

# Weightwise Almost Perfectly Balanced Functions, Construction From A Permutation Group Action View (Extended Abstract).

Deepak Kumar Dalai<sup>1</sup>, Krishna Mallick<sup>2</sup>, Pierrick Méaux<sup>3</sup>

<sup>1</sup> School of Mathematical Sciences, National Institute of Science Education and Research, HBNI,  
Bhubaneswar, Odisha 752050, India.

`deepak@niser.ac.in`

<sup>2</sup> School of Computer Sciences, National Institute of Science Education and Research, HBNI,  
Bhubaneswar, Odisha 752050, India.

`krishna.mallick@niser.ac.in`

<sup>3</sup> University of Luxembourg, Luxembourg

`pierrick.meaux@uni.lu`

**Abstract.** The construction of Boolean functions with good cryptographic properties over a subset of vectors with fixed Hamming weight  $E_{k,n} \subset \mathbb{F}_2^n$  is significant in lightweight stream ciphers like FLIP [MJSC16]. We have presented a general idea to construct a class of weightwise almost perfectly balanced (WAPB) Boolean functions by using the action of a cyclic permutation group on  $\mathbb{F}_2^n$ . Further, considering a special permutation group  $\langle \psi_n \rangle$  (where  $\psi_n$  is a special type of permutation on  $n$  elements), we present a class of WAPB Boolean functions on  $n$  variables. This class generalizes the weightwise perfectly balanced (WPB) Boolean function construction by Liu and Mesnager [LM19]. Further, we studied the nonlinearity and weightwise nonlinearities of this class of functions.

## 1 Introduction

An  $n$ -variable Boolean function  $f$  is a mapping from the  $n$ -dimensional vector space  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$ , where  $\mathbb{F}_2$  is a finite field with two elements  $\{0, 1\}$ . Depending upon the underlying algebraic structure, ‘+’ symbol is used for the addition operation in both  $\mathbb{F}_2$  and  $\mathbb{R}$ . Generally, the cryptographic criteria of the Boolean functions are defined over the entire domain of vector space  $\mathbb{F}_2^n$ . The study of the Boolean functions over a restricted domain became interesting after the proposal of the stream cipher FLIP in 2016 [MJSC16]. In this stream cipher, the Hamming weight of the inputs to the filter function is  $\frac{n}{2}$ . An initial cryptographic study of Boolean function in a restricted domain is introduced by Carlet et al. in [CMR17]. The Boolean functions balanced over the subsets of  $\mathbb{F}_2^n$  containing vectors with constant Hamming weight are said to be weightwise perfectly balanced (WPB). The first weightwise perfectly balanced (WPB) Boolean function construction was introduced in [CMR17] in 2017. There are several studies and constructions [TL19, LM19, LS20, MS21, Su21, ZS22, GM22a, GM22b, GM23, ZLC<sup>+</sup>23, DM24] of WPB and WAPB functions available in the literature. Liu and Mesnager [LM19] presented a class of WPB Boolean functions that are 2-rotation symmetric. These functions have the best weightwise nonlinearities and nonlinearity compared to the available constructions till now. In this paper, we have generalized this construction to get a class of WAPB Boolean functions for any number of variables.

## 2 Preliminaries

Let  $\mathcal{B}_n$  be the set of all  $n$ -variable Boolean functions. The  $2^n$ -length binary sequence  $(f(v_0), f(v_1), \dots, f(v_{2^n-1}))$  is called as the *truth table* of the Boolean function  $f$ , it corresponds to the ordered vectors of  $\mathbb{F}_2^n$  as  $v_0 = (0, 0, \dots, 0), v_1 = (0, 0, \dots, 1), \dots, v_{2^n-1} = (1, 1, \dots, 1)$ . The *Hamming weight* of a vector  $x \in \mathbb{F}_2^n$ , denoted by  $w_H(x)$ , is the number nonzero coordinates (i.e., 1s) in the vector  $x$ . The *support* of  $f \in \mathcal{B}_n$ , denoted by  $\text{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$ . The *Hamming weight* of the Boolean function  $f$  is  $w_H(f) = |\text{supp}(f)|$ . The function  $f$  is called *balanced* if  $w_H(f) = 2^{n-1}$ . Let  $f(x), g(x) \in \mathcal{B}_n$ , then the *Hamming distance* between two Boolean functions  $f, g \in \mathcal{B}_n$  is defined by  $d_H(f, g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}|$  i.e.,  $d_H(f, g) = w_H(f + g)$ .

An  $n$ -variable Boolean function  $f$  can be expressed as a polynomial in the ring  $\mathbb{F}_2[x_1, x_2, \dots, x_n]/\langle x_1^2 + x_1, x_2^2 + x_2, \dots, x_n^2 + x_n \rangle$ , i.e.  $f(x) = \sum_{u \in \mathbb{F}_2^n} c_u x^{u_1} x^{u_2} \dots x^{u_n}$ , where  $c_u$  are the coefficients with a value in  $\mathbb{F}_2$ . It is called as the *algebraic normal form* or ANF and the number of variables in the highest order monomial with nonzero coefficient is called the *algebraic degree* of the function  $f$ , and denoted as  $\deg(f)$ . A function  $f$  is called as *affine function* if  $f(x) = a \cdot x + b$  for  $a \in \mathbb{F}_2^n$  and  $b \in \mathbb{F}_2$ . If  $b = 0$ , then  $f$  is also called a *linear* Boolean function.  $\mathcal{A}_n$  denotes the set of all  $n$ -variable affine functions.

The *Walsh-Hadamard transform* of a function on  $\mathbb{F}_2^n$  is the map  $W_f : \mathbb{F}_2^n \rightarrow \mathbb{R}$ , defined by

$$W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + w \cdot x}.$$

The *nonlinearity* of  $f \in \mathcal{B}_n$  denoted as  $\text{NL}(f)$ , is the minimum Hamming distance of  $f$  to any affine function. That is,  $\text{NL}(f) = \min_{g \in \mathcal{A}_n} d_H(f, g)$ . It can be verified that  $\text{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} |W_f(w)|$ .

We denote  $E_{k,n} = \{x \in \mathbb{F}_2^n : w_H(x) = k\}$  and  $w_{k,n}(f) = |\{x \in E_{k,n} : f(x) = 1\}| = |\text{supp}(f) \cap E_{k,n}|$ . Accordingly, the Hamming distance of two functions  $f, g \in \mathcal{B}_n$  on  $E_{k,n}$  denoted as  $d_{k,n}(f, g) = |\{x \in E_{k,n} : f(x) \neq g(x)\}|$ . The cryptographic criteria like balancedness, nonlinearity and algebraic immunity of a function  $f$  defined over  $\mathbb{F}_2^n$  can also be defined, if we restrict  $f$  to the set  $E_{k,n}$ . For two integers  $m, n$  with  $m \leq n$ , we define  $[m, n] = \{m, m+1, \dots, n\}$ .

A Boolean function  $f \in \mathcal{B}_n$  is said to be *weightwise almost perfectly balanced* (WAPB) if for all  $k \in [0, n]$ ,

$$w_{k,n}(f) = \left( \binom{n}{k} \pm \left( \binom{n}{k} \bmod 2 \right) \right) / 2.$$

A Boolean function  $f \in \mathcal{B}_n$  is said to be *weightwise perfectly balanced* (WPB) if

$$w_{n,k}(f) = \binom{n}{k} / 2, \text{ for all } k \in [1, n-1] \text{ and } f(0, 0, \dots, 0) = 1 + f(1, 1, \dots, 1).$$

Using Lucas' Theorem [Fin47], we have that a WPB function exists only if,  $n$  is a power of 2.

Let  $f$  be an  $n$ -variable Boolean function, then its *weightwise Walsh transform*  $\mathcal{W}_{f,k}(a)$  is defined as:

$$\mathcal{W}_{f,k}(a) = \sum_{x \in E_{k,n}} (-1)^{f(x) + a \cdot x}.$$

The *weightwise nonlinearity* of  $f \in \mathcal{B}_n$  over  $E_{k,n}$ , denoted as  $\text{NL}_k(f)$ , is the Hamming distance of  $f$  to the set of all affine functions  $\mathcal{A}_n$  when evaluated over  $E_{k,n}$ . That is,  $\text{NL}_k(f) = \min_{g \in \mathcal{A}_n} d_{k,n}(f, g) = \min_{g \in \mathcal{A}_n} w_{k,n}(f+g)$ .

The following identity and upper bound on the nonlinearity of a Boolean function over  $E_{k,n}$  is presented in [CMR17]. If  $f \in \mathcal{B}_n$  then for  $k \in [0, n]$ ,

$$\text{NL}_k(f) = \frac{|E_{k,n}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |\mathcal{W}_{f,k}(a)|, \text{ and } \text{NL}_k(f) \leq \frac{1}{2} [|E_{k,n}| - \sqrt{|E_{k,n}|}] = \frac{1}{2} \left[ \binom{n}{k} - \sqrt{\binom{n}{k}} \right].$$

For a positive integer  $n$ , the *Krawtchouk polynomial* [MS78, Page 151] of degree  $k$  is given by

$$\mathcal{K}_k(x, n) = \sum_{j=0}^k (-1)^j \binom{x}{j} \binom{n-x}{k-j} \text{ for } k = 0, 1, \dots, n.$$

Let denote  $P = \langle \rho_n \rangle$  be the cyclic permutation group generated by the permutation  $\rho_n$ . Let  $\mathcal{O} = \{\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_{g_n}\}$  be the set of orbits obtained due the action of  $P$  on  $\mathbb{F}_2^n$ . An orbit leader/representative  $\nu_{\mathcal{O}}$  is chosen for each orbit  $\mathcal{O} \in \mathcal{O}$ . The representatives can be chosen using some ordering, for example it may be the lexicographically smallest element in the orbit.

A Boolean function  $f$  is *2-rotation symmetric* (2-RotS) if and only if for every orbit  $O \in \mathcal{O}$  with representative element  $\nu$ ,

$$f(\rho_n^{2i}(\nu)) = f(\nu) \text{ for every } 1 \leq i < \frac{|O|}{2}; \quad f(\rho_n^{2i-1}(\nu)) = f(\nu) + 1 \text{ for every } 1 \leq i \leq \frac{|O|}{2}.$$

Therefore, 2-RotS Boolean functions have the alternative truth value for the lexicographically ordered vectors in every orbit obtained by the action of permutation group  $P$  on  $\mathbb{F}_2^n$ . As example, a 2-RotS Boolean function on  $n = 5$  satisfies  $f(00001) = f(00100) = f(10000)$  and  $f(00010) = f(01000) = 1 + f(00001)$  for the orbit  $\{00001, 00010, \dots, 10000\}$  with representative 00001.

A construction of a class of 2-RotS WPB Boolean functions is presented by Liu and Mesnager [LM19].

**Proposition 1.** [LM19] *For a Boolean function  $f \in \mathcal{B}_n$  with  $n$  is power of 2, if  $f(x^2) = f(x) + 1$  holds for all  $x \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ , then  $f$  is WPB.*

Since,  $n$  is the power of 2 in the construction proposed in Proposition 1, the cardinality of all orbits in  $\mathbb{F}_{2^n} \setminus \{0, 1\}$  are even. Therefore,  $f(x^2) = f(x) + 1, x \in \mathbb{F}_{2^n} \setminus \{0, 1\}$  is well defined and hence, the truth value 1 and 0 can be assigned alternatively to the half of the vectors in the each orbit. This cannot be assigned when  $n$  is not a power of 2, as some orbits have odd cardinality; therefore, the condition  $f(x^2) = f(x) + 1$  cannot be defined. However, we propose a generalization of this concept in Section 3 to construct WAPB Boolean function for any  $n$  where  $n$  is a natural number in Section 3.

### 3 Construction of WAPB Boolean functions using Group action

In this section, we present a general approach to constructing 2-RotS WAPB Boolean functions using the action of a cyclic permutation group. Let  $G = \langle \pi \rangle$  be a cyclic subgroup of the symmetric group  $\mathbb{S}_n$  on  $n$  elements. The action of  $G$  on  $\mathbb{F}_2^n$  partitions the set into  $g_n$  number of orbits. The orbit generated by  $x \in \mathbb{F}_2^n$  is denoted by  $O_\pi(x) = \{g(x) : g \in G\} = \{x, \pi(x), \pi^2(x), \dots, \pi^{l-1}(x)\}$  where  $l$  is the order of the permutation  $\pi$ . Since  $w_H(\pi^i(x)) = w_H(x)$  for  $1 \leq i \leq l-1$ , the group action of  $G$  splits  $E_{k,n}$  into orbits, we denote by  $g_{k,n}$  the number of orbits in  $E_{k,n}$ , and by  $\nu_{k,n,i}$  the orbit representative of the  $i$ -th orbit  $E_{k,n}$  following some ordering. The construction of 2-RotS WAPB Boolean functions is outlined as follows.

---

#### Construction 1 Construction of 2-RotS WAPB Boolean function

---

**Input:**  $\pi \in \mathbb{S}_n$

**Output:** A 2-RotS WAPB Boolean function  $f_\pi \in \mathcal{B}_n$

Initiate  $\text{supp}(f_\pi) = \emptyset$ , and  $t = 0$

for  $k \leftarrow 0$  to  $n$  do

for  $i \leftarrow 1$  to  $g_{k,n}$  do

$u = \nu_{k,n,i}; l = |O_\pi(u)|$

if  $l$  is even then

for  $j \leftarrow 1$  to  $\frac{l}{2}$  do

$\text{supp}(f_\pi).append(u); u \leftarrow \pi \circ \pi(u)$

end for

else

$u = \pi^t(u)$

for  $j \leftarrow 1$  to  $\lceil \frac{l-t}{2} \rceil$  do

$\text{supp}(f_\pi).append(u); u \leftarrow \pi \circ \pi(u)$

end for

Update  $t \leftarrow 1 - t$

end if

end for

end for

return  $f_\pi$

---

Construction 1 ensures a balanced WAPB Boolean function. The binary variable  $t$  indicates whether the partially constructed is balanced (when  $t = 0$ ) or having an extra 1 (when  $t = 1$ ) during each iteration of orbits.

*Example 1.* Consider  $n = 5$  and the permutation  $\pi = \rho_n$  is the cyclic rotation. Then considering the orbits with representatives 00000, 00001, 00011, 00101, 00111, 01011, 01111, 11111, we have the resultant function  $f_{\rho_n} \in \mathcal{B}_5$  of Construction 1 as  $\text{supp}(f_{\rho_n}) = \{00000, 00010, 01000, 00011, 01100, 10001, 01010, 01001, 00111, 11100, 10011, 10110, 11010, 01111, 11101, 10111\}$  is a 2-RotS WAPB Boolean function.

## 4 Extending Liu-Mesnager construction [LM19] for WAPB Boolean function

In this section, we present a class of 2-RotS WAPB Boolean function which is a special case of the construction presented in Section 3. This construction extends the idea of Liu-Mesnager construction [LM19] to generate WAPB Boolean functions. As Liu-Mesnager construction outputs a WPB Boolean function, the form of  $n$  (the number of variable) needs to be a power of 2. However, in our case, the number of variables  $n$  can be any positive integer for generating a WAPB Boolean function. Let  $n$  be a positive integer with binary representation

$$n = n_1 + n_2 + \dots + n_w \text{ where } n_1 = 2^{a_1}, n_2 = 2^{a_2}, \dots, n_w = 2^{a_w} \text{ and } 0 \leq a_1 < a_2 < \dots < a_w. \quad (1)$$

We denote  $w_H(n) = w$  i.e. the number of 1's in the binary representation of  $n$ . Consider the cyclic subgroup  $G = \langle \psi \rangle$  of the symmetric group  $\mathbb{S}_n$ , where the disjoint cycle form of  $\psi$  contains cycles of length  $n_1, n_2, \dots, n_w$ . Without loss of generality, consider

$$\psi = (x_1, x_2, \dots, x_{n_1})(x_{n_1+1}, x_{n_1+2}, \dots, x_{n_1+n_2}) \cdots (x_{n-n_w+1}, x_{n-n_w+2}, \dots, x_n). \quad (2)$$

Hence, for  $x = (x_1, x_2, \dots, x_n)$ , we have

$$\psi(x) = (\rho_{n_1}(x_1, \dots, x_{n_1}), \rho_{n_2}(x_{n_1+1}, \dots, x_{n_1+n_2}), \dots, \rho_{n_w}(x_{n-n_w+1}, \dots, x_n)) \quad (3)$$

where  $\rho_{n_i}$  is the cyclic shift permutation on  $n_i$  elements. Here,  $\text{ord}(\psi) = 2^{a_w} = n_w$ . Hence, the cardinality of orbits obtained due the action of  $G$  on  $\mathbb{F}_2^n$  are of power of 2 i.e.,  $|O_\psi(x)| = 2^l$  where  $0 \leq l \leq a_w$  for  $x \in \mathbb{F}_2^n$ . Hence, there are some orbits of cardinality 1 and the rest are of even cardinality.

**Lemma 1.** *Let  $n$  be a positive integer and  $\psi \in \mathbb{S}_n$  as in Equation 2. Then there are  $2^w$  orbits of cardinality 1 where  $w = w_H(n)$ .*

Since every orbit contains vectors of the same weight, we define the weight of an orbit as the weight of the vectors within that orbit i.e.  $w_H(O_\psi(x)) = w_H(x)$  for  $x \in \mathbb{F}_2^n$ . Further, for  $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_2^n$ , we say  $y$  covers  $x$  (i.e.  $x \preceq y$ ), if  $x_i \leq y_i, \forall 1 \leq i \leq n$  i.e.  $y_i = 1$  if  $x_i = 1, \forall 1 \leq i \leq n$ . Similarly, given two positive integers  $n$  and  $k$  with binary representation  $n = 2^{a_1} + 2^{a_2} + \dots + 2^{a_w}$  and  $k = 2^{b_1} + 2^{b_2} + \dots + 2^{b_t}$ , we denote  $k \preceq n$  if  $\{b_1, b_2, \dots, b_t\} \subseteq \{a_1, a_2, \dots, a_w\}$ .

**Lemma 2.** *Let  $n$  be a positive integer and  $\psi \in \mathbb{S}_n$  as in Equation 2. For  $k \in [0, n]$ , the number of orbits of weight  $k$  and cardinality 1 is 1 if  $k \preceq n$ , otherwise it is 0.*

Let  $\mathcal{O}$  denote the set of all orbits resulting from the action of  $\psi$  on  $\mathbb{F}_2^n$ . Further, we denote by  $\mathcal{O}_o$  the set of orbits of odd cardinality (i.e. here 1) and we denote by  $\mathcal{O}_e$  the set of orbits of even cardinality. Since the cardinality of all orbits of odd cardinality is 1, abusing the notation, we also denote  $\mathcal{O}_o$  as the set of all vectors belonging in the orbits of odd cardinality. Hence  $\mathcal{O}_o = \{(x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n : x_1 = x_2 = \dots = x_{n_1}; x_{n_1+1} = x_{n_1+2} = \dots = x_{n_1+n_2}; \dots; x_{n-n_w+1} = x_{n-n_w+2} = \dots = x_n\}$ . For example, if  $n = 6$ , there are  $2^{w_H(6)} = 2^2 = 4$  orbits of weight 1 and  $\mathcal{O}_o = \{000000, 000011, 111100, 111111\}$ .

By choosing such permutation  $\psi$  for Construction 1, we ensure that every slice  $E_{k,n}$ , for  $0 \leq k \leq n$ , contains at most one orbit of odd cardinality (namely, 1). Consequently, it becomes simple to construct 2-RotS WAPB functions, as the remaining orbits are of even cardinality. hence, we get the following result.

**Proposition 2.** *Let  $n$  be a positive integer and  $\psi \in \mathbb{S}_n$  as in Equation 2. For a Boolean function  $f_\psi \in \mathcal{B}_n$ , if  $f_\psi(\psi(x)) = 1 + f_\psi(x)$  holds for all  $x \in \mathbb{F}_2^n \setminus \mathcal{O}_o$  where  $\mathcal{O}_o$  is the set of vectors whose orbit cardinality is 1, then  $f_\psi$  is WAPB.*

---

**Construction 2** Construction of 2-RoS WAPB Boolean function using  $\psi \in \mathbb{S}_n$ 


---

**Input:**  $\psi \in \mathbb{S}_n$  as in Equation 2

**Output:** A 2-RoS WAPB Boolean function  $f_\psi \in \mathcal{B}_n$

For every orbit  $O$  in  $\mathbb{F}_2^n$  due to the action of  $G = \langle \psi \rangle$ , do the following:

if  $|O|$  is even **then**

$f$  satisfies  $f_\psi(\psi(x)) = 1 + f(x)$  for  $x \in O$

**end if**

if  $|O| = 1$  **then**

assign  $f_\psi(x) = 0$  or  $1$  to make  $f$  balanced.

**end if**

**return**  $f_\psi$

---

Hence, when  $n = 2^m$ , a power of 2,  $\psi = \rho_n$  and Construction 1 on input  $\psi \in \mathbb{S}_n$  results in the 2-RoS WPB Boolean function by Liu and Mesnager [LM19]. A simplified version of Construction 1 is presented in Construction 2 for input  $\psi$ .

**Theorem 1.** *The number of orbits generated due the action of  $\psi$  on  $\mathbb{F}_2^n$  is  $g_n = \frac{1}{n_w} \sum_{k=1}^{n_w} 2^{\gcd(n_1, k) + \gcd(n_2, k) + \dots + \gcd(n_w, k)}$ .*

There are  $2^w$  many orbits of cardinality 1 and the remaining  $g_n - 2^w$  orbits have even cardinality. Hence,  $\binom{2^w}{2^{w-1}} \times 2^{g_n - 2^w}$  WAPB Boolean functions can be generated using Construction 2. Now, we will study some cryptographic properties of the function  $f_\psi \in \mathcal{B}_n$ .

**Theorem 2.** *Let  $n \geq 2$  be an positive integer as in Equation 1 and  $\psi \in \mathbb{S}_n$  as in Equation 2. Then  $NL(f_\psi) \geq 2^{n-2} - 2^{w-1}$ .*

In the following table we present the maximum and minimum nonlinearity among all  $f_\psi$  for the number of variables  $n = \{4, 5, \dots, 10\}$  along with the upperbound of balanced Boolean functions and lowerbound of  $f_\psi$  as per Theorem 2. We have searched all such Boolean functions for  $n \leq 6$  and from  $2^{20}$  randomly chosen such Boolean functions for  $n > 6$ .

$n$	4	5	6	7	8	9	10
Number of functions	$2^4 \times \binom{2}{1} = 2^5$	$2^8 \times \binom{4}{2} = 3 \times 2^9$	$2^{18} \times \binom{4}{2} = 3 \times 2^{19}$	$2^{36} \times \binom{8}{4} = 35 \times 2^{37}$	$2^{34} \times \binom{2}{1} = 2^{35}$	$2^{68} \times \binom{4}{2} = 3 \times 2^{69}$	$2^{138} \times \binom{4}{2} = 3 \times 2^{139}$
Max Nonlinearity	4	12	26	56	116	236	480
% functions at max nl	100	22.917	0.651042	0.304318	0.008297	0.072575	0.013638
Nonlinearity upper bound	4	12	26	56	116	240	492
Min Nonlinearity	4	6	14	28	64	192	328
% functions at min nl	100	4.17	0.260417	0.014687	0.006199	0.000191	$2^{-20}$
Nonlinearity lower bound	3	6	14	28	63	144	254

Now we study the weightwise nonlinearity of  $f_\psi$ .

**Theorem 3.** *Let  $n \geq 2$  be an positive integer as in Equation 1 and  $\psi \in \mathbb{S}_n$  as in Equation 2. Then*

$$NL_k(f) \geq \frac{1}{4} \left( \binom{n}{k} + \min_{0 \leq l \leq n} K_k(l, n) - 2 \right).$$

## 5 Conclusions and Future work

We have presented a construction of a class of WAPB Boolean functions in  $n$  variables, utilizing the group action of a cyclic permutation group. Considering a special permutation  $\psi_n$ , this class of WAPB Boolean functions generalizes the WBP construction proposed by Liu and Mesnager [LM19]. Subsequently, we studied the nonlinearity and weightwise nonlinearities of this class of Boolean functions. For our future work, we will explore additional cryptographic properties such as algebraic immunity and weightwise algebraic immunities for this class of functions.

## References

- CMR17. Claude Carlet, Pierrick Méaux, and Yann Rotella. Boolean functions with restricted input and their robustness; application to the FLIP cipher. *IACR Trans. Symmetric Cryptol.*, 2017(3), 2017.
- DM24. Deepak Kumar Dalai and Krishna Mallick. A class of weightwise almost perfectly balanced boolean functions. *Advances in Mathematics of Communications*, 18(2):480–504, 2024.
- Fin47. N. J. Fine. Binomial coefficients modulo a prime. *The American Mathematical Monthly*, 54(10):589–592, 1947.
- GM22a. Agnese Gini and Pierrick Méaux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discret. Appl. Math.*, 322:320–341, 2022.
- GM22b. Agnese Gini and Pierrick Méaux. Weightwise almost perfectly balanced functions: Secondary constructions for all  $n$  and better weightwise nonlinearities. In *Progress in Cryptology - INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 492–514. Springer, 2022.
- GM23. Agnese Gini and Pierrick Méaux. On the algebraic immunity of weightwise perfectly balanced functions. In *LATINCRYPT*, volume 14168 of *Lecture Notes in Computer Science*, pages 3–23. Springer, 2023.
- LM19. Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Des. Codes Cryptogr.*, 87(8):1797–1813, 2019.
- LS20. Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced boolean functions with high weightwise nonlinearity. *Discret. Appl. Math.*, 279:218–227, 2020.
- MJSC16. Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. pages 311–343, 2016.
- MS78. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1978.
- MS21. Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced boolean functions. *Cryptography and Communications*, 2021.
- Su21. Sihong Su. The lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced functions. *Discret. Appl. Math.*, 297:60–70, 2021.
- TL19. Deng Tang and Jian Liu. A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity. *Cryptogr. Commun.*, 11(6):1185–1197, 2019.
- ZLC<sup>+</sup>23. Qinglan Zhao, Mengran Li, Zhixiong Chen, Baodong Qin, and Dong Zheng. A unified construction of weightwise perfectly balanced boolean functions. *Discrete Applied Mathematics*, 337:190–201, 2023.
- ZS22. Linya Zhu and Sihong Su. A systematic method of constructing weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. *Discrete Applied Mathematics*, 314:181–190, 2022.