www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 4 No. 4 (2015), pp. 61-74.

www.ui.ac.ir

ON GROUP RINGS AND SOME OF THEIR APPLICATIONS TO COMBINATORICS AND CRYPTOGRAPHY

CLAUDE CARLET* AND YIN TAN

Communicated by Victor Bovdi

Abstract. We give a survey of recent applications of group rings to combinatorics and to cryptography, including their use in the differential cryptanalysis of block ciphers.

1. Introduction

Let R be an arbitrary ring and G be an arbitrary (multiplicative) group, the *group ring* $R[G]$ is defined as the set

$$R[G] = \left\{ \sum_{g\in G} a_g g,\ a_g \in R,\ g \in G \right\},$$

endowed with the addition $+$ and the multiplication $\cdot$, defined as follows:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g, \text{ and}$$

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} \left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g.$$

$R[G]$ is a free module with ring of scalars R and with basis G. Group rings allow generalizing both rings and groups since $R[G]$ contains a subring isomorphic to R, and the group of units in $R[G]$ contains a subgroup isomorphic to G. Furthermore, if R is commutative and has an identity, the group ring $R[G]$ is actually an algebra over R and we usually call it a *group algebra*. In this paper, we

MSC(2010): 05E30, 20C05.
Keywords: Group ring, strongly regular graph, association scheme, cryptanalysis.
Received: 3 May 2014, Accepted: 7 July 2014.
*Corresponding author.

only consider the case that R is a finite commutative ring with identity and G a finite Abelian group, since in many applications of group rings to combinatorics and cryptography, R is a subring of the complex field and G is the direct product of elementary Abelian groups. For more definitions and results on group rings, one may refer, for example, to the textbooks [4, 31].

Group rings have been studied extensively for their close relationship with algebra, number theory and representation theory but also for their applications to other areas. For example, in [1, 29], they are applied to topics in combinatorics, as for examples in difference sets. Combining group rings with representation theory and number theory allowed proving existence and nonexistence results.

In addition to the extensive theoretical research, group rings also receive attention for their applications to cryptography. For instance, group rings are directly used to construct key exchange protocols similar to the Diffe-Hellman protocol in [18]. We should mention that it is not our purpose to cover all applications of group rings to combinatorics and cryptography in this paper, but to give a survey of some recent progress which may be less known. Some new results are also presented.

The rest of the paper is organized as follows. In Section 2, we give some preliminary results related to group rings. The relationship between group rings, highly nonlinear functions and difference sets are discussed in Section 3. We give a unifying treatment of various differential cryptanalyses on block ciphers by group rings in Section 4. Finally, we give some concluding remarks.

2. Group rings and character theory

Character theory is one of the most important tools for applying group rings to combinatorial objects and cryptography. In this section we only review the characters of the group ring $[G]$, where G is an Abelian group. For the theory of the representation of a general group ring, please refer to [26].

In the language of group rings, we identify a subset S of G with the group ring element $\sum_{s\in S} s$ in $[G]$, which will also be denoted by S (by abuse of notation). For $A = \sum_{g\in G} a_g g$ in $[G]$ and for an integer t, we define $A^{(t)} = \sum_{g\in G} a_g g^t$. A character χ of a finite Abelian group G is a homomorphism from G to $\mathbb{C}^*(\triangleq \setminus\{0\})$. A character χ is called *principal* if $\chi(c) = 1$ for all $c \in G$, otherwise it is called *non-principal*. A principal character is usually denoted by χ_0. All characters form a group denoted by $\widehat{G}$, and the *character group* is isomorphic to G. The following result states the well-known *orthogonal relations* of characters.

Result 1 (Orthogonal relations of characters)**.** *Let G be an Abelian group, then the following equations hold:*

$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq \chi_0, \\ |G| & \text{if } \chi = \chi_0; \end{cases}$$

and

$$\sum_{\chi\in \widehat{G}} \chi(g) = \begin{cases} 0 & \text{if } g \neq 1_G, \\ |G| & \text{if } g = 1_G. \end{cases}$$

By linearity, we may extend each character $\chi \in \widehat{G}$ to a ring homomorphism from $\mathbb{C}[G]$ to $\mathbb{C}$, and we denote this homomorphism by χ, again. In particular, if G is the additive group of the finite field $\mathbb{F}_{p^n}$, all characters of G can be represented as follows. Define $\chi_1 : \mathbb{F}_{p^n} \to \mathbb{C}$ as $\chi_1(x) := \zeta_p^{\mathrm{Tr}(x)}$ for all $x \in \mathbb{F}_{p^n}$, where ζ_p is a primitive p-th root of unity and $\mathrm{Tr}(x)$ is the absolute trace function defined as $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{p^i}$. Then χ_1 is an additive character of $\mathbb{F}_{p^n}$ (i.e. χ_1 is a character of the additive group of $\mathbb{F}_{p^n}$). Moreover, every additive character χ is of the form χ_b ($b \in \mathbb{F}_{p^n}$), where χ_b is defined by $\chi_b(x) = \chi_1(bx)$ for all $x \in \mathbb{F}_{p^n}$. Furthermore, if $G = \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, all characters of G can be represented by $\chi_{u,v}$, where $\chi_{u,v}(a,b) = \zeta_p^{\mathrm{Tr}(au+bv)}$ for any $(a,b) \in G$.

For a group ring element $M \in \mathbb{C}[G]$, the *Fourier transform* of M is defined as the element $\widetilde{M} = \sum_{\chi \in \widehat{G}} \chi(M)\chi$ in $\mathbb{C}[\widehat{G}]$. It is easy to verify that $\widetilde{\widetilde{M}} = |G| M^{(-1)}$ by noting that $\widehat{\widehat{G}} \cong G$ (since $g(\chi) := \chi(g)$ for any $g \in G$ defines a character of $\widehat{G}$). The following results are important properties of group rings:

Result 2. *Let $D = \sum_{g \in G} a_g g \in [G]$. Then the following hold:*

$$a_g = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(D)\chi(g^{-1}), \tag{2.1}$$

$$\sum_{g \in G} |a_g|^2 = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} |\chi(D)|^2. \tag{2.2}$$

Equation (2.1) is the so-called *Inversion Formula*, and Equation (2.2) is called *Parseval's relation.* It is worth mentioning that Inversion Formula provides a useful method for showing when two group ring elements are equal.

Corollary 1. *Let $A = \sum_{g \in G} a_g g$ and $B = \sum_{g \in G} b_g g$ be two group ring elements of $[G]$. Then $A = B$ if and only if $\chi(A) = \chi(B)$ for all $\chi \in \widehat{G}$.*

The above corollary will be particularly useful in the next section.

3. Group rings, highly nonlinear functions and related combinatorial objects

Let F be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. The study of highly nonlinear functions is important for symmetric cryptography. In the design of block ciphers and stream ciphers, to avoid various attacks [3, 19, 24, 25], highly nonlinear functions are employed as Substitution boxes (in block ciphers) or filter functions (in stream ciphers). Moreover, highly nonlinear functions are demonstrated to be related to topics in other areas, for instance combinatorics and coding theory. Group rings serve as an important bridge between these two areas. In the following, we first introduce two commonly used parameters evaluating the level of nonlinearity of a function F, together with a brief review of the study of highly nonlinear functions. Finally, we give the recent constructions of various difference sets by highly nonlinear functions. For a more general introduction to highly nonlinear functions, one may refer to [6, 7, 9].

3.1. **Differential and Walsh spectrum.** Let F be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ and $G = \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ be the direct product of the additive group of $\mathbb{F}_{p^n}$ with itself. The *Walsh transform* $\mathcal{W}_F : G \to$ of F is defined as follows:

$$\mathcal{W}_F(a,b) := \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(bF(x)-ax)},\ a,b \in \mathbb{F}_{p^n},$$

where ζ_p is a primitive p-th root of unity, and $\mathrm{Tr}(x)$ denotes the absolute trace function. The multiset $\Lambda_F := \{\ \mathcal{W}_F(a,b) : a,b \in \mathbb{F}_{p^n}, b \neq 0\ \}$ is called the *Walsh spectrum* of F, and each value $\mathcal{W}_F(a,b)$ is called a *Walsh coefficient*. In the case of a "single-output" function[1] $F : \mathbb{F}_{p^n} \to \mathbb{F}_p$, the Walsh transformation of F is more simply defined as $\mathcal{W}_F : \mathbb{F}_{p^n} \to$, where $\mathcal{W}_F(a)$ is defined as $\mathcal{W}_F(a) = \sum_{x\in\mathbb{F}_{p^n}} \zeta_p^{F(x)-\mathrm{Tr}(ax)}$. Particularly, when the modulus of each $\mathcal{W}_F(a)$ equals $p^{n/2}$, the function $F : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is called *bent* (it is called *weakly regular bent* if there exists $u \in \mathbb{C}$ of modulus 1 such that, for every $a \in \mathbb{F}_{p^n}$, we have $\mathcal{W}_F(a) = up^{n/2}\zeta_p^c$ for some $c \in \mathbb{F}_p$); while when $|\mathcal{W}_F(a)| \in \{0, p^{(n+1)/2}\}$ for every a, the function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called *almost bent* (AB). The multiset $\{\ |x| : x \in \Lambda_F\ \}$, where $|x|$ denotes the modulus of x, is called the *extended Walsh spectrum* of F.

If $p = 2$, the *nonlinearity* $\mathrm{NL}(F)$ of $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is defined as

$$\mathrm{NL}(F) \triangleq 2^{n-1} - \frac{1}{2}\max_{x\in\Lambda_F} |x|.$$

It equals the minimum Hamming distance between the so-called component functions $\mathrm{Tr}(bF(x))$, $b \in {\mathbb{F}_{p^n}}^*$, of F and affine functions $\mathrm{Tr}(ax)$, $a \in \mathbb{F}_{p^n}$. It is known that, if n is odd, the nonlinearity $\mathrm{NL}(F)$ is bounded by the tight upper bound $2^{n-1} - 2^{\frac{n-1}{2}}$; and if n is even, it is conjectured that $\mathrm{NL}(F)$ is bounded above by $2^{n-1} - 2^{\frac{n}{2}}$; see [7] for more details. Note that the Walsh coefficient $\mathcal{W}_F(a,b)$ is nothing but the character value of the group ring element corresponding to the graph of F. Precisely, defining the group ring element $D = \sum_{x\in\mathbb{F}_{p^n}} (x, F(x)) \in [\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}]$, one may see without difficulty that $\mathcal{W}_F(a,b) = (\chi_{-a}, \chi_b)(D)$, where χ_{-a}, χ_b are characters of $\mathbb{F}_{p^n}$ and $(\chi_{-a}, \chi_b)(x,y) = \chi_{-a}(x)\chi_b(y)$. It is bounded above by $2^{n-1} - 2^{\frac{n}{2}-1}$. This bound is achieved with equality (by the binary bent functions) if and only if n is even.

Another nonlinearity parameter[2] of functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is defined as follows. For any $a, b \in \mathbb{F}_{p^n}$, define the function

$$\delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n} : F(x+a) - F(x) = b\}.$$

The multiset $\Delta_F := \{\ \delta_F(a,b) : a,b \in \mathbb{F}_{p^n}, a \neq 0\ \}$ is called the *differential spectrum* of F. Let $\Delta = \max(\Delta_F)$, then F is called a *differentially* Δ*-uniform* function and the *differential uniformity of* F equals Δ. Differentially 2-uniform functions, which have optimal differential uniformity when $p = 2$ since Δ must then be even, are called *almost perfect nonlinear* (APN). They were first studied by Nyberg in [27] as they provide when $p = 2$ an optimal resistance to the differential cryptanalysis [3]. In contrast to the case $p = 2$, when p is odd, the lowest possible differential uniformity is 1. Functions

[1] The Walsh transform can also be defined for functions from $\mathbb{F}_{p^n}$ to any of its subfields, and more generally for functions from ${\mathbb{F}_p}^n$ to ${\mathbb{F}_p}^m$ for every n, m, but we shall not consider such functions in the present paper.

[2] The term of nonlinearity being already taken as recalled above, another name is used for this parameter, but it also quantifies the level of nonlinearity of a function, from a different viewpoint, though.

achieving such differential uniformity are called *perfect nonlinear* (PN) or *planar*. More generally, in [9, 28], the concept of perfect nonlinear function was extended to functions from an Abelian group A to an Abelian group B. Such a function F is called *perfect nonlinear* if

$$\#\{g \in A | F(g+a) - F(g) = b\} = m/n, \ \forall a \in A \setminus \{0\}, b \in B,$$

where $\#A = m, \#B = n$.

Finally, we recall the equivalence relations between functions defined on $\mathbb{F}_{p^n}$. Two functions F and G are called *extended affine* (EA) equivalent if there exist affine permutations $L, L' : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and an affine function A such that $G = L' \circ F \circ L + A$. Furthermore, they are called *Carlet-Charpin-Zinoviev* (CCZ) equivalent [8] if their graphs $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$ and $\mathcal{G}_G = \{(x, G(x)) : x \in \mathbb{F}_{p^n}\}$ are affine equivalent, that is, if there exists an affine automorphism L of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ such that $L(\mathcal{G}_F) = \mathcal{G}_G$. It is well known that CCZ-equivalence can be interpreted in the language of coding theory. Regarding the finite field $\mathbb{F}_{p^n}$ as a vector space of dimension n over $\mathbb{F}_p$, and then fixing a basis of $\mathbb{F}_{p^n}$, we may express each element $x \in \mathbb{F}_{p^n}$ as a vector of length n. Define a matrix $C_F \in \mathbb{F}_p^{2n \times p^n}$ as follows:

$$C_F = \begin{bmatrix} \cdots & 1 & \cdots \\ \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{bmatrix},$$

where "$\cdots \ 1 \ \cdots$" is a single row in the matrix and x (as well as $F(x)$) is written as a column vector (which represents then n rows in the matrix) and where some order in $\mathbb{F}_{p^n}$ has been chosen for writing these columns of the matrix. Denoting by $\mathcal{C}_F$ the linear code generated by C_F, two functions F and G are CCZ-equivalent if and only if their corresponding codes $\mathcal{C}_F$ and $\mathcal{C}_G$ are equivalent [8, 5]. It is well known that EA equivalence implies CCZ equivalence, but not vice versa. Moreover, both EA and CCZ equivalence preserve the differential spectrum and the extended Walsh spectrum, and EA equivalence also preserves the algebraic degree when the degree is greater than one.

3.2. **Highly nonlinear functions and difference sets.** The definitions of difference sets and their variants and the notation in this section follow Reference [2]. Let G be a group of size v. A subset D of G of size k is called a (v, k, λ, μ)-*partial difference set* (PDS) if each non-identity element in D can be represented as gh^{-1} $(g, h \in D, g \neq h)$ in exactly λ ways, and if each non-identity element in $G \setminus D$ can be represented as gh^{-1} $(g, h \in D, g \neq h)$ in exactly μ ways. We shall always assume that the identity element 1_G of G is not contained in D. A k-subset D of G is called a (v, k, λ)-*difference set* (DS) if it is a (v, k, λ, λ) PDS, that is, if each nonidentity element of G can be represented in the form $d_1 d_2^{-1}$ $(d_1, d_2 \in D, d_1 \neq d_2)$ in exactly λ ways.

Another type of difference sets interesting to us is that of relative difference sets. The set D is called a $(v/n, n, k, \lambda)$-*relative difference set* (RDS) in G relative to a normal sub-group N of G of size n if the differences gh^{-1} $(g, h \in D, g \neq h)$ cannot represent any nonidentity element in N, and represent each element in $G \setminus N$ in exactly λ times. Finally, if G is Abelian (resp. cyclic), then D is also called an Abelian (resp. cyclic) (partial, relative)-difference set.

Using the language of group rings, we characterize difference sets. The proof is directly from Corollary 1 of Section 2.

Proposition 1. *Let G be a group of size v, D be a subset of G of size k and N be a normal subgroup of G of size n. We denote the identity element of G by 1_G. Then:*

(i) D is a (v,k,λ)-difference set if and only if

$$DD^{(-1)} = k + \lambda(G - 1_G).$$

(ii) D is a $(v/n, n, k, \lambda)$-relative difference set in G relative to N if and only if

$$DD^{(-1)} = k + \lambda(G - N).$$

(iii) D is a (v,k,λ,μ)-partial difference set if and only if

$$DD^{(-1)} = (k-\mu)1_G + (\lambda-\mu)D + \mu G.$$

In general, there are two methods to construct difference sets and their variants from highly non-linear functions. The first method was fruitfully applied in [28]. We first give the following simple but important result to link the differential property of a function $F : A \to B$ and group rings. For the convenience of the reader, we include a short proof. In the rest of this section, we assume that the group G is Abelian, and for convenience, we write the operation of G additively.

Proposition 2. *Let A and B be arbitrary finite Abelian groups and F a function from A to B. We define the group ring element $D_F = \sum_{x\in A}(x, F(x)) \in [A \times B]$. Then*

$$D_F D_F^{(-1)} = \sum_{(a,b)\in A\times B} \delta_F(a,b)(a,b),$$

where $\delta_F(a,b) = \#\{x \in A | F(x+a) - F(x) = b\}$.

Proof. The result can be seen from the following computation:

$$\begin{aligned} D_F D_F^{(-1)} &= \left(\sum_{x\in A}(x, F(x))\right)\left(\sum_{y\in A}(-y, -F(y))\right) \\ &= \sum_{x,y\in A}(x-y, F(x)-F(y)) \\ &= \sum_{a,y\in A}(a, F(y+a)-F(y)) = \sum_{(a,b)\in A\times B}\delta_F(a,b)(a,b). \end{aligned}$$

□

Using Proposition 2, one may easily obtain the following result.

Proposition 3 ([28])**.** *Let A and B be arbitrary finite Abelian groups and F a function from A to B. The set*

$$D_F = \sum_{x\in A}(x, F(x)) \in [A \times B]$$

is an $(|A|,|B|,|A|,|A|/|B|)$*-relative difference set in* $A\times B$ *relative to* $\{0\}\times B$ *if and only if* F *is perfect nonlinear.*

Proof. Assume that F is perfect nonlinear, namely $\delta_F(a,b)=|A|/|B|$ for all nonzero $a\in A$ and for all $b\in B$. By Proposition 2, we have

$$\begin{aligned} D_F D_F^{(-1)} &= \sum_{(a,b)\in A\times B}\delta_F(a,b)(a,b)=|A|(0,0)+\frac{|A|}{|B|}\sum_{(a,b)\in(A\times B)\setminus\{0\}\times B}(a,b)\\ &= |A|(0,0)+\frac{|A|}{|B|}\left(A\times B-\{0\}\times B\right). \end{aligned}$$

Then D_F is clearly a $(|A|,|B|,|A|,|A|/|B|)$-relative difference set in $A\times B$ relative to $\{0\}\times B$. The converse part follows directly from the RDS definition. □

The second important method to construct difference sets and their variants from highly nonlinear functions is to study either the images or the preimages of them. We report some recent progress of such constructions in the rest of this section.

Let f be a ternary bent function from $\mathbb{F}_{3^n}$ to $\mathbb{F}_3$, where n is an even integer. It is shown in [32] that such bent functions may be used to construct PDS.

Theorem 1. [32] *Let* f *be a weakly regular bent function from* $\mathbb{F}_{3^n}$ *to* $\mathbb{F}_3$ *satisfying* $f(-x)=f(x)$ *and* $f(0)=0$*, where* $n=2m$ *is an even integer. Define* $D_i=\{x\in\mathbb{F}_{3^n}|f(x)=i\}$ *for* $i=0,1,2$*. Then*

(i) D_1 *and* D_2 *are both* $(3^{2m},3^{2m-1}+\epsilon 3^{m-1},3^{2m-2},3^{2m-2}+\epsilon 3^{m-1})$*-PDS;*

(ii) The set $D=D\setminus\{0\}$ *is a* $(3^{2m},3^{2m-1}-1-2\epsilon 3^{m-1},3^{2m-2}-2\epsilon 3^{m-1}-2,3^{2m-2}-\epsilon 3^{m-1})$*-PDS,*

where $\epsilon=\pm1$*.*

We should note that group rings are important in the proof of the above result. Indeed, the key to the proof of Theorem 1 is by regarding D_i as a group ring element in $[\mathbb{F}_{p^n}]$, and using that $\mathbb{F}_{p^n}=D_0+D_1+D_2$. As mentioned above, the Walsh coefficient $\mathcal{W}_f(b)$ equals $\chi_b(D_0)+\chi_b(D_1)+\chi_b(D_2)$. Combining this with Corollary 1 of Section 2, the proof may be reached via technical computations. Later on, this construction was generalized to any p-ary weakly regular bent function later on in [11]. First we define a property of p-ary functions f from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ which, when satisfied, allows proving that certain preimage sets of f are actually PDS.

Property A: Let p be an odd prime and $f:\mathbb{F}_{p^{2k}}\to\mathbb{F}_p$ be a weakly regular bent function such that $f(0)=0$ and $f(-x)=f(x)$. We say that f satisfies Property A if there exists an integer ℓ with $(\ell-1,p-1)=1$ such that $f(\alpha x)=\alpha^{\ell}f(x)$ for any $\alpha\in\mathbb{F}_p$ and $x\in\mathbb{F}_{p^{2k}}$. There exists then a p-ary function f^* such that, for each $b\in\mathbb{F}_{p^{2k}}$, $\mathcal{W}_f(b)=\epsilon p^k\zeta_p^{f^*(b)}$, where $\epsilon=(-1)^{\frac{(p-1)k}{2}}\mu$ with $\mu=\pm1$.

Theorem 2. *Let* f *be a function satisfying Property A. Let*

$$D:=\{x:x\in\mathbb{F}_{p^{2k}}^*|f(x)=0\}.$$

Then D is a $(v, d, \lambda_1, \lambda_2)$-PDS, where

$$\begin{array}{rcl} v & = & p^{2k}, \\ d & = & (p^k-\epsilon)(p^{k-1}+\epsilon), \\ \lambda_1 & = & (p^{k-1}+\epsilon)^2-3\epsilon(p^{k-1}+\epsilon)+\epsilon p^k, \\ \lambda_2 & = & (p^{k-1}+\epsilon)p^{k-1}, \end{array} \tag{3.1}$$

where ϵ is defined in Property A.

Theorem 3. *Let f be a function satisfying Property A. Let*

$$D_{\mathcal{S}} := \{x : x \in \mathbb{F}_{p^{2k}}^{*} | f(x) \text{ are non-zero squares}\},$$

then $D_{\mathcal{S}}$ is a $(v, d, \lambda_1, \lambda_2)$-PDS, where

$$\begin{array}{rcl} v & = & p^{2k}, \\ d & = & \frac{1}{2}(p^k-p^{k-1})(p^k-\epsilon), \\ \lambda_1 & = & \frac{1}{4}(p^k-p^{k-1})^2-\frac{3\epsilon}{2}(p^k-p^{k-1})+p^k\epsilon, \\ \lambda_2 & = & \frac{1}{2}(p^k-p^{k-1})(\frac{1}{2}(p^k-p^{k-1})-\epsilon), \end{array} \tag{3.2}$$

where ϵ is defined in Property A.

Theorem 4. *Let f be a function satisfying Property A. Let*

$$D'_{\mathcal{S}} := \{x : x \in \mathbb{F}_{p^{2k}}^{*} | f(x) \text{ are squares}\},$$

then $D'_{\mathcal{S}}$ is a $(v, d, \lambda_1, \lambda_2)$-PDS, where

$$\begin{array}{l} v = p^{2k}, \\ d = \frac{1}{2}(p^k+p^{k-1}+2\epsilon)(p^k-\epsilon), \\ \lambda_1 = \frac{1}{4}(p^k+p^{k-1}+2\epsilon)^2-\frac{3\epsilon}{2}(p^k+p^{k-1}+2\epsilon)+p^k\epsilon, \\ \lambda_2 = \frac{1}{4}(p^k+p^{k-1})(p^k+p^{k-1}+2\epsilon), \end{array} \tag{3.3}$$

where ϵ is defined in Property A.

For more combinatorial objects associated with highly nonlinear functions defined on $\mathbb{F}_{2^n}$, one may refer to [12, 30]. In [10], PDSs are shown to be related to zero-difference balanced functions (notion introduced in [13]). We include their construction below. It should be mentioned that Theorem 5 (i) first appeared in [33]. We include a new but shorter proof of it below. The proof is another classical application of using group rings to obtain difference sets.

We first state some basic facts on the cyclotomic field $K = \mathbb{Q}(\zeta_p)$ which can be found in [17], or [16, Lemma 1].

Lemma 1. (1) *The ring of integers in $\mathbb{K} = \mathbb{Q}(\zeta_p)$ is $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ and $\{\zeta_p : 0 \le i \le p-2\}$ is an integral basis of $\mathcal{O}_{\mathbb{K}}$. The group of roots of unity in $\mathcal{O}_{\mathbb{K}}$ is $W_{\mathbb{K}} = \{\pm\zeta_p^i : 0 \le i \le p-1\}$.*

(2) *The field $\mathbb{K}$ has a unique quadratic subfield $\mathbb{L} = \mathbb{Q}(\sqrt{p^*})$ where $p^* = (\frac{-1}{p})p = (-1)^{\frac{p-1}{2}}p$ and for $1 \le a \le p-1$, $(\frac{a}{p})$ is the Legendre symbol. For each $\sigma_a \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $0 \le a \le p-1$ defined by $\sigma_a(\zeta_p) = \zeta_p^a$, $\sigma_a(\sqrt{p^*}) = (\frac{a}{p})\sqrt{p^*}$. Therefore, $Gal(\mathbb{L}/\mathbb{Q}) = \{1, \sigma_\gamma\}$, where γ is any quadratic non-residue in $\mathbb{F}_p$.*

Theorem 5. *Let $F(x) = G(x^d)$ be a quadratic function from $\mathbb{F}_{p^n}$ to itself, where p is any prime and $\gcd(d, p^n - 1) = p^t + 1$ for some non-negative integer t. Assume that the restriction of G to $C_d = \{x^d : x \in \mathbb{F}_{p^n}^*\} = C_{p^t+1}$ is an injection from C_d to $\mathbb{F}_{p^n}$. Define the set $D = \{F(x) : x \in \mathbb{F}_{p^n}\}\backslash\{0\}$. Then:*

(i) if $t = 0$ and p is an odd prime, then D is a

$$\left(p^n, \tfrac{p^n-1}{2}, \tfrac{p^n-3}{4}\right) \text{ difference set, } \quad \text{when } p^n \equiv 3 \mod 4,$$
$$\left(p^n, \tfrac{p^n-1}{2}, \tfrac{p^n-5}{4}, \tfrac{p^n-1}{4}\right) \text{ partial difference set, } \quad \text{when } p^n \equiv 1 \mod 4.$$

(ii) if $t > 0$ and n is divisible by $2t$, then D is a

$$\left(p^n, \frac{p^n-1}{p^t+1}, \frac{p^n - 3p^t - 2 - \epsilon p^{n/2+2t} + \epsilon p^{n/2+t}}{(p^t+1)^2}, \frac{p^n - \epsilon p^{n/2} + \epsilon p^{n/2+t} - p^t}{(p^t+1)^2}\right)$$

partial difference set, where $n = 2kt$ and $\epsilon = (-1)^k$.

Proof. Without loss of generality, we may assume that $d = p^t + 1$. Let us denote the additive group of $\mathbb{F}_{p^n}$ by $\mathcal{G}$. By Corollary 1, to prove that D is a (partial) difference set with the prescribed parameters, we need to determine the character values of D. Now, for each nontrivial character $\chi_a \in \widehat{\mathcal{G}}, a \in \mathcal{G}^*$, we have $\chi_a(D) = \sum_{x \in C_d} \zeta_p^{\mathrm{Tr}(aG(x))}$, where ζ_p is a primitive p-th root of unity. It is not difficult to see that

$$\mathcal{W}_{\mathrm{Tr}(aF)}(0) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(aF(x))} = 1 + d \sum_{x \in C_d} \zeta_p^{\mathrm{Tr}(aG(x))} = 1 + d\chi_a(D),$$

and hence

$$\chi_a(D) = \frac{1}{d}\left(\mathcal{W}_{\mathrm{Tr}(aF)}(0) - 1\right). \tag{3.4}$$

Denoting $\mathcal{W}_{\mathrm{Tr}(aF)}(0)$ by X_a, we have

$$X_a\overline{X_a} = \sum_{x,y \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(a(F(x)-F(y)))} = \sum_{t \in \mathbb{F}_{p^n}} \left(\sum_{y \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(a(F(y+t)-F(y)))} \right). \tag{3.5}$$

(i): For $t = 0$ we have $d = p^0 + 1 = 2$. By hypothesis, we assume that $F(x) = G(x^2)$ is a quadratic function and that $G|_{C_2}$ is an injection. Then F is a PN function (see [33]) and then $F(y + t) - F(y)$ is a PP over $\mathbb{F}_{p^n}$ for any nonzero t. Therefore, by (3.5) we have $X_a\overline{X_a} = p^n$. By Lemma 1, we have $X_a = \varsigma(\sqrt{p^*})^n$, where $\varsigma \in \{-1, 1\}$ and $p^* = \left(\frac{-1}{p}\right)p$. In the following we divide the proof into two cases.

Case 1: n is even. Note that in this case $p^n \equiv 1 \mod 4$, which implies that $X_a = \varsigma(\sqrt{p^*})^n = \varsigma\left((\frac{-1}{p})p\right)^{n/2} = \varsigma(\frac{-1}{p})^{n/2}p^{n/2}$. Hence we have $\chi_a(D) = \frac{1}{2}(\varsigma(\frac{-1}{p})^{n/2}p^{n/2} - 1)$. It can be verified that $\chi_a(DD^{(-1)}) = \chi_a(D)\chi_a(D^{(-1)}) = \chi_a(D)\overline{\chi_a(D)} = \frac{1}{4}(p^n + 1 - 2\varsigma(\frac{-1}{p})^{n/2}p^{n/2})$. On the other hand, it can be easily computed that $(k-\lambda)+(\mu-\lambda)\chi_a(D) = \frac{1}{4}(p^n+1-2\varsigma(\frac{-1}{p})^{n/2}p^{n/2}))$. Then, by Corollary 1, we have that D is a PDS with the prescribed parameter.

Case 2: $p \equiv 3 \mod 4$ and n is odd. Assume that $n = 2m + 1$. In this case we have $X_a = \varsigma(\sqrt{p^*})^{2m+1} = \varsigma\left((\frac{-1}{p})p\right)^m \sqrt{p^*} = \varsigma\left(\frac{-1}{p}\right)^m p^m\sqrt{p^*}$, then $\chi_a(D) = \frac{1}{2}(\varsigma\left(\frac{-1}{p}\right)^m p^m\sqrt{p^*} - 1)$. On the one hand, note that the complex conjugate of $\sqrt{p^*}$ equals $-\sqrt{p^*}$ (since $\sqrt{p^*}\cdot(-\sqrt{p^*}) = -p^* = -\left(\frac{-1}{p}\right)p = p = |\sqrt{p^*}|^2$). Then $\chi(DD^{(-1)}) = \chi(D)\overline{\chi(D)} = \frac{1}{4}(\varsigma\left(\frac{-1}{p}\right)^m p^m\sqrt{p^*} - 1)(\varsigma\left(\frac{-1}{p}\right)^m p^m\overline{\sqrt{p^*}} - 1) = \frac{1}{4}(\varsigma\left(\frac{-1}{p}\right)^m p^m\sqrt{p^*} - 1)(-\varsigma\left(\frac{-1}{p}\right)^m p^m\sqrt{p^*} - 1) = -\frac{1}{4}(\left(\frac{-1}{p}\right)p^n - 1) = \frac{1}{4}(p^n+1)$ (since $\left(\frac{-1}{p}\right) = -1$ as $p \equiv 3 \mod 4$). On the other hand, one may compute that $k-\lambda = \frac{1}{4}(p^n+1)$. By Corollary 1, we prove that D is the difference set with the prescribed parameters.

The proof of (ii) can be found in [10]. □

As a corollary, certain type of APN functions may be used to construct PDS.

Corollary 2. [10] *Let F be a quadratic APN function on $\mathbb{F}_{2^n}$ with the form $F(x) = G(x^3)$, where $g|_{C_3}$ is an injection and $n = 2k$. Let*

$$D = \{F(x) : x \in \mathbb{F}_{2^n}\} \setminus \{0\}.$$

Then D is a partial difference set with parameters

$$\left(2^n, \tfrac{2^n-1}{3}, \tfrac{1}{9}(2^k+4)(2^k-2), \tfrac{1}{9}(2^k+1)(2^k-2)\right) \quad \text{if } k \text{ is odd},$$

$$\left(2^n, \tfrac{2^n-1}{3}, \tfrac{1}{9}(2^k-4)(2^k+2), \tfrac{1}{9}(2^k-1)(2^k+2)\right) \quad \text{if } k \text{ is even}.$$

4. **Group rings and differential cryptanalysis**

In this section, we discuss the relationship between group rings and the differential cryptanalysis of block ciphers. As we will show below, using group rings, we may give a unifying treatment of various differential cryptanalyses, namely, the classical differential cryptanalysis, impossible differential cryptanalysis, truncated differential cryptanalysis and related-key differential cryptanalysis. One may refer to [20] for the definition and basic results of these differential cryptanalyses.

A block cipher $\mathcal{B}$ with block size b and key length n consists of three parts:

(1) the set of encryption functions $\mathcal{E} = \{\ E \mid E \text{ is a permutation on } \mathbb{F}_{2^b}\}$,
(2) the set of decryption functions $\mathcal{D} = \{\ D \mid D \text{ is a permutation on } \mathbb{F}_{2^b}\}$,
(3) the set of keys $\mathcal{K} \subset \mathbb{F}_{2^n}$,

such that, for each key $k \in \mathcal{K}$, there exists a unique encryption function $E_k \in \mathcal{E}$, and a unique decryption function $D_k \in \mathcal{D}$ such that $E_k \circ D_k = D_k \circ E_k = id$, where id is the identity mapping defined by $id(x) = x$ for all $x \in \mathbb{F}_{2^b}$. In other words, a block cipher is a set of 2^n permutations on $\mathbb{F}_{2^b}$. However, since in most cases 2^n is small compared to the number $(2^b)!$ of all permutations over $\mathbb{F}_{2^b}$, an exhaustive search among all permutations would be much more expensive than an exhaustive search of the key.

Most modern block ciphers iterate a round function depending of a round key and using a substitution-permutation structure. Given a block cipher $\mathcal{B}$, let us assume the number of iterations of the round function R is r and denote the composition of $r-1$ round functions by R^{n-1}. We define the group ring element $X=\sum_{x\in\mathbb{F}_{2^b}}(x,R^{n-1}(x))\in[\mathbb{F}_{2^b}\times\mathbb{F}_{2^b}]$. Similarly to Section 2, we have

$$XX^{(-1)}=2^b(0,0)+\sum_{\substack{\alpha,\beta\in\mathbb{F}_{2^b}\\ \alpha\neq 0}}\delta_{R^{n-1}}(\alpha,\beta)(\alpha,\beta), \tag{4.1}$$

where $\delta_{R^{n-1}}(\alpha,\beta)=\#\{x\in\mathbb{F}_{2^b}\mid R^{n-1}(x+\alpha)+R^{n-1}(x)=\beta\}$.

(1) Classical differential attack: The basic idea behind the classical differential attack on a block cipher is that, choose an input difference α and an output difference β such that

$$\mathrm{pr}=\mathrm{Pr}_{x\in\mathbb{F}_{2^b}}(R^{n-1}(x+\alpha)+R^{n-1}(x)=\beta)$$

is large. Then, by randomly choosing $\lceil 1/\mathrm{pr}\rceil$ pairs of messages $\{M,M+\alpha\}$, an attacker is expected to obtain one pair $M,M+\alpha$ such that $R^{n-1}(M)+R^{n-1}(M+\alpha)=\beta$ in average. Using this, an attacker picks a set of message pairs Ω with difference α and with size T, i.e. $\#\Omega=T$, she randomly guesses a key and using this key computes the internal states from the ciphertexts by going back one round. If for a key, the number of internal states with difference β (computed from the ciphertexts) is approximately equal to $T\cdot pr$, the guessed key is of high chance to be the correct one.

Using the group ring equation (4.1), if an attacker observes one tuple (α,β) such that the value $\delta_{R^{n-1}}(\alpha,\beta)/2^b$ is significantly large, then using the value α as the input difference, and using β as the output difference, she may get a differential characteristic with probability $\delta_{R^{n-1}}(\alpha,\beta)/2^b$;

(2) Impossible differential attack: The idea behind this special differential attack is quite simple. If one attacker finds a tuple (α,β) such that there is no chance that the input difference α will lead to the output difference β, the attacker may exclude all keys such that, after computing the ciphertexts back one round, the output difference is β. This is indeed the case that $\delta_{R^{n-1}}(\alpha,\beta)=0$ in (4.1). It is worthy to notice another similar extreme case an attacker can make use is $\delta_{R^{n-1}}=2^b$.

(3) Truncated differential attack: Sometimes if a block cipher is designed very carefully, it is very hard to find the tuple (α,β) corresponding to the above two cases. In this situation, an attacker may want to discover an input difference α, and an output difference of the form $\beta=(*,*,\cdot,*,\cdots,*)\in\mathbb{F}_2^b$, where $*$ denotes a bit which may equal either 0 or 1, and $\cdot$ means this bit is a specific value, such that

$$\mathrm{pr}=\mathrm{Pr}_{x\in\mathbb{F}_{2^b}}(R^{n-1}(x+\alpha)+R^{n-1}(x)=\beta)$$

is large. In other words, the output difference is a set of elements in $\mathbb{F}_{2^b}$, say Ω. Although the attacker can only recover the key bit in the position that $\cdot$ appears in β, she may make use of this information and then run an exhaustive search for the remaining key bits.

Using the group ring equation (4.1), we may express the truncated differential attack explicitly. Now, letting $\rho':\mathbb{F}_{2^b}\to\mathbb{F}_{2^t}$ be the natural homomorphism defined by

$$\rho'(g)=g+\mathbb{F}_{2^t}.$$

Define a homomorphism ρ from $\mathbb{F}_{2^b} \times \mathbb{F}_{2^b}$ to $\mathbb{F}_{2^b} \times \mathbb{F}_{2^t}$ by $\rho(x, y) = (x, \rho'(y))$. Applying ρ on (4.1), we have

$$\begin{aligned} \rho(XX^{(-1)}) &= \rho(X)\rho(X^{(-1)}) \\ &= \rho\left(\sum_{(a,b)\in\mathbb{F}_{2^b}\times\mathbb{F}_{2^b}} \delta_{R^{n-1}}(a,b)(a,b)\right) \\ &= \sum_{(a',b')\in\mathbb{F}_{2^b}\times\mathbb{F}_{2^t}} \delta'_{R^{n-1}}(a',b')(a',b'). \end{aligned}$$

Note that, for an element $\beta \in \mathbb{F}_{2^t} \leq \mathbb{F}_{2^b}$, we may regard it as a set $\Omega = \{\omega \in \mathbb{F}_{2^b} | \rho'(\omega) = \beta\}$. Now, if an attacker observes a tuple $(\alpha, \beta) \in \mathbb{F}_{2^b} \times \mathbb{F}_{2^t}$ such that $\delta'_{R^{n-1}}(\alpha, \beta)$ is very large, she may then choose α as the input difference, and β as the truncated output difference. The success probability of the truncated differential attack is $\sum_{\beta\in\Omega} \delta_F(\alpha, \beta)$.

(4) Related-key differential attack: assume an attacker found an input difference α and an output difference β such that

$$\Pr_{x\in\mathbb{F}_{2^b}}\left(E_{K_2}(x+\alpha) + E_{K_1}(x) = \beta\right) \gg 0$$

is true for all keys K_1, K_2 with a fixed difference Δ_K. Then an attacker may use Δ_K, α, β to mount an attack (see more details in [20]). Again, we may use group rings to express the idea of related-key differential attack explicitly. Letting $X_i = \sum_{x\in\mathbb{F}_{2^b}} (x, E_{K_i}(x))$ for $i = 1, 2$. Then

$$\begin{aligned} X_1X_2^{(-1)} &= \sum_{x\in\mathbb{F}_{2^b}} (x, E_{K_1}(x)) \cdot \sum_{y\in\mathbb{F}_{2^b}} (y, E_{K_2}(y)) \\ &= \sum_{a,x} (a, E_{K_1}(x+a) + E_{K_2}(x)) \\ &= \sum_{a,b} \eta(a,b)(a,b), \end{aligned}$$

where $\eta(a, b) = \#\{x \in \mathbb{F}_{2^b} \mid E_{K_1}(x + a) + E_{K_2}(x) = b\}$. If an attacker observes that there is one tuple α, β such that $\eta(\alpha, \beta)$ is very large, she may use α, β as input and output difference, respectively. We should note that the group ring operation $X_1X_2^{(-1)}$ appears in the definition of many combinatorial objects, as for examples in difference family.

5. Conclusion

Group ring is a very useful tool to study the topics in combinatorics and cryptography. This paper contains a detailed presentation of the recent results regarding the applications of group rings in combinatorics and symmetric cryptography. We also provide some new results. For instance, we give a shorter proof of the construction of Hadamard difference sets and Payley partial difference sets that are from perfect nonlinear functions. Moreover, we use group rings to give a unifying treatment of various differential cryptanalysis of block ciphers. It would be important and interesting to make use of the fruitful results in group rings to improve the differential cryptanalysis from this connection.

References

[1] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Vol. 182 Springer-Verlag, Berlin-New York, 1971.

[2] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Vol 1, Cambridge University Press, Cambridge, 1999.

[3] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Journal of Cryptology, 4(1) (1991) 3–72.

[4] A. A. Bovdi, A. A., *Group Algebra*, Encyclopedia of Mathematics, Springer, 2001.

[5] K. Browning, J. F. Dillon, R. E. Kibler and M. McQuistan. *APN polynomials and related codes*. Special volume of Journal of Combinatorics, Information and System Sciences, honoring the 75-th birthday of Prof. D.K.Ray-Chaudhuri, vol. 34, Issue 1-4, (2009) pp. 135-159.

[6] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 257-397, 2010. Preliminary version available at `http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html`.

[7] C. Carlet, *Vectorial Boolean Functions for Cryptography*, Chapter of the monograph Boolean Methods and Models, Y. Crama and P. Hammer eds, Cambridge University Press, to appear soon. Preliminary version available at `http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html`.

[8] C. Carlet, P. Charpin, and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Designs, Codes and Cryptography, 15(2), (1998) 125-156.

[9] C. Carlet and C. Ding, *Highly nonlinear mappings*, Journal of Complexity, 20 (2-3), (2004) 205–244.

[10] C. Carlet, G. Gong and Y. Tan, *Quadratic zero-difference balanced functions, APN functions and strongly regular graphs*, Designs, Codes and Cryptography, DOI 10.1007/s10623-014-0022-x.

[11] Y. M. Chee, Y. Tan and X. Zhang, *Strongly regular graphs constructed from p-ary bent functions*, Journal of Algebraic Combinatorics, 34(2), (2011) 251-266.

[12] E. R. van Dam and D. Fon-Der-Flaass, *Codes, graphs, and schemes from nonlinear functions*, European Journal of Combinatorics, 24(1), (2000) 85–98.

[13] C. Ding and Y. Tan, *Zero-difference balanced functions with applications*, Journal of Statistical Theory and Practice, 6(1), (2012) 3-19.

[14] W. Diffe and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory 22, (1976) 644–654.

[15] Y. Edel and A. Pott, *A new almost perfect nonlinear function which is not quadratic*, Advances in Mathematical Communications 3(1), (2009) 59–81.

[16] K. Feng and J. Luo, *Value distributions of exponential sums from perfect nonlinear functions and their applications*, IEEE Transaction on Information Theory, 53(9), (2007) 3035–3041.

[17] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, vol. 84. Springer-Verlag, New York, 1990.

[18] D. Kahrobaei, C. Koupparis and V. Shpilrain, *Public key exchange using matrices over group rings*, arXiv: 1302.1625v1, (2013).

[19] L. Knudsen, *Truncated and higher order differentials*, Lecture Notes in Computer Science, Vol 1008, FSE 1994, (1995) 196-211.

[20] L. Knudsen and M. Robshaw, *The Block Cipher Companion*, Information Security and Cryptography, Springer, 2001.

[21] P. V. Kumar, R. A. Scholtz, and L. R. Welch, *Generalized bent functions and their properties*, Journal of Combinatorial Theory, Series A, 40, (1985) 90-107.

[22] S. Lang, *Cyclotomic Fields* II. Graduate Texts in Mathematics, 69. Springer-Verlag, New York-Berlin, 1980.

[23] S. L. Ma, *A survey of partial difference sets*, Design, Codes and Cryptography, 4, (1994) 221–261.

[24] M. Matsui, *Linear cryptanalysis method for DES cipher*, Lecture Notes in Computer Science, Vol 765, EUROCRYPT 93, (1994) 55–64.

[25] W. Meier and O. Staffelbach. *Fast correlation attacks on stream cipher*, Advances in Cryptology, EUROCRYPT'88, Lecture Notes in Computer Science 330, (1988) 301-314.

[26] C. Milies and S. Sehgal, *An Introduction To Group Rings*, Algebras and applications, Volume 1. Springer, 2002.

[27] K. Nyberg, *Differentially uniform mappings for cryptography*, In Advances in cryptology, EUROCRYPT 93 (Lofthus, 1993), LNCS, volume 765, (1994) 55–64.

[28] A. Pott, *Nonlinear functions in abelian groups and relative difference sets*, Discrete Applied Mathematics 138, (2004) 177-193.

[29] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics, Volume 1601, Springer, 1995.

[30] A. Pott, Y. Tan, T. Feng and S. Ling, *Association schemes arising from bent functions*, Designs, Codes and Cryptography 59(1-3), (2011) 319-331.

[31] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley, New York, 1977.

[32] Y. Tan, A. Pott and T. Feng, *Strongly regular graphs associated with ternary bent functions*, Journal of Combinatorial Theory, Series A 117(6), (2010) 668–682.

[33] G. Weng, W. S. Qiu, Z. Wang and Q. Xiang, *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*, Designs, Codes and Cryptography, 44, (2007) 49–62.

Claude Carlet

LAGA, CNRS Department of Mathematics, Universities of Paris 8 and Paris 13, University of Paris 8, 2 rue de la liberté, 93526 Saint-Denis cedex 02, France

Email: `claude.carlet@univ-paris8.fr`

Yin Tan

Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada

Email: `y24tan@uwaterloo.ca`