Weightwise almost perfectly balanced functions: secondary constructions for all n and better weightwise nonlinearities

Agnese Gini, Pierrick Méaux

University of Luxembourg, Luxembourg
agnese.gini@uni.lu, pierrick.meaux@uni.lu

Abstract. The design of FLIP stream cipher presented at Eurocrypt 2016 motivates the study of Boolean functions with good cryptographic criteria when restricted to subsets of $\mathbb{F}_2^n$. Since the security of FLIP relies on properties of functions restricted to subsets of constant Hamming weight, called slices, several studies investigate functions with good properties on the slices, *i.e.* weightwise properties. A major challenge is to build functions balanced on each slice, from which we get the notion of Weightwise Almost Perfectly Balanced (WAPB) functions. Although various constructions of WAPB functions have been exhibited since 2017, building WAPB functions with high weightwise nonlinearities remains a difficult task. Lower bounds on the weightwise nonlinearities of WAPB functions are known for very few families, and exact values were computed only for functions in at most 16 variables.
In this article, we introduce and study two new secondary constructions of WAPB functions. This new strategy allows us to bound the weightwise nonlinearities from those of the parent functions, enabling us to produce WAPB functions with high weightwise nonlinearities. As a practical application, we build several novel WAPB functions in up to 16 variables by taking parent functions from two different known families. Moreover, combining these outputs, we also produce the 16-variable WAPB function with the highest weightwise nonlinearities known so far.

Keywords: FLIP cipher, Boolean functions, Weightwise (almost) perfectly balanced function, Weightwise nonlinearity.

1 Introduction

The study of Boolean functions with good cryptographic criteria when restricted to subsets of $\mathbb{F}_2^n$ became recently relevant due to their role in the security of FLIP stream cipher introduced by Méaux, Journault, Standaert, and Carlet at Eurocrypt 2016 [MJSC16]. FLIP's filter function is evaluated on a set of vectors of $\mathbb{F}_2^n$ having constant Hamming weight, as a consequence of design choices to make the cipher homomorphic-friendly. Hence, the security of FLIP family relates to certain properties of Boolean functions when they are restricted to some input subsets, *e.g.* slices $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$ of the hypercube $\mathbb{F}_2^n$. In [CMR17], the Boolean cryptographic criteria on restricted sets such as balancedness, nonlinearity and algebraic immunity were first studied. In particular, the concept of balancedness for a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, *i.e.* the preimages of 0 and 1 under f have the same cardinality, is extended to *weightwise perfectly balancedness*, *i.e.* all the restrictions of f to the slices $\mathsf{E}_{k,n}$ are balanced. As balanced functions are generally suitable for avoiding constructions with statistical biases, we expect the same for Weightwise Perfectly Balanced (WPB) functions in the context of inputs with fixed Hamming weight. More precisely, WPB functions are functions balanced on each slice with $1 \leq k \leq n-1$, equal to 0 in 0_n and to 1 in 1_n. However, WPB functions only exist for n a power of 2, since the balancedness on each slice requires the cardinality of each one of these sets to be even. Thus, the authors also introduced the notion of *weightwise almost perfectly balancedness* allowing a tolerance for slices of odd cardinality sufficiently small to preserve the reliability of these functions. Namely, for Weightwise Almost Perfectly Balanced (WAPB) functions we allow the cardinalities of the preimages of 0 and 1 to differ of 1 when the slice $\mathsf{E}_{k,n}$ has an odd cardinality.

Carlet *et al.* also provided in [CMR17] a recursive construction of WAPB functions for all n and a secondary construction of WPB functions. Afterwards, several other constructions have been proposed [LM19, TL19, LS20, MS21, ZS21, MSL21, GS22, ZS22, MPJ+22, GM22]. Being WAPB

function relevant in a cryptographic context, all these works aim to produce W(A)PB functions having good parameters relatively to the other cryptographic criteria such as restricted and global nonlinearity, algebraic immunity and degree. For instance, the functions proposed in [TL19] have optimal algebraic immunity, while the family described in [LM19] has good nonlinearity on all the slices, also called weightwise nonlinearities. In fact, the weightwise nonlinearity is the criterion that got the most attention in these constructions, often used to compare the different families. It is also the criterion with more open problems; differently from $\mathbb{F}_2^n$ (and the associated concept of bent functions), the maximum nonlinearity that can take a function restricted to a slice is unknown, and bounds on this maximum are studied in different works [CMR17, MZD19, GM22]. Furthermore, a notion of restricted Walsh transform has been introduced [MMM+18] to study better the weightwise nonlinearity. Except for the exact weightwise nonlinearities obtained experimentally on functions up to 16 variables, in very few cases, this parameter is known or even bounded for a construction. There are lower bounds known for two families of WPB functions, the recursive construction of [CMR17], whose weightwise nonlinearities are studied in [Su21], and one construction from [LM19].

In this article, we present two novel secondary constructions of WAPB functions for all n with proven bound on their weightwise nonlinearities, and we use them to build a 16-variable WPB function with the highest weightwise nonlinearities exhibited so far. More precisely, our contributions are the following. First, we study the impact of the addition of symmetric functions and of Siegenthaler's construction on the restricted Walsh transform. Secondly, we introduce the notion of Special WAPB (SWAPB) functions, a sub-family where we fix the support size on the slices of odd cardinality. Then, we give two secondary constructions of SWAPB functions, first from an n-variable SWAPB function and an n-variable WAPB function to an $(n+1)$-variable WAPB function, and then from an n-variable SWAPB function to a $n+t$-variable SWAPB function. Very differently from the precedent constructions, these functions are obtained combining Siegenthaler's construction and addition of symmetric functions, which allows to derive a lower bound on the weightwise nonlinearities of the child function from the parameters of the parent functions. Furthermore, we prove that the recursive construction of [CMR17] gives WAPB functions that are inherently special. Finally, we provide an experimental part, where we determine the exact parameters of functions in 8 and 16 variables. Specifically, we first build 8 and 16-variable WPB functions from our second construction seeded with CMR functions and with LM functions, *i.e.* functions from [CMR17] and [LM19], respectively. Thereafter, we combine (slice by slice) these functions in 16 variables to obtain the 16-variable function with the highest weightwise nonlinearities exhibited so far.

Organization: In Section 2 we give the necessary preliminaries on Boolean functions and (weightwise) cryptograhic criteria, and properties on the parity of binary coefficients. In Section 3 we introduce and study special WAPB functions, we give two secondary constructions and prove a lower bound on their weightwise nonlinearities. We prove that CMR WAPB functions are special functions in Section 4. Then, We give concrete functions in 8 and 16 variables, they are obtained from one of our new construction seeded by CMR functions, by LM functions, of mixing such functions to obtain higher weightwise nonlinearities. Finally, we conclude briefly the article in Section 5.

2 Preliminaries

In addition to classic notations we use $[a, b]$ to denote the subset of all integers between a and b: $\{a, a+1, \ldots, b\}$. For readability we use the notation $+$ instead of $\oplus$ to denote the addition in $\mathbb{F}_2$ and $\sum$ instead of $\bigoplus$. For a vector $v \in \mathbb{F}_2^n$ we denote $\mathsf{w_H}(v)$ its Hamming weight $\mathsf{w_H}(v) = |\{i \in [1, n] \,|\, v_i = 1\}|$.

2.1 Boolean functions and weightwise considerations

In this subsection we recall the main concepts on Boolean functions and their weightwise properties we will use in this article. We refer to *e.g.* [Car21] for Boolean functions and cryptographic parame-

ters and to [CMR17] for the weightwise properties, also called properties on the slices. For $k \in [0, n]$ we call slice of the Boolean hypercube (of dimension n) the set $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$. Accordingly, the Boolean hypercube is partitioned into $n+1$ slices where the elements have the same Hamming weight.

Definition 1 (Boolean Function). *A Boolean function f in n variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all n-variable Boolean functions is denoted $\mathcal{B}_n$.*

Definition 2 (Algebraic Normal Form (ANF) and degree). *We call Algebraic Normal Form of a Boolean function f its n-variable polynomial representation over $\mathbb{F}_2$ (i.e. belonging to $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$):*

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq [1,n]} a_I \left(\prod_{i \in I} x_i \right)$$

where $a_I \in \mathbb{F}_2$. The (algebraic) degree of f, denoted $\mathsf{deg}(f)$ is:

$$\mathsf{deg}(f) = \max_{I \subseteq [1,n]} \{|I| \,|\, a_I = 1\} \text{ if } f \text{ is not null}, 0 \text{ otherwise.}$$

To denote when a definition or a property is restricted to a slice we will use the subscript k. For example, for a n-variable Boolean function f we denote its support $\mathsf{supp}(f) = \{x \in \mathbb{F}_2^n \,|\, f(x) = 1\}$ and we refer to $\mathsf{supp}_k(f)$ for its support restricted to a slice, that is $\mathsf{supp}(f) \cap \mathsf{E}_{k,n}$.

Definition 3 (Balancedness). *A Boolean function $f \in \mathcal{B}_n$ is called balanced if $|\mathsf{supp}(f)| = 2^{n-1} = |\mathsf{supp}(f+1)|$.*

For $k \in [0, n]$, f is said balanced on the slice k if $||\mathsf{supp}_k(f)| - |\mathsf{supp}_k(f+1)|| \leq 1$. In particular when $|\mathsf{E}_{k,n}|$ is even $|\mathsf{supp}_k(f)| = |\mathsf{supp}_k(f+1)| = |\mathsf{E}_{k,n}|/2$.

Definition 4 (Weightwise (Almost) Perfectly Balanced Function (WPB and WAPB)). *Let $m \in \mathbb{N}^*$ and f be a Boolean function in $n = 2^m$ variables. It will be called weightwise perfectly balanced (WPB) if, for every $k \in [1, n-1]$, f is balanced on the slice k, that is $\forall k \in [1, n-1], |\mathsf{supp}_k(f)| = \binom{n}{k}/2$, and:*

$$f(0, \cdots, 0) = 0, \quad \text{and } f(1, \cdots, 1) = 1.$$

The set of WPB functions in 2^m variables is denoted $\mathcal{WPB}_m$.

When n is not a power of 2, other weights than $k = 0$ and n give slices of odd cardinality, in this case we call $f \in \mathcal{B}_n$ weightwise almost perfectly balanced (WAPB) if:

$$|\mathsf{supp}_k(f)| = \begin{cases} |\mathsf{E}_{k,n}|/2 & \text{if } |\mathsf{E}_{k,n}| \text{ is even,} \\ (|\mathsf{E}_{k,n}| \pm 1)/2 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd.} \end{cases}$$

The set of WAPB functions in n variables is denoted $\mathcal{WAPB}_n$.

Note that the definition of WAPB functions above (as introduced in [CMR17]) is more general than the one of WPB functions, for $n = 2^m$ the WPB functions are a subset of the WAPB functions since the value in 0_n and 1_n can be taken freely for the latter. Alternatively, $\mathcal{WAPB}_n$ corresponds to the set of functions at maximal distance from the set of n-variable symmetric functions $\mathcal{SYM}_n$, that is $\mathcal{WAPB}_n$ is metrically regular for the Hamming distance and $\mathcal{SYM}_n$ is its metric complement. We refer to [Tok12] for the notion of metrically regular sets and the survey [Obl20]. In [SSB18] various metrically regular sets are considered, WAPB functions are presented under the name of maximally asymmetric functions, and the authors provide the cardinality of $\mathcal{WAPB}_n$ (also given in [IMM13]) and the number of balanced WAPB functions.

Definition 5 (Nonlinearity and weightwise nonlinearity). *The nonlinearity* $\mathsf{NL}(f)$ *of a Boolean function* $f \in \mathcal{B}_n$*, where* n *is a positive integer, is the minimum Hamming distance between* f *and all the affine functions in* $\mathcal{B}_n$*:*

$$\mathsf{NL}(f) = \min_{g,\, \mathsf{deg}(g)\leq 1} \{d_H(f,g)\},$$

where $g(x) = a \cdot x + \varepsilon$*,* $a \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2$ *(where* $\cdot$ *is some inner product in* $\mathbb{F}_2^n$*; any choice of an inner product will give the same value of* $\mathsf{NL}(f)$*).*

For $k \in [0,n]$ *we denote* NL_k *the nonlinearity on the slice* k*, the minimum Hamming distance between* f *restricted to* $\mathsf{E}_{k,n}$ *and the restrictions to* $\mathsf{E}_{k,n}$ *of affine functions over* $\mathbb{F}_2^n$*. Accordingly:*

$$\mathsf{NL}_k(f) = \min_{g,\, \mathsf{deg}(g)\leq 1} |\mathsf{supp}_k(f+g)|.$$

We also recall the concept of Walsh transform, and restricted Walsh transform [MMM+18], which are of particular interest to study the (restricted) nonlinearity or balancedness.

Definition 6 (Walsh transform and restricted Walsh transform). *Let* $f \in \mathcal{B}_n$ *be a Boolean function, its Walsh transform* W_f *at* $a \in \mathbb{F}_2^n$ *is defined as:*

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

Let $f \in \mathcal{B}_n$*,* $S \subset \mathbb{F}_2^n$*, its Walsh transform restricted to* S *at* $a \in \mathbb{F}_2^n$ *is defined as:*

$$W_{f,S}(a) := \sum_{x \in S} (-1)^{f(x)+ax}.$$

For $S = \mathsf{E}_{k,n}$ *we denote* $W_{f,\mathsf{E}_{k,n}}(a)$ *by* $\mathcal{W}_{f,k}(a)$*.*

Property 1 (Nonlinearity on the slice, adapted from [CMR17], Proposition 6)**.** *Let* $n \in \mathbb{N}^*, k \in [0,n]$*, for every* n*-variable Boolean function* f *over* $\mathsf{E}_{k,n}$*:*

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

Property 2 (Balancedness on the slice and restricted Walsh transform)**.** *Let* $n \in \mathbb{N}^*, k \in [0,n]$*,* $f \in \mathcal{B}_n$ *is balanced over* $\mathsf{E}_{k,n}$ *if and only if:*

$$\mathcal{W}_{f,k}(0_{|\mathsf{E}_{k,n}|}) = \begin{cases} 0 & \text{if } |\mathsf{E}_{k,n}| \text{ is even,} \\ \pm 1 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd.} \end{cases}$$

2.2 Siegenthaler's construction, symmetric functions

In the following we recall the Siegenthaler construction, a common secondary construction which combines two n-variable functions to obtain an $(n+1)$-variable function:

Definition 7 (Siegenthaler's Construction). *Let* $n \in \mathbb{N}$*,* $f_0, f_1 \in \mathcal{B}_n$*, we call Siegenthaler's construction* f *from components* f_0 *and* f_1*:*

$$f \in \mathcal{B}_{n+1}, \quad \forall x \in \mathbb{F}_2^n, \forall y \in \mathbb{F}_2,\ f(x,y) = (1+y)\cdot f_0(x) + y \cdot f_1(x).$$

We recall definitions and properties on symmetric functions since they will be used for the main secondary construction we present in the article. Symmetric functions are functions such that changing the order of the inputs does not change the output. They have been the focus of many works for their cryptographic parameters such as [Car04, CV05, BP05, DMS06, QLF07, SM07, QFLW09, CL11], or more recently [TLD16, CM19, CZGC19, Méa19, Méa21, CM22].

Definition 8 (Symmetric Functions). *Let $n \in \mathbb{N}^*$, the Boolean symmetric functions are the functions which are constant on each $\mathsf{E}_{k,n}$ for $k \in [0,n]$. The set of n variable symmetric functions is denoted $\mathcal{SYM}_n$ and $|\mathcal{SYM}_n| = 2^{n+1}$. We distinguish families of symmetric functions:*

- *Elementary symmetric functions. Let $i \in [0,n]$, the elementary symmetric function of degree i in n variables, denoted $\sigma_{i,n}$, is the function which ANF contains all monomials of degree i and no monomials of other degrees.*
- *Threshold Functions. Let $d \in [0,n]$, the threshold function of threshold d is defined as:*
$$\forall x \in \mathbb{F}_2^n, \quad \mathsf{T}_{d,n}(x) = 1 \text{ if and only if } \mathsf{w_H}(x) \geq d.$$
- *Slice indicator functions. Let $k \in [0,n]$, the indicator function of the slice of weight k is defined as:*
$$\forall x \in \mathbb{F}_2^n, \quad \varphi_{k,n}(x) = 1 \text{ if and only if } \mathsf{w_H}(x) = k.$$

The $n+1$ n-variable symmetric functions of each family form a basis of $\mathcal{SYM}_n$ (that is every element of $\mathcal{SYM}_n$ can be written as a linear combination of these $n+1$ functions). Now, we precise on how to express $\varphi_{k,n}$ as a sum of symmetric elementary function. To do so, we use the expression of threshold functions in term of symmetric elementary functions from [Méa19], since $\varphi_{k,n}$ is the sum of two consecutive threshold functions.

Property 3 (Algebraic normal form of threshold functions (adapted from [Méa19], Theorem 1))**.** *Let $n, d \in \mathbb{N}^*$ such that $0 < d \leq n+1$, let $D = 2^{\lceil \log d \rceil}$. For $v \in \mathbb{F}_2^n$ we denote $\overline{v}$ the complementary of $v \in \mathbb{F}_2^n$: $\forall i \in [1,n]$, $\overline{v_i} = 1 - v_i$. We denote $\preceq$ the partial order on $\mathbb{F}_2^n$ defined as $a \preceq b \Leftrightarrow \forall i \in [1,n], a_i \leq b_i$, where $\leq$ denotes the usual order on $\mathbb{Z}$ and the elements a_i and b_i of $\mathbb{F}_2$ are identified to 0 or 1 in $\mathbb{Z}$. We denote the set:*

$$A_d = \{v \in [0, D-1] \,|\, v \preceq D - d\} = \{v \in \mathbb{F}_2^{\lceil \log d \rceil} \,|\, v \preceq \overline{d-1}\},$$

where $d-1$ is considered over $\log D - 1$ bits. We also denote:

$$B_{d,n} = \{kD + d + v \,|\, k \in \mathbb{N}, v \in A_d\} \cap [1,n] = \{kD - v \,|\, k \in \mathbb{N}^*, v \in A_d\} \cap [1,n].$$

The ANF of the threshold function is given by: $\mathsf{T}_{d,n} = \sum_{i \in B_{d,n}} \sigma_{i,n}$.

Since $\varphi_{k,n} = \mathsf{T}_{k,n} + \mathsf{T}_{k+1,n}$ its ANF is given by $B_{k,n} \Delta B_{k+1,n}$, where Δ denotes the symmetric difference of sets (*i.e.* $A \Delta B = (A \cup B) \setminus (A \cap B)$).

2.3 Parity of binomial coefficients

This section contains results about binomial coefficients that will be used in this article. As a convention we set $\binom{a}{b} = 0$ if $b < 0$ and $b > a$.

Property 4 (Pascal's formula)**.** *Let $a, b \in \mathbb{N}$. Then*

$$\binom{a}{b} = \binom{a-1}{b} + \binom{a-1}{b-1}.$$

Property 5 (Vandermonde Convolution)**.** *Let $a, b, c \in \mathbb{N}$. Then*

$$\binom{a+c}{b} = \sum_{j=0}^{b} \binom{c}{b-j} \binom{a}{j}.$$

Property 6 (Lucas' Theorem, *e.g.* [Fin47])**.** *Let $a, b, p \in \mathbb{N}$ be integers such that $a > b$ and p is a prime. Consider their p-adic expansions $a = \sum_{j=0}^{q} a_j p^j$ and $b = \sum_{j=0}^{q} b_j p^j$ such that $0 \leq a_j < p$ and $0 \leq b_j < p$ for each $j \in [0,q]$ and $a_q \neq 0$. Then*

$$\binom{a}{b} \equiv \prod_{j=0}^{q} \binom{a_j}{b_j} \pmod{p}.$$

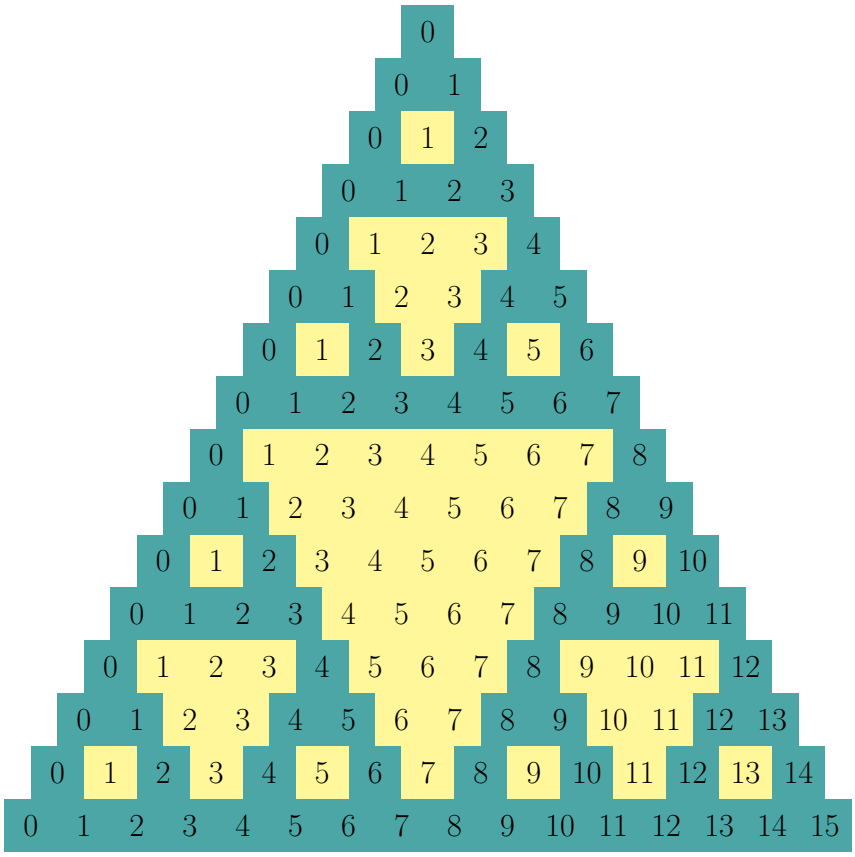

Fig. 1. Binomial coefficients and parity for $n \in [0, 15]$. The square labeled with k at level n corresponds to the binomial coefficient $\binom{n}{k}$and it is colored in yellow if the coefficient is even and teal if the coefficient is odd.

Proposition 1. *Let $a, b \in \mathbb{N}$ and their binary decomposition be $a = \sum_{j=0}^{q_a} a_j 2^j$ and $b = \sum_{j=0}^{q_b} b_j 2^j$ such that $0 \leq a_j < 2$ and $0 \leq b_j < 2$ for each j, and $a_{q_a}, b_{q_b} \neq 0$.*

1. *$\binom{2^a}{b}$ is even for $0 < b < 2^a$.*
2. *If $a \equiv 0 \mod 2$ and $b \equiv 1 \mod 2$, then $\binom{a}{b} \equiv 0 \mod 2$.*
3. *If $a \equiv 1 \mod 2$ and $b \equiv 0 \mod 2$, then $\binom{a}{b} \equiv \binom{a-1}{b} \mod 2$.*
4. *$\binom{a}{b} \equiv 1 \mod 2$ if and only if for all $j \in [0, q_b]$ it holds $a_j \geq b_j$.*

Proof. 1. If $0 < b < 2^a$, there exists at least a coefficient $b_j = 1$ in the binary expansion of b for $j < a$. Then by Property 6 $\binom{2^a}{b} \equiv 0 \mod 2$ since $\binom{0}{b_j} \equiv 0$.

2. If $a \equiv 0 \mod 2$, then $0 \equiv a\binom{a-1}{b-1} \equiv b\binom{a}{b} \equiv \binom{a}{b} \mod 2$.
3. This comes from Property 4 and point 2.
4. From Lucas' theorem we have that $\binom{a}{b} \equiv 1 \mod 2$ if and only if $\binom{a_j}{b_j} \equiv 1 \mod 2$ for each $j \in [0, q_b]$ if and only if $a_j \geq b_j$ for each $j \in [0, q_b]$.

□

We prove the following fact, illustrated by Figure 1 for $n < 16$.

Lemma 1. *Let $u \geq 2$ and $t \in [1, 2^{u-2}]$, for all $k \in [2^{u-1} - 2t + 1, 2^{u-1} - 1]$ the binomial coefficient $\binom{2^u - 2t}{k}$ is even.*

Proof. We write $2^u - 2t = 2^{u-1} + (2^{u-1} - 2t)$, then using Property 5 we obtain

$$\binom{2^u - 2t}{k} = \sum_{j=0}^{k} \binom{2^{u-1} - 2t}{k - j} \binom{2^{u-1}}{j}$$

Since the coefficients $\binom{2^{u-1}}{j}$ are even for $0 < j < 2^{u-1}$ by Proposition 1.1, reducing the convolution modulo 2 we obtain (recall that $\binom{a}{b} = 0$ if $b < 0$ and $b > a$, therefore for certain values of k some addenda can be zero by default):

$$\binom{2^u - 2t}{k} \equiv \binom{2^{u-1} - 2t}{k} + \binom{2^{u-1} - 2t}{k - 2^{u-1}} \mod 2.$$

Therefore, $\binom{2^u-2t}{k}$ is even if $k \in [2^{u-1} - 2t + 1, 2^{u-1} - 1]$. □

3 Special WAPB functions and secondary constructions

In this section, we begin with properties of the restricted Walsh transform relatively to Siegenthaler's construction and addition of symmetric functions. Then, we define a subset of balanced WAPB functions and give a construction to transform any WAPB function into a function in this subclass. Finally, we provide and study a secondary construction of $(n + 1)$-variable WAPB function from two n-variable WAPB functions.

3.1 Restricted Walsh transform and properties

First, we study the weightwise restricted Walsh transform of functions obtained through Siegenthaler's construction.

Proposition 2 (Weightwise restricted Walsh transform and Siegenthaler's construction). *Let $n \in \mathbb{N}$, $f_0, f_1 \in \mathcal{B}_n$, f obtained through Siegenthaler's construction with components f_0 and f_1 has the following property:*

$$\forall k \in [0, n], \forall (a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2, \quad \mathcal{W}_{f,k}(a, b) = \mathcal{W}_{f_0,k}(a) + (-1)^b \mathcal{W}_{f_1,k-1}(a).$$

Proof. We rewrite $\mathcal{W}_{f,k}(a, b)$:

$$\begin{aligned}
\mathcal{W}_{f,k}(a, b) &= \sum_{(x,y)\in \mathsf{E}_{k,n+1}} (-1)^{f(x,y)+(a,b)\cdot(x,y)} \\
&= \sum_{x\in \mathsf{E}_{k,n}} (-1)^{f(x,0)+(a,b)\cdot(x,0)} + \sum_{x\in \mathsf{E}_{k-1,n}} (-1)^{f(x,1)+(a,b)\cdot(x,1)} \\
&= \sum_{x\in \mathsf{E}_{k,n}} (-1)^{f_0(x)+a\cdot x} + \sum_{x\in \mathsf{E}_{k-1,n}} (-1)^{f_1(x)+a\cdot x+b} \\
&= \mathcal{W}_{f_0,k}(a) + (-1)^b \mathcal{W}_{f_1,k-1}(a).
\end{aligned}$$

□

Proposition 3 (Weightwise nonlinearity bound on Siegenthaler's construction). *Let $n \in \mathbb{N}$, $f_0, f_1 \in \mathcal{B}_n$, f obtained through Siegenthaler's construction with components f_0 and f_1 has the following property:*

$$\forall k \in [0, n], \quad \mathsf{NL}_k(f) \geq \mathsf{NL}_k(f_0) + \mathsf{NL}_{k-1}(f_1).$$

Proof. First, we bound $\max_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2} |\mathcal{W}_{f,k}(a, b)|$ using Proposition 2:

$$\begin{aligned}
\max_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2} |\mathcal{W}_{f,k}(a, b)| &= \max_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2} |\mathcal{W}_{f_0,k}(a) + (-1)^b \mathcal{W}_{f_1,k-1}(a)| \\
&= \max_{a\in\mathbb{F}_2^n} \left(|\mathcal{W}_{f_0,k}(a)| + |\mathcal{W}_{f_1,k-1}(a)|\right).
\end{aligned}$$

Then, we use Property 1:

$$\begin{aligned}\max_{a\in\mathbb{F}_2^n}(|\mathcal{W}_{f_0,k}(a)|+|\mathcal{W}_{f_1,k-1}(a)|) &\leq \max_{a\in\mathbb{F}_2^n}|\mathcal{W}_{f_0,k}(a)|+\max_{a\in\mathbb{F}_2^n}|\mathcal{W}_{f_1,k-1}(a)|\\ &\leq |\mathsf{E}_{k,n}|-2\mathsf{NL}_k(f_0)+|\mathsf{E}_{k-1,n}|-2\mathsf{NL}_{k-1}(f_1)\\ &\leq |\mathsf{E}_{k,n+1}|-2(\mathsf{NL}_k(f_0)+\mathsf{NL}_{k-1}(f_1)).\end{aligned}$$

Finally, using again Property 1: $\mathsf{NL}_k(f)\geq \mathsf{NL}_k(f_0)+\mathsf{NL}_{k-1}(f_1)$.

□

In the following we consider the impact on the weightwise restricted Walsh transform of adding a symmetric function.

Proposition 4 (Weightwise restricted Walsh transform and addition of symmetric function). *Let $n\in\mathbb{N}^*$, $k\in[0,n]$ and $f\in\mathcal{B}_n$, the following holds on $f+\varphi_{k,n}$*

$$\forall a\in\mathbb{F}_2^n, \forall i\in[0,n]\setminus\{k\}, \mathcal{W}_{f+\varphi_{k,n},i}(a)=\mathcal{W}_{f,i}(a), \text{ and } \mathcal{W}_{f+\varphi_{k,n},k}(a)=-\mathcal{W}_{f,i}(a).$$

Proof. Rewriting $\mathcal{W}_{f+\varphi_{k,n},i}(a)$ we obtain:

$$\mathcal{W}_{f+\varphi_{k,n},i}(a)=\sum_{x\in\mathsf{E}_{i,n}}(-1)^{(f+\varphi_{k,n})(x)+a\cdot x}=\begin{cases}\mathcal{W}_{f,i}(a) & \text{if } i\neq k,\\ -\mathcal{W}_{f,i}(a) & \text{if } i=k.\end{cases}$$

□

consequently, Proposition 4 directly implies that adding symmetric functions do not alter the weightwise balancedness nor the weightwise nonlinearity of a function.

3.2 Special WAPB functions

In the following we specify a sub-part of balanced WAPB functions called special WAPB. To do so we use the characterization of WAPB through the weightwise restricted Walsh transform.

Definition 9 (Special Weightwise Almost Perfectly Balanced functions (SWAPB)). *Let $n\in\mathbb{N}^*$, f is a WAPB function if:*

$$\mathcal{W}_{f,k}(0_n)=\begin{cases}0 & \text{if } |\mathsf{E}_{k,n}| \text{ is even,}\\ \pm 1 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd.}\end{cases}$$

Additionally, the function is called special WAPB (SWAPB) if:

$$\mathcal{W}_{f,k}(0_n)=\begin{cases}0 & \text{if } |\mathsf{E}_{k,n}| \text{ is even,}\\ 1 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd and } k<n/2,\\ -1 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd and } k>n/2.\end{cases}$$

The set of SWAPB functions in n variables is denoted $\mathcal{SWAPB}_n$.

Property 1 (Basic properties of SWAPB functions). Let $n\in\mathbb{N}^*$, the following hold for $\mathcal{SWAPB}_n$:

- $\mathcal{SWAPB}_n\subset\mathcal{WAPB}_n$,
- if $n=2^m$ then $\mathcal{SWAPB}_n=\mathcal{WPB}_m$,
- $|\mathcal{SWAPB}_n|=\prod_{k=0}^{n}\binom{\nu}{\lfloor\nu/2\rfloor}$ for $\nu=\binom{n}{k}$.

The next proposition allows to build a SWAPB function from a WAPB function.

Proposition 5 (From WAPB to SWAPB). *Let $n \in \mathbb{N}^*$ and $f \in \mathcal{WAPB}_n$. Let $S_f \subset [0,n]$ the set defined as $S_f = \{k \in [0, n/2[,\ |\mathcal{W}_{f,k}(0_n) = -1\} \cup \{k \in]n/2, n],\ |\mathcal{W}_{f,k}(0_n) = 1\}$, the function $f' = f + \sum_{k \in S_f} \varphi_{k,n}$ belongs to $\mathcal{SWAPB}_n$.*

Proof. Using the characterization through the restricted Walsh transform and the definition of S_f we get:

$$\mathcal{W}_{f,k}(0_n) = \begin{cases} 0 & \text{if } |\mathsf{E}_{k,n}| \text{ is even,} \\ 1 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd, } k < n/2, \text{ and } k \notin S_f, \\ -1 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd, } k < n/2, \text{ and } k \in S_f, \\ -1 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd, } k > n/2, \text{ and } k \notin S_f, \\ 1 & \text{if } |\mathsf{E}_{k,n}| \text{ is odd, } k > n/2, \text{ and } k \in S_f. \end{cases}$$

Applying Proposition 4, the value of $\mathcal{W}_{f',k}(0_n)$ is flipped for all $k \in S_f$ and unchanged for the other weights (relatively to f). Thereafter, f' is SWAPB. □

3.3 Secondary constructions of WAPB functions

We introduce a secondary construction from two n-variables SWAPB functions to one $n+1$ SWAPB function. Repetitively using this construction allows us to build WAPB functions for all n.

Construction 1

Input: Let $n \in \mathbb{N}^*$ f_0, f_1 two n-variable SWAPB functions.
Output: f an $n+1$-variable SWAPB function.

1: Define S_n as $S_n = \{k \in [1, n/2[\,|\,\binom{n}{k-1} \equiv \binom{n}{k} \equiv 1 \mod 2\}$.
2: **for** $k \in S_n$ **do**
3: $\quad f_1 \leftarrow f_1 + \varphi_{k-1,n} + \varphi_{n-k,n}$,
4: **end for**
5: Compute $f = (1 + x_{n+1})f_0 + x_{n+1}f_1$.
6: **return** f.

Theorem 1 (Special weightwise almost perfectly balancedness of Construction 1). *Let $n \in \mathbb{N}^*$, $f_0 \in \mathcal{SWAPB}_n$, and $f_1 \in \mathcal{WAPB}_n$, the function f given by Construction 1 belongs to $\mathcal{SWAPB}_{n+1}$.*

Proof. By construction f is obtained from Siegenthaler's construction with components f_0 and $f_1' = f_1 + \sum_{k \in S_n} (\varphi_{k-1,n} + \varphi_{n-k,n})$ where f_0 and f_1 are SWAPB functions. Accordingly, the restricted Walsh transform values of f can be obtained from the ones of f_0 and f_1 using Proposition 2. The values of the restricted Walsh transform of f_0 and f_1 are given by Definition 9 since these two functions are SWAPB. Then, $\mathcal{W}_{f_1',k}(0_n)$ can be determined by using Proposition 4.

We do a disjunction of cases to determine $\mathcal{W}_{f,k}(0_{n+1})$, considering the parity of $\binom{n}{k-1}$ and $\binom{n}{k}$, for $k \in [0, n/2[$:

– Case $\binom{n}{k-1} \equiv \binom{n}{k} \equiv 0 \mod 2$. In this case:

$$\mathcal{W}_{f,k}(0_{n+1}) = \mathcal{W}_{f_0,k}(0_n) + \mathcal{W}_{f_1',k-1}(0_n) = 0 + \mathcal{W}_{f_1,k-1}(0_n) = 0,$$

and

$$\mathcal{W}_{f,n+1-k}(0_{n+1}) = \mathcal{W}_{f_0,n-k+1}(0_n) + \mathcal{W}_{f_1',n-k}(0_n) = 0 + \mathcal{W}_{f_1,n-k}(0_n) = 0.$$

– Case $\binom{n}{k-1} \not\equiv \binom{n}{k} \mod 2$. In this case:

$$\mathcal{W}_{f,k}(0_{n+1}) = \mathcal{W}_{f_0,k}(0_n) + \mathcal{W}_{f'_1,k-1}(0_n) = \mathcal{W}_{f_0,k}(0_n) + \mathcal{W}_{f_1,k-1}(0_n) = 1,$$

and $\mathcal{W}_{f,n+1-k}(0_{n+1}) = \mathcal{W}_{f_0,n-k+1}(0_n) + \mathcal{W}_{f_1,n-k}(0_n) = -1$.

– Case $\binom{n}{k-1} \equiv \binom{n}{k} \equiv 1 \mod 2$. In this case:

$$\mathcal{W}_{f,k}(0_{n+1}) = \mathcal{W}_{f_0,k}(0_n) + \mathcal{W}_{f'_1,k-1}(0_n) = 1 + \mathcal{W}_{f_1+\varphi_{k,n},k-1}(0_n) = 1 - 1 = 0,$$

and

$$\begin{aligned}\mathcal{W}_{f,n+1-k}(0_{n+1}) &= \mathcal{W}_{f_0,n-k+1}(0_n) + \mathcal{W}_{f'_1,n-k}(0_n) \\ &= -1 + \mathcal{W}_{f_1+\varphi_{n-k,n},n-k}(0_n) = -1 + 1 = 0.\end{aligned}$$

Using Pascal's formula $|\mathsf{E}_{k,n+1}|$ is even if and only if $\binom{n}{k-1} \equiv \binom{n}{k} \mod 2$, and regrouping the different cases we obtain:

$$\mathcal{W}_{f,k}(0_{n+1}) = \begin{cases} 0 & \text{if } |\mathsf{E}_{k,n+1}| \text{ is even,} \\ 1 & \text{if } |\mathsf{E}_{k,n+1}| \text{ is odd and } k < (n+1)/2, \\ -1 & \text{if } |\mathsf{E}_{k,n+1}| \text{ is odd and } k > (n+1)/2. \end{cases}$$

Therefore, $f \in \mathcal{SWAPB}_n$.

□

Remark 1. From Proposition 1 we have that for each $n \in \mathbb{N}$ $S_n = \emptyset$ if $n \equiv 0 \mod 2$. Therefore, if n is even, the input function f_1 of Construction 1 is not modified by Step 1 to 4. Thus, one can output directly $f = (1 + x_{n+1})f_0 + x_{n+1}f_1$.

Combining Proposition 5 and Theorem 1 enables us to obtain a SWAPB function in $n + 1$ variable from any n variable WAPB function. Since the obtained function is SWAPB, the theorem can be reapplied with twice this function. Thus, repeating this procedure allows us to build SWAPB functions for all $n' > n$. Moreover, the weightwise nonlinearity of such built functions can be bounded using Proposition 3. Thereafter, we describe the construction obtained by using t times the same SWAPB function, *i.e.* Construction 2.

Theorem 2 (Special weightwise almost perfectly balancedness and weightwise nonlinearity bound of Construction 2). *Let $n, t \in \mathbb{N}^*$ and $f \in \mathcal{SWAPB}_n$, the function g generated by Construction 2 is such that:*

$$g \in \mathcal{SWAPB}_{n+t}, \quad \text{and } \forall k \in [0, n+t],\ \mathsf{NL}_k(g) \geq \sum_{i=0}^{\min\{k,t\}} \binom{t}{i} \mathsf{NL}_{k-i}(f).$$

Proof. Note that for $t = 1$, it corresponds to:

$$\begin{aligned} g =& f + x_{n+1}\left(\sum_{k\in S_n} \varphi_{k-1,n} + \varphi_{n-k,n}\right) \\ =& (1 + x_{n+1})f + x_{n+1}\left(f + \sum_{k\in S_n} \varphi_{k-1,n} + \varphi_{n-k,n}\right), \end{aligned}$$

i.e. the function obtained by Construction 1 from $f_0 = f_1 = f$. Therefore, using Theorem 1, g is SWABP, and Proposition 3 gives the bound on $\mathsf{NL}_k(g)$. The results for $t > 1$ are obtained by immediate recursion. □

Construction 2

Input: Let $n, t \in \mathbb{N}^*$ f a n-variable SWAPB functions.
Output: g an $(n+t)$-variable SWAPB function.

Initialize g, $g \leftarrow f$.
for $i \in [1, t]$ **do**
  $h = 0$
  if $n + i - 1 \equiv 0 \mod 2$ **then**
    $S_{n+i-1} \leftarrow \{k \in [1, (n+i-1)/2[\,|\, \binom{n+i-1}{k-1} \equiv \binom{n+i-1}{k} \equiv 1 \mod 2\}$,
    for $k \in S_{n+i-1}$ **do**
      $h \leftarrow h + \varphi_{k-1,n+i-1} + \varphi_{n+i-1-k,n+i-1}$,
    end for
  end if
  $g \leftarrow g + x_{n+i}h$,
end for
return g.

4 Concrete constructions and parameters

In the first part of this section we recall the CMR construction from [CMR17] of WAPB functions for all n, and we prove that CMR functions are SWAPB. This implies that we can use functions from this family as seeds for Construction 2 to obtain other SWAPB functions. Hence, we collect some relevant cryptographic parameters of new WPB functions in 8 and 16 variables computed by using this strategy. Finally, we also apply Construction 2 with some LM functions from [LM19] as input, and we explain how to combine all these functions to get another function in $\mathcal{WPB}_4$ having high weightwise nonlinearity on every slice.

The methods that we applied to explicitly determine the functions and the value of their cryptographic parameters are discussed in Section 4.4

4.1 Building SWAPB functions from CMR construction

Definition 10 (CMR WAPB construction (adapted from [CMR17], Proposition 5)). *Let $n \in \mathbb{N}, n \geq 2$, the WAPB function f_n is recursively defined by $f_2(x_1, x_2) = x_1$ and for $n \geq 3$:*

$$f_n(x_1, \ldots, x_n) = \begin{cases} f_{n-1}(x_1, \ldots, x_{n-1}) & \text{if } n \text{ odd,} \\ f_{n-1}(x_1, \ldots, x_{n-1}) + x_{n-2} + \prod_{i=1}^{2^{d-1}} x_{n-i} & \text{if } n = 2^d; d > 1, \\ f_{n-1}(x_1, \ldots, x_{n-1}) + x_{n-2} + \prod_{i=1}^{2^d} x_{n-i} & \text{if } n = p \cdot 2^d; p \text{ odd.} \end{cases}$$

For example, the 16-variable function from this construction is:

$$\begin{aligned} f_{16} = {} & x_1 + x_2 + x_2x_3 + x_4 + x_4x_5 + x_6 + x_4x_5x_6x_7 \\ & + x_8 + x_8x_9 + x_{10} + x_8x_9x_{10}x_{11} + x_{12} + x_{12}x_{13} + x_{14} + x_8x_9x_{10}x_{11}x_{12}x_{13}x_{14}x_{15}, \end{aligned}$$

and the function f_i for $i \in [2, 15]$ is given by the ANF of f_{16} reduced to the variables with index smaller than i for i even and $i - 1$ for i odd.

We prove that functions from CMR WAPB construction are SWAPB.

Theorem 3. *Let $n \in \mathbb{N}, n \geq 2$ and f_n be the n-variable WAPB function from CMR construction (Definition 10). Then, $f_n \in \mathcal{SWAPB}_n$.*

Proof. If $n = 2^d$ for $d > 1$ we have that f_n is WPB by [CMR17, Proposition 5], hence it is special by Property 1. If $n = 3$, explicit computations show that $|\mathsf{supp}_0(f_3)| = 0 = (|\mathsf{E}_{0,3}| - 1)/2$,

$|\mathsf{supp}_1(f_3)| = 1 = (|\mathsf{E}_{1,3}| - 1)/2$, $|\mathsf{supp}_2(f_3)| = 2 = (|\mathsf{E}_{2,3}| + 1)/2$ and $|\mathsf{supp}_3(f_3)| = 1 = (|\mathsf{E}_{0,3}| + 1)/2$. This implies that $f_3 \in \mathcal{SWAPB}_3$, too.

Now, we prove that $f_n \in \mathcal{SWAPB}_n$ by induction on n for the missing values. Since our results extends [CMR17, Proposition 5], for the sake of simplicity, we recall here some facts from its proof denoting them by $(\star)$, and we refer to the original paper for details. Specifically, let us assume that for $n \geq 5$ for $2 \leq i < n$ f_i is SWAPB.

- If $n \equiv 1 \mod 2$, we can write it as $2\ell + 1$. For any $k \in [1, n-1]$ it holds $|\mathsf{supp}_k(f_n)| = |\mathsf{supp}_{k-1}(f_{n-1})| + |\mathsf{supp}_k(f_{n-1})|$. Namely, $\mathcal{W}_{f_n,k}(0_n) = \mathcal{W}_{f_{n-1},k}(0_{n-1}) + \mathcal{W}_{f_{n-1},k-1}(0_{n-1})$. From Proposition 1, we get that at least one cardinality between $|\mathsf{E}_{k-1,n-1}|$ and $|\mathsf{E}_{k,n-1}|$ is even. If both are even, $|\mathsf{E}_{k,n-1}| + |\mathsf{E}_{k-1,n-1}| = |\mathsf{E}_{k,n}|$ is even and $\mathcal{W}_{f_n,k}(0_n) = 0$.
  If one is odd, then $|\mathsf{E}_{k,n}|$ is also odd and we have the following cases:
  - Suppose $k < \ell$. Then $|\mathsf{supp}_k(f_n)| = |\mathsf{E}_{k,n-1}|/2 + |\mathsf{E}_{k-1,n-1}|/2 - 1/2 = (|\mathsf{E}_{k,n}| - 1)/2$, *i.e.* $\mathcal{W}_{f_n,k}(0_n) = 1$, since f_{n-1} is SWABP.
  - Suppose $k > \ell + 1$. Then $|\mathsf{supp}_k(f_n)| = |\mathsf{E}_{k,n-1}|/2 + |\mathsf{E}_{k-1,n-1}|/2 + 1/2 = (|\mathsf{E}_{k,n}| + 1)/2$, *i.e.* $\mathcal{W}_{f_n,k}(0_n) = -1$, since f_{n-1} is SWABP.
  - The central binomial $\binom{2\ell}{\ell}$ is always even for $\ell > 1$, since by Pascal's formula (Property 4) $\binom{2\ell}{\ell} \equiv 2^{2\ell} - 2\sum_{j=0}^{\ell-1}\binom{2\ell}{j} \equiv 0 \mod 2$. Being $n - 1 = 2\ell$, we have $|\mathsf{E}_{\ell,n-1}| \equiv 0 \mod 2$. Then, by Pascal's formula we obtain that $|\mathsf{E}_{\ell,n}| \equiv |\mathsf{E}_{\ell-1,n-1}| \mod 2$ and $|\mathsf{E}_{\ell+1,n}| \equiv |\mathsf{E}_{\ell+1,n-1}| \mod 2$.
    Therefore, since f_{n-1} is SWABP

$$\mathcal{W}_{f_n,\ell}(0_n) = \mathcal{W}_{f_{n-1},\ell}(0_{n-1}) + \mathcal{W}_{f_{n-1},\ell-1}(0_{n-1}) = \mathcal{W}_{f_{n-1},\ell-1}(0_{n-1}) = 1,$$

$$\mathcal{W}_{f_n,\ell+1}(0_n) = \mathcal{W}_{f_{n-1},\ell+1}(0_{n-1}) + \mathcal{W}_{f_{n-1},\ell}(0_{n-1}) = \mathcal{W}_{f_{n-1},\ell+1}(0_{n-1}) = -1.$$

  Moreover, $|\mathsf{supp}_0(f_n)| = |\mathsf{supp}_0(f_{n-1})| = 0$ and $|\mathsf{supp}_n(f_n)| = |\mathsf{supp}_n(f_{n-1})| = 1$. Therefore, f_n is SWAPB if $n \equiv 1 \mod 2$.
- Suppose $n = p \cdot 2^d$ and $p > 1$ odd. Let us denote $n_d = n - 2^d$. We have the following cases:
  - If $k = 0$, $|\mathsf{supp}_0(f_n)| = |\mathsf{supp}_0(f_n)| = 0$ $(\star)$.
  - If $k \in [1, 2^d - 1]$, it holds

$$|\mathsf{supp}_k(f_n)| = |\mathsf{supp}_k(f_{n_d})| + \frac{1}{2}\left(\binom{n}{k} - \binom{n_d}{k}\right) \ (\star),$$

    that is $\mathcal{W}_{f_n,k}(0_n) = \mathcal{W}_{f_{n_d},k}(0_{n_d})$.
    If $|\mathsf{E}_{k,n_d}| \equiv 0 \mod 2$, then $\mathcal{W}_{f_n,k}(0_n) = 0$. Conversely, since $(n_d)/2 = 2^{d-1}(p-1) > 2^d$ for $p > 3$, $\mathcal{W}_{f_n,k}(0_n) = \mathcal{W}_{f_{n_d},k}(0_{n_d}) = 1$. If $p = 3$, $\mathcal{W}_{f_n,k}(0_n) = 0$ for each $k \in [1, 2^d - 1]$, since f_{n_d} is WPB.
  - If $k \in [2^d, n-1]$, setting $s = k - 2^d$ it holds

$$|\mathsf{supp}_k(f_n)| = |\mathsf{supp}_k(f_{n_d})| + |\mathsf{supp}_s(f_{n_d})| + \frac{1}{2}\left(\binom{n}{k} - \binom{n_d}{k} - \binom{n_d}{s}\right)(\star).$$

    This is equivalent to

$$\mathcal{W}_{f_n,k}(0_n) = \mathcal{W}_{f_{n_d},k}(0_{n_d}) + \mathcal{W}_{f_{n_d},s}(0_{n_d})$$

    Depending on the value of k by induction we know that

$$\mathcal{W}_{f_{n_d},k}(0_{n_d}) \in \begin{cases} \{1,0\} & \text{if } k < n_d/2, \\ \{-1,0\} & \text{if } k \geq n_d/2. \end{cases}$$

$$\mathcal{W}_{f_{n_d},s}(0_{n_d}) \in \begin{cases} \{1,0\} & \text{if } k < n_d/2 + 2^d, \\ \{-1,0\} & \text{if } k \geq n_d/2 + 2^d. \end{cases}$$

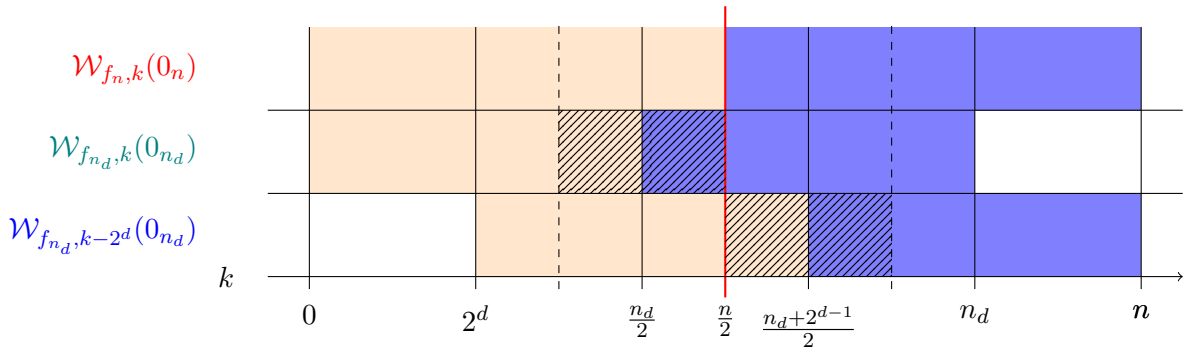

Fig. 2. Light orange and light blue areas correspond to intervals of k where the restricted Walsh transform of the corresponding CMR function is either in $\{0,1\}$ or $\{0,-1\}$, respectively. While, dashed areas correspond to intervals of k where we prove it to be zero. For the studied k we have $\mathcal{W}_{f_n,k}(0_n) = \mathcal{W}_{f_{n_d},k}(0_{n_d}) + \mathcal{W}_{f_{n_d},s}(0_{n_d})$. Therefore, the coloring of the top row is fully determined by those of the rows below.

Notice that, at least one between $|\mathsf{E}_{k,n_d}|$ and $|\mathsf{E}_{s,n_d}|$ is even. Indeed, consider the binary decomposition $n_d = \sum_{j=0}^{q} a_j 2^j$, $k = \sum_{j=0}^{q} k_j 2^j$ and $s = k - 2^d = \sum_{j=0}^{q} s_j 2^j$ (where $q = \lfloor \log_2(n) \rfloor$). If $\binom{n_d}{k}$ is odd, from Proposition 1 we have that $a_j \geq b_j$ for each j. In particular, since $n_d = 2^d(p-1)$, $a_d = 0$ and consequently $k_d = 0$. This implies that $s_d = 1$, hence $\binom{a_d}{s_d} = 0$. Thus, by Lucas' theorem $\binom{n_d}{s}$ is even if $\binom{n_d}{k}$ is odd.
This implies that for $k \in [2^d, n_d/2]$ we have that $\mathcal{W}_{f_n,k}(0_n) \in \{1,0\}$, while that $\mathcal{W}_{f_n,k}(0_n) \in \{-1,0\}$ for $k \in [n_d/2 + 2^d, n-1]$. See Figure 2.
In order to conclude, it is sufficient to show that $\binom{n_d}{k}$ is even for $k \in [n_d/2 - 2^{d-1}, n_d/2]$. Indeed, by using the symmetries of binomial coefficient this implies

$$\mathcal{W}_{f_n,k}(0_n) = \begin{cases} \mathcal{W}_{f_{n_d},s}(0_{n_d}) \in \{1,0\} & \text{if } k \in [n_d/2, n/2], \\ \mathcal{W}_{f_{n_d},k}(0_{n_d}) \in \{-1,0\} & \text{if } k \in [n/2, n_d/2 + 2^d]. \end{cases} \tag{1}$$

Recall that $n_d = 2^d(p-1)$. If $p = 3$, f_{n_d} is WPB and all the $\binom{n_d}{k}$ are even for $k \in [1, n_d - 1]$. Hence, suppose $p > 3$. Setting $L = \lfloor \log_2(p) \rfloor + 1$, since p is odd, we can write $p = 2^{L-1} + \sum_{j=1}^{L-2} p_j 2^j + 1$ with $p_j \in \{0,1\}$. Let $u = d + L$, then $2^d < n_d < n < 2^u$ and

$$\begin{aligned} n_d =& 2^d(p-1) = 2^{d+L-1} + \sum_{j=1}^{L-2} p_j 2^{j+d} = 2^{u-1} + \sum_{j=d+1}^{u-2} p_{j-d} 2^j \\ =& 2^u - 2^{u-1} + \sum_{j=d+1}^{u-2} p_{j-d} 2^j = 2^u - 2(2^{u-2} - \sum_{i=d}^{u-3} p_{i-d+1} 2^i) \end{aligned}$$

This implies that we can write $n_d = 2^u - 2t$ with $t \in [1, 2^{u-2}]$. Therefore, applying Lemma 1 we obtain that for $k \in [2^{u-1} - 2t + 1, 2^{u-1} - t] = [n_d/2 - t + 1, n_d/2]$ the binomial coefficients $\binom{n_d}{k}$ are even.
Furthermore, since $n_d + 2^d = n < 2^{d+L} = 2^u$, we must have $t > 2^{d-1}$, *i.e.* $t \in]2^{d-1}, 2^{u-2}]$. Then, $[n_d/2 - 2^{d-1}, n_d/2] \subseteq [n_d/2 - t + 1, n_d/2]$.
This implies that for $k \in [n_d/2 - 2^{d-1}, n_d/2]$ the coefficients $\binom{n_d}{k}$ are even and consequently (1) holds true.

- If $k = n$, $|\mathsf{supp}_n(f_n)| = 1$ $(\star)$.

Therefore, f_n is SWAPB.

□

Now, we can define a novel family of functions obtained by Construction 2 seeded by the SWAPB CMR functions.

Definition 11 (SWAPB functions $g_{\ell,n}$). *Let $n, \ell \in \mathbb{N}$ with $\ell \in [2, n-1]$, we call $g_{\ell,n}$ the SWAPB function obtained by applying Proposition 5 and Construction 2 with $t = n - \ell$ and f_ℓ, the ℓ-variable WAPB function from CMR construction. We set $g_{n,n} = f_n$.*

In Tables 1 and 2 we report degree, algebraic immunity, nonlinearity and NL_k for $k = 2, \dots, n-2$ of the functions $g_{\ell,n}$ for $n = 8$ and $n = 16$, respectively. Studying only $g_{\ell,n}$ for ℓ even is sufficient, since the following fact holds:

Proposition 6. *Let $n, s \in \mathbb{N}$ and $s \in [1, (n-1)/2]$. Then $g_{2s,n} = g_{2s+1,n}$.*

Proof. Following Definition 11, the function $g_{2s,n}$ is obtained by applying Construction 2 with f_{2s} as input. Therefore, we have

$$g_{2s,n} = f_{2s} + \sum_{i=1}^{n-2s} x_{2s+i} h_{2s+i-1}$$

where $h_j = \sum_{k \in S_j} \varphi_{k-1,j} + \varphi_{j-k,j}$. By Remark 1 we have $S_{2s} = \emptyset$ and consequently $h_{2s} = 0$. Moreover, we have that $f_{2s+1}(x_1, \dots, x_{2s+1}) = f_{2s}(x_1, \dots, x_{2s})$ from Definition 10. This implies that

$$\begin{aligned} g_{2s,n} =& f_{2s} + \sum_{i=1}^{n-2s} x_{2s+i} h_{2s+i-1} = f_{2s} + x_{2s+1} h_{2s} + x_{2s+2} h_{2s+1} + \cdots + x_n h_{n-1} \\ =& f_{2s+1} + x_{2s+2} h_{2s+1} + \cdots + x_n h_{n-1} = g_{2s+1,n}. \end{aligned}$$

□

	degree	AI	NL	NL_2	NL_3	NL_4	NL_5	NL_6
$g_{2,8}$	4	3	88	5	10	16	12	5
$g_{4,8}$	4	3	88	3	7	15	11	3
$g_{6,8}$	4	3	96	2	12	18	12	2
$g_{8,8}$	4	3	88	2	12	19	12	6

Table 1. Cryptographic parameters of the SWAPB functions $g_{\ell,8}$.

4.2 Building other WPB functions from LM construction

In this subsection we study the output of Construction 2 seeded by WPB functions introduced in [LM19]. We recall the definition of these LM functions, referring to the original paper and to [Car21] for the notions of coset leaders of the cyclotomic classes and trace form of a Boolean function.

Definition 12 (LM WPB construction (adapted from [LM19], Corollary 3.5)). *Let $n \in \mathbb{N}, n \geq 2$, we denote by Γ_n the set of all the coset leaders of the cyclotomic classes of 2 modulo $2^n - 1$ and by $o(j)$ the cardinality of the cyclotomic class of 2 modulo $2^n - 1$ containing j. Define $T_j \colon \mathbb{F}_{2^{o(j)}} \to \mathbb{F}_2$ the function $y \mapsto \sum_{i=0}^{o(j)-1} y^{2^i}$. For any fixed β primitive element of $\mathbb{F}_{2^2}$ and any given any function $\iota \colon \Gamma_n \setminus \{0\} \to \{1, 2\}$, the LM WPB function associate to ι is*

$$LM_\iota(x) = \sum_{j \in \Gamma_n \setminus \{0\}} T_j(\beta^{\iota(j)} x^j).$$

	deg	AI	NL	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8	NL_9	NL_{10}	NL_{11}	NL_{12}	NL_{13}	NL_{14}
$g_{2,16}$	8	6	28576	16	97	459	1508	3078	4209	4699	4441	3157	1674	671	170	26
$g_{4,16}$	8	6	28032	14	75	383	1343	2879	4010	4534	4354	3126	1555	627	168	24
$g_{6,16}$	8	6	29792	10	44	344	1458	3110	4502	4947	4321	2897	1326	580	157	20
$g_{8,16}$	8	6	27712	10	44	328	1326	2818	3815	4083	4105	3047	1534	656	144	16
$g_{10,16}$	8	6	29840	5	43	377	1595	3279	4446	5066	4714	3320	1655	507	105	11
$g_{12,16}$	8	5	29152	5	43	265	1397	3148	4439	4971	4803	3396	1712	627	151	13
$g_{14,16}$	8	5	29824	4	56	350	1288	3108	4774	5540	4902	3228	1664	638	152	12
$g_{16,16}$	8	4	29488	4	56	350	1288	3108	4774	5539	4902	3236	1672	654	152	**28**

Table 2. Cryptographic parameters of the SWAPB functions $g_{\ell,16}$.

These functions are proven to be WPB functions defined in 2^m variables, hence SWAPB. Therefore, they can be used to generate other SWAPB by using Construction 2 for all n. We observed that when we apply Construction 2 exhaustively to all LM functions in 4 variables to construct new 8-variable WPB functions we obtain functions having two possible configurations of degree, algebraic immunity, nonlinearity and NL_k for $k = 2, \ldots, n-2$, summarized by Table 3.

	degree	AI	NL	NL_2	NL_3	NL_4	NL_5	NL_6
profile 1	4	4	96	5	13	19	17	5
profile 2	4	4	96	5	16	20	17	5

Table 3. Profiles of WPB functions in 8 variables returned by Construction 2 applied to the LM family in 4 variables.

In order to get new 16-variable WPB functions, we considered in practice two functions as a seed for Construction 2 derived from LM construction having good cryptographic properties. See Table 4.

	degree	AI	NL	NL_2	NL_3	NL_4	NL_5	NL_6
l	7	4	108	6	21	27	22	9
l_0	7	4	105	9	22	27	22	9

Table 4. Cryptographic parameters of two WPB functions in 8 variables derived from LM construction.

Specifically, we took l as a LM WPB function optimizing NL_4, NL_5,and NL_6 for LM construction (see [LM19, Table 1]), while we obtained l_0 as $\varphi_{0,n}(x)l(x) + \sum_{k=1}^{3} \varphi_{k,n}(x)\bar{l}(x) + \sum_{k=4}^{n} \varphi_{k,n}(x)l(x)$, where for any $f \in \mathcal{B}_n$ we denote by $\bar{f}(x)$ the Boolean function $f(x+1_n)$ obtained by the composition of the bit-wise negation of x and f. Applying Construction 2 for $n = t = 8$ and as a input either l or l_0, we get two distinct functions g and g_0, respectively. We collect in Table 5 their degree, algebraic immunity, nonlinearity and NL_k for $k = 2, \ldots, n-2$.

4.3 Hybrid function with high weightwise nonlinearity in $\mathcal{WPB}_4$

In the previous subsections we described the properties of some WPB in 16 variables obtained by Construction 2 seeded both with CMR and LM functions. Namely, we computed some functions in $\mathcal{WPB}_4$ having high weightwise nonlinearity on certain slices. In Table 2 and 5 the maximal

	deg	AI	NL	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8	NL_9	NL_{10}	NL_{11}	NL_{12}	NL_{13}	NL_{14}
g	8	7	30720	22	160	672	1878	3570	4983	**5567**	**5103**	**3629**	**1884**	**688**	**172**	24
g_0	8	7	30592	22	160	672	1865	3581	4951	5455	5071	3603	1880	688	172	24

Table 5. Cryptographic parameters of the WPB functions g and g_0.

realised values are in **red**. Therefore, by combining these functions we can obtain the following *hybrid function*:

$$h_{16}(x) = \sum_{k\in\{1,2\}}^{2} \varphi_{k,n}(x)\bar{f}_{16}(x) + \sum_{k\in\{3,4,5,6,7\}} \varphi_{k,n}(x)\bar{g}(x) + \\ + \sum_{k\in\{8,9,10,11,12,13\}} \varphi_{k,n}(x)g(x) + \sum_{k\in\{14,15,16,0\}} \varphi_{k,n}(x)f_{16}(x) \in \mathcal{WPB}_4$$

Table 6 contains the degree, algebraic immunity, nonlinearity and NL_k for $k = 2, \ldots, n-2$ of h_{16}.

	deg	AI	NL	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8
h_{16}	14	8	30704	28	172	688	1884	3629	5103	5567

Table 6. Cryptographic parameters of h_{16}. By construction $\mathsf{NL}_k(h_{16}) = \mathsf{NL}_{n-k}(h_{16})$.

	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8
h_{16}	28	172	688	1884	3629	5103	5567
lower bound	34	222	803	2016	3774	5443	6141
upper bound	54	268	888	2150	3959	5666	6378

Table 7. Comparison with known lower bound [GM22, Proposition 9] and upper bound [GM22, Proposition 10] for $\mathsf{M}_{k,16}$, *i.e.* the maximum weightwise nonlinearity of $\mathcal{WPB}_4$ over $\mathsf{E}_{k,16}$.

Table 7 shows that the values $\mathsf{NL}_k(h_{16})$ are below the known lower bound of $\mathsf{M}_{k,16}$, the maximum weightwise nonlinearity of $\mathcal{WPB}_4$ over $\mathsf{E}_{k,16}$. Nevertheless, according to [GM22, Table 5], h_{16} is the currently known (explicitly constructed) function with the best weightwise nonlinearity on the slices.

4.4 Computational aspects

We provided the exact value of cryptographic parameters of the WPB functions that we analyzed, both in 8 and 16 variables. We retrieved them by concrete computations via `sagemath` [The22]. Specifically, we used `BooleanFunction` class from the module `sage.crypto.boolean_function` to encode the functions, and we applied the built-in methods for computing degree and algebraic immunity. Then, we computed the weightwise nonlinearity on the slices NL_k for $k = 2, \ldots, n-2$ by adapting the strategy from [GM22]. See Algorithm 1. For Construction 2 we built the $\varphi_{k,n}$ functions via truth tables for compatibility. Another possible approach can be via ANF using Property 3.

Data parallelism and iterators allowed us to obtain these values in less then one hour by using 128 cores, by 2xAMD Epyc ROME 7H12 @ 2.6 GHz [64c/280W], *i.e.* one regular node of the UL

Aion supercomputer `https://hpc.uni.lu/` [VBCG14]. Our code is available at `https://github.com/agnesegini/WAPB_pub`. Additionally, the repository includes functions to explicitly build l, l_0 and h_{16}.

Algorithm 1

Input: Let $n, k \in \mathbb{N}^*$ with $0 < k < n$, and $f \in \mathcal{B}_n$.
Output: $\mathsf{NL}_k(f)$
1: Compute v_f the vector of evaluations of f over the $\mathsf{E}_{k,n}$.
2: Generate $\mathsf{P}_{k,n}$ the spherically punctured Reed Muller code of order 1 of length $\nu = \binom{n}{k}$.
3: Compute δ the distance between v_f and $\mathsf{P}_{k,n}$. ▷ This can be performed in parallel.
4: **return** δ

5 Conclusion

In this article we introduced two secondary constructions of weightwise almost perfectly balanced functions and provided examples up to 16 variables. While former approaches focused on modifying the support of a low degree functions to make it W(A)PB, our technique is based on an iterative application of Siegenthaler's construction and addition of symmetric functions. This directly provides us a theoretical lower bound on the weightwise nonlinearities based on the parameters of the parent function (Theorem 2). Moreover, via this construction, we explicitly built SWAPB functions up to 16 variables and determined exactly their main cryptographic parameters. Finally, we combined these functions by taking for each slice k the one from the function obtaining the highest NL_k, which gave us the function h_{16} with the highest weightwise nonlinearities exhibited so far.

Open questions:

- *Higher weightwise nonlinearities.* The function h_{16} is obtained by combining the functions with highest NL_k built with Construction 2 from CMR of LM functions. One natural next step would be to use other WPB families as seed for Construction 2 and possibly combine those functions with best NL_k. Moreover, it would be interesting to try to reach (or overcome) the non-constructive lower bound from [GM22]. See Table 7.
- *Parameters of equivalent WAPB functions.* Considering W(A)PB functions relatively to classes equivalent up to addition of symmetric functions is a good start to build more constructions, and it has the advantage to group WAPB functions having exactly the same NL_k. As a matter of fact, using special WAPB functions rather than WAPB functions has been useful in this article to exhibit a secondary construction. Taking a special WAPB function is not restrictive since any WAPB function is equivalent to a special one up to the addition of symmetric functions. Major questions relatively to these classes would be to determine the variation of cryptographic parameters inside the same class, and find a criterion to choose the best representative.

Acknowledgments. The two authors were supported by the ERC Advanced Grant no. 787390.

References

BP05. An Braeken and Bart Preneel. On the algebraic immunity of symmetric boolean functions. In *Progress in Cryptology - INDOCRYPT 2005, 6th International Conference on Cryptology in India, Bangalore, India, December 10-12, 2005, Proceedings*, pages 35–48, 2005.

Car04. Claude Carlet. On the degree, nonlinearity, algebraic thickness, and nonnormality of boolean functions, with developments on symmetric functions. *IEEE Trans. Information Theory*, pages 2178–2185, 2004.

Car21. Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

CL11. Y. Chen and P. Lu. Two classes of symmetric boolean functions with optimum algebraic immunity: Construction and analysis. *IEEE Transactions on Information Theory*, 57(4):2522–2538, April 2011.

CM19. Claude Carlet and Pierrick Méaux. Boolean functions for homomorphic-friendly stream ciphers. *Algebra, Codes and Cryptology*, pages 166–182, 11 2019.

CM22. Claude Carlet and Pierrick Méaux. A complete study of two classes of boolean functions: Direct sums of monomials and threshold functions. *IEEE Transactions on Information Theory*, 68(5):3404–3425, 2022.

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.

CV05. Anne Canteaut and Marion Videau. Symmetric boolean functions. *IEEE Trans. Information Theory*, pages 2791–2811, 2005.

CZGC19. Yindong Chen, Liu Zhang, Fei Guo, and Weihong Cai. Fast algebraic immunity of 2^{m+2} and 2^{m+3} variables majority function. *IEEE Access*, 7:80733–80736, 2019.

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*, 2006.

Fin47. N. J. Fine. Binomial coefficients modulo a prime. *The American Mathematical Monthly*, 54(10):589–592, 1947.

GM22. Agnese Gini and Pierrick Maux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discrete Applied Mathematics*, 322:320–341, 2022.

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.

IMM13. I. Ivchenko, Yu. I. Medvedev, and V. A. Mironova. Symmetric boolean functions and their metric properties matrices of transitions of differences when using some modular groups. *Mat. Vopr. Kriptogr.*, pages 49–63, 2013.

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. *Discrete Applied Mathematics*, 279:218–227, 2020.

Méa19. Pierrick Méaux. On the fast algebraic immunity of majority functions. In Peter Schwabe and Nicolas Thériault, editors, *Progress in Cryptology - LATINCRYPT*, volume 11774 of *LNCS*, pages 86–105. Springer, 2019.

Méa21. Pierrick Méaux. On the fast algebraic immunity of threshold functions. *Cryptography and Communications*, 13(5):741–762, 2021.

MJSC16. Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 311–343. Springer, Heidelberg, May 2016.

MMM+18. Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy, and Pantelimon Stanica. Tools in analyzing linear approximation for boolean functions related to FLIP. In *Progress in Cryptology - INDOCRYPT 2018 - 19th International Conference on Cryptology in India, New Delhi, India, December 9-12, 2018, Proceedings*, pages 282–303, 2018.

MPJ+22. Luca Mario, Stjepan Picek, Domagoj Jakobovic, Marko Djurasevic, and Alberto Leporati. Evolutionary construction of perfectly balanced boolean functions. 2022.

MS21. Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced boolean functions. *Cryptography and Communications*, 2021.

MSL21. Sihem Mesnager, Sihong Su, and Jingjing Li. On concrete constructions of weightwise perfectly balanced functions with optimal algebraic immunity and high weightwise nonlinearity. *Boolean Functions and Applications*, 2021.

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.

Obl20. A. K. Oblaukhov. On metric complements and metric regularity in finite metric spaces. *Prikl. Diskr. Mat.*, (49):35–45, 2020.

QFLW09. Longjiang Qu, Keqin Feng, Feng Liu, and Lei Wang. Constructing symmetric boolean functions with maximum algebraic immunity. *IEEE Transactions on Information Theory*, 55:2406–2412, 05 2009.

QLF07. Longjiang Qu, Chao Li, and Keqin Feng. A note on symmetric boolean functions with maximum algebraic immunity in odd number of variables. *IEEE Transactions on Information Theory*, 53, 2007.

SM07. Palash Sarkar and Subhamoy Maitra. Balancedness and correlation immunity of symmetric boolean functions. *Discrete Mathematics*, pages 2351 – 2358, 2007.

SSB18. Pantelimon Stanica, Tsutomu Sasao, and Jon T. Butler. Distance duality on some classes of boolean functions. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 107:181–198, 2018.

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.

The22. The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2022. `https://www.sagemath.org`.

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.

TLD16. Deng Tang, Rong Luo, and Xiaoni Du. The exact fast algebraic immunity of two subclasses of the majority function. *IEICE Transactions*, pages 2084–2088, 2016.

Tok12. Natalia N. Tokareva. Duality between bent functions and affine functions. *Discrete Mathematics*, 312(3):666–670, 2012.

VBCG14. Sbastien Varrette, Pascal Bouvry, Hyacinthe Cartiaux, and Fotis Georgatos. Management of an academic HPC cluster: The UL experience. In *2014 International Conference on High Performance Computing & Simulation (HPCS)*, pages 959–967, 2014.

ZS21. Rui Zhang and Sihong Su. A new construction of weightwise perfectly balanced boolean functions. *Advances in Mathematics of Communications*, 0:–, 2021.

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.

A Explicit WPB functions

In the following we display the algebraic normal form of function l from Table 4.

$$
\begin{aligned}
l =& x_1x_2x_3x_4x_5x_6x_8 + x_1x_2x_3x_4x_5x_7 + x_1x_2x_3x_4x_5x_8 + x_1x_2x_3x_4x_5 + \\
& x_1x_2x_3x_4x_6x_7x_8 + x_1x_2x_3x_4x_6x_7 + x_1x_2x_3x_4x_6 + x_1x_2x_3x_4 + x_1x_2x_3x_5x_7x_8 + \\
& x_1x_2x_3x_6x_7x_8 + x_1x_2x_3x_6x_7 + x_1x_2x_3x_6x_8 + x_1x_2x_3x_7x_8 + x_1x_2x_3x_7 + \\
& x_1x_2x_3 + x_1x_2x_4x_5x_6x_7x_8 + x_1x_2x_4x_5x_6x_8 + x_1x_2x_4x_5x_7x_8 + x_1x_2x_4x_5x_8 + \\
& x_1x_2x_4x_5 + x_1x_2x_4x_6x_7 + x_1x_2x_4x_6x_8 + x_1x_2x_4x_6 + x_1x_2x_4x_7x_8 + x_1x_2x_4x_7 + \\
& x_1x_2x_4x_8 + x_1x_2x_4 + x_1x_2x_5x_6 + x_1x_2x_5x_8 + x_1x_2x_5 + x_1x_2x_6 + \\
& x_1x_2x_7x_8 + x_1x_3x_4x_5x_6x_7 + x_1x_3x_4x_5x_6x_8 + x_1x_3x_4x_5x_8 + \\
& x_1x_3x_4x_5 + x_1x_3x_4x_6x_8 + x_1x_3x_4x_6 + x_1x_3x_5x_6x_7x_8 + \\
& x_1x_3x_5x_7 + x_1x_4x_5x_6x_7x_8 + x_1x_4x_5x_6x_8 + x_1x_4x_5x_6 + x_1x_4x_5x_7x_8 + \\
& x_1x_4x_6x_7x_8 + x_1x_4x_6x_8 + x_1x_4x_6 + x_1x_4 + x_1x_5x_6x_7x_8 + x_1x_5x_6x_8 + \\
& x_1x_5x_6 + x_1x_5x_7x_8 + x_1x_6x_8 + x_1x_7x_8 + x_1x_8 + x_1 + x_2x_3x_4x_5x_6x_7x_8 + \\
& x_2x_3x_4x_5x_6x_7 + x_2x_3x_4x_5x_8 + x_2x_3x_4x_6x_7x_8 + x_2x_3x_4x_6x_7 + x_2x_3x_4x_6x_8 + \\
& x_2x_3x_4x_6 + x_2x_3x_4x_7 + x_2x_3x_5x_6x_7x_8 + x_2x_3x_5x_6x_7 + \\
& x_2x_3x_5x_6x_8 + x_2x_3x_6x_7x_8 + x_2x_3x_6x_8 + x_2x_3x_7x_8 + x_2x_3x_8 + x_2x_3 + \\
& x_2x_4x_5x_6x_7 + x_2x_4x_5x_6x_8 + x_2x_4x_5x_7x_8 + x_2x_4x_5x_8 + x_2x_4x_5 + \\
& x_2x_4x_6x_7x_8 + x_2x_4x_6x_7 + x_2x_4x_6 + x_2x_4x_7x_8 + x_2x_4x_7 + x_2x_4x_8 + + \\
& x_2x_4 + x_2x_5x_6x_7x_8 + x_2x_5x_6x_8 + x_2x_5x_6 + \\
& x_2x_5x_7x_8 + x_2x_5x_8 + x_2x_6x_7x_8 + x_2x_6x_8 + x_2x_6 + x_2x_7x_8 + x_2x_7 + x_2x_8 + \\
& x_3x_4x_5x_6x_7 + x_3x_4x_5x_6x_8 + x_3x_4x_5x_6 + x_3x_4x_5 + x_3x_4x_6x_7 + \\
& x_3x_4x_6x_8 + x_3x_4x_6 + x_3x_4x_7x_8 + x_3x_4x_7 + x_3x_4x_8 + x_3x_5x_6x_7 + \\
& x_3x_5x_6x_8 + x_3x_6x_7x_8 + x_3x_6x_8 + x_3x_6 + x_3x_7x_8 + x_3 + x_4x_5x_6x_8 + \\
& x_4x_5 + x_4x_6x_7 + x_4x_6x_8 + x_4x_6 + x_4x_7x_8 + x_4x_8 + x_5x_6x_7x_8 + \\
& x_5x_6x_7 + x_5x_6x_8 + x_5x_8 + x_5 + x_6x_7 + x_6x_8 + x_7
\end{aligned}
$$

This is function can be built in `sagemath` along with l_0 and h_{16} by using the public code available at `https://github.com/agnesegini/WAPB_pub`.