On some cosets of the first-order Reed-Muller code with high minimum weight

Article *in* IEEE Transactions on Information Theory · June 1999

DOI: 10.1109/18.761276 · Source: IEEE Xplore

1 author:

Caroline Fontaine
CNRS Lab-STICC and Telecom Bretagne
71 PUBLICATIONS **1,862** CITATIONS

REFERENCES

[1] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2010–2017, 1998.

[2] G. Brassard, C. Crépeau, and M. Santha, "Oblivious transfers and intersecting codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1769–1780, 1996.

[3] A. E. Brouwer and T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 662–677, 1993.

[4] G. D. Cohen and A. Lempel, "Linear intersecting codes," *Discr. Math.*, vol. 56, pp. 35–43, 1985.

[5] G. D. Cohen and G. Zémor, "Intersecting codes and independent families," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1872–1881, 1984.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[7] N. J. A. Sloane, "Covering arrays and intersecting codes," *J. Comb. Des.*, vol. 1, pp. 51–63, 1993.

[8] G. Zémor and G. D. Cohen, "The threshold probability of a code," *IEEE Trans. Inform. Theory*, vol. 41, pp. 469–477, 1995.

On Some Cosets of the First-Order Reed–Muller Code with High Minimum Weight

Caroline Fontaine

***Abstract*— We study a family of particular cosets of the first-order Reed–Muller code $R(1,m)$: those generated by special codewords, the *idempotents*. Thus we obtain new *maximal* weight distributions of cosets of $R(1,7)$ and 84 distinct *almost maximal* weight distributions of cosets of $R(1,9)$, that is, with minimum weight 240. This leads to crypotographic applications in the context of stream ciphers.**

***Index Terms*— Boolean function, covering radius, idempotent, Reed–Muller code, stream cipher.**

I. INTRODUCTION

The purpose of this correspondence is to study the weight distributions of cosets of the binary *first-order Reed–Muller code* generated by *idempotents*. We are particularly interested in the *maximal* weight distributions, that is, those weight distributions whose minimum weight is equal to the *covering radius* $\rho(1,m)$ of the first-order Reed–Muller code.

We will often use the correspondence between the binary *rth-order Reed–Muller code of length* 2^m, denoted by $R(r,m)$, and the Boolean functions of m variables with *degree* at most r. Thus we use both terminologies: the one of the Reed–Muller codes, and the one of the Boolean functions. This correspondence underlines the link between coding theory and cryptography, since $\rho(1,m)$ is the highest *nonlinearity* of Boolean functions, that is, the greatest distance from the affine functions; this criterion is very important, as well for block ciphers as for stream ciphers.

Manuscript received July 23, 1997; revised November 4, 1998. The material in this correspondence was presented in part at EUROCRYPT'98, Espoo, Linland, June 1–4, 1998, and at the IEEE International Symposium on Information Theory, Boston, MA, August 16–21, 1998.

The author was with INRIA, projet CODES, Domaine de Voluceau, 78153 Le Chesnay Cedex, France. She is now with LRI, Université de Paris-Sud, F-91405 Orsay Cedex, France.

Communicated by T. Kløve, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(99)03165-X.

The *weight of a coset* D of $R(1,m)$ is the minimum weight of the words of D; the coset D is said to be *maximal* if its weight is equal to $\rho(1,m)$. When m is even we know that $\rho(1,m) = 2^{m-1} - 2^{\frac{m}{2}-1}$ and the associated Boolean functions are called *bent functions* [1]; moreover, there is a unique weight distribution for the maximal cosets. But in the case when m is odd we do not know the exact value of $\rho(1,m)$ for arbitrary m; we only know that for all odd m we have

$$2^{m-1} - 2^{\frac{m-1}{2}} \leq \rho(1,m) < 2^{m-1} - 2^{\frac{m}{2}-1}.$$

More precisely we know that for $m = 3,5,7$ we have $\rho(1,m) = 2^{m-1} - 2^{\frac{m-1}{2}}$ [2], [3] and that for odd $m \geq 15$, $\rho(1,m) > 2^{m-1} - 2^{\frac{m-1}{2}}$ [4]–[6]. But for $m = 9,11,13$ we do not know if $\rho(1,m)$ matches the lower bound $2^{m-1} - 2^{\frac{m-1}{2}}$ or not.

In Section II we recall some important definitions and we introduce our notation. Section III is entirely devoted to the *idempotents*: what they are and why they are interesting. In Section IV we recall the knowledge about the maximal weight distributions of cosets of $R(1,m)$; Sections V and VI are devoted to our theoretical and numerical results: we mostly exhibit four distinct maximal weight distributions for $m = 7$, and 84 distinct weight distributions with minimum weight $2^{m-1} - 2^{\frac{m-1}{2}} = 240$ for $m = 9$. At last, we present in Section VII some cryptographic applications of these results.

The main references are [7] and [8] for the Boolean functions, [9] for the theory of finite fields, and [10] for coding theory.

II. DEFINITIONS AND NOTATION

In this correspondence, we treat binary primitive codes of length $n = 2^m - 1$ or 2^m. We denote by $\boldsymbol{F}_q$ the Galois field of order q. The binary words x^* of length n can be regarded as polynomials of $\boldsymbol{F}_2[Z]/(Z^n - 1)$, which is the classical algebra for cyclic codes

$$x^*(Z) = \sum_{i=0}^{n-1} x_i Z^i. \tag{1}$$

From now on, α will be a fixed primitive element of $\boldsymbol{F}_{2^m}$.

Definition 1: The *punctured rth-order Reed–Muller code of length n*, denoted by $R(r,m)^*$, is defined as the cyclic code which has as zeroes α^i for all i satisfying $0 < w_2(i) < m-r$ (where $w_2(i)$ denotes the number of 1's in the binary expansion of i). Then a codeword x^* of $R(r,m)^*$ is regarded as a polynomial $x^*(Z)$ such that $x^*(\alpha^i) = 0$ for all i satisfying $0 < w_2(i) < m - r$. The *rth-order Reed–Muller code of length* 2^m, denoted by $R(r,m)$, is obtained from $R(r,m)^*$ by adding an overall parity-check symbol: $R(r,m)$ is an "extended cyclic" code.

Any word $x = (x_\infty, x_0, \cdots, x_{n-1})$ of length $2^m = n + 1$ can be identified with a Boolean function of m variables, taking $f(0) = x_\infty$ and $f(\alpha^i) = x_i$ for all $i = 0, \cdots, n-1$. Let f be such a function; its *Algebraic Normal Form* (ANF) is the polynomial Q_f in $\boldsymbol{F}_2[z_1, \cdots, z_m]/(z_1^2 - z_1, \cdots, z_m^2 - z_m)$ such that $Q_f(z_1, \cdots, z_m) = f(z_1, \cdots, z_m)$ for all $(z_1, \cdots, z_m) \in \boldsymbol{F}_2^m$, and the *degree* of f is the global degree of Q_f.

In the following, the correspondence between a word and the associated Boolean function will be often used, and both terminologies equivalently employed.

Since the codewords of $R(r,m)$ are the Boolean functions of degree at most r the codewords of $R(1,m)$ are the affine functions.

For a given word x, we denote by $\mathrm{wt}\,(x)$ its Hamming weight, and define the *weight of the coset* $x \oplus R(1,m)$ as the minimum weight

for a word lying in this coset, that is, the minimal distance between the Boolean function f corresponding to x and the set of the affine functions. It measures the *nonlinearity* of f, and this criterion is very important in cryptography, for example if f is designed to combine the outputs of some linear feedback shift registers and produce a running-key in the context of a stream cipher.

We can define the *covering radius* of $R(1,m)$, denoted by $\rho(1,m)$, as the maximum weight of a coset of $R(1,m)$. Notice that $\rho(1,m)$ is the highest nonlinearity for Boolean functions of m variables.

The *weight distribution of the coset* $x \oplus R(1,m)$ is the set $\{W_i\}_{0\le i\le 2^m}$ where W_i denotes the number of words of Hamming weight i lying in this coset.

We know that $R(1,m)^*$ can be obtained from $R(1,m)$ by deleting the first coordinate. But another important remark is that we can obtain the *Simplex* code $S(m)$ of length n from $R(1,m)^*$ by removing the all-one vector from the set of the generating vectors. We recall that $S(m)$ is the dual of the Hamming code of length n. We can recover the weight distribution $\{W_i\}_{0\le i\le 2^m}$ of a coset $(0,x^*)\oplus R(1,m)$ from the weight distribution $\{w_i\}_{0\le i\le n}$ of $x^*\oplus S(m)$: we have $W_0 = W_{2^m} = w_0$, and for all $1 \le i \le 2^{m-1}$, $W_i = W_{2^m-i} = w_i + w_{2^m-i}$.

At last we introduce another representation for words of length n by means of their *Mattson–Solomon polynomial* [11].

Definition 2: Let x^* be a binary vector of length n. It's *Mattson–Solomon* (MS) *polynomial*, denoted by $\mathrm{MS}_{x^*}(Z)$, belongs to $\boldsymbol{F}_{2^m}[Z]$ and is given by

$$\mathrm{MS}_{x^*}(Z) = \sum_{j=1}^{n} A_j Z^{n-j}, \qquad \text{with } A_j = x^*(\alpha^j).$$

$\mathrm{MS}_{x^*}(Z)$ is in fact a discrete Fourier transform of x^*, and we can recover the coefficients of $x^*(Z)$ by inverting this transformation: $x_k = \mathrm{MS}_{x^*}(\alpha^k)$.

Proposition 1 [10]: If x^* and y^* are binary vectors of length n, then we have $\mathrm{MS}_{x^*\oplus y^*}(Z) = \mathrm{MS}_{x^*}(Z) + \mathrm{MS}_{y^*}(Z)$. Moreover, the coefficent A_n of $\mathrm{MS}_{x^*}(Z)$ is equal to $\mathrm{wt}\,(x^*) \bmod 2$.

III. The Idempotents

Here we are interested in some particular cosets of $R(1,m)$: those generated by *idempotents*. This study is motivated by the following points: first, the best nonlinearity obtained by picking idempotents at random is higher than the one obtained by picking regular Boolean functions; moreover, the only examples we know for cosets of $R(1,m)$ whose minimum weight is greater than $2^{m-1} - 2^{\frac{m-1}{2}}$, when m is odd, are given by N. J. Patterson and D. H. Wiedemann in [4], [5] and are generated by idempotents.

We give here the definition and some well-known properties of *idempotents* [12].

Definition 3: The codeword x^* of length n is an *idempotent* if and only if

$$x^*(Z) = \sum_{i=0}^{n-1} x_i Z^i, \qquad \text{with } x_{2i} = x_i \text{ for all } i. \tag{2}$$

Moreover, a word $x = (0, x_0, \cdots, x_{n-1})$ of length 2^m such that $(x_0, \cdots, x_{n-1})$ is an idempotent of length n is called here an *idempotent* too.

Notice that we are not interested here in the words $x = (1, x_0, \cdots, x_{n-1})$ such that $(x_0, \cdots, x_{n-1})$ is an idempotent of length n: actually, this word is in the same coset of $R(1,m)$ as $(0, 1+x_0, \cdots, 1+x_{n-1})$ (since $R(1,m)$ contains the all-one vector) which is an idempotent in our definition. So, considering both $(0,x^*)$ and $(1,y^*)$, where x^* and y^* range in the set of the idempotents of length n, would give each coset of $R(1,m)$ twice.

We present now some useful properties of the MS polynomials of idempotents. Notice that we can immediatly deduce from (2) that a codeword x^* is an idempotent if and only if $x^*(Z)$ is of the form

$$x^*(Z) = \sum_{s\in S}\sum_{i\in C_s} Z^i$$

where $C_s = \{s, 2s, \cdots, 2^{m-1}s\}$. Moreover, (2) also implies the following results.

Proposition 2: The codeword x^* is an idempotent if and only if for all i we have $x^*(\alpha^i)^2 = x^*(\alpha^i)$.

Proof: Consider x^* in $\boldsymbol{F}_2[Z]/(Z^n-1)$. It is an idempotent if and only if we have for all i in $[0\cdots n-1]$

$$x^*(\alpha^i)^2 = \left(\sum_{j=0}^{n-1} x_j \alpha^{ij}\right)^2 = \sum_{j=0}^{n-1} x_j \alpha^{2ij}$$
$$= \sum_{j=0}^{n-1} x_{2j}\alpha^{ij} = \sum_{j=0}^{n-1} x_j\,\alpha^{ij} = x^*(\alpha^i). \qquad \square$$

Proposition 3: The codeword x^* is an idempotent if and only if $\mathrm{MS}_{x^*}(Z)$ is an idempotent.

Proof: Consider x^*in $\boldsymbol{F}_2[Z]/(Z^n-1)$. By Proposition 2, x^* is an idempotent if and only if the coefficients of $\mathrm{MS}_{x^*}(Z)$ belong to $\boldsymbol{F}_2$ and are constant on each 2-cyclotomic coset modulo n—that is, $x^*(\alpha^j) = x^*(\alpha^i)$ for all j in C_i. In other words, x^* is an idempotent if and only if its Mattson–Solomon polynomial is an idempotent. $\square$

We can use this result to represent an idempotent by a *short MS polynomial*, keeping only the index of one nonzero term of the MS polynomial for each class of nonzero coefficients.

Example 1: Take $m = 3$, and consider the idempotent x^* whose support is $\{\alpha^0, \alpha, \alpha^2, \alpha^4\}$, where α is a root of $X^3 + X + 1$: its MS polynomial is $Z^3 + Z^5 + Z^6$. The nonzero coefficients are $x^*(\alpha^4), x^*(\alpha^2)$, and $x^*(\alpha)$. But 1, 2, 4 are all in the cyclotomic coset containing 1; so the short MS polynomial of x^* has only one nonzero coefficient—$x^*(\alpha)$—and is equal to Z^6.

Another important point concerning idempotents is that every cyclic code contains an idempotent which generates it entirely: its *primitive idempotent*. The Simplex code $S(m)$ contains only one primitive idempotent: its MS polynomial is $T_m(Z) = Z + Z^2 + \cdots + Z^{2^{m-1}}$.

IV. The Weight Distributions: What Is Known

Before presenting our results let us recall what is known about the weight distributions of the cosets of $R(1,m)$.

From now on, a coset D of $R(1,m)$ will be called *maximal* if $\rho(1,m)$ is known and $\mathrm{wt}\,(D) = \rho(1,m)$, and *almost maximal* if $\rho(1,m)$ is unknown and $\mathrm{wt}\,(D) \ge 2^{m-1} - 2^{\frac{m-1}{2}}$.

For any m, the weight distributions of the cosets $x \oplus R(1,m)$ with $x \in R(2,m)\backslash R(1,m)$ are known. Those with the highest minimum weight are

- for even m:

weight	$2^{m-1} \pm 2^{\frac{m}{2}-1}$
number of words	2^m

- for odd m:

weight	$2^{m-1} \pm 2^{\frac{m-1}{2}}$	2^{m-1}
number of words	2^{m-1}	2^m

These weight distributions are called the *maximal quadratic weight distributions*.

Proposition 4: The Boolean functions generating cosets with the maximal quadratic weight distribution are of degree at most $\frac{m}{2}$ for even $m \geq 4$, and $\frac{m+1}{2}$ for odd m.

Proof: The proof for even m can be found in [1], [10]. For odd m, the functions f which generate cosets with the maximal quadratic weight distribution satisfy

$$\sum_{u \in \boldsymbol{F}_2^m} (-1)^{f(u)+a.u} \in \left\{0, 2^{\frac{m+1}{2}}, -2^{\frac{m+1}{2}}\right\}$$

for all $a \in \boldsymbol{F}_2^m$ [10, p. 415], and the final result is obtained by applying [13, Lemma 3]. □

For even m, all maximal cosets have the maximal quadratic weight distribution. The Boolean functions generating them are called *bent functions* and their degree is at most $\frac{m}{2}$ (see the preceding proposition).

For odd m, we must distinguish two cases.

- For $m = 3, 5, 7$ we know that $\rho(1, m) = 2^{m-1} - 2^{\frac{m-1}{2}}$ [2], [3], and all the weight distributions of the maximal cosets are known for $m = 3, 5$; E. R. Berlekamp and L. R. Welch have shown in [2] that for $m = 5$ there are two maximal weight distributions: the quadratic one and another one. We will show that for $m = 7$ there are also several maximal weight distributions.
- For $m \geq 9$ we do not know the exact value of $\rho(1, m)$. It is conjectured that the almost maximal cosets $D = x \oplus R(1, m)$ with $x \in R(3, m) \backslash R(2, m)$ have the maximal quadratic weight distribution. X.-D. Hou has proved in [14] that for $m = 9, 11, 13$ the weight of D cannot exceed $2^{m-1} - 2^{\frac{m-1}{2}}$ (see also the result of P. Langevin in [15] for $m = 9$). He has also shown in [16] that for $m = 9$ the weight of a coset $x \oplus R(1, m)$ with $x \in R(4, m) \backslash R(3, m)$ can not exceed $2^{m-1} - 2^{\frac{m-1}{2}}$.

Even if we know some theoretical results, it is still an important problem to exhibit some generators of maximal cosets. We will give in the next two sections our results, showing that idempotents enable us to obtain quite easily (almost) maximal cosets and new (almost) maximal weight distributions.

V. The Weight Distributions: New Theoretical Results

We present here two kinds of theoretical results: first we analyze the weight distributions of some particular cosets of $R(1, m)$; the second and third paragraphs deal with some constructions of new good cosets, that is, with a high minimum weight, from other ones.

A. Cosets $x \oplus R(1, m)$, Where $x = (0, x^*)$ and $MS_{x^*} = T_m(\lambda Z^{n-t})$

We describe here a general result on cosets whose generators have an MS polynomial of the form $T_m(\lambda Z^{n-t})$, where λ lies in $\boldsymbol{F}_{2^m}$ and T_m denotes the trace function over $\boldsymbol{F}_{2^m}$. Our proof is based on a result of T. Kasami [17].

Theorem 1: Let m be odd and $x^* \notin S(m)$ be such that its MS polynomial is equal to $T_m(\lambda Z^{n-t})$, with λ in $\boldsymbol{F}_{2^m}$, and t prime to n, $t \not\equiv -1 \bmod n$. If x is the word of length 2^m such that $x = (0, x^*)$, then $\mathrm{wt}\,(x \oplus R(1, m)) \leq 2^{m-1} - 2^{\frac{m-1}{2}}$, and if the equality holds, then the weight distribution of $x \oplus R(1, m)$ is the following one:

weight	$2^{m-1} \pm 2^{\frac{m-1}{2}}$	2^{m-1}
number of words	2^{m-1}	2^m

Proof: We denote by $\mathcal{C}$ the cyclic code of length n and nonzeroes α^{n-1} and α^t (and their conjugates). Since t is prime to n, $t \not\equiv -1 \bmod n$, $\mathcal{C}$ has dimension $2m$. The codewords of $\mathcal{C}$ have an MS polynomial of the form $T_m(\mu Z^{n-t}) + T_m(\nu Z)$, with μ and ν in $\boldsymbol{F}_{2^m}$. The set of words of the MS polynomial $T_m(\nu Z)$, with ν ranging in $\boldsymbol{F}_{2^m}$, is the Simplex code $S(m)$. Then $\mathcal{C}$ contains $S(m)$ and $x^* \oplus S(m)$; thus $\mathcal{C}^\perp$ is contained in $S(m)^\perp = H(m)$, the $[n, n-m, 3]$ Hamming code, and then has no word of weight 1 nor 2. So we can apply Theorem 13 of T. Kasami [17] (see a proof in [18, Theorem 3.30]): let a_w denote the number of codewords of $\mathcal{C}$ with Hamming weight w, and w_0 the smallest integer $0 < w < 2^{m-1}$ such that $a_w + a_{2^m-w} \neq 0$; then we have $w_0 \leq 2^{m-1} - 2^{\frac{m-1}{2}}$, and if the equality holds, the weight distribution of $\mathcal{C}$ is the same as the one of the dual code of a double-error-correcting Bose–Chaudhuri–Hocquenghem (BCH) code, i.e., the only nonzero values of a_w are

w	a_w
0	1
$2^{m-1} - 2^{\frac{m-1}{2}}$	$(2^m - 1)\left(2^{m-2} + 2^{\frac{m-3}{2}}\right)$
2^{m-1}	$(2^m - 1)(2^{m-1} + 1)$
$2^{m-1} + 2^{\frac{m-1}{2}}$	$(2^m - 1)\left(2^{m-2} - 2^{\frac{m-3}{2}}\right)$

Now, if we remove from $\mathcal{C}$ all the words of $S(m)$, we obtain the set of words whose MS polynomials are of the form $T_m(\mu Z^{n-t}) + T_m(\nu Z)$, with $\mu \neq 0$. Since t is prime to n, $t \not\equiv -1 \bmod n$, this set is in fact $\{\mathit{shift}(x^*) \oplus S(m)\}$ where $\mathit{shift}(x^*)$ denotes all the possible vectors obtained by shifting the vector x^*; it is a union of cosets of $S(m)$ which have all the same weight distribution. The one of $x \oplus R(1, m)$ is obtained from it by adding for each i the number of words of weight i and the number of words of weight $2^m - i$. □

B. Constructing New Good Orphan Cosets from Other Ones

The notion of "orphan cosets" has been introduced by T. Helleseth and H. F. Mattson Jr. in [19] with the "urcosets" terminology, and then studied by R. A. Brualdi and V. S. Pless in [20], [6] with the "orphan cosets" terminology. We call a minimum-weight word in some coset a *leader* of that coset. Let $\mathcal{C}'$ and $\mathcal{C}''$ be two cosets of a binary linear code. We use the notation $\mathcal{C}' \preceq \mathcal{C}''$ if and only if there exists leaders x' of $\mathcal{C}'$ and x'' of $\mathcal{C}''$ such that x'' covers x' (i.e., $x'_i = 1$ implies $x''_i = 1$). $\mathcal{C}'$ is a *child* of $\mathcal{C}''$ if and only if $\mathcal{C}' \prec \mathcal{C}''$ and there does not exist $\mathcal{D}$ such that $\mathcal{C}' \prec \mathcal{D} \prec \mathcal{C}''$; then we also say that $\mathcal{C}''$ is a *parent* of $\mathcal{C}'$. The coset $\mathcal{C}'$ is called an *orphan* if and only if it has no parent. We can remark that $\mathcal{C}' \preceq \mathcal{C}''$ implies that $\mathrm{wt}\,(\mathcal{C}') \leq \mathrm{wt}\,(\mathcal{C}'')$. Another important property is that all maximal cosets are orphans, but in general the converse is not true. In [6], the authors give a construction of orphan cosets of $R(1, m)$, and they show the following fact: if for a given odd m there exist an orphan coset of weight greater than $2^{m-1} - 2^{\frac{m-1}{2}}$, then for any odd $m' > m$ there exists an orphan coset of $R(1, m')$ of weight greater than $2^{m'-1} - 2^{\frac{m'-1}{2}}$; in their proof they construct the second coset from the first one, and from this construction we can deduce the following.

Theorem 2: Let m be an integer, and $\mathcal{C}_1 = f \oplus R(1, m)$ be an orphan coset with weight distribution $\{W_i\}_{0 \leq i \leq 2^m}$. Thus for any integer m' which is of the form $m' = m + 2u$, with $u > 0$, the coset $\mathcal{C}'_1 = g \oplus R(1, m')$, where the ANF of g is obtained from the one of f by

$$g(z_1, \cdots, z_{m'}) = f(z_1, \cdots z_m) + z_{m+1}z_{m+2} + \cdots + z_{m'-1}z_{m'}$$

is orphan, and its weight distribution $\{W'_j\}_{0 \leq j \leq 2^{m'}}$ satisfy

$$W'_{2^{m'-1} \pm (2^{m'-u-1} - 2^{u}i)} = 2^{2u} \times W_i, \qquad \text{for all } 0 \leq i \leq 2^{m-1}$$

which is equivalent to

$$W'_{2^{m'-1} \pm (2^{u}i)} = 2^{2u} \times W_{2^{m-1}-i}, \qquad \text{for all } 0 \leq i \leq 2^{m-1}$$

the other W'_j's being all zero.

This result enables us to deduce some weight distributions of cosets of $R(1,m')$ from the ones of cosets of $R(1,m)$, and to construct these cosets.

Example 2: According to the results presented by E. R. Berlekamp and L. R. Welch in [2], and to the preceding theorem, we can construct, for any odd $m \geq 5,208\,320$ orphan cosets of $R(1,m)$, with minimum weight $2^{m-1}-2^{\frac{m-1}{2}}$, and with the following weight distribution:

weight	$2^{m-1}\pm 2^{\frac{m-1}{2}}$	$2^{m-1}\pm 2^{\frac{m-3}{2}}$	2^{m-1}
number of words	$2^{m-5}\times 12$	$2^{m-5}\times 16$	$2^{m-5}\times 8$

C. Constructing New Good Idempotents from Other Ones

Now let us look at the action of the Linear Group on our idempotents and on the cosets of $R(1,m)$ generated by them. We will call 2-*permutation polynomial* a polynomial

$$P(X)=\sum_{i=0}^{m-1} p_i X^{2^i} \in \boldsymbol{F}_2[X]$$

such that the mapping $c \mapsto P(c)$ is a permutation on $\boldsymbol{F}_{2^m}$ (since it is a linear mapping, this means that its kernel is $\{0\}$).

Let us denote by $\mathcal{P}$ the set of such polynomials. Let $\beta \in \boldsymbol{F}_{2^m}$. By *class*$(\beta)$ we will denote the set $\{\beta,\beta^2,\cdots,\beta^{2^{m-1}}\}$, that is, the conjugacy class of β.

Lemma 1: Let P be in $\mathcal{P}$ and let $(\gamma,\gamma^2,\cdots,\gamma^{2^{m-1}})$ be a normal basis of $\boldsymbol{F}_{2^m}$. Then its image by P is also a normal basis of $\boldsymbol{F}_{2^m}$.

Proof: First we will show that the image of $(\gamma,\gamma^2,\cdots,\gamma^{2^{m-1}})$ by P is of the form $(\delta,\delta^2,\cdots,\delta^{2^{m-1}})$ with $\delta=P(\gamma)$: for all $j=0,\cdots,m-1$ we have

$$P(\gamma^{2^j})=\sum_{i=0}^{m-1} p_i(\gamma^{2^j})^{2^i}=\sum_{i=0}^{m-1} p_i(\gamma^{2^i})^{2^j}$$
$$=\left(\sum_{i=0}^{m-1} p_i\gamma^{2^i}\right)^{2^j}=P(\gamma)^{2^j}$$

and thus

$$\{P(y), y\in \textit{class}\,(\gamma)\}=\{P(\gamma^{2^j}), j=0,\cdots,m-1\}$$
$$=\{P(\gamma)^{2^j}, j=0,\cdots,m-1\}$$
$$=\textit{class}\,(P(\gamma)).$$

Now, since P is an $\boldsymbol{F}_2$-linear permutation polynomial, the image of a basis is also a basis. This concludes the proof. □

In the following we will denote by $\log(\beta)$, where β is an element of $\boldsymbol{F}_{2^m}$, the unique integer of $[0\cdots 2^m-2]$ such that $\alpha^{\log(\beta)}=\beta$.

Proposition 5: Let x be an idempotent. Let $\mathcal{P}_P$ be the function

$$\mathcal{P}_P:\sum_{i=0}^{n-1} x_i Z^i \mapsto \sum_{i=0}^{n-1} x_i Z^{\log(P(\alpha^i))}.$$

If P belongs to $\mathcal{P}$, then $\mathcal{P}_P(x)$ is an idempotent too, and the Boolean functions associated with these idempotents have the same degree. Moreover, the cosets $\mathcal{P}_P(x)\oplus R(1,m)$ and $x\oplus R(1,m)$ have the same weight distributions.

Proof: Since x is an idempotent, it can be written as $\sum_{s\in S}\sum_{i\in C_s} Z^i$ for some set S of representatives of some 2-cyclotomic cosets modulo n. So $\mathcal{P}_P(x)$ is equal to

$$\sum_{s\in S}\sum_{i\in C_s} Z^{\log(P(\alpha^i))}=\sum_{s\in S}\sum_{i\in C_{\log(P(\alpha^s))}} Z^i$$
$$=\sum_{s\in\{\log(P(\alpha^t)),t\in S\}}\sum_{i\in C_s} Z^i$$

and $\mathcal{P}_P(X)$ is an idempotent.

We know that the automorphism group of $R(1,m)$ is the general affine group [10, p. 399], thus since P is a linear permutation, $x\oplus R(1,m)$ and $\mathcal{P}_P(x)\oplus R(1,m)$ have the same weight distribution. The remark concerning the degree of the Boolean functions also comes from the linearity of P. □

The set of the 2-permutation polynomials is then a subset of the automorphism group of the idempotents. But actually we do not know if it is the whole group. This defines a kind of equivalence between idempotents and enables us to construct, from one coset, a lot of cosets with the same weight distribution.

Example 3: When $m=15$ we can construct from each of the two cosets given by N. J. Patterson and D. H. Wiedemann in [4] and [5] 675 other cosets with the same weight distribution.

VI. The Weight Distributions: Numerical Results

After some explanations on our algorithm, we present new numerical results, distinguishing between the cases when $\rho(1,m)$ is known and the cases when it is not already known.

A. Algorithm

We present here our algorithm, which generates idempotents whose MS polynomials have all the same number of terms. This enables us to compute all the idempotents for small values of m, and to study a complete subclass of idempotents for large values of m. This approach is motivated by the fact that the short MS polynomials of the idempotents given by N. J. Paterson and D. H. Wiedemann are sparse, since they have, respectively, three and five terms.

Algorithm 1 (Inputs: m,T,b): Generate all the short MS polynomials $\mathrm{MS}_{x^*}(Z)^*$ with T nonzero coefficients, and such that $A_{2^{m-1}-1}=0$ (to obtain each coset only once). For each of them

1) compute the weight distribution of $(0,x^*)\oplus R(1,m)$. If there is a word of weight less than b, then go directly to the next short MS polynomial;
2) display $\mathrm{MS}_{x^*}(Z)^*$ and the weight distribution of $(0,x^*)\oplus R(1,m)$.

Remark 1: We know that the idempotents x^* and $x^*\oplus s^*$ (where s^* denotes the idempotent which generates the Simplex code $S(m)$) are in the same coset. Since the short MS polynomial of s^* has only one nonzero coefficient—$s^*(\alpha^{2^{m-1}-1})$—we will look only at idempotents such that $x^*(\alpha^{2^{m-1}-1})=0$. Then we are sure not to obtain the same coset twice.

Remark 2: In our computations we looked only at the proper cosets of $R(1,m)$, that is, those which are distinct from $R(1,m)$. This means that if there are j 2-cyclotomic cosets, there are $2^{j-1}-1$ proper cosets of $R(1,m)$ generated by the 2^j-2 idempotents.

Remark 3: When m is odd and the short MS polynomial of the idempotent x^* is Z^{n-t} with t prime to n, $t\not\equiv -1 \bmod n$: the weight of the coset $x\oplus R(1,m)$ (where $x=(0,x^*)$) is at most $2^{m-1}-2^{\frac{m-1}{2}}$, and if the equality holds, its weight distribution is the maximal quadratic one (see Theorem 1). This enables us to find

TABLE I
$m = 7$: MAXIMAL WEIGHT DISTRIBUTIONS

weights	56	57	58	59	60	61	62	63	64	number	
of the words	72	71	70	69	68	67	66	65		of cosets	
	35		36		28		28		2	126	(I)
weight	50				56				44	1176	(II)
distributions	56		8				56		16	28	(III)
of the cosets	64								128	1617	(IV)

very easily some idempotents, generating cosets with the maximal quadratic weight distribution.

Remark 4: When m is odd, the major part of the almost maximal nonquadratic weight distributions corresponds to idempotents of degree at least $\frac{m+1}{2} + 1$ (see Proposition 4). So the short MS polynomial of such idempotents must have at least one nonzero coefficient $x^*(\alpha^i)$ with $w_2(i) \geq \frac{m-3}{2}$. It is now easy to think that when the number of classes of nonzero coefficients we choose increases, thus the chance of obtaining an idempotent of high degree increases also, and then the chance of getting an almost maximal weight distribution which is not the maximal quadratic one.

B. When $\rho(1, m)$ Is Known

$m = 5$: E. R. Berlekamp and L. R. Welch give in their paper [2] all the weight distributions of the cosets of $R(1,5)$, and they show that there are two maximal weight distributions.

In computing the weight distributions of the $2^6 - 1$ proper cosets of $R(1,5)$ generated by idempotents, we found the quadratic maximal one for nine of the cosets, but never the other maximal distribution.

Here are some examples of short MS polynomials of idempotents which generate maximal cosets: $Z^{24} + Z^{20} + Z^{16}$ (degree 2), $Z^{26} + Z^{24} + Z^{16}$ (degree 3).

$m = 6$: We computed all weight distributions of the $2^{12} - 1$ proper cosets of $R(1,6)$ generated by idempotents. We found 12 maximal cosets corresponding to the bent functions, classified by O. S. Rothaus in [1].

Here are some examples of the short MS polynomials of idempotents generating them: $Z^{48} + Z^{40} + Z^{36} + Z^{32}$ (degree 2), $Z^{56} + Z^{42} + Z^{36}$ (degree 3).

$m = 7$: We computed all the $2^{18} - 1$ proper cosets generated by idempotents. 2947 of them are maximal, and we observed four different maximal weight distributions, which are listed in Table I. The links between these weight distributions according and T are presented in Table II. Since all these cosets are orphan ones (because they are maximal cosets), we can deduce from Theorem 2 cosets of $R(1,m)$ with "these" weight distributions for all odd $m > 7$.

Here we give some examples of the short MS polynomials of idempotents giving these weight distributions:

- for the first one: $Z^{126} + Z^{120} + Z^{118} + Z^{114} + Z^{104} + Z^{100} + Z^{96} + Z^{80} + Z^{64}$ (degree 6);
- for the second one: $Z^{124} + Z^{114} + Z^{108} + Z^{104} + Z^{100} + Z^{98} + Z^{84} + Z^{80} + Z^{72}$ (degree 5);
- for the third one: $Z^{126} + Z^{124} + Z^{122} + Z^{118} + Z^{116} + Z^{112} + Z^{104} + Z^{98} + Z^{96}$ (degree 6);
- for the quadratic one: Z^{96} (degree 2), $Z^{112} + Z^{104} + Z^{100} + Z^{96} + Z^{84}$ (degree 3), $Z^{120} + Z^{114} + Z^{108} + Z^{106} + Z^{96} + Z^{80} + Z^{64}$ (degree 4).

$m = 8$: We computed all weight distributions of the $2^{34} - 1$ proper cosets of $R(1,8)$ generated by idempotents. We found 3776 maximal cosets corresponding to the bent functions.

TABLE II
$m = 7$: LINKS BETWEEN THE MAXIMAL WEIGHT DISTRIBUTIONS AND T

	number of cosets			
T	(I)	(II)	(III)	(IV)
1				10
2		2		29
3	2	9		92
4		32		176
5	2	53		247
6	9	130		271
7	17	191	2	295
8	23	250	7	269
9	30	229	9	163
10	22	154	8	51
11	10	72	2	10
12	5	42		4
13	6	4		
14		8		
15				
16				
17				

Here we give some examples of the short MS polynomials of idempotents generating them: $Z^{192} + Z^{136}$ (degree 2), $Z^{224} + Z^{208} + Z^{194} + Z^{192} + Z^{164} + Z^{136}$ (degree 3), Z^{240} (degree 4).

C. When $\rho(1, m)$ Is Unknown

Fixing T to small values enabled us to obtain very easily cosets of $R(1,m)$ with the maximal quadratic weight distribution, for $m = 9, 11, 13, 15$. Moreover, for $m = 9$ we have found new almost maximal weight distributions, that is nonquadratic ones, but their minimum weight is still 240, that is the lower bound on $\rho(1,9)$.

We summarize our results in Table III, giving new almost maximal weight distributions, sorted according to the number of words of weight $2^{m-1} - 2^{\frac{m-1}{2}}$; for each of them we give the number of cosets we found and for some of them, as an index, the degree of the functions lying in these cosets.

When we look at this table, we can see that there are 83 almost maximal nonquadratic weight distributions. And each time we increase the number of classes of nonzero coefficients, we obtain new ones (see Remark 4). Some of these weight distributions are just obtained a few times, but it is possible by applying the 2-permutation polynomials on their idempotent generators to construct a lot of other cosets with the same weight distributions.

Another remark is that we obtained some idempotents of degree $\frac{m+1}{2} = 5$ which give an almost maximal nonquadratic weight distribution. So we can say that even if the elements giving the maximal quadratic weight distribution are necessarily of degree at most $\frac{m+1}{2}$, the converse does not hold. But our numerical results make us think that the maximal elements of degree at most $\frac{m-1}{2}$ always give the quadratic weight distribution.

Concerning the notion of "orphan cosets," all the almost maximal cosets we checked are orphans, and we can construct from Theorem 2 cosets of $R(1,m)$ with "these" weight distributions for all odd $m > 9$.

VII. CRYPTOGRAPHIC APPLICATIONS

Let us consider a stream cipher. The running-key, which will be added to the plaintext is given by a pseudorandom generator, generally based on Linear Feedback Shift Registers (LFSR's) which are combined, or filtered by a Boolean function f. In order to

TABLE III
$m = 9$: LINKS BETWEEN THE ALMOST MAXIMAL WEIGHT DISTRIBUTIONS AND T

Weight Distributions									number of nonzero coefficients							
240	242	244	246	248	250	252	254	256	4	5	6	7	8	9	10	11
272	270	268	266	264	262	260	258		number of cosets $_{degree}$							
108		208		112		48		72								1
109		201		126		39		74								1
111		190		136		66		18								1
117		190		112		66		54								3
117		192		108		64		62							1_6	
117		201		90		55		98								1
117		210		72		46		134								1
120		181		118		75		36								1
120		190		100		66		72								2
121		198		72		90		62							1_7	1
126		172		112		84		36							1_6	7
126		174		108		82		44								3
126		181		94		75		72								4
126		183		90		73		80							1_7	2
126		190		76		66		108							1_7	
127		165		126		75		38							1_7	1
127		174		108		66		74								1
129		163		118		93		18								1
129		172		100		84		54							4_6	4
129		181		82		75		90							2_7	2
135		154		112		102		18								2
135		156		108		100		26						$1_6, 1_7$	1_6	4
135		163		94		93		54								2

TABLE III *(Continued)*

Weight Distributions									number of nonzero coefficients							
240	242	244	246	248	250	252	254	256	4	5	6	7	8	9	10	11
272	270	268	266	264	262	260	258		number of cosets $_{degree}$							
135		165		90		91		62							2_7	5
135		172		76		84		90							1_6	5
135		174		72		82		98						2_7		3
136		147		126		93		20								1
136		156		108		84		56							1_7	3
136		165		90		75		92								4
136		171		66		117		44								1
138		154		100		102		36								5
138		163		82		93		72							2_7	6
138		172		64		84		108								1
139		180		36		108		98							1_7	
144		136		112		120								1_6		3
144		145		94		111		36						1_7		3
144		147		90		109		44								8
144		154		76		102		72						1_7	5_7	9
144		156		72		100		80						1_7	1_6	12
144		163		58		93		108							1_7	
145		129		126		111		2								1
145		138		108		102		38							3_7	3
145		147		90		93		74								4
145		156		72		84		110							2_7	8
147		136		100		120		18						1_7	2_6	7
147		145		82		111		54						1_7	3_7	12
147		154		64		102		90						1_7	2_7	5
153		127		94		129		18								1
153		129		90		127		26								1

TABLE III *(Continued)*

Weight Distributions									number of nonzero coefficients							
240	242	244	246	248	250	252	254	256	4	5	6	7	8	9	10	11
272	270	268	266	264	262	260	258		number of cosets $_{degree}$							
153		136		76		120		54							$1_6, 2_7$	12
153		138		72		118		62								2
153		145		58		111		90								2
153		147		54		109		98							1_7	2
154		120		108		120		20						1_7		
154		129		90		111		56							2_7	
154		138		72		102		92						1_7	1_7	9
156		118		100		138									1_7	
156		127		82		129		36								7
156		136		64		120		72						2_7		6
162		118		76		138		36								1
162		120		72		136		44						1_6	1_7	2
162		129		54		127		80								2
162		136		40		120		108						1_7	2_7	
162		156				100		188								3
163		111		90		129		38								3
163		120		72		120		74							2_7	5
165		118		64		138		54						2_7		1
171		102		72		154		26								1
171		118		40		138		90					1_7	2_7		2
172		102		72		138		56								1
174		100		64		156		36								1
180		120				136		152						1_6	2_6	11
181				300				62					2_6	3	14	59
184				288				80			1_6	1_6	$6_5, 5_6$	26	72	280
190				264				116				3_6	7_6	87	409	1835

TABLE III *(Continued)*

Weight Distributions									number of nonzero coefficients							
240	242	244	246	248	250	252	254	256	4	5	6	7	8	9	10	11
272	270	268	266	264	262	260	258		number of cosets $_{degree}$							
193				252				134			4_6	16_6	73_6	373	1520	5542
199				228				170		1_6	11_6	47_6	256_6	1212	4864	17811
202				216				188	1_6	6_6	11_6	77_6	429_6	1811	7104	23864
208				192				224				13_6	108_6	628	3331	14321
211				180				242			6_6	26_6	126_6	630	2784	10778
217				156				278			2_6	12_6	97_6	468	2218	8555
220				144				296					8_6	36	200	1097
226				120				332					4_6	36	219	1228

resist cryptanalysis, f must satisfy some criteria; first, it must be *balanced*—this means that its weight must be 2^{m-1} (where m is the number of variables); moreover, if f is combining the outputs of the LFSR's, it must also have a high degree (in order to resist Berlekamp–Massey's attack [21], [22]), have a high *order of correlation immunity* (in order to resist Siegenthaler's attack [23]), and be highly nonlinear (in order to resist fast correlation attacks [24], [25]).

Let us recall that a Boolean function f of m variables is *tth order correlation-immune* if, for any subset $T \subset \{1, 2, \cdots, m\}$ of size t, the probability distribution of its output is unaltered when the x_i are fixed, for $i \in T$. Moreover a balanced tth-order correlation-immune function is said to be *t-resilient.*

In general, the balanced functions we obtained with the best known nonlinearity are not correlation-immune, and it is actually very difficult to find a balanced function which has a high order of correlation immunity and a high nonlinearity.

In 1991, P. Camion, C. Carlet, P. Charpin, and N. Sendrier have presented in [26] a construction of t-resilient functions: let f be a t-resilient function of m variables, and g be the function of $m+1$ variables defined by (the ANF's are expressed in the canonical basis)

$$g(z_1, \cdots, z_m, z_{m+1}) = f(z_1, \cdots, z_m) + z_{m+1}.$$

Then g is $(t+1)$-resilient.

We will apply it to our balanced highly nonlinear functions in order to construct balanced highly nonlinear functions with a good order of correlation immunity.

Theorem 3: The degree and nonlinearity of g can be deduced from the ones of f by

$$\deg(g) = \deg(f)$$
$$\mathrm{wt}(g + R(1, m+1)) = 2\mathrm{wt}(f + R(1, m)).$$

Then if we use a 0-correlation-immune balanced function of m variables with nonlinearity nl, we obtain by iterating t times this construction a t-resilient function of $m+t$ variables with nonlinearity $2^t nl$.

For $m = 7$ we obtained 700 balanced functions of degree 6, and 51 744 balanced functions of degree 5, all with the best nonlinearity, that is 56. So by applying the construction twice, we obtain 700 (resp., 51 744) 2-resilient functions of nine variables with degree 6 (resp., 5) and nonlinearity $2^2 * 56 = 224$. Notice that those of degree 6 satisfy the best posssible tradeoff between the resilience order and the degree, according to the inequality given by Siegenthaler in [23]: if $t \neq m-1$, then $\deg(f) + t \leq m-1$.

Here we obtained balanced Boolean functions with the best known nonlinearity for $m = 5, 6, 7, 8, 9, 11, 13, 15$, and this construction can be applied to get balanced functions with a high nonlinearity and a sufficient order of correlation immunity to resist Siegenthaler's attack [27].

VIII. Conclusion

We have presented a new approach to the study of the weight distributions of cosets of the first-order Reed–Muller code $R(1, m)$, looking at the cosets generated by idempotents. We thus obtained new maximal-weight distributions of cosets of $R(1, 7)$, and new almost maximal-weight distributions of cosets of $R(1, 9)$, that is, with minimal weight $2^{m-1} - 2^{\frac{m-1}{2}} = 240$. The diversity of these weight distributions incline us to conclude that cosets generated by idempotents give a good overview of the general corpus of cosets; and so it could be conjectured that the covering radius of $R(1, 9)$ is 240. Moreover, these results lead to cryptographic applications, in the context of stream ciphers.

Acknowledgment

We are very grateful to P. Charpin and C. Carlet for their motivating discussions and N. Sendrier for valuable improvements concerning the implementation. We wish to thank H. F. Mattson and E. F. Assmus for their enriching discussions and valuable suggestions.

References

[1] O. S. Rothaus, "On bent functions," *J. Comb. Theory*, no. 20, pp. 300–305, 1976.

[2] E. R. Berlekamp and L. R. Welch, "Weight distributions of the cosets of the $(32, 6)$ Reed–Muller code," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 203–207, Jan. 1972.

[3] J. Mykkeltveit, "The covering radius of the $[128, 8]$ Reed–Muller code is 56," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 358–362, May 1980.

[4] N. J. Patterson and D. H. Wiedemann, "The covering radius of the $[2^{15}, 16]$ Reed–Muller code is at least 16276," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 354–356, May 1983.

[5] ——, "Correction to [4]," *IEEE Trans. Inform. Theory*, vol. 36, p. 443, Mar. 1990.

[6] R. A. Brualdi, N. Cai, and V. S. Pless, "Orphan structure of the first-order Reed-Muller codes," *Discr. Math.*, no. 102, pp. 239–247, 1992.

[7] C. Carlet, "Codes de reed et muller, codes de kerdock et de preparata," Ph.D. dissertation, Université Paris VI, Paris, France, 1990.

[8] ——, "Fonctions booléennes en théorie des codes correcteurs d'erreurs et en cryptologie," Habilitation à diriger les recherches, Université de Picardie, 1994.

[9] R. Lidl and H. Niederreiter, "Finite Fields," no. 20 in *Encyclopedia of Mathematics and Its Applications*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[11] H. F. Mattson and G. Solomon, "A new treatment of Bose-Chaudhuri codes," *J. Soc. Industr. Appl. Math.*, vol. 9, pp. 654–669, Dec. 1961.

[12] V. S. Pless, "An introduction to algebraic codes," in *Handbook of Coding Theory*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, to be published.

[13] C. Carlet, "Two new classes of bent functions," in *Advances in Cryptology—EUROCRYPT'93, Lecture Notes in Computer Science*, vol. 765, T. Helleseth, Ed. Berlin, Germany: Springer-Verlag, 1994, pp. 77–101.

[14] X.-D. Hou, "On the covering radius of $R(1, m)$ in $R(3, m)$," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1035–1037, 1996.

[15] P. Langevin, "Covering radius of $\mathrm{RM}(1, 9)$ in $\mathrm{RM}(3, 9)$," *EUROCODE'90*, *Lecture Notes in Computer Science*, vol. 514, G. Cohen and P. Charpin, Eds. Berlin, Germany: Springer-Verlag, 1991, pp. 51–59.

[16] X.-D. Hou, "The covering radius of $R(1, 9)$ in $R(4, 9)$," *Des., Codes Cryptogr.*, vol. 8, pp. 285–292, 1996.

[17] T. Kasami, "Weight distributions of Bose-Chaudhuri-Hocquenghem codes," in *Combinatorial Mathematics and Applications*, R. C. Bose and T. A. Dowlings, Eds. Chapel Hill, NC: Univ. North Carolina Press, 1969, ch. 20.

[18] P. Charpin, "Open problems on cyclic codes," in *Handbook of Coding Theory*, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, to be published.

[19] T. Helleseth and H. F. Mattson Jr., "On the cosets of the simplex code," *Discr. Math.*, no. 56, pp. 169–189, 1985.

[20] R. A. Brualdi and V. S. Pless, "Orphans of the first order Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 399–401, Mar. 1990.

[21] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[22] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122–127, 1969.

[23] T. Siegenthaler, "Correlation-immunity of nonlinear combining fonctions for cryptographic applications," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 776–780, Sept. 1984.

[24] W. Meier and O. Staffelbach, "Fast correlation attacks on stream ciphers," in *Advances in Cryptology—EUROCRYPT'88, Lecture Notes in Computer Science*, vol. 330, C. G. Günther, Ed. Berlin, Germany: Springer-Verlag, 1988, pp. 301–314.

[25] V. Chepyzhov and B. Smeets, "On a fast correlation attack on certain stream ciphers," in *Advances in Cryptology—EUROCRYPT'91, Lecture Notes in Computer Science*,vol. 547, D. W. Davis, Ed. Berlin, Germany: Springer-Verlag, 1991, pp. 176–185.

[26] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in *Advances in Cryptology—CRYPTO'91, Lecture Notes in Computer Science*, vol. 576, J. Feigenbaum, Ed. Berlin, Germany: Springer-Verlag, 1992, pp. 86–100.

[27] E. Filiol and C. Fontaine, "Highly nonlinear balanced Boolean functions with a good correlation-immunity," in *Advances in Cryptology—EUROCRYPT'98, Lecture Notes in Computer Science*, vol. 1403, K. Nyberg, Ed. Berlin, Germany: Springer-Verlag, 1998, pp. 475–488.