linear code, and is a generalization of the corresponding result in [12], [23].

Theorem 17: Let $\mathcal{C}$ be an $[n,k,d;q]$ code, and let $G = [\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{n-1}]$ be its generator matrix. We use $d^\perp$ to denote the minimum distance of its dual code $\mathcal{C}^\perp$. If each nonzero codeword of $\mathcal{C}$ is minimal, then in the secret sharing scheme based on $\mathcal{C}^\perp$ there are altogether q^{k-1} minimal-access sets.

- When $d^\perp = 2$, the access structure is as follows.
  If $\boldsymbol{g}_i$ is a multiple of $\boldsymbol{g}_0$, $1 \le i \le n-1$, then participant P_i must be in every minimal access set. Such a participant is called a *dictatorial participant*.
  If $\boldsymbol{g}_i$ is not a multiple of $\boldsymbol{g}_0$, $1 \le i \le n-1$, then participant P_i must be in $(q-1)q^{k-2}$ out of q^{k-1} minimal-access sets.
- When $d^\perp \ge 3$, for any fixed
  $$1 \le t \le \min\{k-1, d^\perp - 2\}$$
  every group of t participants is involved in
  $$(q-1)^t q^{k-(t+1)}$$
  out of q^{k-1} minimal-access sets.

Proof: We first prove that the total number of minimal-access sets is q^{k-1}. At the very beginning of this section, we assumed that every column vector of any generator matrix is nonzero. Hence, $\boldsymbol{g}_0 \neq 0$. Thus, the inner product $\boldsymbol{u}\boldsymbol{g}_0$ takes on each element of GF(q) exactly q^{k-1} times when $\boldsymbol{u}$ ranges over all elements of GF$(q)^k$. Hence, there are altogether $q^k - q^{k-1}$ codewords in $\mathcal{C}$ whose first coordinator is nonzero. Since each nonzero codeword is minimal, a codeword covers another one if and only if they are multiples of each other. Hence, the total number of minimal codewords is $(q^k - q^{k-1})/(q-1) = q^{k-1}$, which is the number of minimal-access sets.

Suppose that $d^\perp = 2$. We determine the access structure. For any $1 \le i \le n-1$, if $\boldsymbol{g}_i = a\boldsymbol{g}_0$ for some $a \in$ GF$(q)^*$, then $\boldsymbol{u}\boldsymbol{g}_0 = 1$ implies that $\boldsymbol{u}\boldsymbol{g}_i = a \neq 0$. Thus Participant P_i is in every minimal access set. For any $1 \le i \le n-1$, if $\boldsymbol{g}_0$ and $\boldsymbol{g}_i$ are linearly independent, $(\boldsymbol{u}\boldsymbol{g}_0, \boldsymbol{u}\boldsymbol{g}_i)$ takes on each element of GF$(q)^2$ q^{k-2} times when the vector $\boldsymbol{u}$ ranges over GF$(q)^k$. Hence,

$$|\{\boldsymbol{u} : \boldsymbol{u}\boldsymbol{g}_0 \neq 0 \text{ and } \boldsymbol{u}\boldsymbol{g}_i \neq 0)\}| = (q-1)^2 q^{k-2}$$

and

$$|\{\boldsymbol{u} : \boldsymbol{u}\boldsymbol{g}_0 = 1 \text{ and } \boldsymbol{u}\boldsymbol{g}_i \neq 0)\}| = (q-1) q^{k-2}$$

which is the number of minimal-access sets in which P_i is involved.

Suppose that $d^\perp \ge 3$ and $1 \le t \le \min\{k-1, d^\perp - 2\}$. Let $1 \le i_1 < i_2 < \cdots < i_t \le n-1$ be a set of positive integers. Then $\boldsymbol{g}_0, \boldsymbol{g}_{i_1}, \boldsymbol{g}_{i_2}, \ldots, \boldsymbol{g}_{i_t}$ are linearly independent and $(\boldsymbol{u}\boldsymbol{g}_0, \boldsymbol{u}\boldsymbol{g}_{i_1}, \ldots, \boldsymbol{u}\boldsymbol{g}_{i_t})$ takes on each element of GF$(q)^{t+1}$ $q^{k-(t+1)}$ times when the vector $\boldsymbol{u}$ ranges over GF$(q)^k$. Hence,

$$|\{\boldsymbol{u} : \boldsymbol{u}\boldsymbol{g}_0 \neq 0, \boldsymbol{u}\boldsymbol{g}_{i_1} \neq 0, \ldots \boldsymbol{u}\boldsymbol{g}_{i_t} \neq 0)\}| = (q-1)^{t+1} q^{k-(t+1)}$$

and

$$|\{\boldsymbol{u} : \boldsymbol{u}\boldsymbol{g}_0 = 1, \boldsymbol{u}\boldsymbol{g}_{i_1} \neq 0, \ldots, \boldsymbol{u}\boldsymbol{g}_{i_t} \neq 0)\}| = (q-1)^t q^{k-(t+1)}$$

which is the number of minimal-access sets in which P_i is involved by Proposition 16.

The minimum distance d of the code $\mathcal{C}$ gives the lower bound $d-1$ for the cardinality of any minimal access set, while the minimum distance $d^\perp$ of the dual code $\mathcal{C}^\perp$ indicates the extent of democracy of the secret sharing scheme. However, there is a tradeoff between the two parameters, i.e., $d + d^\perp \le n+2$. The equality is achieved if $\mathcal{C}$ is maximum-distance separable (MDS).

In view of Theorem 17, it is an interesting problem to construct codes where each nonzero codeword is minimal. Such a linear code gives a secret sharing scheme with the interesting access structure described in Theorem 17.

If the weights of a linear code are close enough to each other, then each nonzero codeword of the code is minimal, as described by the following theorem.

Theorem 18: [23], [12] In an $[n,k;q]$ code $\mathcal{C}$, let $w_{\min}$ and $w_{\max}$ be the minimum and maximum nonzero weights, respectively. If

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}$$

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

C. Extending a Secret Sharing Scheme With a Small Secret Space

Given a secret sharing scheme in which the secret space $\mathcal{S}$ is small, one could extend it into a secret sharing scheme where the secret space is $\mathcal{S}^l$ for any positive integer l. The extension is very simple and as follows.

For a chosen integer l, the new secret space is $\mathcal{S}^l$. Each secret in the new secret space is a sequence $s_1 s_2 \ldots s_l$ of length l, where each $s_i \in \mathcal{S}$. In the extended scheme we use the original secret sharing scheme to share this secret $s_1 s_2 \ldots s_l$ component by component. For each component s_i, a share component corresponding to s_i is computed using the original secret sharing scheme. Hence, each participant will get a sequence of share components. The secret $s_1 s_2 \ldots s_l$ will be recovered by recovering each s_i one by one using the original secret sharing scheme when a group of participants meet together with their shares.

The information rate of the extended scheme is the same as the original secret sharing scheme. Thus, secret sharing schemes with a small secret space are as useful as those with large secret spaces. In the secret sharing schemes described in the sequel, the secret space is GF(q). Here q could be 3 or a power of any odd prime. Due to the extension given above, such schemes are all useful. The information rate of all the secret sharing schemes presented in this paper is 1, the best possible.

D. Secret Sharing Schemes Based on the Duals of the Linear Codes From Perfect Nonlinear Functions

Having described the general construction of secret sharing schemes based on error correcting codes and their extensions, we now use the duals of these linear codes from perfect nonlinear functions to construct secret sharing schemes and analyze their access structures.

For the code $\mathcal{C}_\Pi$ of Theorem 4, we have the following general result.

Theorem 19: Let $\mathcal{C}_\Pi$ be the $[p^m-1, 2m/h, d]$ code over GF(p^h) of Theorem 4, and let $G=[\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{p^m-2}]$ denote a generator matrix of $\mathcal{C}_\Pi$. If $p^h < (p^{m/2}+1)/2$, then in the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$, the total number of participants is p^m-2, and there are altogether p^{2m-h} minimal-access sets.

- When $d^\perp = 2$, the access structure is as follows.
  If $\boldsymbol{g}_i$ is a multiple of $\boldsymbol{g}_0$, $1 \le i \le p^m-2$, then participant P_i must be in every minimal access set.
  If $\boldsymbol{g}_i$ is not a multiple of $\boldsymbol{g}_0$, $1 \le i \le p^m-2$, then participant P_i must be in $(p^h-1)p^{2m-2h}$ out of p^{2m-h} minimal-access sets.
- When $d^\perp \ge 3$, for any fixed $1 \le t \le \min\{(2m/h)-1, d^\perp-2\}$ every group of t participants is involved in $(p^h-1)^t p^{2m-(t+1)h}$ out of p^{2m-h} minimal-access sets.

Proof: As before, let $w_{\min}$ and $w_{\max}$ denote the minimum and maximum nonzero weights in $\mathcal{C}_\Pi$, respectively. By Theorem 4 we have

$$\frac{w_{\min}}{w_{\max}} \ge \frac{p^m-p^{m/2}}{p^m+p^{m/2}} = \frac{p^{m/2}-1}{p^{m/2}+1} > \frac{p^h-1}{p^h}$$

because $p^h < (p^{m/2}+1)/2$. It follows from Theorem 18 that every codeword in $\mathcal{C}_\Pi$ is minimal. The conclusions of this theorem then follow from Theorem 17.

This theorem gives the access structure of the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$ whose dual $\mathcal{C}_\Pi$ is from any perfect nonlinear function Π under the condition $p^h < (p^{m/2}+1)/2$. If this condition is not satisfied, the covering problem for the code $\mathcal{C}_\Pi$ is still open and so is the access structure of the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$. On the other hand, this condition is derived from the lower and upper bounds on the weights in $\mathcal{C}_\Pi$ given in Theorem 4. If all the weights in $\mathcal{C}_\Pi$ can be determined, it is possible to relax this condition to some extent so that the access structure can still be determined.

Open Problem 4: Let $\mathcal{C}_\Pi$ be the $[p^m-1, 2m/h, d]$ code over GF(p^h) of Theorem 4. Determine the access structure of the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$ for the case that $p^h \ge (p^{m/2}+1)/2$.

As seen earlier, it is possible that $d^\perp = 2$. In this case, some participants must be involved in every minimal-access set and thus, in every access set. This means that these participants must be involved in order to recover a secret. These participants are thus called dictatorial participants. When $d^\perp \ge 3$, every participant is involved in the same number of minimal-access sets. In this case, the secret sharing scheme is called *democratic*. The minimum distance $d^\perp$ indicates the extent of democracy of the secret sharing scheme. To give a better description of the access structure, we need to determine $d^\perp$.

In the following, we shall give a detailed description of the access structure of the secret sharing schemes based on several specific classes of codes $\mathcal{C}_\Pi^\perp$ constructed in Section III.

Theorem 20: Let $\mathcal{C}_\Pi$ be the code of Theorem 10. If $m \ge 3$, then in the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$, the total number of participants is p^m-2 and there are altogether q^{2m-1} minimal-access sets.

- When $p > 3$, every participant is involved in $(p-1)p^{2m-2}$ out of p^{2m-1} minimal-access sets.
- When $p = 3$, for any fixed $1 \le t \le 2$ every group of t participants is involved in $(p-1)^t p^{2m-(t+1)}$ out of p^{2m-1} minimal-access sets.

Proof: Similar to the proof of Theorem 19, it can be proved that every codeword of $\mathcal{C}_\Pi$ is minimal if $m \ge 3$. The conclusions then follow from Theorems 17 and 11.

Open Problem 5: Let $\mathcal{C}_\Pi$ be the code of Theorem 10. Determine the access structure of the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$ for $m = 2$.

Theorem 21: Let $\mathcal{C}_\Pi$ be the $[3^m-1, 2m, d]$ ternary code from the perfect nonlinear function $\Pi(x) = x^{(3^k+1)/2}$. If $m \ge 3$, then in the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$, the total number of participants is 3^m-2, and there are altogether 3^{2m-1} minimal-access sets. For any fixed $1 \le t \le 2$, every group of t participants is involved in $2^t 3^{2m-(t+1)}$ out of 3^{2m-1} minimal-access sets.

Proof: The conclusions follow from Theorem 13 and its proof as well as Theorem 19.

The condition $m \ge 3$ in Theorem 21 is necessary for the access structure of the secret sharing scheme to be democratic. The following example shows the necessity.

Example 2: Let $\mathcal{C}_\Pi$ be the $[3^m-1, 2m, d]$ ternary code from the perfect nonlinear function $\Pi(x) = x^{(3^k+1)/2}$ where $(m,k)=(2,1)$. We now determine the access structure of the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$.

$\mathcal{C}_\Pi$ is an $[8,4,4;3]$ with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 2 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 \end{bmatrix}.$$

$\mathcal{C}_\Pi^\perp$ is an $[8,4,4;3]$ code with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 2 & 0 & 2 \\ 0 & 1 & 0 & 0 & 2 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 \end{bmatrix}.$$

Both $\mathcal{C}_\Pi$ and $\mathcal{C}_\Pi^\perp$ are optimal and have weight distribution

$$1 + 20x^4 + 32x^5 + 8x^6 + 16x^7 + 4x^8.$$

Not every nonzero codeword of $\mathcal{C}_\Pi$ is minimal. The secret sharing scheme based on $\mathcal{C}_\Pi^\perp$ involves seven participants. There are altogether 15 minimal-access sets

$$\{1,2,5\},\{1,4,7\},\{2,4,6\},\{3,4,5\},\{3,6,7\},$$
$$\{1,2,3,4\},\{1,2,3,7\},\{1,2,6,7\},\{1,3,4,6\},\{1,3,5,6\},$$
$$\{1,5,6,7\},\{2,3,5,6\},\{2,3,5,7\},\{2,4,5,7\},\{4,5,6,7\}.$$

The fourth participant is involved in seven of the minimal-access sets, while each of the remaining participants is involved in eight of the minimal-access sets. Hence, the secret sharing scheme is not democratic when the condition $m \ge 3$ is not satisfied.

Theorem 22: Let $\mathcal{C}_\Pi$ be the $[3^m-1, 2m, d]$ ternary code from the perfect nonlinear function $\Pi(x) = x^{10}+x^6-x^2$. If $m \ge 3$, then in the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$, the total number

of participants is 3^m-2, and there are altogether 3^{2m-1} minimal-access sets. Each participant is involved in $2\times 3^{2m-2}$ out of 3^{2m-1} minimal-access sets.

Proof: The conclusions follow from Theorem 14 and its proof as well as Theorem 19.

Theorem 23: Let $m>1$, and let $\mathcal{C}_\Pi$ be the $[p^m-1, 2m/h, d]$ code over GF(p^h) from the perfect nonlinear function $\Pi(x)=x^{p^k+1}$. If $p^h<(p^{m/2}+1)/2$, then in the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$, the total number of participants is p^m-2, and there are altogether p^{2m-h} minimal-access sets. In addition, every participant is involved in $(p^h-1)p^{2m-2h}$ out of p^{2m-h} minimal-access sets.

In particular, if $p=3$, for any fixed $1\le t\le 2$ every group of t participants is involved in $(p-1)^t p^{2m-(t+1)}$ out of p^{2m-1} minimal-access sets.

Proof: The conclusions follow from Theorems 19 and 15.

Open Problem 6: Let $m>1$, and let $\mathcal{C}_\Pi$ be the $[p^m-1, 2m/h, d]$ code over GF(p^h) from the perfect nonlinear function $\Pi(x)=x^{p^k+1}$. Determine the access structure of the secret sharing scheme based on $\mathcal{C}_\Pi^\perp$ for the case $p^h\ge (p^{m/2}+1)/2$.

V. Codes From Another Class of Perfect Nonlinear Functions and Their Secret Sharing Schemes

Section III gives a general construction of two types of related codes using perfect nonlinear mappings from GF(p^m) to GF(p^m), and Section IV describes the secret sharing schemes based on their dual codes. In this section, we use a class of perfect nonlinear mappings from GF$(q)^2$ to GF(q) to construct a class of three-weight codes and describe the access structure of the secret sharing schemes based on their dual codes.

Let $a,b_1,b_2,x,y\in$ GF(q^t), and let $\mathrm{Tr}(x)$ denote the trace function from GF(q^t) to GF(q) in this section. Define the function

$$f_{a,b_1,b_2}(x,y)=\mathrm{Tr}(axy+b_1x+b_2y).$$

Let

$$(\mathrm{GF}(q^t))^2\setminus\{(0,0)\}=\{(l_0,r_0),(l_1,r_1),\ldots,(l_{q^{2t}-2},r_{q^{2t}-2})\}.$$

Then any given set of $a,b_1,b_2\in$ GF(q^t) defines the following vector:

$$\boldsymbol{c}_{a,b_1,b_2}=(f_{a,b_1,b_2}(l_0,r_0),\ldots,f_{a,b_1,b_2}(l_{q^{2t}-2},r_{q^{2t}-2})).$$

We now define the following linear code:

$$\mathcal{C}_t=\{\boldsymbol{c}_{a,b_1,b_2}: a,b_1,b_2\in \mathrm{GF}(q^t)\}.$$

To determine the weight distribution of the code $\mathcal{C}_t$, we prove the following lemma.

Lemma 24: Let $N(a)$ denote the number of solutions $(z_1,z_2,\ldots,z_{2t})\in$ GF$(q)^{2t}$ of the equation

$$\sum_{i=1}^{t} z_{2i-1}z_{2i}=a,\qquad a\in \mathrm{GF}(q). \tag{25}$$

Then we have

$$N(a)=\begin{cases} q^{2t-1}+(q-1)q^{t-1}, & a=0\\ q^{2t-1}-q^{t-1}, & a\neq 0.\end{cases} \tag{26}$$

Proof: When q is even, (26) follows from [15, Theorem 6.32, p. 288].

When q is odd, the determinant of the quadratic form $\sum_{i=1}^{t} z_{2i-1}z_{2i}$ is $(-1)^t(2^{-t})^2$. By [15, Theorem 6.26, p. 282]

$$\begin{aligned}N(a)&=q^{2t-1}+\nu(a)\eta((-1)^{2t}(2^{-t})^2)q^{t-1}\\&=q^{2t-1}+\nu(a)q^{t-1}\end{aligned}$$

where η is the quadratic character of GF(q), $\nu(a)=-1$ for $a\in$ GF$(q)^*$, and $\nu(0)=q-1$. This completes the proof.

Theorem 25: $\mathcal{C}_t$ is a $[q^{2t}-1, 3t; q]$ code with weight distribution as follows:

weight	frequency
0	1
$q^{2t}-q^{2t-1}$	$q^{2t}-1$
$q^{2t}-q^{2t-1}-q^t+q^{t-1}$	$(q^t-1)[q^{2t-1}+(q-1)q^{t-1}]$
$q^{2t}-q^{2t-1}+q^{t-1}$	$(q^t-1)^2(q-1)q^{t-1}$

Proof: To determine the weight distribution of $\mathcal{C}_t$, we discuss the number of solutions of $f_{a,b_1,b_2}(x,y)=0$ for all $(a,b_1,b_2)\in$ GF$(q^t)^3$. We study the case $a=0$ and the case $a\neq 0$ separately below.

When $a=0$, we consider the following subcases.

1. If $b_1=b_2=0$, $\boldsymbol{c}_{a,b_1,b_2}$ is the zero codeword.
2. If $b_1\neq 0$, $b_2=0$, then $f_{a,b_1,b_2}(x,y)=\mathrm{Tr}(b_1x)$. The number of solutions of $f_{a,b_1,b_2}(x,y)=0$ is q^tq^{t-1}. There are q^t-1 such cases.
3. If $b_1=0$, $b_2\neq 0$, then $f_{a,b_1,b_2}(x,y)=\mathrm{Tr}(b_2y)$. The number of solutions of $f_{a,b_1,b_2}(x,y)=0$ is q^tq^{t-1}. There are q^t-1 such cases.
4. If $b_1\neq 0$, $b_2\neq 0$, then for all $x\in$ GF(q^t), there are q^{t-1} y's such that $f_{a,b_1,b_2}(x,y)=0$. So the number of solutions of $f_{a,b_1,b_2}(x,y)=0$ is q^tq^{t-1}. There are $(q^t-1)^2$ such cases.

When $a\neq 0$, let $\alpha_1,\alpha_2,\ldots,\alpha_t$ be a basis of GF(q^t) over GF(q). Suppose under this basis the coordinates of x and y are $\boldsymbol{x}\in$ GF$(q)^t$ and $\boldsymbol{y}\in$ GF$(q)^t$, respectively.

Let

$$\begin{aligned}\boldsymbol{v}_1&=(\mathrm{Tr}(b_1\alpha_1),\mathrm{Tr}(b_1\alpha_2),\ldots,\mathrm{Tr}(b_1\alpha_t))\\ \boldsymbol{v}_2&=(\mathrm{Tr}(b_2\alpha_1),\mathrm{Tr}(b_2\alpha_2),\ldots,\mathrm{Tr}(b_2\alpha_t))\end{aligned}$$

and

$$\boldsymbol{M}=\begin{pmatrix}\mathrm{Tr}(a\alpha_1\alpha_1) & \mathrm{Tr}(a\alpha_1\alpha_2) & \ldots & \mathrm{Tr}(a\alpha_1\alpha_t)\\ \mathrm{Tr}(a\alpha_2\alpha_1) & \mathrm{Tr}(a\alpha_2\alpha_2) & \ldots & \mathrm{Tr}(a\alpha_2\alpha_t)\\ \vdots & \vdots & \ldots & \vdots\\ \mathrm{Tr}(a\alpha_t\alpha_1) & \mathrm{Tr}(a\alpha_t\alpha_2) & \ldots & \mathrm{Tr}(a\alpha_t\alpha_t)\end{pmatrix}.$$

Then

$$f_{a,b_1,b_2}(x,y)=\boldsymbol{x}\boldsymbol{M}\boldsymbol{y}^T+\boldsymbol{v}_1\boldsymbol{x}^T+\boldsymbol{v}_2\boldsymbol{y}^T.$$

We now prove that $\boldsymbol{M}$ is nonsingular when $a\neq 0$. Suppose the column vectors of $\boldsymbol{M}$ are linearly dependent. Then there exist $c_1,c_2,\ldots,c_t\in$ GF(q) such that, $\forall\ 1\le i\le t$, $\mathrm{Tr}(a\alpha_i\sum_{j=1}^{t}c_j\alpha_j)=0$. Then $a\sum_{j=1}^{t}c_j\alpha_j=0$, and since

$a \neq 0$, $\sum_{j=1}^{t} c_j \alpha_j = 0$. Thus, $c_j = 0$ for $1 \leq j \leq t$ and $\boldsymbol{M}$ is nonsingular.

Since $\boldsymbol{M}$ is nonsingular, $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ range over GF$(q)^t$ when b_1 and b_2 range over GF(q^t). This is proved by expressing b_i as

$$b_i = \sum_{j=1}^{t} b_{ij} \alpha_j,$$

where all $b_{ij} \in$ GF(q).

Since $\boldsymbol{M}$ is nonsingular, there exist nonsingular matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ such that $\boldsymbol{AMB} = \boldsymbol{I}$ where $\boldsymbol{I}$ is the identity matrix. Let $\boldsymbol{x}' = \boldsymbol{x}\boldsymbol{A}^{-1}$, $\boldsymbol{y}' = \boldsymbol{y}(\boldsymbol{B}^{-1})^T$. As $\boldsymbol{x}, \boldsymbol{y}$ range over GF$(q)^t$, $\boldsymbol{x}', \boldsymbol{y}'$ range over GF$(q)^t$. Then

$$\begin{aligned} f_{a,b_1,b_2}(x,y) &= (\boldsymbol{x}\boldsymbol{A}^{-1})(\boldsymbol{AMB})(\boldsymbol{B}^{-1}\boldsymbol{y}^T) + \boldsymbol{v}_1\boldsymbol{x}^T + \boldsymbol{v}_2\boldsymbol{y}^T \\ &= \boldsymbol{x}'\boldsymbol{y}'^T + \boldsymbol{v}_1\boldsymbol{A}^T\boldsymbol{x}'^T + \boldsymbol{v}_2\boldsymbol{B}\boldsymbol{y}'^T. \end{aligned}$$

Let $\boldsymbol{v}_1' = \boldsymbol{v}_1\boldsymbol{A}^T$, $\boldsymbol{v}_2' = \boldsymbol{v}_2\boldsymbol{B}$. As $\boldsymbol{v}_1, \boldsymbol{v}_2$ range over GF$(q)^t$, $\boldsymbol{v}_1', \boldsymbol{v}_2'$ range over GF$(q)^t$. Then

$$f_{a,b_1,b_2}(x,y) = \boldsymbol{x}'\boldsymbol{y}'^T + \boldsymbol{v}_1'\boldsymbol{x}'^T + \boldsymbol{v}_2'\boldsymbol{y}'^T.$$

Let $\boldsymbol{x}'' = \boldsymbol{x}' + \boldsymbol{v}_2'$, $\boldsymbol{y}'' = \boldsymbol{y}' + \boldsymbol{v}_1'$, then

$$f_{a,b_1,b_2}(x,y) = \boldsymbol{x}''\boldsymbol{y}''^T - \boldsymbol{v}_1'\boldsymbol{v}_2'^T.$$

Let $N(a)$ be defined as in Lemma 24. Note that $\boldsymbol{v}_1'$ and $\boldsymbol{v}_2'$ range over GF$(q)^t$ when b_1 and b_2 range over GF(q^t), respectively. It follows from Lemma 24 and the preceding discussions that the weights and frequency of appearance in all the codewords $\boldsymbol{c}_{a,b_1,b_2}$, $a \neq 0$, are given by

weight	frequency
$q^{2t} - N(0)$	$(q^t - 1)N(0)$
$q^{2t} - N(1)$	$(q^t - 1)(q^{2t} - N(0))$

where $N(0)$ and $N(1)$ are given in Lemma 24.

$\mathcal{C}_t$ is clearly a linear code with length $q^{2t} - 1$. The preceding discussions show that $\mathcal{C}_t$ has q^{3t} codewords. Hence, $\mathcal{C}_t$ is a $[q^{2t} - 1, 3t; q]$ code.

In the cases of $q = 2$ and $t = 2, 3, 4$, the code $\mathcal{C}_t$ has parameters

$$[15,6,6;2], [63,9,28;2], [255,12,120;2]$$

among which the first two are optimal, and the last one is the best code known according to [3]. In the case $p = 2$, the code $\mathcal{C}_t$ has the same weights as the Kasami code [14]. But it is an open problem whether they are equivalent.

Lemma 26: For $t \geq 2$, every nonzero codeword of $\mathcal{C}_t$ is minimal.

Proof: By Theorem 25, the inequality

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}$$

is reduced to

$$q^{t+1} - q^t > q^2 - 1$$

which is true when $t \geq 2$, because $q^{t+1} - q^t \geq q^t > q^2 - 1$.

Now we discuss the access structure of the secret sharing scheme based on $\mathcal{C}_t^{\perp}$. To apply Theorem 17, we need the following lemma.

Lemma 27: $\mathcal{C}_t^{\perp}$ is a $[q^{2t} - 1, q^{2t} - 1 - 3t, d^{\perp}; q]$ code, where $d^{\perp} = 3$ if $q = 2$, and $d^{\perp} = 2$ if $q > 2$.

Proof: For any fixed $(x, y) \neq (0, 0)$, the function $\mathrm{Tr}(axy + b_1 x + b_2 y)$ cannot be the zero function. Hence, $d^{\perp} \neq 1$.

If $d^{\perp} = 2$, then there exist $c \in$ GF$(q)^*$ and two distinct pairs

$$(x_i, y_i) \in \mathrm{GF}(q^t)^2 \setminus \{(0,0)\}, \qquad i = 1, 2$$

such that

$$\mathrm{Tr}(ax_1y_1 + b_1x_1 + b_2y_1) = c\mathrm{Tr}(ax_2y_2 + b_1x_2 + b_2y_2)$$

for all $(a, b_1, b_2) \in$ GF$(q^t)^3$. This is possible if and only if

$$ax_1y_1 + b_1x_1 + b_2y_1 = cax_2y_2 + cb_1x_2 + cb_2y_2 \tag{27}$$

for all $(a, b_1, b_2) \in$ GF$(q^t)^3$, which is equivalent to

$$x_1 = cx_2,\ y_1 = cy_2,\ x_1y_1 = cx_2y_2. \tag{28}$$

This is impossible if $q = 2$, because $(x_1, y_1) \neq (x_2, y_2)$.

When $q = 2$, a sufficient and necessary condition for $d^{\perp} = 3$ is that there exist pairwise distinct $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in$ GF$(q^t)^2$ such that

$$\begin{aligned} \mathrm{Tr}(ax_1y_1 + b_1x_1 + b_2y_1) + \mathrm{Tr}(ax_2y_2 + b_1x_2 + b_2y_2) \\ + \mathrm{Tr}(ax_3y_3 + b_1x_3 + b_2y_3) = 0 \end{aligned}$$

for all $(a, b_1, b_2) \in$ GF$(q^t)^3$. This is equivalent to

$$\begin{cases} x_1y_1 + x_2y_2 + x_3y_3 = 0 \\ x_1 + x_2 + x_3 = 0 \\ y_1 + y_2 + y_3 = 0. \end{cases} \tag{29}$$

Let α be a primitive element of GF(q^t), then

$$\begin{aligned} (x_1, y_1) &= (1 + \alpha, 1 + \alpha) \\ (x_2, y_2) &= (1, 1) \\ (x_3, y_3) &= (\alpha, \alpha) \end{aligned}$$

is a solution to (29). So $d^{\perp} = 3$ when $q = 2$.

If $q > 3$, (28) is possible only when $x_1y_1 = x_2y_2 = 0$. In fact, for any nonzero $a \in$ GF(q^t) and any $c \in$ GF$(q) \setminus \{0, 1\}$, the following pairs:

$$(x_1, y_1) = (0, ac), (x_2, y_2) = (0, a)$$

or

$$(x_1, y_1) = (ac, 0), (x_2, y_2) = (a, 0)$$

are solutions of (28). Hence, $d^{\perp} = 2$ if $q > 2$.

Now we characterize the access structure of the secret sharing scheme based on $\mathcal{C}_t^{\perp}$ as follows.

Theorem 28: Let $t \geq 2$. In the secret sharing scheme based on $\mathcal{C}_t^{\perp}$, the total number of participants is $q^{2t} - 2$ and there are altogether q^{3t-1} minimal-access sets.

If $q > 2$, we have the following conclusion.

- When $l_0 = 0$ or $r_0 = 0$, there are $q - 2$ participants who must be in every minimal access set. Each of the other $q^{2t} - q$ participants is involved in $(q - 1)q^{3t-2}$ minimal-access sets.

- When $l_0 \neq 0$ and $r_0 \neq 0$, every participant is involved in $(q-1)q^{3t-2}$ minimal-access sets.
  If $q = 2$, every participant is involved in $(q-1)q^{3t-2}$ minimal-access sets.

Proof: The conclusion follows from Theorem 17, Lemma 26, and the proof of Lemma 27.

We can now construct a class of codes $\overline{\mathcal{C}}_t$ which are related to $\mathcal{C}_t$. Below is the construction of $\overline{\mathcal{C}}_t$.

Let $a, b_1, b_2, x, y \in \mathrm{GF}(q^t)$, $c \in \mathrm{GF}(q)$. Define the function

$$f_{a,b_1,b_2,c}(x,y) = \mathrm{Tr}(axy + b_1 x + b_2 y) + c.$$

Let

$$(\mathrm{GF}(q^t))^2 = \{(l_0, r_0), (l_1, r_1), \ldots, (l_{q^{2t}-1}, r_{q^{2t}-1})\}.$$

Then any given set of $a, b_1, b_2 \in \mathrm{GF}(q^t)$ and $c \in \mathrm{GF}(q)$ defines the following vector:

$$\boldsymbol{c}_{a,b_1,b_2,c} = (f_{a,b_1,b_2,c}(l_0, r_0), \ldots, f_{a,b_1,b_2,c}(l_{q^{2t}-1}, r_{q^{2t}-1})).$$

We now define the following linear code:

$$\overline{\mathcal{C}}_t = \{\boldsymbol{c}_{a,b_1,b_2,c} : a, b_1, b_2 \in \mathrm{GF}(q^t), c \in \mathrm{GF}(q)\}.$$

Theorem 29: $\overline{\mathcal{C}}_t$ is a $[q^{2t}, 3t+1, (q-1)q^{t-1}(q^t-1); q]$ code with the following nonzero weights:

$q^{2t} - q^{2t-1}$
$q^{2t} - q^{2t-1} - q^t + q^{t-1}$
$q^{2t} - q^{2t-1} + q^{t-1}$
q^{2t}

Proof: The proof is a slight modification of that of Theorem 25 and is omitted.

Theorem 30: $\overline{\mathcal{C}}_t^{\perp}$ is a $[q^{2t}, q^{2t} - 3t - 1, \overline{d_t}^{\perp}; q]$ code, where $\overline{d_t}^{\perp} = 4$ if $q = 2$, and $\overline{d_t}^{\perp} = 3$ if $q \geq 3$.

Proof: Similar to Theorem 7, we have $\overline{d_t}^{\perp} > 2$. $\overline{\mathcal{C}}_t^{\perp}$ has a codeword of weight 3 if and only if there exist three pairwise distinct pairs $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathrm{GF}(q^t)^2$ and two elements $c_2, c_3 \in \mathrm{GF}(q)^*$ such that

$$\begin{cases} 1 + c_2 + c_3 = 0 \\ x_1 y_1 + c_2 x_2 y_2 + c_3 x_3 y_3 = 0 \\ x_1 + c_2 x_2 + c_3 y_3 = 0 \\ y_1 + c_2 y_2 + c_3 y_3 = 0. \end{cases} \tag{30}$$

We consider $q = 2$ and $q > 2$, respectively.

- $q = 2$: In this case, we must have $c_2 = c_3 = 1$ and (30) cannot hold. So $\overline{d_t}^{\perp} > 3$. On the other hand, $\overline{\mathcal{C}}_t^{\perp}$ is a $[q^{2t}, q^{2t} - 3t - 1; \overline{d_t}^{\perp}; q]$ code. We have

  $$\sum_{i=0}^{2} \binom{q^{2t}}{i} (q-1)^i - q^{3t+1} \geq 0.$$

  By the sphere-packing bound, $\overline{d_t}^{\perp} < 5$. So we have $\overline{d_t}^{\perp} = 4$ if $q = 2$.
- $q > 2$: Let α be a primitive element of $\mathrm{GF}(q)$. One can verify that (30) is satisfied with $c_2 = -\alpha$, $c_3 = \alpha - 1$, $(x_1, y_1) = (1, 1)$, $(x_2, y_2) = (1, \alpha)$, $(x_3, y_3) = (1, 1+\alpha)$. So $\overline{d_t}^{\perp} = 3$ if $q > 2$.

$\overline{\mathcal{C}}_t$ gives optimal codes when $p = 2$ and $t = 2, 3$, and 4. Thus, the codes $\mathcal{C}_t$ and $\overline{\mathcal{C}}_t$ contain optimal codes when $p = 2$. However, they are not among the best codes known when $p \geq 3$, although they are good codes. We are interested only in $\mathcal{C}_t$ for our secret sharing purpose.

The code $\mathcal{C}_t$ is constructed using a class of perfect nonlinear functions

$$f_{a,b_1,b_2}(x,y) = \mathrm{Tr}(axy + b_1 x + b_2 y)$$

where $a \neq 0$, and a class of linear functions

$$f_{0,b_1,b_2}(x,y) = \mathrm{Tr}(b_1 x + b_2 y).$$

VI. Concluding Remarks

The main objectives of this paper are to construct good linear codes and derive secret sharing schemes based on them with nice access structures. The linear codes presented in this paper do contain many optimal and almost optimal codes, as shown in some of the previous sections. If a perfect nonlinear function Π from $\mathrm{GF}(3^m)$ to itself satisfies the two simple conditions in Theorem 6, then the ternary code $\mathcal{C}_\Pi^{\perp}$ has parameters

$$[3^m - 1, 3^m - 1 - 2m, 4; 3]$$

and is thus optimal due to the sphere-packing bound.

We pointed out in Section III-A that when $\Pi(x)$ is a power function, the code $\mathcal{C}_\Pi$ is equivalent to the dual of a cyclic code with two zeros. In this case, the code $\mathcal{C}_\Pi$ and its dual are not new. But our contribution to the study of these codes is the very tight lower bounds on the minimum distance of $\mathcal{C}_\Pi$ and $\overline{\mathcal{C}}_\Pi$ described in Theorems 4 and 5. As mentioned earlier, some perfect nonlinear functions Π are not power functions. In this case, the code $\mathcal{C}_\Pi$ is not cyclic and could be new. Note that our constructions of the codes $\mathcal{C}_\Pi$ and $\overline{\mathcal{C}}_\Pi$ are generic. As long as we discover new perfect nonlinear functions, we will obtain new linear codes.

Here we inform that Ding and Yuan [13] have just discoverd a new family of perfect nonlinear functions which are discribed in the following proposition.

Proposition 31: (Ding and Yuan [13]) For any $u \in \mathrm{GF}(3^m)^*$, $g_u(x) = x^{10} - ux^6 - u^2x^2$ is a perfect nonlinear function from $\mathrm{GF}(3^m)$ to $\mathrm{GF}(3^m)$, where m is odd.

A k-element subset D of a finite Abelian group G of order v is called a (v, k, λ)-*difference set* in G provided that the multiset $\{d_1 - d_2 : d_1, d_2 \in D, d_1 \neq d_2\}$ contains each nonidentity element of G exactly λ times. A difference set D in an additive group G is called a skew difference set (or antisymmetric difference set) if and only if G is the disjoint union of D, $-D$, and $\{0\}$.

Ding and Yuan [13] have also proved the following.

Proposition 32: (Ding and Yuan [13]) Let m be odd, and $u \in \mathrm{GF}(3^m)^*$. The set $\mathrm{Image}(g_u) \setminus \{0\}$ is a $(3^m, (3^m-1)/2, (3^m-3)/4)$ skew difference set in the Abelian group $(\mathrm{GF}(3^m), +)$.

The new family of perfect nonlinear functions of Proposition 31 yields more linear codes within the generic construction of this paper. In addition, the difference set property given in Proposition 32 may be used to prove more properties of the linear codes.

The secret sharing schemes based on the dual codes of the error-correcting codes from perfect nonlinear functions have two types of access structures. The first type is democratic, and

the second type has a few dictatorial participants. Both types could be useful in applications.

Regarding the linear codes and the secret sharing schemes we proposed seven open problems. It would be nice if advances on these open problems could be made. We invite the reader to attack these open problems.

Finally, we mention functions from GF (2^m) to GF (2^m) with optimal nonlinearity were used to construct $[2^m-1, 2m]$ binary codes in [5] and [4], where good and optimal binary codes were obtained.

ACKNOWLEDGMENT

The authors wish to thank the referees and Prof. Khaled Abdel-Ghaffar for their comments and suggestions that improved the presentation of this paper.

REFERENCES

[1] R. J. Anderson, C. Ding, T. Helleseth, and T. Kløve, "How to build robust shared control systems," *Des., Codes Cryptogr.*, vol. 15, pp. 111–124, 1998.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Nat. Computer Conf.*, vol. 48, New York, Jun. 1979, pp. 313–317.

[3] A. E. Brouwer. Bounds on the Minimum Distance of Linear Codes. [Online]. Available: http://www.win.tue.nl/ aeb/voorlincod.html

[4] A. Canteaut, P. Charpin, and H. Dobbertin, "Weight divisibility of cyclic codes, highly nonlinear functions on GF(2^m), and cross correlation of maximum-length sequences," *SIAM J. Discr. Math.*, vol. 13, pp. 105–137, 2000.

[5] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Des., Codes Cryptogr.*, vol. 15, pp. 125–156, 1998.

[6] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complexity*, vol. 20, no. 2, pp. 205–244, 2004.

[7] P. Charpin, A. Tietäväinen, and V. Zinoviev, "On the minimum distances of nonbinary cyclic codes," *Des., Codes Cryptogr.*, vol. 17, pp. 81–85, 1999.

[8] R. S. Coulter and R. W. Mathews, "Planar functions and planes of Lenz-Barlotti class II," *Des., Codes Cryptogr.*, vol. 10, pp. 167–184, 1997.

[9] P. Delsarte, "On subfield subcodes of modified Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 5, pp. 575–576, Sep. 1975.

[10] C. Ding, T. Helleseth, T. Kløve, and X. Wang, "A general construction of Cartesian authentication codes," *Discr. Math.*, to be published.

[11] C. Ding, D. Kohel, and S. Ling, "Secret sharing with a class of ternary codes," *Theor. Comp. Sci.*, vol. 246, pp. 285–298, 2000.

[12] C. Ding and J. Yuan, "Covering and secret sharing with linear codes," in *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, 2003, vol. 2731, pp. 11–25.

[13] ——, "A new family of skew Paley-Hadamard difference sets," *J. Comb. Theory A*, to be published.

[14] T. Kasami, "Weight distribution formula for some classes of cyclic codes," Coordinated Sci. Lab., University of Illinois at Urbana-Champaign, Urbana, IL, Tech. Rep. R-285 (AD 632574), 1966.

[15] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1978.

[17] J. L. Massey, "Minimal codewords and secret sharing," in *Proc. 6th Joint Swedish-Russian Workshop on Information Theory*, Mölle, Sweden, Aug. 1993, pp. 276–279.

[18] ——, "Some applications of coding theory in cryptography," in *Codes and Ciphers: Cryptography and Coding IV*. Esses, U.K.: Formara Ltd, 1995, pp. 33–47.

[19] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed-Solomon codes," *Commun. ACM*, vol. 24, pp. 583–584, 1981.

[20] J. Pieprzyk and X. M. Zhang, "Ideal secret sharing schemes from MDS codes," in *Proc. 5th Int. Conf. Information Security and Cryptology (ICISC 2002)*, Seoul, Korea, Nov. 2002, pp. 269–279.

[21] A. Renvall and C. Ding, "The access structure of some secret-sharing schemes," in *Information Security and Privacy (Lecture Notes in Computer Science)*. Heidelberg, Germany: Springer-Verlag, 1996, vol. 1172, pp. 67–78.

[22] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, Dec. 1979.

[23] J. Yuan and C. Ding, "Secret sharing schemes from two-weight codes," in *Proc. The Bose Centenary Symp. Discrete Mathematics and Applications*, Kolkata, India, Dec. 2002, pp. 1–7.