HAL
archives-ouvertes.fr

Matriochka symmetric Boolean functions

Cédric Lauradoux, Marion Videau

▶ **To cite this version:**

Cédric Lauradoux, Marion Videau. Matriochka symmetric Boolean functions. IEEE International Symposium on Information Theory - ISIT 2008, Jul 2008, Toronto, Canada. IEEE, pp.1631-1635, 2008, <10.1109/ISIT.2008.4595264>. <inria-00338085>

HAL Id: inria-00338085
https://hal.inria.fr/inria-00338085

Submitted on 10 Nov 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Matriochka symmetric Boolean functions

Cédric Lauradoux
Princeton University
Department of Electrical Engineering
Princeton, NJ 08544, USA
claurado@princeton.edu

Marion Videau
Université Henri Poincaré, Nancy 1
LORIA
B.P. 239, 54506 Vandœuvre-lès-Nancy cedex, FRANCE
marion.videau@loria.fr

***Abstract*— We present the properties of a new class of Boolean functions defined as the sum of m symmetric functions with decreasing number of variables and degrees. The choice of this construction is justified by the possibility to study these functions by using tools existing for symmetric functions. On the one hand we show that the synthesis is well understood and give an upper bound on the gate complexity. On the other hand, we investigate the Walsh spectrum of the sum of two functions and get explicit formulae for the case of degree at most three.**

I. Introduction

Boolean functions play a critical role in the design of symmetric algorithms. There is an ongoing need to find functions of cryptographic significance and new methods to construct them. From a designer's point of view, the synthesis of the function is also critical but asymptotically it requires $\frac{2^n}{n}$ gates [Sha49]. Thus, it is highly valuable to find Boolean functions with relevant cryptographic properties and with low gate complexity.

The first attempt to mix the two requirements was done with symmetric Boolean functions. They deserve firstly attention in cryptography since they guarantee that no input variables has greater or lesser significance [Bru84]. Moreover, Shannon has shown in his early works [Sha49] that synthesising them requires at most n^2 gates. Following those results, their significant cryptographic properties have been systematically studied, *e.g.* in [Mit90], [YG95], [CV05]. Unfortunately, it seems that there are not enough good functions in this set. Most notably, it was proved in [Sav94], [MS02] and [Car04] that the highest possible nonlinearity for a function in this set is only achieved by quadratic functions. Moreover, in [vzGR97], the thorough study of several classes of symmetric Boolean functions has lead to the conjecture that these functions might be at most 3-resilient. As the symmetry property seems to be over-restrictive, new classes of Boolean functions have been proposed like rotation symmetric functions [SM03]. However, there is currently no results on their gate complexity.

In this paper, we propose a new construction based on symmetric functions. We consider the sum of m symmetric functions f_i with decreasing number of variables and degrees. We call this construction matriochka for the following hold: each circuit which implements f_i is nested in the circuit of f_{i-1}. This new class of functions is included in the set of partially symmetric functions as it was defined by Harrison [Har62], [AH63]. Then, we provide tools to derive the gate complexity (Section III) and the Walsh spectrum (Section IV) of our construction for the sum of two functions. Indeed, the Walsh spectrum of a Boolean function allows to derive directly its nonlinearity and its order of resiliency among other properties. We prove that the expression of the Walsh coefficients relies in this case on the periodically lacunary sums of Krawtchouk polynomials. In the case where degree is at most 3, we provide some explicit formulae.

II. Preliminary results and notation

In the rest of the paper, we will denote by $\mathcal{B}_n$ the set of Boolean functions of n variables, $f : \mathbf{F}_2^n \to \mathbf{F}_2$, and by $\mathcal{S}_n$ the set of all symmetric functions of n variables.

We also recall that for all f in $\mathcal{B}_n$ and for all vectorial subspaces $V \subset \mathbf{F}_2^n$, the *restriction of f to a coset of V* is the function defined by: $a \in \overline{V}, \forall y \in V,\ f_{a+V} : y \mapsto f(a+y)$, where $\overline{V} \oplus V = \mathbf{F}_2^n$. The function f_{a+V} can be immediately identified with a Boolean function in $\dim(V)$ variables.

A. Symmetric Boolean functions

Definition 1: A function $f \in \mathcal{B}_n$ is (*totally*) symmetric if its value is invariant under any permutation σ of its input bits:

$$f(x_1, x_2, \cdots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)}).$$

The value $f(x)$ only depends on the Hamming weight of x, denoted by $\mathrm{wt}(x)$, *i.e.* there exists a function $v_f : \{0, \ldots, n\} \to \mathbf{F}_2$ such that $f(x) = v_f(\mathrm{wt}(x))$. The vector $v(f) = (v_f(0), \ldots, v_f(n))$ is the *simplified value vector* of f.

Any Boolean function admits a unique representation by means of its algebraic normal form (ANF). More specifically, $f \in \mathcal{B}_n$ is symmetric if and only if its ANF is a linear combination of elementary symmetric polynomials:

$$f(x) = \bigoplus_{i=0}^{n} \lambda_f(i) X_{i,n}(x),\ \lambda_f(i) \in \mathbf{F}_2, \tag{1}$$

where $X_{i,n}$ is the elementary symmetric polynomial of degree i in n variables:

$$X_{i,n}(x) = \bigoplus_{1 \le j_1 < \cdots < j_i \le n} \prod_{k=1}^{i} x_{j_k}.$$

The ANF of f can be represented by the $(n+1)$-bit vector, $\lambda(f) = (\lambda_f(0), \ldots, \lambda_f(n))$, the *simplified ANF vector* of f.

In the sequel we will need the following lemma for the implementation of elementary symmetric polynomials.

978-1-4244-2571-6/08/$25.00 ©2008 IEEE

Lemma 2: The elementary symmetric functions verify:

$$X_{d+1,n} \oplus x_{n+1}X_{d,n} = X_{d+1,n+1} \quad \forall\, 0 \le d \le n \tag{2}$$

$$X_{d_1,n}X_{d_2,n} = \begin{cases} X_{d_1 \vee d_2,n} & \text{if } d_1 \vee d_2 \le n \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

Property (2) is simply the decomposition of $X_{d+1,n+1}$ on subspaces of dimension n and Property (3) can be viewed as a direct application of [CV05, Prop. 2]:

$$\forall i \in \{0,\dots,n\}, v_f(i) = \bigoplus_{k \preceq i} \lambda_f(k) \text{ and } \lambda_f(i) = \bigoplus_{k \preceq i} v_f(k),$$

where $(x_1,\dots,x_n) \preceq (y_1,\dots,y_n)$ if and only if $\forall i,\ x_i \le y_i$.

The above property is also at the basis of [CV05, Th. 1] which shows that the simplified value vector of a symmetric Boolean function with degree d such that $d < 2^t$ is periodic with period equal to 2^t, property that we will use in the sequel.

B. Matriochka Boolean functions

The matriochka construction is thought as a sum of functions of decreasing degrees defined on nested subspaces, hence the name of matriochka.

Definition 3: A Boolean matriochka function $h \in \mathcal{B}_n$ is defined by:

$$h(x) = \bigoplus_{i=1}^{m} f_i(\pi_{V_{n_i}}(x)),$$

where V_{n_i} is spanned by n_i vectors of the canonical basis of $\mathbf{F}_2^n$, $V_{n_i} = \langle e_{k_1},\dots,e_{k_{n_i}}\rangle$, $\pi_{V_i}(x)$ is the projection of x on V_i, $\mathbf{F}_2^n = V_{n_1} \supset \cdots \supset V_{n_m}$, $f_i : V_{n_i} \to \mathbf{F}_2$ and $\deg(f_1) \ge \cdots \ge \deg(f_m)$. We will call m the *depth* of the matriochka function.

We are interested in matriochka symmetric functions as our purpose is to explore a subset of partially symmetric functions. The constraints on the degrees and the inclusion of subspaces are related to the complexity of the implementation as it will be clarified in section III.

Definition 4: A function $h \in \mathcal{B}_n$ is matriochka symmetric, if all the functions in the sum of its matriochka expression are symmetric functions.

One can also notice that due to the symmetry property, it is equivalent to consider the subspaces spanned by the n_i first vectors of the canonical basis of $\mathbf{F}_2^n$ for matriochka symmetric functions. As a consequence, we will consider in the sequel that $V_{n_i} = \langle e_1,\dots,e_{n_i}\rangle$.

C. Restrictions of matriochka symmetric functions

The first idea is to study the restrictions to the cosets of the smallest subspace which means focusing on the restrictions of symmetric functions.

Proposition 5: [CV05, Prop. 7] Let f be in $\mathcal{S}_n$. Then for all $a \in \overline{V_k}$, the restriction of f to $a + V_k$ is symmetric in k variables and only depends on $\mathrm{wt}(a)$. Moreover the simplified value vector and the simplified ANF vector of f_{a+V_k} are given by: $\forall\ i,\ 0 \le i \le k$,

$$v_{f_{a+V_k}}(i) = v_f(i + \mathrm{wt}(a)) \quad \lambda_{f_{a+V_k}}(i) = \bigoplus_{j \preceq \mathrm{wt}(a)} \lambda_f(i+j).$$

This result also shows that the restrictions of f to all $a+V_k$, where $\deg(f) \le k \le n$, have degree $\deg(f)$ [CV05, Cor. 1].

We will also use a second corollary related to the degree of f and the periodicity of $v(f)$, that we deduce from [CV05, Prop. 7] and [CV05, Th. 1]. It shows that there are in fact at most $\min(n-k+1, 2^t)$, $\deg(f) < 2^t$, distinct restrictions to consider.

Corollary 6: Let consider $f \in \mathcal{S}_n$, $\deg(f) < 2^t$ and V_k. Then, the restrictions of f to all $a + V_k$, $a \in \overline{V_k}$, only depend on $\mathrm{wt}(a) \bmod (2^t)$.

These properties lead to the following characterisation of the restrictions of a matriochka symmetric function.

Proposition 7: Let $h \in \mathcal{B}_n$ be a matriochka symmetric function of depth m:

$$h(x) = \bigoplus_{i=1}^{m} f_i(\pi_{V_{n_i}}(x)).$$

Then for all $k \le n_m$ and $a \in \overline{V_k}$, the restriction of h to $a + V_k$ is a symmetric Boolean function of k variables which only depends on the vector:

$$L = \left(\ell_j = \mathrm{wt}(\pi_{V_{n_j}}(a)) \bmod (2^{\lfloor \log_2 \deg(h) \rfloor + 1}), 1 \le j \le m\right).$$

We will denote it $h_{L,k}$. Then, the simplified value vector and the simplified ANF vector of $h_{L,k}$ are given by: $\forall\ i,\ 0 \le i \le k$,

$$v_{h_{L,k}}(i) = \bigoplus_{j=1}^{m} v_{f_i}(i + \ell_j) \quad \lambda_{h_{L,k}}(i) = \bigoplus_{j=1}^{m} \bigoplus_{u \preceq \ell_j} \lambda_{f_i}(i+u).$$

III. Synthesis of the sum of symmetric functions

There exists several possibilities to synthesise symmetric functions and partially symmetric functions. For instance, Arnold and Harrisson [AH63] has proposed a representation and a synthesis using threshold functions. Numerous works exists on the synthesis of symmetric functions [AH63], [Nie81]. Here, we propose a synthesis based on the decomposition of all the symmetric functions f_i of the matriochka into elementary symmetric functions of degree 2^i. To compute all $X_{2^i,n}$, we use a network of half adders (HA). One half adder computes $X_{1,2} = x_1 \oplus x_2$, $X_{2,2} = x_1 \wedge x_2$ (one XOR gate and one AND gate). We can compute recursively all $X_{2^i,n}$, $i \ge 1$ by using the properties (2) and (3). For instance, the computation of $X_{4,5}$ is obtained in the following way:

$$X_{4,5} = x_5 X_{1,4} X_{2,4} \oplus x_4 X_{1,3} X_{2,3}.$$

While we compute all $X_{2^i,n}$, we obtain all the elementary symmetric functions $X_{2^i,n}$ for $n \le 5$ and $i \le 4$ as shown in Figure 1.

As a consequence, the elementary symmetric functions derived for the f_i, $i \ne 1$, are also obtained when we compute all $X_{2^i,n}$ derived from f_1. In a matriochka symmetric, the basic components X_{2^i,n_i} are nested. The next step in the construction of a matriochka symmetric consists in the computation of all X_{d,n_i} with $d \ne 2^j$ which are in the decomposition of f_i.

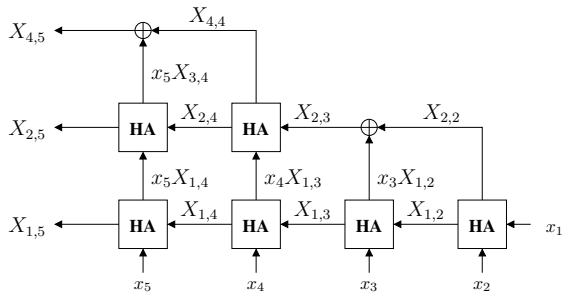

Fig. 1. Circuit for $X_{d,n}$, $n \leq 5$.

Proposition 8: Any elementary symmetric function $X_{d,n}$, can be computed with only one AND gate assuming that we have computed all $X_{j,n}$ such that $\mathrm{wt}(j) < \mathrm{wt}(d)$, $0 \leq j \leq d-1$.

Proof: Let consider that we have computed all $X_{j,n}$ with $\mathrm{wt}(j) = k-1$ and all functions $X_{2^i,n}$ such that $0 \leq i \leq \lfloor \log_2 d \rfloor$. Then, we can compute any function $X_{d,n}$ such that $\mathrm{wt}(d) = k$, by using the property 3:

$$X_{d,n} = X_{j,n} X_{2^i,n}$$

where $d \leq n$ and $d = 2^i \oplus j$ (if we want $\mathrm{wt}(d) = k$). ∎

Proposition 9: The gate complexity $\mathcal{C}$ of a matriochka symmetric function h on n variables is bounded by:

$$\mathcal{C}(h) \leq 2n\lfloor \log_2 d \rfloor + n - 2^{\lfloor \log_2 d \rfloor + 2} + 2d + 2dm - m^2 + m - \sum_{i=0}^{m} \lfloor \log_2(d-i+1) \rfloor + 1.$$

Proof: This upper bound is computed for $h = \bigoplus_{i=1}^{m} f_i$ on n variables such that:

$$wt(\lambda_{f_i}) = d - i + 2, \ i \in [1, m]$$

The synthesis of f is based on five components. The first three components are unchanged.

1. A HA network that computes all $X_{2^i,m}$, $0 \leq i \leq \lfloor \log_2 d \rfloor - 1$, $2^i \leq m \leq n$. There are $\lfloor \log_2 d \rfloor + 1$ stages, each stages consists of $(n - 2^{i+1} + 1)$ HAs and $(2^i - 1)$ XOR gates. Then, the complexity of the HA network is:
$$2n\lfloor \log_2 d \rfloor - 2^{\lfloor \log_2 d \rfloor + 2} + 2\lfloor \log_2 d \rfloor + 4.$$
2. For each stage of the HA network except the last one that will be treated differently, we have at the beginning of the stage a tree of XOR gates. These XOR gates can be view as the truncation of HAs since the computation of the product is equal to zero. For the i-th stage, there are $2^i - 1$ XOR gates at the beginning as said before. The complexity is:
$$\sum_{i=0}^{\lfloor \log_2 d \rfloor - 1} 2^i - 1 = 2^{\lfloor \log_2 d \rfloor} - \lfloor \log_2 d \rfloor - 1 \text{ XOR gates.}$$
3. The output of the last stage of the HA network are xored to compute $X_{2^{\lfloor \log_2 d \rfloor},n}$. There are $n - 2^{\lfloor \log_2 d \rfloor}$ XOR gates.
4. The fourth component computes all elementary symmetric functions of degree $k \neq 2^i$ but now it is for all functions f_i:
$$\sum_{i=1}^{m} \#\{k, \ 1 \leq k \leq d-i+1, \ wt(k) \neq 1\} = dm - \frac{1}{2}m(m+1) - \sum_{i=0}^{m} \lfloor \log_2(d-i+1) \rfloor.$$
5. The last component computes the sum of all elementary symmetric functions in the decomposition of each f_i using each time a XOR tree:
$$\sum_{i=1}^{m} (\mathrm{wt}(\lambda_{f_i}) - 1) = \sum_{i=1}^{m} (d-i+1) = dm - \frac{1}{2}m(m-1).$$

In addition, we also need $m-1$ XOR gates to sum all f_i functions. ∎

Proposition 10: The gate complexity $\mathcal{C}$ of $f \in \mathcal{S}_n$, $\deg(f) = d$ is:

$$C(f) \leq 2n\lfloor \log_2 d \rfloor + n - 2^{\lfloor \log_2 d \rfloor + 2} + 2d + 2.$$

Proof: This proposition is proved in the same way that the proposition 9 This upper bound is computed in a similar way than for a function f of degree d such that $wt(\lambda_f) = d+1$. ∎

With our construction, totally symmetric functions require $\mathcal{O}(n\lfloor \log_2 d \rfloor)$ gates, while a matriochka symmetric is $\mathcal{O}(n\lfloor \log_2 d \rfloor + md - m^2)$.

IV. Walsh spectrum of matriochka symmetric functions of depth 2

A. Walsh spectrum of symmetric functions

It is well known ([Sav94]) that symmetric functions are also characterised by the symmetry of their Walsh transform.

Proposition 11: The Walsh spectrum of $f \in \mathcal{S}_n$ can be summed up as a vector of $(n+1)$ integers $\mathsf{F}_f(j)$ given by:

$$\forall j, \ 0 \leq j \leq n, \quad \mathsf{F}_f(j) = \sum_{w=0}^{n} (-1)^{v_f(w)} P_w(j,n),$$

where P_w is the binary Krawtchouk polynomial of degree w, *i.e.* the coefficient of x^w in the expanded form of the polynomial $K_{j,n}(x) = (1-x)^j (1+x)^{(n-j)}$,

$$P_w(j,n) = \sum_{k=0}^{w} \binom{j}{k} \binom{n-j}{w-k} (-1)^k.$$

Using a generalisation of the technique used in [CV05, section VI] we are able to get an expression of the coefficients that can be particularly interesting for small degrees, *i.e.* small period of the simplified value vector.

Let $f \in \mathcal{S}_n$ with $\deg(f) < 2^\ell$. For $0 \le j \le n$:

$$\begin{aligned}\mathsf{F}_f(j) &= \sum_{w=0}^{2^\ell-1} (-1)^{v_f(w)} \sum_{\substack{0\le k\le n\\ k\equiv w \bmod 2^\ell}} P_k(j,n)\\ &= \sum_{w=0}^{2^\ell-1} (-1)^{v_w} S_{K_{j,n}}(w, 2^\ell).\end{aligned}$$

We call $S_{K_{j,n}}(w,T)$ the *periodically lacunary sum of Krawtchouk polynomials* of parameter (w,T). We will see in the sequel that we also need these values to express the Walsh spectrum of a matriochka symmetric function of depth 2. We show in IV-C how to handle the formula, especially for periodicity 4.

B. Matriochka symmetric functions

Proposition 12: Let consider $h \in \mathcal{B}_n$ a matriochka symmetric function of depth 2 and of degree d:

$$h(x) = f(x) + g(\pi_{V_m}(x))$$

$f \in \mathcal{S}_n$ and $g \in \mathcal{S}_m$ with $\deg(g) \le \deg(f)$ and $m < n$. For all $\alpha \in \mathbf{F}_2^n$, we write $\alpha = \alpha_1 + \alpha_2$ with $\alpha_1 \in \overline{V_m}$ and $\alpha_2 \in V_m$. Then the Walsh coefficients of h are given by:

$$\begin{aligned}&\mathcal{F}(h + \varphi_{\alpha_1+\alpha_2})\\ &= \sum_{k=0}^{2^{\lfloor \log_2 d\rfloor+1}-1} \mathsf{F}_{h_{k,m}}(\mathrm{wt}(\alpha_2)) S_{K_{\mathrm{wt}(\alpha_1),n-m}}(k, 2^{\lfloor \log_2 d\rfloor+1}).\end{aligned}$$

These coefficients only depends on $\mathrm{wt}(\alpha_1)$ and $\mathrm{wt}(\alpha_2)$. Thus it is possible to represent the Walsh spectrum of h as a vector of size $(n-m+1)(m+1)$.

Proof: This result is obtained using two facts. The first one consists in the expression of the Walsh coefficients of h using its restrictions. We get:

$$\mathcal{F}(h + \varphi_{\alpha_1+\alpha_2}) = \sum_{w=0}^{n-m} \mathsf{F}_{h_{w,m}}(\mathrm{wt}(\alpha_2)) P_w(\mathrm{wt}(\alpha_1), n-m).$$

The second fact is the corollary 6 which leads to our result. ∎

C. Lacunary sums of Krawtchouk polynomials

1) General expression: Using the formula of *series multisection* (see *e.g.* [Com74]), we get some explicit expressions for the lacunary sums of Krawtchouk polynomials:

$$S_{K_{j,n}}(w, 2^\ell) = \frac{1}{2^\ell} \sum_{t=0}^{2^\ell-1} e^{-\frac{2i\pi}{2^\ell} wt} K_{j,n}(e^{\frac{2i\pi}{2^\ell} t}), \text{ where } i^2 = -1.$$

When $T = 2^\ell$, we handle the formula by the use of trigonometric formulae. We get:

- when $j = 0$, $K_{0,n} = B_n$, sum of binomial coefficients:

$$\begin{aligned}S_{B_n}(w,T) &= 2^{n-\ell}\\ &+ 2^{1-\ell} \sum_{t=1}^{2^{\ell-1}-1} \cos\left(t(n-2w)\frac{\pi}{2^\ell}\right)\left(2\cos\left(t\frac{\pi}{2^\ell}\right)\right)^n\end{aligned}$$

- when $j = n$, $K_{n,n} = A_n$, alternated sum of binomial coefficients. When n is even:

$$\begin{aligned}S_{A_n}(w,T) &= (-1)^{\frac{j}{2}} \cos\left((n-2w)\frac{\pi}{2}\right) 2^{n-\ell}\\ &+ 2^{1-\ell} \sum_{t=1}^{2^{\ell-1}-1} (-1)^{\frac{n}{2}} \cos\left(t(n-2w)\frac{\pi}{2^\ell}\right)\left(2\sin\left(t\frac{\pi}{2^\ell}\right)\right)^n\end{aligned}$$

- when $j = n$, odd:

$$\begin{aligned}S_{A_n}(w,T) &= (-1)^{\frac{j}{2}} \sin\left((n-2w)\frac{\pi}{2}\right) 2^{n-\ell}\\ &+ 2^{1-\ell} \sum_{t=1}^{2^{\ell-1}-1} (-1)^{\frac{n-1}{2}} \sin\left(t(n-2w)\frac{\pi}{2^\ell}\right)\left(2\sin\left(t\frac{\pi}{2^\ell}\right)\right)^n\end{aligned}$$

- when j is even, $j \neq 0$ et $j \neq n$:

$$\begin{aligned}S_{K_{j,n}}(w, 2^\ell) &= 2^{1-\ell} \sum_{t=1}^{2^{\ell-1}-1} (-1)^{\frac{j}{2}} \cos\left(t(n-2w)\frac{\pi}{2^\ell}\right)\\ &\times \left(2\cos\left(t\frac{\pi}{2^\ell}\right)\right)^{n-j}\left(2\sin\left(t\frac{\pi}{2^\ell}\right)\right)^j\end{aligned}$$

- when j is odd, $j \neq 0$ et $j \neq n$:

$$\begin{aligned}S_{K_{j,n}}(w, 2^\ell) &= 2^{1-\ell} \sum_{t=1}^{2^{\ell-1}-1} (-1)^{\frac{j-1}{2}}\\ &\times \sin\left(t(n-2w)\frac{\pi}{2^\ell}\right)\left(2\cos\left(t\frac{\pi}{2^\ell}\right)\right)^{n-j}\left(2\sin\left(t\frac{\pi}{2^\ell}\right)\right)^j.\end{aligned}$$

2) The case of periodicity 4: The values of the lacunary sums depend on $n-2w \bmod 4$. For the sake of readability of the formulae, we will denote by (k) the case where $n-2w \equiv k \bmod 4$.

- when j is even, $j \neq 0$ and $j \neq n$,

$$S_{K_{j,n}}(w,4) = \begin{cases}(-1)^{\frac{j}{2}}(-1)^{\frac{n-2w}{4}} 2^{\frac{n}{2}-1} & \text{if } (0)\\ (-1)^{\frac{j}{2}}(-1)^{\frac{n-2w-1}{4}} 2^{\frac{n-3}{2}} & \text{if } (1)\\ 0 & \text{if } (2)\\ (-1)^{\frac{j}{2}}(-1)^{\frac{n-2w+1}{4}} 2^{\frac{n-3}{2}} & \text{if } (3)\end{cases}$$

- when j is odd, $j \neq 0$ and $j \neq n$,

$$S_{K_{j,n}}(w,4) = \begin{cases}0 & \text{if } (0)\\ (-1)^{\frac{j-1}{2}}(-1)^{\frac{n-2w-1}{4}} 2^{\frac{n-3}{2}} & \text{if } (1)\\ (-1)^{\frac{j-1}{2}}(-1)^{\frac{n-2w-2}{4}} 2^{\frac{n}{2}-1} & \text{if } (2)\\ (-1)^{\frac{j-1}{2}}(-1)^{\frac{n-2w-3}{4}} 2^{\frac{n-3}{2}} & \text{if } (3)\end{cases}$$

- when $j = 0$,

$$S_{B_n}(w,4) = \begin{cases}2^{n-2} + (-1)^{\frac{n-2w}{4}} 2^{\frac{n}{2}-1} & \text{if } (0)\\ 2^{n-2} + (-1)^{\frac{n-2w-1}{4}} 2^{\frac{n-3}{2}} & \text{if } (1)\\ 2^{n-2} & \text{if } (2)\\ 2^{n-2} + (-1)^{\frac{n-2w+1}{4}} 2^{\frac{n-3}{2}} & \text{if } (3)\end{cases}$$

- when $j = n$, n even,

$$S_{A_n}(w,4) = \begin{cases}(-1)^{\frac{n}{2}} 2^{n-2} + & \\ \quad (-1)^{\frac{n}{2}}(-1)^{\frac{n-2w}{4}} 2^{\frac{n}{2}-1} & \text{if } (0)\\ (-1)^{\frac{n}{2}+1} 2^{n-2} & \text{if } (2)\end{cases}$$

- when $j = n$, n odd,

$$S_{A_n}(w,4) = \begin{cases} (-1)^{\frac{n-1}{2}} 2^{n-2} + \\ \quad (-1)^{\frac{n-1}{2}} (-1)^{\frac{n-2w-1}{4}} 2^{\frac{n-3}{2}} & \text{if (1)} \\ (-1)^{\frac{n+1}{2}} 2^{n-2} + \\ \quad (-1)^{\frac{n-1}{2}} (-1)^{\frac{n-2w-3}{4}} 2^{\frac{n-3}{2}} & \text{if (2).} \end{cases}$$

D. Walsh coefficients of symmetric functions of degree 3

The explicit formulae (including the signs) for the Walsh coefficients of a symmetric Boolean function are known for functions of degree 2 [CV05] and the magnitude is known for functions of degree 3. We complete the formulae for functions of degree 3 thanks to the expressions of the lacunary sums of Krawtchouk polynomials we have derived in IV-C.

Proposition 13: Let $f \in \mathcal{S}_n$ be a function of degree 3, $n \geq 3$ with simplified ANF vector $\lambda(f) = (0, \lambda_1, \lambda_2, 1, 0, \ldots, 0)$, $\lambda_1,\ \lambda_2 \in \mathbf{F}_2$. If we denote by (k) the case $n \equiv k \bmod 4$, then its Walsh coefficient values are given by:

$$\mathsf{F}_f(0) = \left(1 + (-1)^{\lambda_1} + (-1)^{\lambda_2} + (-1)^{\lambda_1+\lambda_2+1}\right) 2^{n-2} + \begin{cases} (-1)^{\frac{n}{4}} (1 + (-1)^{\lambda_2+1}) 2^{\frac{n}{2}-1} & \text{if (0)} \\ (-1)^{\frac{n-1}{4}} (1 + (-1)^{\lambda_1} + (-1)^{\lambda_2+1} + \\ \quad (-1)^{\lambda_1+\lambda_2}) 2^{\frac{n-3}{2}} & \text{if (1)} \\ (-1)^{\frac{n-2}{4}} (-1)^{\lambda_1} (1 + (-1)^{\lambda_2}) 2^{\frac{n}{2}-1} & \text{if (2)} \\ (-1)^{\frac{n+1}{4}} (1 + (-1)^{\lambda_1+1} + (-1)^{\lambda_2+1} + \\ \quad (-1)^{\lambda_1+\lambda_2+1}) 2^{\frac{n-3}{2}} & \text{if (3)} \end{cases}$$

When j is even, $j \neq 0$ and $j \neq n$:

$$\mathsf{F}_f(j) = \begin{cases} (-1)^{\frac{j}{2}} (-1)^{\frac{n}{4}} (1 + (-1)^{\lambda_2+1}) 2^{\frac{n}{2}-1} & \text{if (0)} \\ (-1)^{\frac{j}{2}} (-1)^{\frac{n-1}{4}} (1 + (-1)^{\lambda_2+1} \\ \quad + (-1)^{\lambda_1} + (-1)^{\lambda_1+\lambda_2}) 2^{\frac{n-3}{2}} & \text{if (1)} \\ (-1)^{\frac{j}{2}} (-1)^{\frac{n-2}{4}} (-1)^{\lambda_1} (1 + (-1)^{\lambda_2}) 2^{\frac{n}{2}-1} & \text{if (2)} \\ (-1)^{\frac{j}{2}} (-1)^{\frac{n+1}{4}} (1 + (-1)^{\lambda_2+1} \\ \quad + (-1)^{\lambda_1+1} + (-1)^{\lambda_1+\lambda_2+1}) 2^{\frac{n-3}{2}} & \text{if (3)} \end{cases}$$

When j is odd, $j \neq n$:

$$\mathsf{F}_f(j) = \begin{cases} (-1)^{\frac{j-1}{2}} (-1)^{\frac{n}{4}-1} (-1)^{\lambda_1} (1 + (-1)^{\lambda_2}) 2^{\frac{n}{2}-1} & \text{if (0)} \\ (-1)^{\frac{j-1}{2}} (-1)^{\frac{n-1}{4}} (1 + (-1)^{\lambda_2+1} \\ \quad + (-1)^{\lambda_1+1} + (-1)^{\lambda_1+\lambda_2+1}) 2^{\frac{n-3}{2}} & \text{if (1)} \\ (-1)^{\frac{j-1}{2}} (-1)^{\frac{n-2}{4}} (1 + (-1)^{\lambda_2+1}) 2^{\frac{n}{2}-1} & \text{if (2)} \\ (-1)^{\frac{j-1}{2}} (-1)^{\frac{n-3}{4}} (1 + (-1)^{\lambda_2+1} \\ \quad + (-1)^{\lambda_1} + (-1)^{\lambda_1+\lambda_2}) 2^{\frac{n-3}{2}} & \text{if (3)} \end{cases}$$

When $j = n$, n even:

$$\mathsf{F}_f(n) = \begin{cases} 2^{n-2} \left(1 + (-1)^{\lambda_2} + (-1)^{\lambda_1+1} + (-1)^{\lambda_1+\lambda_2}\right) \\ \quad + (-1)^{\frac{n}{4}} 2^{\frac{n}{2}-1} \left(1 + (-1)^{\lambda_2+1}\right) & \text{if (0)} \\ 2^{n-2} \left(1 + (-1)^{\lambda_2} + (-1)^{\lambda_1+1} + (-1)^{\lambda_1+\lambda_2}\right) \\ \quad - (-1)^{\frac{n-2}{4}} 2^{\frac{n}{2}-1} \left((-1)^{\lambda_1} + (-1)^{\lambda_1+\lambda_2}\right) & \text{if (2)} \end{cases}$$

When $j = n$, n odd:

$$\mathsf{F}_f(n) = \begin{cases} 2^{n-2} \left(1 + (-1)^{\lambda_2} + (-1)^{\lambda_1+1} + (-1)^{\lambda_1+\lambda_2}\right) \\ \quad + (-1)^{\frac{n-1}{4}} 2^{\frac{n-3}{2}} (1 + (-1)^{\lambda_2+1} \\ \quad + (-1)^{\lambda_1+1} + (-1)^{\lambda_1+\lambda_2+1}) & \text{if (1)} \\ 2^{n-2} \left(1 + (-1)^{\lambda_2} + (-1)^{\lambda_1+1} + (-1)^{\lambda_1+\lambda_2}\right) \\ \quad - (-1)^{\frac{n-3}{4}} 2^{\frac{n-3}{2}} (1 + (-1)^{\lambda_1} + (-1)^{\lambda_2+1} \\ \quad + (-1)^{\lambda_1+\lambda_2}) & \text{if (3)} \end{cases}$$

V. Conclusion

In this paper, we have proposed the new set of matriochka symmetric functions as functions that may be suitable to investigate for cryptographic purposes as they have good implementation properties. We think that such a construction may give new ideas on how to find more suitable functions in regard of both implementation and security constraints. Towards the investigation of cryptographic properties, we have shown nice combinatorial properties arising from the study of this set of functions that has to be generalised. Most notably, finding a general expression of the lacunary sums of Krawtchouk polynomials for larger periods will be the next step in order to classify functions of higher degree.

References

[AH63] R. F. Arnold and M. A. Harrison. Algebraic Properties of Symmetric and Partially Symmetric Boolean Functions. *IEEE Trans. Comput.*, 12:244–251, 1963.

[Bru84] J. O. Bruer. On pseudorandom sequences as crypto generators. In *Proc. of the 1984 International Zurich Seminar on Digital Communications*, pages 157–161. IEEE, 1984.

[Car04] C. Carlet. On the Degree, Nonlinearity, Algebraic Thickness, and Nonnormality of Boolean Functions, With Developments on Symmetric Functions. *IEEE Trans. Inform. Theory*, 50(9):2178–2185, 2004.

[Com74] L. Comtet. *Advanced Combinatorics*. D. Reidel Pub. Co., 1974.

[CV05] A. Canteaut and M. Videau. Symmetric Boolean functions. *IEEE Trans. Inform. Theory*, 51(8):2791–2811, 2005.

[Har62] M. A. Harrison. Symmetric and partially symmetric Boolean functions. Technical report, University of Michigan, 1962.

[Mit90] C. J. Mitchell. Enumerating Boolean Functions of Cryptographic Significance. *J. Cryptology*, 2(3):155–170, 1990.

[MS02] S. Maitra and P. Sarkar. Maximum nonlinearity of symmetric Boolean functions on odd number of variables. *IEEE Trans. Inform. Theory*, 48(9):2626–2630, 2002.

[Nie81] H. A. Nienhaus. Efficient multiplexer realizations of symmetric functions. *Southeastcon '81*, 15:522–525, 1981.

[Sav94] P. Savicky. On the Bent Functions That are Symmetric. *European J. Combin.*, 15:407–410, 1994.

[Sha49] C. E. Shannon. The synthesis of two-terminal switching circuits. *Bell System Technical Journal*, 28:59–98, 1949.

[SM03] P. Stanica and S. Maitra. A constructive count of rotation symmetric functions. *Inform. Process. Lett.*, 88(6):299–304, 2003.

[vzGR97] J. von zur Gathen and J. R. Roche. Polynomials with two values. *Combinatorica*, 17(3):345–362, 1997.

[YG95] Y. Xian Yang and B. Guo. Further enumerating Boolean functions of cryptographic significance. *J. Cryptology*, 8(3):115–122, 1995.