Weightwise Almost Perfectly Balanced Functions, Construction From A Permutation Group Action View.

No Author Given

No Institute Given

Abstract. The construction of Boolean functions with good cryptographic properties over a subset of vectors with fixed Hamming weight is significant in lightweight stream ciphers like FLIP. We present 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 particular permutation group $\langle\psi_n\rangle$ (where ψ_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. Further, we studied the nonlinearity and weightwise nonlinearities of this class of functions.

Keywords: Boolean function, Weightwise perfectly balanced (WPB), Weightwise almost perfectly balanced (WAPB), Nonlinearity

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 $\mathbb{F}_2$ denotes a finite field with two elements $\{0,1\}$. Depending upon the underlying algebraic structure, the symbol'+' is to indicate addition operations in both $\mathbb{F}_2$ and $\mathbb{R}$. Typically, the cryptographic criteria of the Boolean functions are defined over the entire domain of vector space $\mathbb{F}_2^n$. However, the study of Boolean functions over restricted domains gained interest following the introduction of the stream cipher FLIP in 2016 [MJSC16]. In FLIP, the inputs to the filter function have a fixed Hamming weight of $\frac{n}{2}$. An initial cryptographic study of Boolean function in a restricted domain was conducted by Carlet et al. in [CMR17]. Boolean functions that are balanced over the subsets of $\mathbb{F}_2^n$ containing vectors with constant Hamming weight are said to be Weightwise Perfectly Balanced (WPB). Such functions exist only when n is a power of two,; otherwise, only functions that are *almost balanced* can exist. Here, *almost balanced* means that the counts of preimages of 0 and 1 differ by at most one. Functions that are almost balanced on each subset of constant Hamming weight are termed Weightwise Almost Perfectly Balanced (WAPB).

The first weightwise perfectly balanced (WPB) Boolean function construction was introduced in [CMR17] in 2017. Multiple studies and constructions [TL19, LM19, LS20, MS21, Su21, ZS22, GM22a, MPJ+22, MKL22, GM22b, MSLZ22, GS22, GM23c, GM23b, ZLC+23, DM23, ZS23, ZJZQ23, YCL+23, GM23a, DM24, Méa24] of WPB and WAPB functions are 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 compared to the currently available constructions. In this article, we have generalize this construction to create a class of WAPB Boolean functions for any number of variables.

[**PM:** add more detailed contribution part]

2 Preliminaries

Let $\mathbb{F}_2^n$ be the vector space of dimension n over the binary field $\mathbb{F}_2$. For any two vectors $a=(a_1,a_2,\dots,a_n)$ and $b=(b_1,b_2,\dots,b_n)$ in $\mathbb{F}_2^n$, the dot product is defined as $a\cdot b=a_1b_1+a_2b_2+\cdots+a_nb_n \bmod 2$.

A Boolean function of n variables is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and $\mathcal{B}_n$ is 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 $v_0=(0,0,\dots,0), v_1=$

$(0,0,\ldots,1),\ldots,v_{2^n-1}=(1,1,\ldots,1)$. The Hamming weight of a vector $x\in\mathbb{F}_2^n$, denoted by $\mathsf{w_H}(x)$, is the number nonzero coordinates (i.e., 1s) in the vector x. The support of $f\in\mathcal{B}_n$, denoted by $\mathsf{supp}(f)=\{x\in\mathbb{F}_2^n : f(x)=1\}$. Therefore, the Hamming weight of the Boolean function f, is cardinality of $\mathsf{supp}(f)$ and is denoted by $\mathsf{w_H}(f)$. The function f is called balanced if $\mathsf{w_H}(f)=2^{n-1}$. 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 $\mathsf{d_H}(f,g)=|\{x\in\mathbb{F}_2^n : f(x)\neq g(x)\}|$ i.e., $\mathsf{d_H}(f,g)=\mathsf{w_H}(f+g)$.

An n-variable Boolean function f can be expressed as a polynomial in the ring $\mathbb{F}_2[x_1,x_2,\ldots,x_n]/<x_1^2+x_1,x_2^2+x_2,\ldots,x_n^2+x_n>$, i.e. $f(x)=\sum\limits_{u\in\mathbb{F}_2^n} c_u x^{u_1}x^{u_2}\cdots x^{u_n}$, 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.

Definition 1 (Walsh-Hadamard Transform). *The Walsh-Hadamard transform of a function on $\mathbb{F}_2^n$ is the map $W_f:\mathbb{F}_2^n\to\mathbb{R}$, defined by*

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

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

We denote $\mathsf{E}_{k,n}=\{x\in\mathbb{F}_2^n : \mathsf{w_H}(x)=k\}$ and $\mathsf{w}_{k,n}(f)=|\{x\in\mathsf{E}_{k,n} : f(x)=1\}|=|\mathsf{supp}(f)\cap\mathsf{E}_{k,n}|$. Accordingly, the Hamming distance of two functions $f,g\in\mathcal{B}_n$ on $\mathsf{E}_{k,n}$ denoted as $d_{k,n}(f,g)=|\{x\in\mathsf{E}_{k,n} : f(x)\neq g(x)\}|$. 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 $\mathsf{E}_{k,n}$. For two integers m,n with $m\leq n$, we define $[m,n]=\{m,m+1,\ldots,n\}$.

Definition 3 (Weightwise Almost Perfectly Balanced (WAPB)). *A Boolean function $f\in\mathcal{B}_n$ is said to be weightwise almost perfectly balanced (WAPB) if for all $k\in[0,n]$,*

$$\mathsf{w}_{k,n}(f)=\begin{cases}\frac{\binom{n}{k}}{2} & \text{if } \binom{n}{k} \text{ is even,}\\ \frac{\binom{n}{k}\pm 1}{2} & \text{if } \binom{n}{k} \text{ is odd.}\end{cases}$$

Definition 4 (Weightwise Perfectly Balanced (WPB)). *A Boolean function $f\in\mathcal{B}_n$ is said to be weightwise perfectly balanced (WPB) if for all $k\in[1,n-1]$,*

$$\mathsf{w}_{k,n}(f)=\frac{\binom{n}{k}}{2},$$

and $f(0,0,\ldots,0)=0=1+f(1,1,\ldots,1)$.

Using Lucas' Theorem [Fin47], we have that a WPB function exists only if, n is a power of 2. Hence, there are $\prod\limits_{k=1}^{n-1}\binom{\binom{n}{k}}{\binom{n}{k}/2}$ WPB Boolean functions.

Definition 5 (Restricted Walsh Transform). *Let f be an n-variable Boolean function, then its Walsh transform $\mathcal{W}_{f,k}(a)$ is defined as:*

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

Definition 6 (Weightwise Nonlinearity). *The nonlinearity of $f \in \mathcal{B}_n$ over $\mathsf{E}_{k,n}$, denoted as $\mathsf{NL}_k(f)$, is the Hamming distance of f to the set of all affine functions $\mathcal{A}_n$ when evaluated over $\mathsf{E}_{k,n}$. That is, $\mathsf{NL}_k(f) = \min_{g \in \mathcal{A}_n} d_{k,n}(f,g) = \min_{g \in \mathcal{A}_n} \mathsf{w}_{k,n}(f+g)$.*

The following identity and upper bound on the nonlinearity of a Boolean function over $\mathsf{E}_{k,n}$ can be derived. The upper bound is further improved by Mesnager et al. in [MZD19].

Lemma 1 ([CMR17], Propositions 4 and 5). *If $f \in \mathcal{B}_n$ then for $k \in [0,n]$,*

$$\mathsf{NL}_k(f) = \frac{|\mathsf{E}_{k,n}|}{2} - \frac{1}{2}\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_{f,k}(a)|, \text{ and}$$

$$\mathsf{NL}_k(f) \leq \frac{1}{2}[|\mathsf{E}_{k,n}| - \sqrt{|\mathsf{E}_{k,n}|}] = \frac{1}{2}[\binom{n}{k} - \sqrt{\binom{n}{k}}].$$

Definition 7 (Algebraic immunity and weightwise algebraic immunity). *The algebraic immunity of a Boolean function $f \in \mathcal{B}_n$, denoted as $\mathsf{AI}(f)$, is defined as:*

$$\mathsf{AI}(f) = \min_{g \neq 0}\{\mathsf{deg}(g) \mid fg = 0 \text{ or } (f+1)g = 0\},$$

where $\mathsf{deg}(g)$ is the algebraic degree of g. The function g is called an annihilator of f (or $f+1$).

The weightwise algebraic immunity of $f \in \mathcal{B}_n$ for $k \in [0,n]$, denoted as $\mathsf{AI}_k(f)$, is defined as:

$$\mathsf{AI}_k(f) = \min_{g \neq 0 \text{ over } \mathsf{E}_{k,n}}\{\mathsf{deg}(g) \mid fg = 0 \text{ or } (f+1)g = 0\}.$$

2.1 Permutation symmetric Boolean functions

We denote $\mathbb{S}_n$ be the symmetric group on n elements. For a permutation $\pi \in \mathbb{S}_n$, the action of permutation group $P = \langle \pi \rangle$ on $\mathbb{F}_2^n$ makes a partition of $\mathbb{F}_2^n$, called orbits. The set of orbits is denoted as $\mathcal{O}$. For $x \in \mathbb{F}_2^n$, we denote the orbit containing x as $O(x) = \{y \in \mathbb{F}_2^n | \pi^k(y) = x \text{ for some } k \in \mathbb{Z}\}$. Now we define two special permutations as follows.

1. **Rotation (or, cyclic) permutation (σ)**: The permutation $\sigma \in \mathbb{S}_n$ is called rotation permutation if $\sigma((x_1, x_2, \ldots, x_n)) = (x_n, x_1, \ldots, x_{n-1})$ for every $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$. We denote the rotation permutation on n elements by σ (or, σ_n to specify the number n). The cyclic group $P = \langle \sigma \rangle$ is called rotation symmetric group.
2. **Distinct binary-cycle permutation(ψ)**: Let n be a positive integer with binary representation as

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

A permutation $\psi \in \mathbb{S}_n$ is called a distinct binary-cycle permutation if its disjoint cycle form contains cycles of length $n_1, n_2, \ldots, n_w$. We denote the permutation on n elements by ψ (or, ψ_n to specify the number n). Without loss of generality, we consider

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

Note that, $\sigma = \psi$ when $n = 2^m$ is a power of 2. For $\pi \in \mathbb{S}_n$, we define π symmetric Boolean functions and 2-π symmetric Boolean functions as follows.

Definition 8 (π Symmetric Boolean function (πS)). *Let $\pi \in \mathbb{S}_n$ be a permutation on n elements with order $o(\pi)$. A Boolean function f is π symmetric (in short, πS) if and only if for any $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$,*

$$f(\pi^k(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n) \text{ for every } 1 \leq k \leq o(\pi)$$

where $\pi^k = \pi \circ \pi^{k-1}$ for $k > 1$ and $\pi^1 = \pi$. Therefore, πS Boolean functions have the same truth value for all vectors in every orbit obtained by the action of permutation group $P = \langle \pi \rangle$ on $\mathbb{F}_2^n$.

For $\pi = \sigma$, the σS Boolean functions are known as Rotation Symmetric Boolean functions(in short, RotS). The σS Boolean functions are very well studied functions in the literature [PQ99, CS02, SM08]. However, no study on ψS Boolean functions is available in the literature. When n is power of 2, the class of σS Boolean functions and the class of ψS Boolean functions are same.

Definition 9 (2-π Symmetric Boolean function(2-πS)). *Let $\pi \in \mathbb{S}_n$ be a permutation on n elements and $\mathcal{O}$ be the set of all orbits due to the group action of $P = \langle \pi \rangle$ on $\mathbb{F}_2^n$. A Boolean function f is 2-π symmetric (in short, 2-πS) if and only if for every orbit $\mathsf{O} \in \mathcal{O}$ with a fixed representative element ν_o,*

$$f(\pi^{2i}(\nu_o)) = f(\nu_o); \quad f(\pi^{2i+1}(\nu_o)) = f(\nu_o) + 1 \text{ for every } 0 \le i < \lfloor \frac{|\mathsf{O}|}{2} \rfloor.$$

Note that, if $|\mathsf{O}|$ is odd then $f(\pi^{|\mathsf{O}|-1}(\nu))$ can be any value from $\mathbb{F}_2$.

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

A construction of a class of 2-σS 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.*

The Boolean function proposed in Proposition 1 is 2-σS. Since, n is the power of 2 in the construction, 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 can not be assigned when n is not a power of 2 as there are some orbits with cardinality odd and hence the $f(x^2) = f(x) + 1$ can not be defined. However, we have proposed an generalization of this concept to construct WAPB Boolean function on any n where n is a natural number in Section 4. When n is power of 2, the class of 2-σS Boolean functions and the class of 2-ψS Boolean functions are same.

2.2 Some Results on Krawtchouk Polynomials

We present some results on Krawtchouk polynomials and sequences which are useful for later results.

Definition 10 (Krawtchouk polynomial). *For a positive integer n, the Krawtchouk polynomial [MS78, Page 151] of degree k is given by*

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

Some nice properties of the Krawtchouk polynomials from [DMS06, Proposition 4, Corollary 1] are presented in the following Proposition.

Proposition 2. *1. $\mathsf{K}_0(l, n) = 1, \mathsf{K}_1(l, n) = n - 2l$.*
2. $\mathsf{K}_k(l, n) = (-1)^l \mathsf{K}_{n-k}(l, n)$ (that impies, $\mathsf{K}_{\frac{n}{2}}(l, n) = 0$ for n even and l odd).
3. $\mathsf{K}_k(l, n) = (-1)^k \mathsf{K}_k(n - l, n)$, (that impies, $\mathsf{K}_k(\frac{n}{2}, n) = 0$ for n even and k odd).
4. For n odd, $|\mathsf{K}_k(1, n)| \ge |\mathsf{K}_k(l, n)|$ where $0 \le k \le n$ and $1 \le l \le n - 1$,
5. For n even, $|\mathsf{K}_k(1, n)| \ge |\mathsf{K}_k(l, n)|$ where $0 \le k \le n$ and $1 \le l \le n - 1$ except $k = \frac{n}{2}$ or $l = \frac{n}{2}$.
6. $(n - l)\mathsf{K}_k(l + 1, n) = (n - 2k)\mathsf{K}_k(l, n) - l\mathsf{K}_k(l - 1, n)$.

The following relations are derived from some results in [DMS06, GM22a],

Theorem 1 (Krawtchouk polynomials relations). *For integers $n > 0$, $0 \le k \le n$ and fixed $a \in \mathbb{F}_2^n$ such that $\mathsf{w_H}(a) = \ell$, the following relations hold.*

1. $\sum_{x \in \mathsf{E}_{k,n}} (-1)^{a.x} = \mathsf{K}_k(\ell, n)$.
2. If $l_{a,b}(x) = a \cdot x + b$, where $a \in \mathbb{F}_2^n, b \in \mathbb{F}_2$, be an affine Boolean function then

$$\mathsf{w}_{k,n}(l_{a,b}) = \frac{1}{2}(|\mathsf{E}_{k,n}| - (-1)^b \mathsf{K}_k(\ell, n)).$$

Now we present some results on the sequences from Krawtchouk polynomial.

Lemma 2. *Let n be a positive integer and $k \in [0, n]$. Then*

1. $\mathsf{K}_k(1, n) \geq 0$ *if* $k \leq \lfloor \frac{n}{2} \rfloor$ *and* $\mathsf{K}_k(1, n) < 0$ *if* $k > \lfloor \frac{n}{2} \rfloor$. *In particular,* $\mathsf{K}_k(1, n) = 0$ *if n is even and* $k = \frac{n}{2}$.
2. $\mathsf{K}_k(2, n) \geq 0$ *iff* $k \leq \frac{n}{2} - \frac{\sqrt{n}}{2}$ *or,* $k \geq \frac{n}{2} + \frac{\sqrt{n}}{2}$.
   In particular, $\mathsf{K}_k(2, n) = 0$ *if n is an even square integer and* $k = \frac{n}{2} \pm \frac{\sqrt{n}}{2}$.
3. $\mathsf{K}_k(l+1, n) + \mathsf{K}_k(l, n) = 2\mathsf{K}_k(l, n-1)$ *and* $\mathsf{K}_k(l+1, n) - \mathsf{K}_k(l, n) = -2\mathsf{K}_{k-1}(l, n-1)$.
4. $\mathsf{K}_k(l, n) + \mathsf{K}_{k-1}(l, n) = \mathsf{K}_k(l, n+1)$ *and* $\mathsf{K}_k(l, n) - \mathsf{K}_{k-1}(l, n) = \mathsf{K}_k(l+1, n+1)$.

Proof. 1. The proof can be derived from the expression $\mathsf{K}_k(1, n) = \binom{n-1}{k} - \binom{n-1}{k-1}$.

2. $\mathsf{K}_k(2, n) = \binom{n-2}{k} - 2\binom{n-2}{k-1} + \binom{n-2}{k-2} = \frac{(n-2)!((2k-n)^2 - n)}{k!(n-k)!}$.
   Hence, $\mathsf{K}_k(2, n) \geq 0 \iff (2k-n)^2 - n \geq 0 \iff (2k-n)^2 \geq n \iff 2k - n \geq \sqrt{n}$ or, $2k - n \leq -\sqrt{n} \iff k \geq \frac{n}{2} + \frac{\sqrt{n}}{2}$ or, $k \leq \frac{n}{2} - \frac{\sqrt{n}}{2}$. The particular case follows similarly.
3. We have,

$$\begin{aligned}
\mathsf{K}_k(l+1, n) + \mathsf{K}_k(l, n) &= \sum_{j=0}^{k} (-1)^j \binom{l+1}{j}\binom{n-l-1}{k-j} + \sum_{j=0}^{k})(-1)^j \binom{l}{j}\binom{n-l}{k-j} \\
&= \sum_{j=0}^{k} (-1)^j \left[\binom{l+1}{j}\binom{n-l-1}{k-j} + \binom{l}{j}\binom{n-l}{k-j}\right] \\
&= \sum_{j=0}^{k} (-1)^j \left[\binom{l+1}{j}\binom{n-l-1}{k-j} + \binom{l}{j}\left(\binom{n-l-1}{k-j} + \binom{n-l-1}{k-j-1}\right)\right] \\
&= \sum_{j=0}^{k} (-1)^j \left[\left(\binom{l+1}{j} + \binom{l}{j}\right)\binom{n-l-1}{k-j} + \binom{l}{j}\binom{n-l-1}{k-j-1}\right] \\
&= \sum_{j=0}^{k} (-1)^j \left[\left(\binom{l+1}{j} + \binom{l}{j}\right)\binom{n-l-1}{k-j} + \sum_{j=1}^{k+1} (-1)^{j-1} \binom{l}{j-1}\binom{n-l-1}{k-j}\right] \\
&= \sum_{j=0}^{k} (-1)^j \left[\left(\binom{l+1}{j} + \binom{l}{j}\right)\binom{n-l-1}{k-j} + \sum_{j=0}^{k} (-1)^{j-1} \binom{l}{j-1}\binom{n-l-1}{k-j}\right] \\
&= \sum_{j=0}^{k} (-1)^j \left(\binom{l+1}{j} + \binom{l}{j} - \binom{l}{j-1}\right)\binom{n-l-1}{k-j} \\
&= 2\sum_{j=0}^{k} (-1)^j \binom{l}{j}\binom{n-l-1}{k-j} = 2\mathsf{K}_k(l, n-1).
\end{aligned}$$

   The second part of this Item be proved using the similar technique as above.
4. These can be proved by adding and subtracting the equalities in Item 3.

□

We present the minimum of the sequence $\mathsf{K}_k(l, n), 0 \leq l \leq n$ for a fixed k and n in the following theorem.

Theorem 2. *1. Let $n = 2m+1$ be an odd integer for some $m \in \mathbb{Z}^+$. Then for $k \in [0, n]$*

$$\min_{0 \le l \le n-1} \mathsf{K}_k(l,n) = \begin{cases} \mathsf{K}_k(n-1,n) = -\mathsf{K}_k(1,n) & \text{for } k \in [0, \frac{n-1}{2}] \text{ and odd,} \\ \mathsf{K}_k(1,n) & \text{for } k \in [\frac{n+1}{2}, n]. \end{cases}$$

In particular, $\min_{0 \le l \le n-1} \mathsf{K}_m(l,n) = \mathsf{K}_m(2,n) = -\mathsf{K}_m(1,n)$.

*2. Let $n = 2m$ be an even integer for some $m \in \mathbb{Z}^+$.
Then for $k \in [m+1, n]$ and even, $\min_{0 \le l \le n} \mathsf{K}_k(l,n) = \mathsf{K}_k(1,n)$. In particular,*

(a) $\min_{0 \le l \le n} \mathsf{K}_m(l,n) = \mathsf{K}_m(2,n)$ if m is even;

(b) for $n \ge 10$, $\min_{0 \le l \le n} \mathsf{K}_{m-1}(l,n) = \mathsf{K}_{m-1}(2,n)$ if m is odd.

3. $\min_{0 \le l \le n} \mathsf{K}_2(l,n) = -\lfloor \frac{n}{2} \rfloor$.

4. $\max_{0 \le l \le n} \mathsf{K}_k(l,n) = \mathsf{K}_k(0,n) = \binom{n}{k}$.

5. $\mathsf{K}_k(n,n) = \begin{cases} \max_{0 \le l \le n} \mathsf{K}_k(l,n) & \text{if } k \text{ is even;} \\ \min_{0 \le l \le n} \mathsf{K}_k(l,n) & \text{if } k \text{ is odd.} \end{cases}$

Proof. 1. From Proposition 2[Item 4], for $k \in [0, n]$, we have $|\mathsf{K}_k(1,n)| \ge |\mathsf{K}_k(l,n)|$ for all $l \in [1, n-1]$. For $k \in [\frac{n+1}{2}, n]$, $\mathsf{K}_k(1,n) < 0$ (from Lemma 2[Item 1]), we have $\min_{1 \le l \le n-1} \mathsf{K}_k(l,n) = \mathsf{K}_k(1,n)$.

Further, k being odd in $[0, \frac{n-1}{2}]$, using Proposition 2[Item 3], we have $\mathsf{K}_k(1,n) = -\mathsf{K}_k(n-1,n)$. Hence, for $k \in [0, \frac{n-1}{2}]$, as $\mathsf{K}_k(1,n) \ge 0$ (from Lemma 2[Item 1]), $\max_{1 \le l \le n-1} \mathsf{K}_k(l,n) = \mathsf{K}_k(1,n)$ i.e., $\min_{1 \le l \le n-1} \mathsf{K}_k(l,n) = \mathsf{K}_k(n-1,n)$.

As $\mathsf{K}_k(0,n) = \binom{n}{k} > 0$, we have $\min_{0 \le l \le n-1} \mathsf{K}_k(l,n) = \min_{1 \le l \le n-1} \mathsf{K}_k(l,n)$ and the result of the first part of the Theorem.

As $n = 2m+1$, we have from Lemma 2[Item 3 and Item 1] that $\mathsf{K}_m(2,n) + \mathsf{K}_m(1,n) = 2\mathsf{K}_m(1,n-1) = 0$. That implies, $\mathsf{K}_m(2,n) = -\mathsf{K}_m(1,n) \le 0$.

As $\mathsf{K}_m(0,n) = \binom{n}{m} > 0$, $\min_{0 \le l \le n} \mathsf{K}_m(l,n) = \min_{1 \le l \le n-1} \mathsf{K}_m(l,n) = \mathsf{K}_m(2,n)$ (from Proposition 2[Item 4]). Hence the second part is done.

2. As $k \ge m+1$, from Proposition 2[Item 5], we have $|\mathsf{K}_k(1,n)| \ge |\mathsf{K}_k(l,n)|$ for $l \in [1, n-1]$. As $\mathsf{K}_k(1,n) \le 0$ (from Lemma 2[Item 1]) and $\mathsf{K}_k(0,n) = \mathsf{K}_k(n,n) = \binom{n}{k} > 0$, $\min_{0 \le l \le n} \mathsf{K}_k(l,n) = \min_{1 \le l \le n-1} \mathsf{K}_k(l,n) = \mathsf{K}_k(1,n)$.

Hence, the first part is done.

Further from Lemma 2[Item 2]), we have $\mathsf{K}_m(2,n) \le 0$ as $m = \frac{n}{2}$.

(a) Here, $m = \frac{n}{2}$ is even. We will show $|\mathsf{K}_m(2,n)| \ge |\mathsf{K}_m(l,n)|$ for $1 \le l \le n-1$. At first, we will use induction on l to show it for l even and $2 \le l \le \frac{n}{2}$.

For $l = 2$, it is already $|\mathsf{K}_m(2,n)| = |\mathsf{K}_m(l,n)|$.

Assume that $|\mathsf{K}_m(2,n)| \ge |\mathsf{K}_m(l,n)|$ for some even l and $2 \le l \le \frac{n}{2} - 2$. Then, we need to prove that $|\mathsf{K}_m(2,n)| \ge |\mathsf{K}_m(l+2,n)|$. From Proposition 2[Item 6], for $2 \le l \le \frac{n-4}{2} = \frac{n}{2} - 2$, we have

$$\begin{aligned} (n-(l+1))\mathsf{K}_m(l+2,n) &= (n-2m)\mathsf{K}_m(l+1,n) - (l+1)\mathsf{K}_m(l,n) \\ &= -(l+1)\mathsf{K}_m(l,n), \text{ as } n = 2m \\ \implies |(n-l-1)\mathsf{K}_m(l+2,n)| &= |-(l+1)\mathsf{K}_m(l,n)| \\ \implies |\mathsf{K}_m(l+2,n)| &= \frac{l+1}{n-l-1}|\mathsf{K}_m(l,n)| \le |\mathsf{K}_m(l,n)| \le |\mathsf{K}_m(2,n)| \text{ as } \frac{l+1}{n-l-1} \le 1. \end{aligned}$$

Therefore, $|\mathsf{K}_m(2,n)| \ge |\mathsf{K}_m(l,n)|$ for all $2 \le l \le \frac{n}{2}$ and even. From Proposition 2[Item 2], $\mathsf{K}_m(l,n) = 0$ for l odd. Hence, $|\mathsf{K}_m(2,n)| \ge |\mathsf{K}_m(l,n)|$ for all $1 \le l \le \frac{n}{2}$. Further, from Proposition 2[Item 3], $\mathsf{K}_m(l,n) = \mathsf{K}_m(n-l,n)$ as m even. Hence, $|\mathsf{K}_m(2,n)| \ge |\mathsf{K}_m(l,n)|$ for all $1 \le l \le n-1$. Therefore, as $\mathsf{K}_m(2,n) < 0$ and $\mathsf{K}_m(0,n) = \mathsf{K}_m(n,n) = \binom{n}{m} > 0$, $\min_{0 \le l \le n} \mathsf{K}_m(l,n) = \min_{1 \le l \le n-1} \mathsf{K}_m(l,n) = \mathsf{K}_m(2,n)$ for m even.

(b) Now $m = \frac{n}{2}$ is odd. At first, we will show that $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l,n)|$ for $2 \leq l \leq \frac{n}{2}$ using induction on l.

For $l = 2$, it is already $|\mathsf{K}_{m-1}(2,n)| = |\mathsf{K}_{m-1}(l,n)|$.

We will prove it for $l = 3$ i.e. $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(3,n)|$. This is needed as we will see later that the induction has a recursion with depth two. It can be checked from Lemma 2[Item 2] that $\mathsf{K}_{m-1}(2,n) \leq 0$ for $n \geq 4$. To prove $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(3,n)|$, we need to show that $\mathsf{K}_{m-1}(2,n) \leq \mathsf{K}_{m-1}(3,n) \leq -\mathsf{K}_{m-1}(2,n)$ i.e., $\mathsf{K}_{m-1}(3,n) - \mathsf{K}_{m-1}(2,n) \geq 0$ and $\mathsf{K}_{m-1}(3,n) + \mathsf{K}_{m-1}(2,n) \leq 0$.

From Lemma 2[Item 3 and Item 1], we have $\mathsf{K}_{m-1}(3,n) + \mathsf{K}_{m-1}(2,n) = 2\mathsf{K}_{m-1}(2,n-1) = 2\left(2\mathsf{K}_{m-1}(1,n-2) - \mathsf{K}_{m-1}(1,n-1)\right) = -2\mathsf{K}_{m-1}(1,n-1) \leq 0$.

Similarly, $\mathsf{K}_{m-1}(3,n) - \mathsf{K}_{m-1}(2,n) = -2\mathsf{K}_{m-2}(2,n-1) \geq 0$ if $m - 2 \geq \frac{n-1-\sqrt{n-1}}{2}$ i.e., if $n \geq 10$ (Lemma 2[Item 2]). Hence, $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(3,n)|$ if $n \geq 10$.

Assume that $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l-1,n)|$ and $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l,n)|$ for some $3 \leq l \leq \frac{n}{2} - 1$. Then, we need to prove that $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l+1,n)|$.

Using Proposition 2[Item 6], we have

$$
\begin{aligned}
(n-l)\mathsf{K}_{m-1}(l+1,n) &= (n-2(m-1))\mathsf{K}_{m-1}(l,n) - l\mathsf{K}_{m-1}(l-1,n) \\
&= 2\mathsf{K}_{m-1}(l,n) - l\mathsf{K}_{m-1}(l-1,n) \\
\implies (n-l)|\mathsf{K}_{m-1}(l+1,n)| &\leq 2|\mathsf{K}_{m-1}(l,n)| + l|\mathsf{K}_{m-1}(l-1,n)| \leq (2+l)|\mathsf{K}_{m-1}(2,n)| \\
\implies |\mathsf{K}_{m-1}(l+1,n)| &\leq \frac{l+2}{n-l}|\mathsf{K}_{m-1}(2,n)| \\
\implies |\mathsf{K}_{m-1}(l+1,n)| &\leq |\mathsf{K}_{m-1}(2,n)| \qquad \text{as } \frac{l+2}{n-l} \leq 1 \text{ for } 2 \leq l \leq \frac{n}{2} - 1.
\end{aligned}
$$

Hence, $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l,n)|$ for $2 \leq l \leq \frac{n}{2}$.

Then $|\mathsf{K}_{m+1}(2,n)| \geq |\mathsf{K}_{m+1}(l,n)|$ for $2 \leq l \leq \frac{n}{2}$ as $|\mathsf{K}_{m+1}(l,n)| = |\mathsf{K}_{m-1}(l,n)|$ (from Proposition 2[Item 2]).

Now, we will show that $\min\limits_{0 \leq l \leq n} \mathsf{K}_{m+1}(l,n) = \mathsf{K}_{m+1}(1,n)$. From Lemma 2[Item 3 and Item 1], we have $\mathsf{K}_{m+1}(2,n) - \mathsf{K}_{m+1}(1,n) = -2\mathsf{K}_{m}(1,n-1) > 0$. Similarly, $\mathsf{K}_{m+1}(2,n) + \mathsf{K}_{m+1}(1,n) = 2\mathsf{K}_{m+1}(1,n-1) \leq 0$. That implies $-\mathsf{K}_{m+1}(1,n) \leq \mathsf{K}_{m+1}(2,n) < \mathsf{K}_{m+1}(1,n)$ i.e., $|\mathsf{K}_{m+1}(2,n)| \leq |\mathsf{K}_{m+1}(1,n)|$.

From Lemma 2[Item 1], we have $\mathsf{K}_{m+1}(1,n) \leq 0$. Hence $\min\limits_{0 \leq l \leq n} \mathsf{K}_{m+1}(l,n) = \mathsf{K}_{m+1}(1,n)$.

3. We have

$$
\mathsf{K}_k(l,n) = \sum_{j=0}^{k}(-1)^j \binom{l}{j}\binom{n-l}{k-j} = \sum_{j=0}^{k}\binom{l}{j}\binom{n-l}{k-j} - 2\sum_{\substack{j=0 \\ j:\text{odd}}}^{k}\binom{l}{j}\binom{n-l}{k-j} = \binom{n}{k} - 2\sum_{\substack{j=0 \\ j:\text{odd}}}^{k}\binom{l}{j}\binom{n-l}{k-j}. \quad (3)
$$

Hence, $\mathsf{K}_2(l,n) = \binom{n}{2} - 2\binom{l}{1}\binom{n-l}{1} = \binom{n}{2} - 2l(n-l)$. For real value of l, the function $\mathsf{K}_2(l,n)$ has minima at $l = \frac{n}{2}$ as $\frac{d(\mathsf{K}_2(l,n))}{dl} = 4l - 2n = 0$ at $l = \frac{n}{2}$ and $\frac{d^2(\mathsf{K}_2(l,n))}{dl^2} = 4 > 0$. In our case, as $l = \mathsf{w_H}(a + \psi^{-1}(a))$ for $a \in \mathbb{F}_2^n$ is an integer, we have $\min\limits_{0 \leq l \leq n} \mathsf{K}_2(l,n)$ is $\binom{n}{2} - 2(\frac{n}{2})^2 = -\frac{n}{2}$ when n is even. For n is odd, it can be checked that $\mathsf{K}_2(l,n)$ has minimum at $l = \frac{n-1}{2}$ and $l = \frac{n+1}{2}$ with value $\min\limits_{0 \leq l \leq n} \mathsf{K}_2(l,n) = \binom{n}{2} - 2\frac{n-1}{2}\frac{n+1}{2} = -\frac{n-1}{2}$. Hence, combining both the cases, we have $\min\limits_{0 \leq l \leq n} \mathsf{K}_2(l,n) = -\lfloor \frac{n}{2} \rfloor$.

4. From Equation 3, we have $\mathsf{K}_k(l,n) = \binom{n}{k} - 2\sum\limits_{\substack{j=0 \\ j:\text{odd}}}^{k}\binom{l}{j}\binom{n-l}{k-j} \leq \binom{n}{k} = \mathsf{K}_k(0,n)$. Hence, we are done.

5. From Proposition 2[Item 3], we have $\mathsf{K}_k(n,n) = (-1)^k\mathsf{K}_k(0,n)$. Hence, for k is even, $\mathsf{K}_k(n,n) = \mathsf{K}_k(0,n)$ is maximum in $\mathsf{K}_k(l,n), l \in [0,n]$. Like Equation 3, we have $\mathsf{K}_k(l,n) = 2\sum\limits_{\substack{j=0 \\ j:\text{even}}}^{k}\binom{l}{j}\binom{n-l}{k-j} - \binom{n}{k} \geq -\binom{n}{k} = -\mathsf{K}_k(0,n)$. Hence, for odd k, we have $\mathsf{K}_k(n,n) = -\mathsf{K}_k(0,n) \leq \mathsf{K}_k(l,n)$ for $l \in [0,n]$. Hence we are done.

□

3 Construction of WAPB Boolean functions using Group action

In this section we will present a construction of 2-πS WAPB Boolean functions using the group action of a cyclic permutation group $P = \langle \pi \rangle$. Let $P = \langle \pi \rangle$ be a cyclic subgroup of the symmetric group $\mathbb{S}_n$ on n elements. Let the group action of P 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 as $O_\pi(x) = \{g(x) : g \in P\} = \{x, \pi(x), \pi^2(x), \ldots, \pi^{l-1}(x)\}$ where l is the order of the permutation π. As $\mathsf{w_H}(\pi^i(x)) = \mathsf{w_H}(x)$ for $1 \le i \le l-1$, the group action P splits each $\mathsf{E}_{k,n}$ into orbits and let $g_{k,n}$ be the number of orbits in $\mathsf{E}_{k,n}$. Denote $\nu_{k,n,i}$ be the orbit representative of i-th orbit $\mathsf{E}_{k,n}$ with some ordering. The construction of 2-πS WAPB Boolean functions is presented in Construction 1.

Construction 1 Construction of 2-πS WAPB Boolean function

Input: $\pi \in \mathbb{S}_n$
Output: A 2-πS WAPB Boolean function $f_\pi \in \mathcal{B}_n$

```
Initiate supp(f_π) = φ
t = 0
for k ← 0 to n do
    for i ← 1 to g_{k,n} do
        u = ν_{k,n,i}; l = |O_π(u)|
        if l is even then
            for j ← 1 to l/2 do
                supp(f_π).append(u)
                u ← π ∘ π(u)
            end for
        else
            u = π^t(u)
            for j ← 1 to ⌈(l−t)/2⌉ do
                supp(f_π).append(u)
                u ← π ∘ π(u)
            end for
            Update t ← 1 − t
        end if
    end for
end for
return f_π
```

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 $\pi = \sigma$ is the rotation permutation. Then considering the orbits with representatives $00000, 00001, 00011, 00101, 00111, 01011, 01111, 11111$, we have the resultant function $f_\sigma \in \mathcal{B}_5$ of Construction 1 as $\mathsf{supp}(f_\sigma) = \{00000, 00010, 01000, 00011, 01100, 10001, 01010, 01001, 00111, 11100, 10011, 10110, 11010, 01111, 11101, 10111\}$. Hence, f_σ is a 2-RotS (i.e., 2-σS) WAPB Boolean function.

Theorem 3. *Nonlinearity and Weightwise nonlinearity bound.*

In the following sections we will study 2-πS WAPB Boolean functions for two different permutations $\psi, \sigma \in \mathbb{S}_n$ for any positive integer n. Here, σ is the rotation permutation and ψ is defined in Section 4. Both functions generalizes the Liu-Mesnager construction [LM19] of WPB Boolean functions on $n = 2^m$ variables.

4 Construction and Study of 2-ψS WAPB Boolean functions

In this section, we present a class of 2-ψS 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 functions.

Let n be a positive integer with binary representation as $n = n_1 + n_2 + \cdots + n_w$ as defined in Equation 1. We denote $\mathsf{w_H}(n) = w$ i.e., the number of 1's in the binary representation of n. For $x = (x_1, x_2, \ldots, x_n)$, we have

$$\psi(x) = (\sigma_{n_1}(x_1, \ldots, x_{n_1}), \sigma_{n_2}(x_{n_1+1}, \ldots, x_{n_1+n_2}), \ldots, \sigma_{n_w}(x_{n-n_w+1}, \ldots, x_n)) \tag{4}$$

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

Lemma 3. *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 $w = \mathsf{w_H}(n)$.*

Proof. For a vector $x \in \mathbb{F}_2^n$ is having an orbit of cardinality 1 i.e., $|O_\psi(x)| = 1$ if and only if the coordinates of x present in the cycles are of same value i.e.,

$$x_1 = x_2 = \ldots = x_{n_1}; \qquad x_{n_1+1} = x_{n_1+2} = \ldots = x_{n_1+n_2}; \quad \cdots, \quad x_{n-n_w+1} = x_{n-n_w+2} = \ldots = x_n. \tag{5}$$

As each partition of coordinates can be either 0 or 1, there are 2^w vectors x in $\mathbb{F}_2^n$ satisfying Equation 5 and hence $|O_\psi(x)| = 1$. □

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

Lemma 4. *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.*

Proof. Let $k = 2^{b_1} + 2^{b_2} + \cdots + 2^{b_t}$ where $0 \le b_1 < b_2 < \cdots < b_t$.
Case I: Let $k \preceq n$ i.e., $\{b_1, b_2, \ldots, b_t\} \subseteq \{a_1, a_2, \ldots, a_w\}$. Since the only way of writing k as sum of powers of 2 is $k = 2^{b_1} + 2^{b_2} + \cdots + 2^{b_t}$ and satisfying the condition in Equation 5, there is only one vector x with $\mathsf{w_H}(x) = k$ and $|O_\psi(x)| = 1$. In this case, the coordinates of x in the partitions of cardinality $2^{b_1}, 2^{b_2}, \ldots, 2^{b_t}$ are having value 1 and other coordinates have value 0.
Case II: Let $k \not\preceq n$, then $\{b_1, b_2, \ldots, b_t\} \not\subseteq \{a_1, a_2, \ldots, a_w\}$. Therefore, if $\mathsf{w_H}(x) = k$, the nonzero coordinates of x can not be partitioned of (distinct) sizes from the set $\{2^{a_1}, 2^{a_2}, \ldots, 2^{b_w}\}$. As a result, the coordinates of x will not satisfy the Equation 5. Hence, $|O_\psi(x)| > 1$. Hence, in this case there is no orbit of weight k and cardinality 1. □

Let denote $\mathcal{O}$ be the set of all orbits due the action of ψ on $\mathbb{F}_2^n$. Further, we denote $\mathcal{O}_o$ be the set of orbits of odd cardinality (i.e., here 1) and $\mathcal{O}_e$ be the set of orbits of even cardinality. Since the cardinality of all orbits of carinality odd 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 from Equation 5, $\mathcal{O}_o = \{(x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n : x_1 = x_2 = \cdots = x_{n_1};\ \ x_{n_1+1} = x_{n_1+2} = \cdots = x_{n_1+n_2};\ \ \cdots;\ x_{(n-n_w)+1} = x_{(n-n_w)+2} = \cdots = x_n\}$. For example, if $n = 6$, there are there are $2^{\mathsf{w_H}(6)} = 2^2 = 4$ orbits of weight 1 and $\mathcal{O}_o = \{000000, 000011, 111100, 111111\}$.

By choosing such permutation ψ for Construction 1, we have every slice $\mathsf{E}_{k,n}$, $0 \le k \le n$, contains at most one orbit of odd cardinality (and i.e., 1). Therefore, it becomes easy to construct 2-ψS WAPB Boolean functions as other orbits are of even cardinality. Hence, we have the following result.

Proposition 3. *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_ψ is WAPB.*

Hence, when $n = 2^m$, a power of 2, $\psi = \sigma$ and Construction 1 on input $\psi \in \mathbb{S}_n$ results the 2-RotS WPB Boolean function by Liu and Mesnager [LM19]. A simplified version of Construction 1 is presented in Construction 4 for input ψ.

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

Input: $\psi \in \mathbb{S}_n$ as in Equation 2
Output: A 2-ψS WAPB Boolean function $f_\psi \in \mathcal{B}_n$
For every orbit O in $\mathbb{F}_2^n$ due to the action of $P = \langle\psi\rangle$, do the following:
if $|\mathsf{O}|$ is even **then**
  f satisfies $f_\psi(\psi(x)) = 1 + f(x)$ for $x \in \mathsf{O}$
end if
if $|\mathsf{O}| = 1$ **then**
  assign $f_\psi(x) = 0$ or 1 to make f balanced.
end if
return f_ψ

[**PM:** For construction 2, I propose the following modifications:

- in input we add a representative ν_i
- in input we add a binary vector v of length the number of orbits.
- then, for every orbit f takes the value v_i on ν_i, and we keep "f satisfies $f_\psi(\psi(x)) = 1 + f(x)$ for $x \in \mathsf{O}$"
- we withdraw the last part, forcing f_ψ to be balanced.

The advantage of the extra inputs would be to define more easily each function later on (if we use an order to list the representatives, we can identify a function in n variables only from the the vector v). Regarding the balancedness, WAPB functions are not required to be balanced, so we would have a more general description (I do not think the balancedness is used in the proofs after). We would make a remark on the restriction that is sufficient to be balanced, or even than the weight of f is determined by the weight of v restricted to the orbits of size 1.]

Theorem 4. *The number of orbits generated due the action of ψ on $\mathbb{F}_2^n$ is*

$$g_n = \frac{1}{n_w} \sum_{k=1}^{n_w} 2^{\gcd(n_1,k)+\gcd(n_2,k)+\cdots+\gcd(n_w,k)}.$$

Proof. As $ord(\psi) = 2^{a_w} = n_w$, let denote $G =< \psi >= \{\psi_n^1, \psi_n^2, \ldots, \psi_n^{n_w}\}$ where $\psi_n^1 = \psi$ and $\psi_n^i = \psi \circ \psi_n^{i-1}$ for $i \geq 2$. From the disjoint cycle form of ψ as in Equation 4, we have

$$\psi(x) = (\sigma_{n_1}(x_1, \ldots, x_{n_1}), \sigma_{n_2}(x_{n_1+1}, \ldots, x_{n_1+n_2}), \ldots, \sigma_{n_w}(x_{n-n_w+1}, \ldots, x_n))$$

where σ_{n_i} is the rotation permutation on n_i elements. Hence, we denote, $\psi_n = (\sigma_{n_1}, \sigma_{n_2}, \ldots, \sigma_{n_w})$ and for positive integers k, we have $\psi_n^k = (\sigma_{n_1}^k, \sigma_{n_2}^k, \ldots, \sigma_{n_w}^k)$.

Now to apply Burnside's lemma, for every $k \in \{1, 2, \ldots, n_w\}$, we need to compute the number of fixed vectors $z \in \mathbb{F}_2^n$ by ψ_n^k i.e., $\psi_n^k(z) = z$. That is, for every $k \in \{1, 2, \ldots, n_w\}$, we need to compute the number of vectors $z \in \mathbb{F}_2^n$ such that $\rho_{n_1}^k(z_1) = z_1, \rho_{n_2}^k(z_2) = z_2, \ldots, \rho_{n_w}^k(z_w) = z_w$ where $z = (z_1, z_2, \ldots, z_w)$ and $z_1 \in \mathbb{F}_2^{n_1}, z_2 \in \mathbb{F}_2^{n_2}, \ldots, z_w \in \mathbb{F}_2^{n_w}$.

Here, the number of permutation cycles in $\sigma_{n_i}^k = \gcd(n_i, k)$ for $1 \leq i \leq w$ and $1 \leq k \leq n_w$. So, the length of each permutation cycle in $\sigma_{n_i}^k$ is $\frac{n_i}{\gcd(n_i,k)}$. Therefore, the total number of permutation cycles in ψ^k is

$$\gcd(n_1, k) + \gcd(n_2, k) + \cdots + \gcd(n_w, k).$$

As every permutation cycle fixes all 0's or all 1's, each permutation cycle has two choices. $\sigma_{n_i}^k$ fixes $2^{\gcd(n_i,k)}$ number of $z_i \in \mathbb{F}_2^{n_i}$. Therefore, ψ^k fixes $2^{\gcd(n_1,k)+\gcd(n_2,k)+\cdots+\gcd(n_w,k)}$ number of $z \in \mathbb{F}_2^n$. Hence, by using the Burnside Lemma, the number of orbits is

$$g_n = \frac{1}{n_w} \sum_{\pi \in G} |fix_{\mathbb{F}_2^n}(\pi)| = \frac{1}{n_w} \sum_{k=1}^{n_w} 2^{\gcd(n_1,k)+\gcd(n_2,k)+\cdots+\gcd(n_w,k)}. \qquad \square$$

The representative of each orbit can be be assigned 0 or 1 and accordingly other vectors in the orbit are assigned. Hence, there are 2^{g_n} WAPB 2-ψS Boolean functions on n variables. Further, we can count the number of balanced WAPB 2-ψS Boolean functions on n variables. There are 2^w many orbits of cardinality 1 and remaining $g_n - 2^w$ orbits are having cardinality even. Further, 2^{w-1} orbits from the 2^w orbits of cardinality 1 are to be assigned 1 to make f_ψ balanced. Hence $\binom{2^w}{2^{w-1}} \times 2^{g_n - 2^w}$ balanced WAPB 2-ψS Boolean functions can be generated using Construction 4. Now we will study some cryptographic properties of the function $f_\psi \in \mathcal{B}_n$.

Proposition 4. *For $n \geq 2$ as in Equation 1, let $\psi \in \mathbb{S}_n$ be the permutation as defined in Equation 2.Then*

$$|\{x \in \mathbb{F}_2^n \setminus \mathcal{O}_o : c \cdot (x + \psi(x)) = 1\}| = \begin{cases} 2^{n-1} & \text{if } c \in \mathbb{F}_2^n \setminus \mathcal{O}_o \\ 0 & \text{if } c \in \mathcal{O}_o. \end{cases}$$

Proof. Now for any $x = (x_1, x_2, \ldots, x_n), c = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n$,

$$c \cdot (x + \psi(x)) = c \cdot x + c \cdot \psi(x) = c \cdot x + \psi^{-1}(c) \cdot x = (c + \psi^{-1}(c)) \cdot x \tag{6}$$

Therefore, $c \cdot (x + \psi(x))$ is a linear Boolean function on n variables. $c \cdot (x + \psi(x))$ is the zero Boolean function if and only if $c = \psi^{-1}(c)$ i.e., $c \in \mathcal{O}_o$. Hence,

$$|\{x \in \mathbb{F}_2^n : c \cdot (x + \psi(x)) = 1\}| = \mathsf{w_H}(c \cdot (x + \psi(x))) = \begin{cases} 2^{n-1} \text{ if } c \in \mathbb{F}_2^n \setminus \mathcal{O}_o \\ 0 \quad\ \text{ if } c \in \mathcal{O}_o \end{cases} \tag{7}$$

Now further, if $x = (x_1, x_2, \ldots, x_n) \in \mathcal{O}_o$, then $\psi(x) = x$ and that implies $c \cdot (x + \psi(x)) = 0$. Hence,

$$\begin{aligned} &|\{x \in \mathcal{O}_o : c \cdot (x + \psi(x)) = 0\}| = |\mathcal{O}_o| = 2^w \\ \implies &|\{x \in \mathcal{O}_o : c \cdot (x + \psi(x)) = 1\}| = 0. \end{aligned} \tag{8}$$

Now combining Equation 7 and Equation 8 we have the desired result

$$|\{x \in \mathbb{F}_2^n \setminus \mathcal{O}_o : c \cdot (x + \psi(x)) = 1\}| = \begin{cases} 2^{n-1} & \text{if } c \in \mathbb{F}_2^n \setminus \mathcal{O}_o \\ 0 & \text{if } c \in \mathcal{O}_o. \end{cases}$$

$\square$

Theorem 5. *Let $n \geq 2$ be an positive integer as in Equation 1 and $\psi \in \mathbb{S}_n$ as in Equation 2. Then* $\mathsf{NL}(f_\psi) \geq 2^{n-2} - 2^{w-1}$.

Proof. Let $a \in \mathbb{F}_2^n$ and $\psi \in \mathbb{S}_n$ be the permutation defined as in Equation 2. As $\mathsf{w_H}(n) = w$, from Lemma 3 there are 2^w orbits with cardinality 1 and remaining orbits are of even cardinality. Then the Walsh spectrum of f_ψ at a is as follows.

$$W_{f_\psi}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f_\psi(x) + a \cdot x} = \sum_{\mathsf{O} \in \mathcal{O}} \sum_{x \in \mathsf{O}} (-1)^{f_\psi(x) + a \cdot x} = \sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O}} (-1)^{f_\psi(x) + a \cdot x} + \sum_{\mathsf{O} \in \mathcal{O}_o} \sum_{x \in \mathsf{O}} (-1)^{f_\psi(x) + a \cdot x}$$

$$\implies |W_{f_\psi}(a)| \leq |\sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O}} (-1)^{f_\psi(x) + a \cdot x}| + |\sum_{\mathsf{O} \in \mathcal{O}_o} \sum_{x \in \mathsf{O}} (-1)^{f_\psi(x) + a \cdot x}|. \tag{9}$$

Since the number of orbits of cardinality odd (i.e., 1) is 2^w, we have a bound for second sum as

$$|\sum_{\mathsf{O}\in\mathcal{O}_o}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}| \leq 2^w. \tag{10}$$

Now we will work on the first sum.

$$\begin{aligned}
\sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} &= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} + \sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(\psi(x))+a\cdot\psi(x)}\right] \\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} + (-1)^{f_\psi(\psi(x))+a\cdot\psi(x)}\right] \\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} - (-1)^{f_\psi(x)+a\cdot\psi(x)}\right] \qquad (\text{as } f_\psi(\psi(x)) = 1 + f_\psi(x)) \\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)}\left((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}\right)\right].
\end{aligned}$$

There are some vectors x in even orbits such that $((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}) = 0$ i.e., $a\cdot(x+\psi(x)) = 0$. As these vectors contributes 0 to the sum, we now separate them in the equation. Hence, we have

$$\begin{aligned}
\sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} &= \frac{1}{2}\Bigg[\sum_{\mathsf{O}\in\mathcal{O}_e}\Bigg(\sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=0}(-1)^{f_\psi(x)}((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}) \\
&\qquad + \sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=1}(-1)^{f_\psi(x)}((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)})\Bigg)\Bigg] \\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=1}(-1)^{f_\psi(x)}((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)})\right] \\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=1}2\times(-1)^{f_\psi(x)+a\cdot x}\right] = \sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=1}(-1)^{f_\psi(x)+a\cdot x} \\
&= \sum_{x\in\mathbb{F}_2^n\setminus\mathsf{O}_o:a\cdot(x+\psi(x))=1}(-1)^{f_\psi(x)+a\cdot x}.
\end{aligned}$$

Now, using the Proposition 4, we have an upper bound to the sum

$$\left|\sum_{\mathsf{O}\in\mathcal{O}_e}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}\right| = \left|\sum_{x\in\mathbb{F}_2^n\setminus\mathsf{O}_o:a\cdot(x+\psi(x))=1}(-1)^{f_\psi(x)+a\cdot x}\right| \leq \begin{cases} 2^{n-1} & \text{if } a\in\mathbb{F}_2^n\setminus\mathcal{O}_o \\ 0 & \text{if } a\in\mathcal{O}_o. \end{cases} \tag{11}$$

Hence, from Equation 9, Equation 10 and Equation 11, we have

$$|W_{f_\psi}(a)| \leq \begin{cases} 2^{n-1} + 2^w & \text{if } a\in\mathbb{F}_2^n\setminus\mathcal{O}_o \\ 2^w & \text{if } a\in\mathcal{O}_o. \end{cases} \tag{12}$$

Hence, the nonlinearity of f_ψ satisfies

$$\begin{aligned}
&\mathsf{NL}(f_\psi) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}|W_{f_\psi}(a)| \;\geq\; 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\{2^{n-1}+2^w, 2^w\} \;=\; 2^{n-1} - 2^{n-2} - 2^{w-1} \\
\implies &\mathsf{NL}(f_\psi) \geq 2^{n-2} - 2^{w-1}.
\end{aligned}$$

□

In the following table we have presented the maximum and minimum nonlinearity among all f_ψ for the number of variables $n = \{4, 5, \ldots, 10\}$ along with the upperbound of balanced Boolean functions and lowerbound of f_ψ as per Theorem 5. 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 will study the weightwise nonlinearity of f_ψ.

Lemma 5. *For $n \geq 2$ as in Equation 1, let $\psi \in \mathbb{S}_n$ be the permutation as defined in Equation 2. Then*

$$|\{x \in \mathsf{E}_{k,n} \setminus \mathcal{O}_o : c \cdot (x + \psi(x)) = 1\}| = \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l, n)),$$

where $l = \mathsf{w_H}(c + \psi^{-1}(c))$.

Proof. Let $x = (x_1, x_2, \ldots, x_n) \in \mathsf{E}_{k,n}$ and $c = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n$. Then as in Equation 6, we have

$$c \cdot (x + \psi(x)) = (c + \psi^{-1}(c)) \cdot x$$

is a linear function on n variable defined over the slice $\mathsf{E}_{k,n}$. Therefore, using Theorem 1, we have

$$|\{x \in \mathsf{E}_{k,n} : c \cdot (x + \psi(x)) = 1\}| = \mathsf{w}_{n,k}((c + \psi^{-1}(c)) \cdot x) = \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l, n))$$

where $l = \mathsf{w_H}(c + \psi^{-1}(c))$. If $x \in \mathsf{E}_{k,n}$ and $|\mathcal{O}_\psi(x)| = 1$ i.e., $x \in \mathsf{E}_{k,n} \cap \mathcal{O}_o$ then $c \cdot (x + \psi(x)) = 0$. Hence,

$$|\{x \in \mathsf{E}_{k,n} \setminus \mathcal{O}_o : c \cdot (x + \psi(x)) = 1\}| = \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l, n)).$$

$\square$

Theorem 6. *Let $n \geq 2$ be an positive integer as in Equation 1 and $\psi \in \mathbb{S}_n$ as in Equation 2. Then*

$$\mathsf{NL}_k(f_\psi) \;\geq\; \begin{cases} \dfrac{1}{4}\left(\dbinom{n}{k} + \min\limits_{\substack{2 \leq l \leq n \\ l \text{ even}}} \mathsf{K}_k(l, n)\right) & \text{if } k \not\preceq n \\ \dfrac{1}{4}\left(\dbinom{n}{k} + \min\limits_{\substack{2 \leq l \leq n \\ l \text{ even}}} \mathsf{K}_k(l, n) - 2\right) & \text{if } k \preceq n. \end{cases}$$

Proof. Let $\mathcal{O}_k$ be the set of all orbits of the group action $G = \langle\psi\rangle$ on $\mathsf{E}_{k,n}$. Let $\mathcal{O}_{e,k}$ and $\mathcal{O}_{o,k}$ be the set of all orbits in $\mathcal{O}_k$ of cardinality even and cardinality odd respectively.

The restricted Walsh spectrum of f_ψ at $a \in \mathbb{F}_2^n$ is as follows.

$$
\begin{aligned}
\mathcal{W}_{f_\psi,k}(a) &= \sum_{x\in \mathsf{E}_{k,n}} (-1)^{f_\psi(x)+a\cdot x} = \sum_{\mathsf{O}\in\mathcal{O}_k}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}\\
&= \sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} + \sum_{\mathsf{O}\in\mathcal{O}_{o,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}\\
\implies |\mathcal{W}_{f_\psi,k}(a)| &\le |\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}| + |\sum_{\mathsf{O}\in\mathcal{O}_{o,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}|\\
&= \begin{cases} |\sum\limits_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum\limits_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}| & \text{if } k \not\preceq n\\ |\sum\limits_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum\limits_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}| + 1 & \text{if } k \preceq n.\end{cases}
\end{aligned}
\tag{13}
$$

$$
\begin{aligned}
\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} &= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} + \sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(\psi(x))+a\cdot \psi(x)}\right]\\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} + (-1)^{f_\psi(\psi(x))+a\cdot \psi(x)}\right]\\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} - (-1)^{f_\psi(x)+a\cdot \psi(x)}\right] \qquad (\text{as } f_\psi(\psi(x)) = 1 + f_\psi(x))\\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)}\left((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}\right)\right]\\
&= \frac{1}{2}\left[\sum_{x\in\mathsf{E}_{k,n}\setminus\mathcal{O}_o}(-1)^{f_\psi(x)}\left((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}\right)\right].
\end{aligned}
\tag{14}
$$

Here, $\mathcal{O}_o$ is the set of vectors with orbit cardinalty 1. The vectors x for which $((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}) = 0$ i.e., $a\cdot(x+\psi(x)) = 0$ have contribution 0 to the sum in Equation 14. Hence, we have

$$
\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f(x)+a\cdot x} = \frac{1}{2}\left[\sum_{\substack{x\in\mathsf{E}_{k,n}\setminus\mathcal{O}_o\\ a\cdot(x+\psi(x))=1}}(-1)^{f_\psi(x)}((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)})\right] = \sum_{\substack{x\in\mathsf{E}_{k,n}\setminus\mathcal{O}_o\\ a\cdot(x+\psi(x))=1}}(-1)^{f_\psi(x)+a\cdot x}.
$$

Hence from Equation 13 and Lemma 5, we have

$$
\begin{aligned}
|\mathcal{W}_{f_\psi,k}(a)| &\le \begin{cases} |\sum\limits_{\substack{x\in\mathsf{E}_{k,n}\setminus\mathcal{O}_o\\ a\cdot(x+\psi(x))=1}}(-1)^{f_\psi(x)+a\cdot x}| & \text{if } k \not\preceq n\\ |\sum\limits_{\substack{x\in\mathsf{E}_{k,n}\setminus\mathcal{O}_o\\ a\cdot(x+\psi(x))=1}}(-1)^{f_\psi(x)+a\cdot x}| + 1 & \text{if } k \preceq n.\end{cases}\\
&= \begin{cases} \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)) & \text{if } k \not\preceq n\\ \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)) + 1 & \text{if } k \preceq n.\end{cases}
\end{aligned}
\tag{15}
$$

where $l = \mathsf{w_H}(a+\psi^{-1}(a))$. Hence, the nonlinearity of f_ψ satisfies

$$\mathsf{NL}_k(f_\psi) = \frac{|\mathsf{E}_{k,n}|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}|\mathcal{W}_{f_\psi,k}(a)| \geq \begin{cases} \frac{|\mathsf{E}_{k,n}|}{2} - \frac{1}{4}\max_{a\in\mathbb{F}_2^n}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)) & \text{if } k \not\preceq n \\ \frac{|\mathsf{E}_{k,n}|}{2} - \frac{1}{4}\max_{a\in\mathbb{F}_2^n}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)) - \frac{1}{2} & \text{if } k \preceq n \end{cases}$$

$$= \begin{cases} \frac{|\mathsf{E}_{k,n}|}{4} + \frac{1}{4}\min_{0\le l\le n}\mathsf{K}_k(l,n) & \text{if } k \not\preceq n \\ \frac{|\mathsf{E}_{k,n}|}{4} + \frac{1}{4}\min_{0\le l\le n}\mathsf{K}_k(l,n) - \frac{1}{2} & \text{if } k \preceq n \end{cases}$$

$$= \begin{cases} \frac{1}{4}\left(\binom{n}{k} + \min_{0\le l\le n}\mathsf{K}_k(l,n)\right) & \text{if } k \not\preceq n \\ \frac{1}{4}\left(\binom{n}{k} + \min_{0\le l\le n}\mathsf{K}_k(l,n) - 2\right) & \text{if } k \preceq n. \end{cases}$$

Further, $l = \mathsf{w_H}(a+\psi^{-1}(a))$ is always even as $\mathsf{w_H}(a) = \mathsf{w_H}(\psi^{-1}(a))$. Hence, we have

$$\mathsf{NL}_k(f_\psi) \geq \begin{cases} \frac{1}{4}\left(\binom{n}{k} + \min_{\substack{0\le l\le n \\ l \text{ even}}}\mathsf{K}_k(l,n)\right) & \text{if } k \not\preceq n \\ \frac{1}{4}\left(\binom{n}{k} + \min_{\substack{0\le l\le n \\ l \text{ even}}}\mathsf{K}_k(l,n) - 2\right) & \text{if } k \preceq n. \end{cases}$$

Using Theorem 2[Item 4], we have further,

$$\mathsf{NL}_k(f_\psi) \geq \begin{cases} \frac{1}{4}\left(\binom{n}{k} + \min_{\substack{2\le l\le n \\ l \text{ even}}}\mathsf{K}_k(l,n)\right) & \text{if } k \not\preceq n \\ \frac{1}{4}\left(\binom{n}{k} + \min_{\substack{2\le l\le n \\ l \text{ even}}}\mathsf{K}_k(l,n) - 2\right) & \text{if } k \preceq n. \end{cases}$$

□

Corollary 1. *Let $n \geq 2$ be an positive integer as in Equation 1 and $\psi \in \mathbb{S}_n$ as in Equation 2. If k is even or, n is odd then*

$$\mathsf{NL}_k(f_\psi) \geq \begin{cases} \frac{1}{4}\left(\binom{n}{k} + \min_{\substack{2\le l\le n-1 \\ l \text{ even}}}\mathsf{K}_k(l,n)\right) & \text{if } k \not\preceq n \\ \frac{1}{4}\left(\binom{n}{k} + \min_{\substack{2\le l\le n-1 \\ l \text{ even}}}\mathsf{K}_k(l,n) - 2\right) & \text{if } k \preceq n. \end{cases}$$

Otherwise (i.e., k is odd and n is even), $\mathsf{NL}_k(f_\psi) \geq 0$. **[DKD:** *need to something for this case]*

Proof. From Theorem 2[Item 5], if k is even then $\max_{0\le l\le n}\mathsf{K}_k(l,n) = \mathsf{K}_k(n,n)$. Further, then $\mathsf{K}_k(n,n)$ is not included in the minimum finding. Hence we are done for the case k is even or, n is odd.

If k is odd and n is even, then $\min_{\substack{2\le l\le n \\ l \text{ even}}}\mathsf{K}_k(l,n) = \mathsf{K}_k(n,n) = -\binom{n}{k}$. Further, in this case $k \not\preceq n$. Hence, $\mathsf{NL}_k(f_\psi) \geq 0$, which is infact always true. □

Now substituting the results of Theorem 2[Item 1 and Item 2] in Corollary 6, we have nonlinearity bounds for some k.

n \ k	2	3	4	5	6	7	8	9	10
	n-2	n-3	n-4	n-5	n-6	n-7	n-8	n-9	n-10
15	24	0	330	0	1215	0	-	-	-
	0	45	0	500	0	1506	-	-	-
16	28	0	443	0	1931	0	3003	-	-
	8	0	228	0	1502	0	-	-	-
17	32	0	580	0	3003	0	5720	-	-
	0	60	0	910	0	4004	0	-	-
18	36	0	750	0	4550	0	10725	0	-
	8	0	340	0	3094	0	9724	0	-
19	40	0	950	0	6650	0	18343	0	-
	0	76	0	1530	0	9282	0	21879	-
20	45	0	1190	0	9524	0	30719	0	43758
	10	0	484	0	5814	0	25194	0	43758

Table 1. A lower bound of $\mathsf{NL}_k(f_\psi)$ as per Theorem 6

Theorem 7. *1. If n is odd then*

$$\mathsf{NL}_k(f_\psi) \geq \begin{cases} \frac{1}{2}\binom{n-1}{k-1} & \text{if } k \in [0, \frac{n-1}{2}], \text{ odd and } k \not\preceq n; \\ \frac{1}{2}\left(\binom{n-1}{k-1} - 1\right) & \text{if } k \in [0, \frac{n-1}{2}], \text{ odd and } k \preceq n; \\ \frac{1}{2}\binom{n-1}{k} & \text{if } k \in [\frac{n+1}{2}, n] \text{ and } k \not\preceq n; \\ \frac{1}{2}\left(\binom{n-1}{k} - 1\right) & \text{if } k \in [\frac{n+1}{2}, n] \text{ and } k \preceq n. \end{cases}$$

2. If n is even and $k \in [\frac{n}{2}+1, n]$ is even then

$$\mathsf{NL}_k(f_\psi) \geq \begin{cases} \frac{1}{2}\binom{n-1}{k} & \text{if } k \not\preceq n; \\ \frac{1}{2}\left(\binom{n-1}{k} - 1\right) & \text{if } k \preceq n. \end{cases}$$

As $\mathsf{E}_{\lfloor \frac{n}{2} \rfloor, n}$ is a largest slice among all slices $\mathsf{E}_{k,n}, k \in [0, n]$, studying the nonlinearity at this domain is useful for cryptographic purpose. The cipher FLIP also uses the domain $\mathsf{E}_{\frac{n}{2}, n}$ for its design. We have the nonlinearity bounds for the largest slice (i.e., $k = \lfloor \frac{n}{2} \rfloor$) in the following Theorem.

Theorem 8. *1. If $n = 2m+1$ is odd then*

$$\mathsf{NL}_m(f_\psi) \geq \begin{cases} \frac{1}{2}\binom{n-1}{m-1} & \text{if } m \not\preceq n \text{ (i.e., } n \text{ is not of the form } 2^t - 1); \\ \frac{1}{2}\left(\binom{n-1}{m-1} - 1\right) & \text{if } m \preceq n \text{ (i.e., } n \text{ is of the form } 2^t - 1). \end{cases}$$

2. If $n = 2m$ is even then
(a) $\mathsf{NL}_m(f_\psi) \geq \binom{n-2}{m}$ if m is even.
(b) $\mathsf{NL}_{m-1}(f_\psi) \geq \frac{1}{2}\left(\binom{n-2}{m-1} + \binom{n-2}{m-3}\right)$ if m is odd and $n \geq 10$.

k \ n	2 n-2	3 n-3	4 n-4	5 n-5	6 n-6	7 n-7	8 n-8	9 n-9	10 n-10
15	24 0	0 45	330 0	0 500	1215 0	0 1506	- -	- -	- -
16	28 8	0 0	443 228	0 0	1931 1502	0 0	3003 -	- -	- -
17	32 0	0 60	580 0	0 910	3003 0	0 4004	5720 0	- -	- -
18	36 8	0 0	750 340	0 0	4550 3094	0 0	10725 9724	0 0	- -
19	40 0	0 76	950 0	0 1530	6650 0	0 9282	18343 0	0 21879	- -
20	45 10	0 0	1190 484	0 0	9524 5814	0 0	30719 25194	0 0	43758 43758

Table 2. A lower bound of $\mathsf{NL}_k(f_\psi)$ as per Theorem 6

Now we will study the restricted nonlinearity $\mathsf{NL}_2(f_\psi)$.
Denote $\mathsf{NL}_k^n = \min\{\mathsf{NL}_k^n(f_\psi) | f_\psi \in \mathcal{B}_n \text{constructed as in Proposition 3}\}$.

Theorem 9. *Let $n \geq 2$ be an positive integer and $\psi \in \mathbb{S}_n$ as in Equation 2. Then*

$$\mathsf{NL}_2(f_\psi) \;\geq\; \begin{cases} \frac{n(n-2)}{8} & \textit{if } n \textit{ is even} \\ \lfloor \frac{(n-1)^2}{8} \rfloor & \textit{if } n \textit{ is odd.} \end{cases}$$

Moreover, if $n = 2^m$ for $m \geq 1$, $\quad \dfrac{n(n-2)}{8} \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2 n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^i n} \leq \cdots,$
and if $n = 2^{a_w} + 2^{a_{w-1}} + \cdots + 2^{a_1}$ for $a_w > a_{w-1} > \cdots > a_1 \geq 0$ as defined in 1,

$$\left\lfloor \frac{(n+1)(n-4)+n}{8} \right\rfloor \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2 n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^i n} \leq \cdots .$$

Proof. From Theorem 2, we have $\min\limits_{0 \leq l \leq n} \mathsf{K}_2(l, n) = -\lfloor \frac{n}{2} \rfloor$. Using it in Theorem 6 we have,

$$\mathsf{NL}_2(f_\psi) \;\geq\; \begin{cases} \frac{1}{4}\left(\binom{n}{2} - \lfloor \frac{n}{2} \rfloor\right) & \text{if } 2 \npreceq n \\ \frac{1}{4}\left(\binom{n}{2} - \lfloor \frac{n}{2} \rfloor - 2\right) & \text{if } 2 \preceq n. \end{cases}$$

Therefore, for $2 \npreceq n$, we have $\mathsf{NL}_2(f_\psi) \geq \begin{cases} \frac{n(n-2)}{8} & \text{if } n \text{ is even (i.e., } n = 4t \text{ form)} \\ \frac{(n-1)^2}{8} & \text{if } n \text{ is odd (i.e., } n = 4t+1 \text{ form),} \end{cases}$
and for $2 \preceq n$, we have $\mathsf{NL}_2(f_\psi) \geq \begin{cases} \frac{n(n-2)}{8} - \frac{1}{2} & \text{if } n \text{ is even (i.e., } n = 4t+2 \text{ form)} \\ \frac{(n-1)^2}{8} - \frac{1}{2} & \text{if } n \text{ is odd (i.e., } n = 4t+3 \text{ form).} \end{cases}$
We can check that for n even, $\frac{n(n-2)}{8}$ is always an integer and for n odd, $\frac{(n-1)^2}{8}$ is an integer iff $2 \npreceq n$. Hence, combining the cases, we have

$$\mathsf{NL}_2(f_\psi) \geq \begin{cases} \frac{n(n-2)}{8} & \text{if } n \text{ is even} \\ \lfloor \frac{(n-1)^2}{8} \rfloor & \text{if } n \text{ is odd.} \end{cases}$$

To prove the second part of the theorem, we use the technique followed in the proof of [LM19, Theorem-3.14]. It can be checked that $\mathsf{NL}_R(f) \leq \mathsf{NL}_E(f)$ if $R \subseteq E$. When $n = 2^m$, for a fixed integer $j \in [1, m]$, consider the set

$$R_j = \{(y,y) : y \in \mathbb{F}_2^{\frac{n}{2}}, \mathsf{w_H}(y) = 2^{j-1}\} = \{(y,y) : y \in \mathsf{E}_{2^{j-1},n}\} \subseteq \mathsf{E}_{2^j,n}.$$

It can be checked that for $x = (y,y) \in R_j$, the orbit containing x, $\mathsf{O}_x = \{(z,z) : z \in \mathsf{O}_y\}$. Then for a WPB $f \in \mathcal{B}_n$ satisfying Proposition 3, we have a WPB $g \in \mathcal{B}_{\frac{n}{2}}$ such that $g(y) = f(x)$ for all $y \in \mathbb{F}_2^{\frac{n}{2}}$. This implies,

$$\mathsf{NL}_2^{\frac{n}{2}}(g) = \mathsf{NL}_{\mathsf{E}_{2,\frac{n}{2}}}(g) = \mathsf{NL}_{R_2}(f) \leq \mathsf{NL}_{\mathsf{E}_{4,n}}(f) \leq \mathsf{NL}_4^n(f).$$

The equality $\mathsf{NL}_{\mathsf{E}_{2,\frac{n}{2}}}(g) = \mathsf{NL}_{R_2}(f)$ can be proved as follows.

$$\begin{aligned}
\mathsf{NL}_{R_2}(f) = \frac{|R_2|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\sum_{x\in R_2}(-1)^{f(x)+a.x} &= \frac{|\mathsf{E}_{2,\frac{n}{2}}|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\sum_{y\in\mathsf{E}_{2,\frac{n}{2}}}(-1)^{g(y)+a.(y,y)} \\
&= \frac{|\mathsf{E}_{2,\frac{n}{2}}|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\sum_{y\in\mathsf{E}_{2,\frac{n}{2}}}(-1)^{g(y)+(a_l+a_r).y} \quad \text{where } a = (a_l,a_r) \text{ with } a_l,a_r \in \mathbb{F}_2^{\frac{n}{2}} \\
&= \frac{|\mathsf{E}_{2,\frac{n}{2}}|}{2} - \frac{1}{2}\max_{b\in\mathbb{F}_2^{\frac{n}{2}}}\sum_{y\in\mathsf{E}_{2,\frac{n}{2}}}(-1)^{g(y)+b.y} = \mathsf{NL}_{\mathsf{E}_{2,\frac{n}{2}}}(g).
\end{aligned}$$

Then we have the generalised result (by proving $\mathsf{NL}_{\mathsf{E}_{2^t,\frac{n}{2}}}(g) = \mathsf{NL}_{R_{t+1}}(f)$)as

$$\frac{n(n-2)}{8} \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^in} \leq \cdots.$$

Now consider $n = n_w + n_{w-1} + \cdots + n_1 = 2^{a_w} + 2^{a_{w-1}} + \cdots + 2^{a_1}$ such that $a_w > a_{w-1} > \cdots > a_1 \geq 0$ as defined in 1. Let $y \in \mathsf{E}_{2,n}$ for $y = y_{n_w}y_{n_{w-1}}\ldots y_{n_1}$ where $y_{n_i} = (y_{n_{i+1}+1}, y_{n_{i+1}+2}, \ldots, y_{n_{i+1}+n_i})$ and $\mathsf{w_H}(y) = 2$. Let us define,

$$R = \{(y_{n_w},y_{n_w})(y_{n_{w-1}},y_{n_{w-1}})\ldots(y_{n_1},y_{n_1}) : y = y_{n_w}y_{n_{w-1}}\ldots y_{n_1} \in \mathbb{F}_2^n \text{ and } \mathsf{w_H}(y) = 2\} \subseteq \mathsf{E}_{4,2n}.$$

Now for $x = (y_{n_w},y_{n_w})(y_{n_{w-1}},y_{n_{w-1}})\ldots(y_{n_1},y_{n_1}) \in R$, we have

$$\mathsf{O}_x = \{(z_{n_w},z_{n_w})(z_{n_{w-1}},z_{n_{w-1}})\ldots(z_{n_1},z_{n_1}) : z_{n_w}z_{n_{w-1}}\ldots z_{n_1} \in \mathsf{O}_y\}$$

Then for a $f \in \mathcal{B}_{2n}$ satisfying Proposition 3, we have a WAPB $g \in \mathcal{B}_n$ such that $\forall y \in \mathbb{F}_2^n$, $g(y) = f(x)$ for $x \in R$. This implies, $\mathsf{NL}_2^n(g) = \mathsf{NL}_R(f) \leq \mathsf{NL}_{\mathsf{E}_{4,2n}}(f) = \mathsf{NL}_4^{2n}(f)$. If we generalise the result, we have

$$\left\lfloor \frac{(n+1)(n-4)+n}{8} \right\rfloor \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^in}.$$

□

Thus, the above theorem provides a better lower bound for the weightwise nonlinearity $\mathsf{NL}_k(f_\psi)$, as proved in the paper [LM19].

Proposition 5. *[LM19] For any $n = 2^m \geq 8$ and f_ψ be a WPB Boolean function as defined in 1, then*

$$\mathsf{NL}_{2^i}^{(n)}(f_\psi) \;\geq\; \begin{cases} 5, & \text{if } 1 \leq i \leq m-3, \\ 6, & \text{if } i = m-2, \\ 19, & \text{if } i = m-1. \end{cases}$$

5 Construction and Study of 2-RotS WAPB Boolean functions

[**DKD:** We can add another section on WAPB Boolean function due to the action of cyclic group.

1. Need to compute number of orbits of size odd in $\mathbb{F}_2^n$
2. Need to compute number of orbits of size odd in $\mathsf{E}_{k,n}$
3. $\mathsf{NL}(f_\sigma), \mathsf{NL}_k(f_\sigma)$
4. ...

]

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.

CS02. Thomas W. Cusick and Pantelimon Stanica. Fast evaluation, weights and nonlinearity of rotation-symmetric functions. *Discrete Mathematics*, 258(1-3):289–301, 2002.

DM23. Deepak Kumar Dalai and Krishna Mallick. A class of weightwise almost perfectly balanced Boolean functions with high weightwise nonlinearity. In *8th International Workshop on Boolean Functions and their Applications (BFA)*, 2023.

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.

DMS06. Deepak Kumar Dalai, Subhamoy Maitra, and Sumanta Sarkar. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. *Designs, Codes and Cryptography*, 40:41–58, 2006.

Fin47. N. J. Fine. Binomial coefficients modulo a prime. *The American Mathematical Monthly*, (10):589–592, 1947.

GM22a. Agnese Gini and Pierrick Méaux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discrete Applied Mathematics*, 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.

GM23a. Agnese Gini and Pierrick Méaux. S_0-equivalent classes, a new direction to find better weightwise perfectly balanced functions, and more. *IACR Cryptol. ePrint Arch.*, page 1101, 2023.

GM23b. 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.

GM23c. Agnese Gini and Pierrick Méaux. Weightwise perfectly balanced functions and nonlinearity. In *Codes, Cryptology and Information Security*, volume 13874 of *Lecture Notes in Computer Science*, pages 338–359. Springer, 2023.

GS22. Xiaoqi Guo and Sihong Su. Construction of weightwise almost perfectly balanced Boolean functions on an arbitrary number of variables. *Discrete Applied Mathematics*, 307:102–114, 2022.

LM19. Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Designs, Codes and Cryptography*, 87(8):1797–1813, 2019.

LS20. Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced Boolean functions with high weightwise nonlinearity. *Discrete Applied Mathematics*, 279:218–227, 2020.

Méa24. Pierrick Méaux. Weightwise (almost) perfectly balanced functions based on total orders. *IACR Cryptol. ePrint Arch.*, page 647, 2024.

MJSC16. Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. In *Advances in Cryptology - EUROCRYPT*, volume 9665 of *Lecture Notes in Computer Science*, pages 311–343. Springer, 2016.

MKL22. Sara Mandujano, Juan Carlos Ku-Cauich, and Adriana Lara. Studying special operators for the application of evolutionary algorithms in the seek of optimal Boolean functions for cryptography. In *Advances in Computational Intelligence*, volume 13612 of *Lecture Notes in Computer Science*, pages 383–396. Springer, 2022.

MPJ+22. Luca Mariot, Stjepan Picek, Domagoj Jakobovic, Marko Djurasevic, and Alberto Leporati. Evolutionary construction of perfectly balanced Boolean functions. In *IEEE Congress on Evolutionary Computation (CEC)*, page 1–8. IEEE Press, 2022.

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*, 13(6):951–979, 2021.

MSLZ22. Sihem Mesnager, Sihong Su, Jingjing Li, and Linya Zhu. Concrete constructions of weightwise perfectly balanced (2-rotation symmetric) functions with optimal algebraic immunity and high weightwise nonlinearity. *Cryptography and Communications*, 14(6):1371–1389, 2022.

MZD19. Sihem Mesnager, Zhengchun Zhou, and Cunsheng Ding. On the nonlinearity of Boolean functions with restricted input. *Cryptography and Communications*, 11(1):63–76, 2019.

PQ99. Josef Pieprzyk and Cheng Xin Qu. Fast hashing and rotation-symmetric functions. *Journal of Universal Computer Science*, 5:20–31, 1999.

SM08. Pantelimon Stanica and Subhamoy Maitra. Rotation symmetric Boolean functions - count and cryptographic properties. *Discrete Applied Mathematics*, 156(10):1567–1580, 2008.

Su21. Sihong Su. The lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced functions. *Discrete Applied Mathematics*, 297:60–70, 2021.

TL19. Deng Tang and Jian Liu. A family of weightwise (almost) perfectly balanced Boolean functions with optimal algebraic immunity. *Cryptography and Communications*, 11(6):1185–1197, 2019.

YCL+23. Lili Yan, Jingyi Cui, Jian Liu, Guangquan Xu, Lidong Han, Alireza Jolfaei, and Xi Zheng. Iga: An improved genetic algorithm to construct weightwise (almost) perfectly balanced Boolean functions with high weightwise nonlinearity. In *ACM Asia Conference on Computer and Communications Security*, page 638–648. Association for Computing Machinery, 2023.

ZJZQ23. Qinglan Zhao, Yu Jia, Dong Zheng, and Baodong Qin. A new construction of weightwise perfectly balanced functions with high weightwise nonlinearity. *Mathematics*, 11(5), 2023.

ZLC+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.

ZS23. Rui Zhang and Sihong Su. A new construction of weightwise perfectly balanced Boolean functions. *Advances in Mathematics of Communications*, 17(4):757–770, 2023.