Weightwise (almost) perfectly balanced functions based on total orders

Pierrick Méaux

Luxembourg university, Luxembourg
pierrick.meaux@uni.lu

Abstract. The unique design of the FLIP cipher necessitated a generalization of standard cryptographic criteria for Boolean functions used in stream ciphers, prompting a focus on properties specific to subsets of $\mathbb{F}_2^n$ rather than the entire set. This led to heightened interest in properties related to fixed Hamming weight sets and the corresponding partition of $\mathbb{F}_2^n$ into $n+1$ such sets. Consequently, the concept of Weightwise Almost Perfectly Balanced (WAPB) functions emerged, which are balanced on each of these sets. Various studies have since proposed WAPB constructions and examined their cryptographic parameters for use in stream cipher filters.

In this article, we introduce a general approach to constructing WAPB functions using the concept of total order relation, which simplifies implementation and enhances cryptographic strength. We present two new constructions: a recursive method employing multiple orders on binary strings, and another utilizing just two orders. We establish lower bounds for nonlinearity and weightwise nonlinearities within these classes. By instantiating specific orders, we demonstrate that some achieve minimal algebraic immunity, while others provide functions with guaranteed optimal algebraic immunity. Experimental results in 8 and 16 variables indicate that using orders based on field representation significantly outperforms other methods in terms of both global and weightwise algebraic immunity and nonlinearity. Additionally, we extend the recursive construction to create WAPB functions for any value of n, with experiments in 10, 12, and 14 variables confirming that these order-based functions exhibit robust cryptographic parameters. In particular, those based on field orders display optimal degrees and algebraic immunity, and strong weightwise nonlinearities and algebraic immunities.

Keywords: Boolean functions, Weightwise perfectly balanced functions, Cryptographic criteria.

1 Introduction

With the design of FLIP [26], established cryptographic criteria for Boolean functions—traditionally used to assess the security of filtered Linear Feedback Shift Register (LFSR), combined LFSR, or more complex stream cipher designs—no longer apply. In the context of this cipher, the relevant properties of the Boolean function used as a filter to determine security are not based on the entire $\mathbb{F}_2^n$ but only on a specific identified subset. This change has necessitated the generalization of standard attacks and the establishment of new criteria for subsets and specific partitions of $\mathbb{F}_2^n$, beginning with the study of restricted criteria for Boolean functions [4].

In the case of FLIP, the input to the filtering function always has a fixed, known Hamming weight, thus tailoring attacks to this specificity enhances their effectiveness. This adaptation exemplifies a broader phenomenon where additional information about a cipher's internal values can significantly simplify attacks, as seen in multiple contexts like (algebraic) side-channel attacks [32] or lattice reduction with side information [5]. From the FLIP study, the focus has been on the partition of the Boolean hypercube into $n+1$ slices, defined as sets with elements of the same Hamming weight $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \mid \mathsf{w_H}(x) = k\}$ for $k \in [0, n]$. Notably, the Hamming weight of an intermediate value is also commonly leveraged as leakage in side channel attacks, *e.g.* [8,16,35], although a leakage with an approximate Hamming weight is considered more realistic *e.g.* [1,15,31].

A fundamental security criterion for a Boolean function is balancedness; the function is balanced if it outputs 1 for half of the inputs and 0 for the other half, to prevent statistical biases exploitable by various attacks. Functions that are balanced over each slice were introduced in [4] as Weightwise (Almost) Perfectly Balanced (WAPB) functions. The term "almost" differentiates cases where n is a power of two—here, the function is perfectly balanced on all slices except for those with k equal to 0 or n. For other values of n, where many slices have an odd cardinality, the functions output 1 one more (or one less) time than 0. Since 2017, multiple studies have focused on developing new constructions of W(A)PB functions with improved parameters for use as filter functions. These efforts include enhancing globally recognized cryptographic parameters such as algebraic degree, Algebraic Immunity (AI), and nonlinearity, as well as important criteria on the slices, like weightwise nonlinearities and weightwise algebraic immunity.

We provide a concise overview of the main families of WAPB functions showcased in previous studies, noting that most of them focus primarily on WPB functions. Initially, a recursive approach for both WPB and WAPB was introduced in [4], followed by a secondary construction. In 2019, the work in [21] (and later [29]) utilized field representations to develop WPB functions that are 2-rotation symmetric and achieve high weightwise nonlinearities. The construction in [37] (and an adaptation with better weightwise nonlinearities in [28]) compare the weight of inputs split into two halves, resulting in constructions affine equivalent to the majority function, thus reaching optimal algebraic immunity. The construction in [27] start from a linear or quadratic function near WPB status, and modify their algebraic normal form to achieve balancedness over all slices. This methodology was later expanded to generate WAPB functions from functions of low degrees, as detailed in [14,18,40,41,42].

Additional methods for constructing WAPB functions have been introduced, utilizing direct sums [43] or Sieghentaler's construction and addition of symmetric function [10]. Furthermore, various families have been developed by slightly altering the support of non-WPB functions, as reported in studies focusing on the distribution of cryptographic parameters of WPB functions, particularly on weightwise nonlinearity [9], nonlinearity [13], and algebraic immunity [11]. Recent efforts have also employed evolutionary algorithms to enhance the parameters of WPB functions, concentrating on weightwise nonlinearities [24, 38], and on nonlinearity [23]. Additional constructions and properties of restricted criteria have been explored in a range of works (a non-exhaustive list includes [6, 7, 12, 30]).

In this article, we explore a novel general approach for WAPB, where the input is split in two halves, and the function value is determined by an ordering on binary vectors of length $n/2$. This method simplifies the implementation of WPB functions and offers superior parameters compared to previously exhibited functions.

Firstly, we introduce two novel constructions of WPB functions: a recursive construction employing multiple orders for binary vectors (one for each power of 2 between 2 and $n/2$ for an n-variable WPB function) and a second, simpler construction involving just two orders. We quantify the number of functions within these categories and examine their nonlinearities. We establish a lower bound for the nonlinearity of any function from these families—at least half that of a bent function—and we derive lower bounds for the weightwise nonlinearities across the full classes.

Then, we instantiate the constructions with specific orders. We implement prevalent orders—lexicographic and cool—alongside orders that respect the Hamming weight (termed weightwise order) and others based on the field representation of $\mathbb{F}_{2^t}$. We examine the algebraic immunity of these constructions, proving that those based on the lexicographic order achieve the minimal AI for WPB functions, whereas weightwise orders result in optimal AI. We provide experimental results detailing the relevant parameters of WPB functions in 8 and 16 variables for these different orders, where we observe that the new constructions using the field representation outperform the other ones in both algebraic immunity and nonlinearity, both globally and weightwise.

Finally, we extend the recursive construction to furnish WAPB functions for all n. We report outcomes for global parameters—such as resilience order, nonlinearity, degree, and algebraic immunity—as well as weightwise parameters, specifically weightwise nonlinearities and algebraic immunities. Experimentally, we determine these parameters for functions in 10, 12, and 14 variables. Similar to WPB functions, this study underscores that order-based WAPB functions can exhibit robust cryptographic parameters. Notably, those based on field orders showcase optimal degrees, optimal algebraic immunity, and strong weightwise algebraic immunities and nonlinearities.

2 Preliminaries

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

2.1 Boolean functions, cryptographic criteria, and weightwise properties

In this section, we recall fundamental concepts concerning Boolean functions and their weightwise properties, which are utilized throughout this article. For a more comprehensive introduction to Boolean functions and their cryptographic parameters, we recommend consulting the book by Carlet [2], and for insights into weightwise properties—also known as properties on the slices—the article by [4]. We denote by $\mathsf{E}_{k,n}$ the set $\{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$ for $k \in [0, n]$, referring to it as a slice of the Boolean hypercube (of dimension n). Consequently, the Boolean hypercube is divided into $n + 1$ slices, where the elements share 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 Boolean functions in n variables is denoted by $\mathcal{B}_n$.*

When a property or a definition is restricted to a slice, we denote it by using the subscript k. For example, for an n-variable Boolean function f we denote its support $\mathsf{supp}(f) = \{x \in \mathbb{F}_2^n \,|\, f(x) = 1\}$. Furthermore, we denote by $\mathsf{supp}_k(f)$ the support of f restricted to a slice, which is defined as $\mathsf{supp}(f) \cap \mathsf{E}_{k,n}$.

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

For $k \in [0, n]$ the function is said almost 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 the function is balanced on the slide: $|\mathsf{supp}_k(f)| = |\mathsf{supp}_k(f+1)| = |\mathsf{E}_{k,n}|/2$.

Using the notion of restricted balancedness we can define the weightwise (almost) perfectly balanced functions, the focus of our work.

Definition 3 (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 can lead to slices of odd cardinality, 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 $\mathcal{WAPB}_n$.

We define additional crucial concepts for studying Boolean functions, namely the algebraic normal form and the Walsh transform. Subsequently, we introduce key cryptographic criteria for these functions, including algebraic immunity (both general and weightwise) and nonlinearity (both general and weightwise).

Definition 4 (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:

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

Definition 5 (Algebraic immunity and restricted 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 restricted algebraic immunity of a Boolean function $f \in \mathcal{B}_n$ on the set $S \subset \mathbb{F}_2^n$, denoted as $\mathsf{AI}_S(f)$, is defined as:

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

For $S = \mathsf{E}_{k,n}$ we denote $\mathsf{AI}_{\mathsf{E}_{k,n}}(f)$ by $\mathsf{AI}_k(f)$ and call it weightwise algebraic immunity.

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:

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

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

For ease of notation, we will denote the inner product $a \cdot x = \sum_{i=1}^{n} a_i x_i$ by ax.

Property 1 (WAPB functions and restricted Walsh transform)**.** *Let $n \in \mathbb{N}^*$, $f \in \mathcal{B}_n$ is WAPB if and only if: $\forall k \in [0, n]$, $\mathcal{W}_{f,k}(0_n) = 0$ if $|\mathsf{E}_{k,n}|$ is even, ± 1 otherwise. If $n = 2^m$ with $m \in \mathbb{N}^*$, $f \in \mathcal{B}_n$ is WPB if and only if:*

$$\mathcal{W}_{f,0}(0_n) = 1, \quad \mathcal{W}_{f,n}(0_n) = -1, \; \textit{and} \quad \forall k \in [1, n-1], \mathcal{W}_{f,k}(0_n) = 0.$$

Definition 7 (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 $\mathcal{B}_n$:*

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

where $g(x) = a \cdot x + \varepsilon$, $a \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2$. The nonlinearity can also be defined from the Walsh transform:

$$\mathsf{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)|.$$

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:

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

Property 2 (Nonlinearity on the slice, adapted from [4], Proposition 6)**.** *Let $n \in \mathbb{N}^*, k \in [0, n]$, for every n-variable Boolean function f over $\mathsf{E}_{k,n}$:*

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

2.2 Orders

In this part we recall the notion of order. This notion is the key concept for the new constructions of WPB and WAPB functions we present in the article.

Definition 8 (Order). *A binary relation $\preceq$ on a set X is called partial order if $\preceq$ is reflexive, transitive and antisymmetric. Moreover, $\preceq$ is a total order if for all $a, b \in X$ it holds $a \preceq b$ or $b \preceq a$.*

We give two examples of orders on n-length binary strings, more examples can be found in *e.g.* [36] that also considers order on sets of fixed Hamming weight:

- Lexicographic, given $a, b \in \mathbb{F}_2^n$ as $a = a_1, \ldots, a_n$ and $b = b_1, \ldots, b_n$, $a \preceq b$ if and only if $a_i < b_i$ on the first index $i \in [1, n]$ such that $a_i \neq b_i$, or $a = b$.
- Cool [34], a first element of $\mathbb{F}_2^n$ is chosen and a successor rule is used to determine the following element, allowing to generate the 2^n elements with no repetition. The successor rule for $a_1, a_2, \ldots, a_n$ is: Let i be the minimum value such that $(a_i, a_{i+1}) = (1, 0)$ and $i > 1$. If i exists, then rotate i bits, otherwise flip a_1 (that is, replace a_1 by $a_1 \oplus 1$) and then rotate $n - 1$ bits.

2.3 Krawtchouk polynomials

We use Krawtchouk polynomials and some of their properties to prove one of our results, we give necessary preliminaries here and refer to *e.g.* [22] for more details.

Definition 9 (Krawtchouk Polynomials). *The Krawtchouk polynomial of degree k, with $0 \leq k \leq n$ is given by:* $\mathsf{K}_k(\ell, n) = \sum_{j=0}^{k} (-1)^j \binom{\ell}{j}\binom{n-\ell}{k-j}$.

Property 3 (Krawtchouk polynomials relation)**.** *Let $n \in \mathbb{N}^*$ and $k \in [0, n]$, the following hold: $\mathsf{K}_k(\ell, n)$ is the value of the restricted Walsh transform on $\mathsf{E}_{k,n}$ in 0_n of any n-variable linear function $a \cdot x$ such that $\mathsf{w_H}(a) = \ell$.*

Proof. Let a such that $\mathsf{w_H}(a) = \ell$, the linear function $a \cdot x$ has the following restricted Walsh transform on $\mathsf{E}_{k,n}$ by Definition 6:

$$\begin{aligned}\mathcal{W}_{a\cdot x,k}(0_n) &= \sum_{x \in \mathsf{E}_{k,n}} (-1)^{a\cdot x} = \sum_{j=0}^{\ell} \sum_{\substack{x \in \mathsf{E}_{k,n} \\ |\mathsf{supp}(a) \cap \mathsf{supp}(x)| = j}} (-1)^{a\cdot x} \\ &= \sum_{j=0}^{\ell} (-1)^j \sum_{\substack{x \in \mathsf{E}_{k,n} \\ |\mathsf{supp}(a) \cap \mathsf{supp}(x)| = j}} 1 = \sum_{j=0}^{\ell} (-1)^j \binom{\ell}{j}\binom{n-\ell}{k-j} = \mathsf{K}_k(\ell, n)\end{aligned}$$

□

2.4 Tang-Liu WPB functions

We recall the construction of WPB functions from Tang and Liu [37] and one on its properties. We use these results to prove the algebraic immunity of special cases of our main constructions.

Definition 10 (TL WPB construction (adapted from [37], Construction 1)). *Let $m \in \mathbb{N}^*$ and $n = 2^m \geq 4$, a TL WPB Boolean function h on n variables is such that:*

- *$h(0_n) = 0$ and $h(1_n) = 1$,*
- *$h(x, y) = 0$ if $\mathsf{w_H}(x) < \mathsf{w_H}(y)$,*
- *$h(x, y) = 1$ if $\mathsf{w_H}(x) > \mathsf{w_H}(y)$,*
- *the cardinality of $U_j = \mathsf{supp}(h) \cap \left\{(x, y) \in \mathbb{F}_2^{2^{m-1}} \times \mathbb{F}_2^{2^{m-1}} : \mathsf{w_H}(x) = \mathsf{w_H}(y) = j\right\}$ is exactly $\binom{2^{m-1}}{j}^2/2$ for all j such that $0 < j < 2^{m-1}$.*

Remark 1. While Definition 10 may appear quite different from the original paper, it is equivalent when considering the restriction that n be a power of two, and the values in 0_n and 1_n imposed by Definition 3.

Property 4 (TL WPB functions properties [37])**.** *Let $m \in \mathbb{N}^*$ and $n = 2^m$, a n-variable TL function h_n has optimal algebraic immunity $\mathsf{AI}(h_n) = \frac{n}{2}$.*

3 Constructions based on total orders

We present our two main constructions of weightwise perfectly balanced functions based on the notion of order. First, we introduce Construction 1, which utilizes an order for each length of bit strings ranging from 2 to 2^{m-1} and is constructed recursively. Then, we present Construction 2, which is defined using only two orders. Finally, we analyze the nonlinearities of the WPB functions generated by these constructions. We provide a lower bound on the nonlinearity and the weightwise nonlinearities of all functions within these families.

3.1 Recursive construction

Definition 11 (Construction 1**).** *Let $m \in \mathbb{N}^*$, and for $i \in [0, m-1]$ $\preceq_i$ be a total order on the set of 2^i-length binary strings.*

Let f_m be the 2^m-variable function defined as:

- $f_m(0_{2^m}) = 0$, $f_m(1_{2^m}) = 1$,
- $$f_m(x,y) = \begin{cases} f_{m-1}(x) & \textit{if } x = y, \\ 0 & \textit{if } x \prec_{m-1} y, \\ 1 & \textit{if } y \prec_{m-1} x, \end{cases}$$

where $x, y \in \mathbb{F}_2^{m-1}$.

Theorem 1. *Let f_m defined as in Definition 11, f_m is weightwise perfectly balanced.*

Proof. We prove it by recursion. First, $f_1(x,y)$ takes the value 0 in $(0,0)$ and 1 in $(1,1)$ since by definition $f_m(0_{2^m}) = 0$ and $f_m(1_{2^m}) = 1$. For the two elements $(x,y) \in \mathbb{F}_2^m$ such that $x \neq y$, that is $\mathsf{E}_{1,n}$, it holds $0 \prec_0 1$ or $1 \prec_0 0$, hence f_1 takes the value 1 on exactly one of them. Consequently f_1 is WPB, which proves the basis of the recursion.

Then, if for $j \in [1, m-1]$ f_j is WPB we show that f_{j+1} is also WPB. We denote $n = 2^{j+1}$, $f_{j+1}(x,y)$ takes the value 0 in (0_n) and 1 in (1_n) by definition. Then, for any weight $k \in [1, n-1]$ the set $\mathsf{E}_{k,n}$ can be split in the two sets $A = \{(x,y) \in \mathsf{E}_{k,n} \,|\, x = y\}$ and $B = \{(x,y) \in \mathsf{E}_{k,n} \,|\, x \neq y\}$. On the set A, which is empty when k is odd, $f_{j+1}(x,y)$ takes the value of $f_j(x)$, and since $\{x \in \mathbb{F}_2^{n/2} \,|\, (x,x) \in A\} = \mathsf{E}_{k/2,n/2}$, the weightwise perfect balancedness of f_j implies the balancedness of f_{j+1} on A. Finally, the set B can be split in pairs (x,y) and (y,x) (since all elements of B are such that $x \neq y$). For each pair, either $x \prec_j y$ or $y \prec_j x$ hence $f_{j+1}(x,y) = 1 + f_{j+1}(y,x)$. Accordingly, f_{j+1} is balanced on each of these pairs, hence on B, and therefore on the full slice $\mathsf{E}_{k,n}$. It allows to conclude the proof by recursion, f_m is WPB.

□

Proposition 1. *Let $m \in \mathbb{N}^*$ and, the number $\mathcal{C}_m$ of 2^m-variable WPB functions from the family of Definition 11 is:*

$$\mathcal{C}_m = \prod_{i=0}^{m-1} 2^{2^i}!.$$

Proof. First, we note that if two functions f and g from the family are defined with a different order for i in $[0, m-1]$ there exist two elements x and y in $\mathbb{F}_2^{2^i}$ such that $x \prec_{f,i} y$ and $y \prec_{g,i} x$ (where the subscript f or g indicate the order used in the definition of f or g respectively). Then, by Definition 11 $f(x,y) = 0$ and $g(x,y) = 1$, hence f and g are different functions. Therefore, the quantity of different WPB functions from this family is the product, with index i ranging on the integers between 1 and m, of the number of total orders over binary strings of length 2^{i-1}. Since there are $n!$ possible total orders on a set of size n, it gives the final result: $\prod_{i=0}^{m-1} 2^{2^i}!$.

□

3.2 Construction based on two orders

Definition 12 (Construction 2). *Let $m \in \mathbb{N}^*$, and $\preceq$ be a total order on the set of 2^{m-1}-length binary strings. Let $\preceq'$ be a total order on the set of 2^{m-1}-length binary strings such that for all $k \in [1, 2^{m-1}-1]$ exactly half of the elements of Hamming weight k are in the smallest half. We denote by u the 2^{m-2}-th element in the order $\preceq'$.*

Let g_m be the 2^m-variable function defined as:

- $g_m(0_{2^m}) = 0$, $g_m(1_{2^m}) = 1$,
-
$$g_m(x,y) = \begin{cases} 0 & \text{if } x \prec y, \\ 1 & \text{if } y \prec x, \\ 0 \text{ if } x \preceq' u, 1 \text{ otherwise} & \text{if } x = y, \end{cases}$$

where $x, y \in \mathbb{F}_2^{m-1}$.

Theorem 2. *Let f_m as defined in Definition 12, f_m is weightwise perfectly balanced.*

Proof. We denote $n = 2^m$. By definition $g_m(0_{2^m}) = 0$ and $g_m(1_{2^m}) = 1$, so we focus on the balancedness of g_m on the slices $\mathsf{E}_{k,n}$ for $k \in [1, n-1]$. Each slice $\mathsf{E}_{k,n}$ can be written as $A \cup B$ where A is the set of elements such that $x = y$, that is $A = \{(x,x) \,|\, x \in \mathbb{F}_2^{n/2}\} \cap \mathsf{E}_{k,n}$, and B is the set of elements such that $x \neq y$, that is $B = \{(x,y) \,|\, x, y \in \mathbb{F}_2^{n/2}, x \neq y\} \cap \mathsf{E}_{k,n}$. By construction $A \cap B = \emptyset$.

First, we show that g_m is balanced over A. We remark that $|A| = |\mathsf{E}_{k/2,n/2}|$ and more precisely $\{x \,|\, (x,x) \in A\} = \mathsf{E}_{k/2,n/2}$. By definition of $\preceq'$ we have $|\{x \in \mathsf{E}_{k/2,n/2} \,|\, x \preceq' u\}| = |\mathsf{E}_{k/2,n/2}|/2$, hence g_m is balanced on A.

Then, we prove the balancedness on B. B can be partitioned into set of pairs (x,y) and(y,x) and since $x \prec y$ or $y \prec x$ since $x \neq y$, g_m is balanced on all the pairs and therefore on all B. Finally, g_m is balanced on $A \cup B = \mathsf{E}_{k,n}$ for all $k \in [1, n-1]$ which allows to conclude g_m is WPB.

□

Proposition 2. *Let $m \in \mathbb{N}^*$, the number $\mathcal{D}_m$ of 2^m-variable WPB functions from the family of Definition 12 is:*

$$\mathcal{D}_m = 2^{2^{m-1}}! \times \prod_{k=1}^{2^{m-1}-1} \binom{\binom{2^{m-1}}{k}}{\frac{1}{2}\binom{2^{m-1}}{k}}.$$

Proof. First, using the same argument as for Proposition 1, a different order for $\preceq$ gives a different function. Then, two functions f and g with only $\preceq'$ different can still be the same function if and only if for each $k \in [1, n/2-1]$ (where $n = 2^m$) the same half of $\mathsf{E}_{k,n/2}$ is in the smallest half. Indeed, if for all $k \in [1, n/2-1]$, the sets $\{x \in \mathsf{E}_{k,n/2} \,|\, x \preceq'_f u_f\}$ and $\{x \in \mathsf{E}_{k,n/2} \,|\, x \preceq'_g u_g\}$ are equal then $f(x,x) = g(x,x)$ for all $x \in \mathbb{F}_2^{n/2}$. And since we assumed $\preceq_f = \preceq_g$, for all $(x,y) \in \mathbb{F}_2^n \,|\, x \neq y$ we have $f(x,y) = g(x,y)$ therefore $f = g$. Conversely, if there exists $k \in [1, n/2-1]$ such that $x \in \mathsf{E}_{k,n}$ satisfies $x \preceq'_f u_f$ and $x \not\preceq'_g u_g$ (without loss of generality) then $f(x,x) = 0$ and $g(x,x) = 1$, proving that $f \neq g$.

Finally, we derive the number of different functions, combining the number of different total order on binary strings of length 2^{m-1} and the number of partitions of $\mathsf{E}_{k,2^{m-1}}$ in two parts of same size:

$$\mathcal{D}_m = 2^{2^{m-1}}! \times \prod_{k=1}^{2^{m-1}-1} \binom{\binom{2^{m-1}}{k}}{\frac{1}{2}\binom{2^{m-1}}{k}}.$$

□

We study the nonlinearity and algebraic immunity of these families. First, we show a lower bound on the nonlinearity of any function from the two constructions. Then, we give a lower bound on the weightwise nonlinearity of the WPB constructions in terms of Krawtchouk polynomials. Finally, we address the AI of the first construction in Section 4, exhibiting WPB functions with minimal and maximal AI.

3.3 A nonlinearity lower bound

Theorem 3. *Let $m \in \mathbb{N}^*$, $n = 2^m$ and f be a function from the constructions of Definition 11 or Definition 12, then:* $\mathsf{NL}(f) \geq 2^{n-2} - 2^{n/2-1}$.

Proof. We compute the Walsh transform of f. For all $c \in \mathbb{F}_2^n$:

$$\begin{aligned} W_f(c) &= \sum_{z \in \mathbb{F}_2^n} (-1)^{f(z)+cz} \\ &= \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{f(x,x)+(a+b)x} + \sum_{x \in \mathbb{F}_2^{n/2},\, y \in \mathbb{F}_2^{n/2} \setminus \{x\}} (-1)^{f(x,y)+ax+by}, \end{aligned}$$

where $(a,b) = c$, that is a denotes the first $n/2$ bits of c and b denotes the second half.

First, we can bound the absolute value of the first term: $|\sum_{x\in\mathbb{F}_2^{n/2}}(-1)^{f(x,x)+(a+b)x}| \leq 2^{n/2}$. Then, we rewrite the second term:

$$\begin{aligned}
C &= \sum_{x\in\mathbb{F}_2^{n/2},\, y\in\mathbb{F}_2^{n/2}\setminus\{x\}} (-1)^{f(x,y)+ax+by} \\
&= \frac{1}{2}\sum_{\substack{x\in\mathbb{F}_2^{n/2}\\ y\in\mathbb{F}_2^{n/2}\setminus\{x\}}} (-1)^{f(x,y)+ax+by} + \frac{1}{2}\sum_{\substack{x\in\mathbb{F}_2^{n/2}\\ y\in\mathbb{F}_2^{n/2}\setminus\{x\}}} (-1)^{f(x,y)+ax+by} \\
&= \frac{1}{2}\sum_{x\in\mathbb{F}_2^{n/2},\, y\in\mathbb{F}_2^{n/2}\setminus\{x\}} \left((-1)^{f(x,y)+ax+by} + (-1)^{f(y,x)+ay+bx}\right) \\
&= \frac{1}{2}\sum_{x\in\mathbb{F}_2^{n/2},\, y\in\mathbb{F}_2^{n/2}\setminus\{x\}} (-1)^{f(x,y)}\left((-1)^{ax+by} - (-1)^{ay+bx}\right).
\end{aligned}$$

Then, to bound $|C|$, we determine the cardinal of the set $S = \{(x,y)\,|\,x \in \mathbb{F}_2^{n/2},\, y \in \mathbb{F}_2^{n/2}\setminus\{x\},\, (-1)^{ax+by} - (-1)^{ay+bx} = 0\}$. The condition $(-1)^{ax+by} - (-1)^{ay+bx} = 0$ is equivalent to $ax+by = ay+bx \pmod 2$, that is $(a+b)(x+y) = 0 \pmod 2$. First, note that if $a = b$ then $|S| = |\{(x,y)\,|\,x\in\mathbb{F}_2^{n/2},\, y\in\mathbb{F}_2^{n/2}\setminus\{x\}\}| = 2^{n/2}\cdot(2^{n/2}-1)$. Hence we focus on the case $d = a + b \neq 0_{n/2}$.

The addition by a constant $y \in \mathbb{F}_2^{\ell}$, ψ_y, defined by $\psi_y(x) = x + y$ (for $x \in \mathbb{F}_2^{\ell}$) is a bijection over $\mathbb{F}_2^{\ell}$. Then, the image of $\psi_y(x)$ for $x \in \mathbb{F}_2^{\ell}\setminus\{y\}$ is $\mathbb{F}_2^{\ell}\setminus\{0_\ell\}$. Accordingly, the sum $(x+y)$ such that $x \in \mathbb{F}_2^{\ell}, y \in \mathbb{F}_2^{\ell}\setminus\{x\}$ takes each element of $\mathbb{F}_2^{\ell}\setminus\{0_\ell\}$ exactly 2^{ℓ} times. Since for $d \neq 0_\ell$ we have $|\{x \in \mathbb{F}_2^{\ell}\,|\,d\cdot x = 0\}| = 2^{\ell-1}$ and $d\cdot 0_\ell = 0$ we obtain $|S| = 2^{n/2}(2^{n/2-1}-1) = 2^{n-1} - 2^{n/2}$. It allows to bound $|C|$:

$$\begin{aligned}
|C| &= |\frac{1}{2}\sum_{x\in\mathbb{F}_2^{n/2},\, y\in\mathbb{F}_2^{n/2}\setminus\{x\}} (-1)^{f(x,y)}\left((-1)^{ax+by} - (-1)^{ay+bx}\right)| \\
&= \frac{1}{2}|\sum_{\substack{x\in\mathbb{F}_2^{n/2},\, y\in\mathbb{F}_2^{n/2}\setminus\{x\}\\ (x,y)\notin S}} 2(-1)^{f(x,y)+ax+by} + \sum_{\substack{x\in\mathbb{F}_2^{n/2},\, y\in\mathbb{F}_2^{n/2}\setminus\{x\}\\ (x,y)\in S}} 0| \\
&\leq \frac{1}{2}|2\left(2^{n/2}(2^{n/2}-1) - 2^{n-1} + 2^{n/2}\right)| = |2^n - 2^{n/2} - 2^{n-1} + 2^{n/2}| = 2^{n-1}
\end{aligned}$$

Finally, using the relation between nonlinearity and Walsh transform (Definition 7) we obtain:

$$\mathsf{NL}(f) = 2^{n-1} - \frac{1}{2}\max_{c\in\mathbb{F}_2^n}|W_f(c)| \geq 2^{n-1} - \frac{1}{2}\left(2^{n-1} + 2^{n/2}\right) = 2^{n-2} - 2^{n/2-1}.$$

□

We remark that the bound of Theorem 3 is half of the covering radius bound, so it cannot guarantee the nonlinearity of these functions is close to optimal.

Nevertheless, this nonlinearity bound is more than sufficient for functions used in the context of FLIP [26] or FiLIP [25] based on their security analyses.

Theorem 4. *Let $m \in \mathbb{N}^*$, $n = 2^m$ and f be a function from the constructions of Definition 11 or Definition 12, then, for all $k \in [0, n]$:*

$$\mathsf{NL}_k(f) \geq \frac{1}{4}\binom{n}{k} - \binom{\frac{n}{2}}{\frac{k}{2}} - \frac{1}{2}\max_{\ell \in [1,n]} |\sum_{t=0}^{k} \mathsf{K}_t(\ell, \frac{n}{2})\mathsf{K}_{k-t}(\ell, \frac{n}{2})|.$$

Proof. We compute the restricted Walsh transform of f on $\mathsf{E}_{k,n}$. For all $c \in \mathbb{F}_2^n$:

$$\begin{aligned}
&\mathcal{W}_{f,k}(c) = \sum_{z \in \mathsf{E}_{k,n}} (-1)^{f(z)+cz} \\
&= \sum_{x \in \mathsf{E}_{k/2,n/2}} (-1)^{f(x,x)+(a+b)x} + \sum_{(x,y) \in \mathsf{E}_{k,n},\, x \neq y} (-1)^{f(x,y)+ax+by} \\
&= \sum_{x \in \mathsf{E}_{\frac{k}{2},\frac{n}{2}}} (-1)^{f(x,x)+(a+b)x} + \sum_{t=0}^{k} \sum_{\substack{x \in \mathsf{E}_{t,n/2},\, y \in \mathsf{E}_{k-t,n/2} \\ x \neq y}} (-1)^{f(x,y)+ax+by} \\
&= \sum_{x \in \mathsf{E}_{\frac{k}{2},\frac{n}{2}}} (-1)^{f(x,x)+(a+b)x} + \frac{1}{2}\sum_{t=0}^{k} \sum_{\substack{x \in \mathsf{E}_{t,\frac{n}{2}} \\ y \in \mathsf{E}_{k-t,\frac{n}{2}} \setminus \{x\}}} (-1)^{f(x,y)} \left((-1)^{ax+by} - (-1)^{ay+bx}\right)
\end{aligned}$$

where $(a, b) = c$, that is a denotes the first $n/2$ bits of c and b denotes the second half. Similarly, $(x, y) = z$, where x denotes the first $n/2$ variables of z and y the second half.

Similarly to the proof of Theorem 3, we are looking for the number of elements (x, y) such that $(-1)^{ax+by} - (-1)^{ay+bx} = 0$. This is equivalent to the number of elements (x, y) such that $(a + b)(x + y) = 0 \mod 2$ where this time $x \in \mathsf{E}_{t,n/2}$ and $y \in \mathsf{E}_{k-t,n/2}$. Denoting $a + b$ as d we have that all elements lead to 0 if $d = 0_{n/2}$, for the other values of d we determine it in function of $\ell = \mathsf{w_H}(d)$:

$$\begin{aligned}
&|S_d| = |\{x \in \mathsf{E}_{t,\frac{n}{2}}, y \in \mathsf{E}_{k-t,\frac{n}{2}} \,|\, (x + y)d = 0\}| \\
&= |\{x \in \mathsf{E}_{t,\frac{n}{2}}, y \in \mathsf{E}_{k-t,\frac{n}{2}} \,|\, xd = yd = 0\}| + |\{x \in \mathsf{E}_{t,\frac{n}{2}}, y \in \mathsf{E}_{k-t,\frac{n}{2}} \,|\, xd = yd = 1\}| \\
&= |\{x \in \mathsf{E}_{t,\frac{n}{2}} \,|\, xd = 0\}||\{y \in \mathsf{E}_{k-t,\frac{n}{2}} \,|\, yd = 0\}| + |\{x \in \mathsf{E}_{t,\frac{n}{2}} \,|\, xd = 1\}||\{y \in \mathsf{E}_{k-t,\frac{n}{2}} \,|\, yd = 1\}|
\end{aligned}$$

Then, we determine $|\{x \in \mathsf{E}_{t,n/2} \,|\, xd = 0\}|$ using the definition of Krawtchouk polynomials (Definition 9):

$$
\begin{aligned}
|\{x \in \mathsf{E}_{t,n/2} \,|\, xd = 0\}| &= \sum_{\substack{j=0\\ j \text{ even}}}^{t} \binom{\ell}{j}\binom{n/2-\ell}{t-j} \\
&= \frac{1}{2}\left(\sum_{\substack{j=0\\ j \text{ even}}}^{t} \binom{\ell}{j}\binom{n/2-\ell}{t-j} + \sum_{j=0}^{t} \binom{\ell}{j}\binom{n/2-\ell}{t-j} - \sum_{\substack{j=0\\ j \text{ odd}}}^{t} \binom{\ell}{j}\binom{n/2-\ell}{t-j} \right) \\
&= \frac{1}{2}\left(\mathsf{K}_t(\ell, n/2) + \sum_{j=0}^{t} \binom{\ell}{j}\binom{n/2-\ell}{t-j} \right) = \frac{1}{2}\left(\mathsf{K}_t(\ell, n/2) + \binom{n/2}{t} \right),
\end{aligned}
$$

where the last equation comes from the Vandermonde convolution. Using similar formulas for the other sets we obtain:

$$
\begin{aligned}
|S_d| &= \frac{1}{4}\left(\binom{\frac{n}{2}}{t} + \mathsf{K}_t(\ell, \frac{n}{2}) \right)\left(\binom{\frac{n}{2}}{k-t} + \mathsf{K}_{k-t}(\ell, \frac{n}{2}) \right) \\
&\quad + \frac{1}{4}\left(\binom{\frac{n}{2}}{t} - \mathsf{K}_t(\ell, \frac{n}{2}) \right)\left(\binom{\frac{n}{2}}{k-t} - \mathsf{K}_{k-t}(\ell, \frac{n}{2}) \right) \\
&= \frac{1}{4}\left(2\binom{\frac{n}{2}}{t}\binom{\frac{n}{2}}{k-t} + 2\mathsf{K}_t(\ell, \frac{n}{2})\mathsf{K}_{k-t}(\ell, \frac{n}{2}) \right).
\end{aligned}
$$

Using the value of $|S_d|$ we can derive an lower bound on $|\mathcal{W}_{f,k}(c)|$:

$$
\begin{aligned}
|\mathcal{W}_{f,k}(c)| &= |\sum_{x \in \mathsf{E}_{k/2,n/2}} (-1)^{f(x,x)+(a+b)x} + \frac{1}{2}\sum_{t=0}^{k} \sum_{\substack{x \in \mathsf{E}_{t,n/2}\\ y \in \mathsf{E}_{k-t,n/2} \setminus \{x\}}} (-1)^{f(x,y)}\left((-1)^{ax+by} - (-1)^{ay+bx}\right)| \\
&\leq \binom{n/2}{k/2} + |\frac{1}{2}\sum_{t=0}^{k} \sum_{\substack{x \in \mathsf{E}_{t,n/2},\, y \in \mathsf{E}_{k-t,n/2}\\ x \neq y}} (-1)^{f(x,y)}\left((-1)^{ax+by} - (-1)^{ay+bx}\right)| \\
&\leq \binom{n/2}{k/2} + |\frac{1}{2}\sum_{t=0}^{k} \left(\sum_{\substack{x \in \mathsf{E}_{t,\frac{n}{2}},\, y \in \mathsf{E}_{k-t,\frac{n}{2}}\\ x \neq y,\, (x,y) \in S_d}} (-1)^{f(x,y)}(0) + \sum_{\substack{x \in \mathsf{E}_{t,\frac{n}{2}},\, y \in \mathsf{E}_{k-t,\frac{n}{2}}\\ x \neq y,\, (x,y) \notin S_d}} 2(-1)^{f(x,y)+ax+by} \right)| \\
&\leq \binom{\frac{n}{2}}{\frac{k}{2}} + |\frac{1}{2}\left(\sum_{t=0}^{k} 2\left(\binom{\frac{n}{2}}{t}\binom{\frac{n}{2}}{k-t} - \frac{1}{2}\binom{\frac{n}{2}}{t}\binom{\frac{n}{2}}{k-t} - \mathsf{K}_t(\ell, \frac{n}{2})\mathsf{K}_{k-t}(\ell, \frac{n}{2}) \right) \right)| + |\frac{1}{2}2\binom{\frac{n}{2}}{\frac{k}{2}}| \\
&\leq 2\binom{\frac{n}{2}}{\frac{k}{2}} + |\sum_{t=0}^{k} \left(\frac{1}{2}\binom{\frac{n}{2}}{t}\binom{\frac{n}{2}}{k-t} - \mathsf{K}_t(\ell, \frac{n}{2})\mathsf{K}_{k-t}(\ell, \frac{n}{2}) \right)| \\
&\leq 2\binom{\frac{n}{2}}{\frac{k}{2}} + \frac{1}{2}\binom{n}{k} + |\sum_{t=0}^{k} \mathsf{K}_t(\ell, \frac{n}{2})\mathsf{K}_{k-t}(\ell, \frac{n}{2})|,
\end{aligned}
$$

where the last equation comes from Vandermonde's convolution.

Finally, we can give the bound on the NL_k using the relation with the restricted Walsh transform:

$$\begin{aligned}
\mathsf{NL}_k(f) &= \frac{1}{2}\binom{n}{k} - \frac{1}{2}\max_{c\in\mathbb{F}_2^n}|\mathcal{W}_{f,k}(c)| \\
&\geq \frac{1}{2}\binom{n}{k} - \frac{1}{2}\max_{\ell\in[1,n]}\left(2\binom{\frac{n}{2}}{\frac{k}{2}} + \frac{1}{2}\binom{n}{k} + |\sum_{t=0}^{k}\mathsf{K}_t(\ell,\frac{n}{2})\mathsf{K}_{k-t}(\ell,\frac{n}{2})|\right) \\
&\geq \frac{1}{4}\binom{n}{k} - \binom{\frac{n}{2}}{\frac{k}{2}} - \frac{1}{2}\max_{\ell\in[1,n]}|\sum_{t=0}^{k}\mathsf{K}_t(\ell,\frac{n}{2})\mathsf{K}_{k-t}(\ell,\frac{n}{2})|.
\end{aligned}$$

□

4 Concrete constructions and parameters

4.1 WPB from popular orders

We can take different orders to compare the properties reached in practice by the construction of Definition 11. For example we will consider the orders lexicographic and cool [36]. For these two cases we use the lexicographic order (respectively cool order taking 0 as the first element) to define the orders on the 2^i-length binary strings for $i \in [0, m-1]$. We give the properties of the produced WPB functions in 8 and 16 variables in Table 1 and 2, (in our code, binary strings are encoded as integers, considering the least significant bit in position n). We observe that most of the parameters of the function given by the cool order are better than the one given by the lexicographic order. The AI of the construction from the lexicographic order is the minimal possible for a WPB function in more than 2 variables (see [11], Theorem 1). In the following proposition we show that any WPB function f built from Definition 11 or 12 with the lexicographic order as $\prec_{m-1}$ has AI only 2.

Function	res	deg	NL	AI	NL_2	NL_3	NL_4	NL_5	NL_6	AI_2	AI_3	AI_4	AI_5	AI_6
Lex	0	6	60	2	4	13	12	13	4	1	2	2	2	1
Cool	0	7	84	3	4	12	20	14	6	1	2	2	2	2

Table 1. Cryptographic parameters of Construction 1 in 8 variables instantiated with the lexicographic order (Lex) and the cool order (Cool)

Function	res	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}
Lex	0	16316	24	150	484	1183	1987	2717	2980	2717	1987	1183	484	150	24
Cool	0	26420	24	56	526	1204	3057	3220	4804	3222	3001	1162	652	126	26

Function	deg	AI	AI_2	AI_3	AI_4	AI_5	AI_6	AI_7	AI_8	AI_9	AI_{10}	AI_{11}	AI_{12}	AI_{13}	AI_{14}
Lex	14	2	1	2	2	2	2	2	2	2	2	2	2	2	1
Cool	15	7	1	2	3	3	4	4	4	4	4	3	3	2	2

Table 2. Cryptographic parameters of Construction 1 in 8 variables instantiated with the lexicographic order (Lex) and the cool order (Cool)

Proposition 3. *Let $m \in \mathbb{N}$, $m \geq 2$, and f be a Boolean function from Construction 1 with the lexicographic order as $\preceq_{m-1}$ or Construction 2 with the lexicographic order as $\preceq$, then f satisfies:*

$$\mathsf{AI}(f) = 2, \qquad \text{and} \qquad \forall k \in [1, 2^m - 1]\, \mathsf{AI}_k(f) \leq 2.$$

Proof. First we show the result on the algebraic immunity. We denote each input of $\mathbb{F}_2^{2^m}$ as $(x, y) = (x_1, \dots, x_r, y_1, \dots, y_r)$, where $r = 2^{m-1}$. When $x \neq y$ both constructions use the lexicographic order on x and y to determine the output. By definition of the lexicographic order (Definition 8), if $x_1 = 1$ and $y_1 = 0$ then $y \preceq x$ and $f(x, y) = 1$, if $x_1 = 0$ and $y_1 = 1$ then $x \preceq y$ and $f(x, y) = 0$. Then, the function $g(x, y) = (x_1+y_1)(1+x_1) = x_1y_1+y_1$ is non null and an annihilator of f. Finally, since $\mathsf{deg}(g) = 2$ and the algebraic immunity of a WPB function in more than 2 variables is at least 2 ([11], Theorem 1), it gives the algebraic immunity of f.

Regarding the weightwise algebraic immunity, we show that the function g is not constant on $\mathsf{E}_{k,2^m}$ for $k \in [1, 2^m - 1]$, therefore it is also a non null annihilator of f on the slice, implying $\mathsf{AI}_k(f) \leq 2$. We focus on the values taken by x_1 and y_1, g takes the value 1 when $x_1 = 1 + y_1 = 0$ and the value 0 when $x_1 = 1+y_1 = 1$. Therefore, using an element (x', y') of Hamming weight $k-1$ (for each k) to instantiate the $2^m - 2$ other variables, we obtain $(0, x', 1, y') \in \mathsf{E}_{k,2^m}$ and $(1, x', 0, y') \in \mathsf{E}_{k,2^m}$ such that $g(0, x', 1, y') \neq g(1, x', 0, y')$ hence g is not constant on $\mathsf{E}_{k,2^m}$. It allows us to conclude $\mathsf{AI}_k(f) \leq 2$. □

Proposition 3 can be extended to other orders than the lexicographic one, such as reverse lexicographic. Indeed, if for $\preceq_{m-1}$ or $\preceq$ there is one position i such that $f(x, y) = 1 + f(x + e_i, y + e_i)$ (where e_i denotes the vector having a one only in position i) when $x_i \neq y_i$ then the same reasoning applies, and the function admit a degree two annihilator. The properties of the functions given in Table 2 are low, compared for example with h_{16} in [10] which has degree 14, AI 8, and better nonlinearities. In the next part we study different orders leading to better degree and algebraic immunity.

4.2 WPB from weightwise orders

In this part we consider the notion of weightwise order, *i.e.* an order $\preceq$ that satisfies for all $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^n$ if $w(x) < w(y)$ then $x \prec y$. Note that the graded lexicographic order is an example of weightwise order. First, we show that any function built using Construction 1 with a weightwise order for $\preceq_{m-1}$ or Construction 2 with a weightwise order as $\preceq$ has optimal AI. Then, we show that these WPB functions are a (strict) subset of TL functions. Finally, we give the parameters of 2 functions in 8 and 16 variables.

Proposition 4. *Let $m \in \mathbb{N}$, $m \geq 2$, and f be a Boolean function from Construction 1 with a weightwise order as $\preceq_{m-1}$ or Construction 2 with a weightwise order as $\preceq$, then f satisfies: $\mathsf{AI}(f) = 2^{m-1}$.*

Proof. The proof consists in showing that f belongs to the TL family of WPB functions, hence Property 4 allows to conclude its algebraic immunity is 2^{m-1}. We use the characterization of TL functions given in Definition 10, we use the notation $n = 2^m$ for simplicity. The first property $f(0_n) = 0$ and $f(1_n) = 1$ is true since f is WPB by Theorem 1 (respectively Theorem 2 for Construction 2). The properties $f(x, y) = 0$ if $\mathsf{w_H}(x) < \mathsf{w_H}(y)$. and $h(x, y) = 1$ if $\mathsf{w_H}(x) > \mathsf{w_H}(y)$ are respected since f is build with a weightwise order. The last property to check is: $\forall j \in [1, 2^{m-1} - 1], \mathsf{supp}(f) \cap A_j = |A_j|/2$, where $A_j = \left\{(x, y) \in \mathbb{F}_2^{2^{m-1}} \times \mathbb{F}_2^{2^{m-1}} : \mathsf{w_H}(x) = \mathsf{w_H}(y) = j\right\}$.

If f is from Construction 1, then for all x and y such that $x \neq y$ only one of the two elements between (x, y) and (y, x) is in the support of f. For the elements (x, x) such that $x \in \mathbb{F}_2^{m-1} \setminus \{0_{2^{m-1}}, 1_{2^{m-1}}\}$ the value of f is defined by f_{m-1} which is WPB by Theorem 1 hence over all x of Hamming weight j, half are in the support of f_{m-1} and therefore half of the elements (x, x) are in the support of f. It allows to conclude $\mathsf{supp}(f) \cap A_j = |A_j|/2$, hence f is a TL function.

If f is from Construction 2, as before we have that for all x and y such that $x \neq y$ only one of the two elements between (x, y) and (y, x) is in the support of f. For the elements (x, x) such that x has Hamming weight j, by definition of the order $\preceq'$ (in Definition 12), f takes the value 0 for half of the values and 1 on the other half. It allows to conclude $\mathsf{supp}(f) \cap A_j = |A_j|/2$, therefore f is a TL function.

□

Remark 2. In the proof of Proposition 4, the AI is derived from the membership to the TL family. The functions considered in that proposition are a strict subset of the TL family. For two different elements of $\mathbb{F}_2^{m-1}$ with the same Hamming weight, say x and y, only one of the two elements between (x, y) and (y, x) can be in the support of an order-based WPB function. Conversely, there are TL functions such that (x, y) and (y, x) are both in the support or in the co-support since $m \geq 2$ (see Definition 10).

Function	res	deg	NL	AI	NL_2	NL_3	NL_4	NL_5	NL_6	AI_2	AI_3	AI_4	AI_5	AI_6
HWlex	0	7	74	4	4	8	14	8	4	1	2	2	2	1
HWcool	0	7	78	4	4	8	18	8	6	1	2	2	2	1

Table 3. Cryptographic parameters of Construction 1 in 8 variables instantiated with the weightwise lexicographic order HWlex and weightwise cool order (HWcool)

Function	res	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}
HWlex	0	23276	24	112	564	1120	2525	3152	3964	3152	2525	1120	564	112	24
HWcool	0	23544	24	112	578	1120	2595	3152	4042	3152	2567	1120	590	112	26

Function	deg	AI	AI_2	AI_3	AI_4	AI_5	AI_6	AI_7	AI_8	AI_9	AI_{10}	AI_{11}	AI_{12}	AI_{13}	AI_{14}
HWlex	14	8	1	2	2	3	3	4	4	4	3	3	2	2	1
HWcool	14	8	1	2	2	3	3	4	4	4	3	3	2	2	1

Table 4. Cryptographic parameters of Construction 1 in 16 variables instantiated with the weightwise lexicographic order (HWlex) and weightwise cool order (HWcool).

Both functions with parameters displayed in Table 3 and 4 have better degree and algebraic immunity than the one from Section 4.1. Regarding nonlinearity and weightwise nonlinearities, the values are similar or worse.

We also remark that for k odd any WPB function produced with a weightwise order with Construction 1 or Construction 2 will have NL_k and NL_{n-k} equal. This comes from the fact that for these values of k the two parts x and y cannot have the same Hamming weight, then f takes the opposite value on (x, y) and $(x, y) + 1_{2^m}$ for all $(x, y) \in \mathsf{E}_{k,n}$. Therefore, the distance between an affine function $a(x, y) + \varepsilon$ and f over $\mathsf{E}_{k,n}$ is the same as the one between $a((x, y) + 1_{2^m}) + \varepsilon + 1$ and f over $\mathsf{E}_{n-k,n}$. Regarding the case k even, x and y can have the same Hamming weight, and it this case the relation between $f(x, y)$ and $f((x, y) + 1_{2m})$ is not constant.

4.3 Orders from a field representation

We consider orders that come from a different representation of $\mathbb{F}_2^n$, as it has been fruitful to build Boolean function with optimal algebraic immunity. Various constructions using the univariate representation [3,17,33,39] (as functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$) or modifications of these constructions [19, 20], give families with optimal algebraic immunity and other good cryptographic properties such as high algebraic degree and good nonlinearity. The Carlet-Feng construction for example identifies $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$ and for α a primitive element of $\mathbb{F}_{2^n}$, the function f is defined by its support: 0 and α^i for $i \in [0, 2^{n-1} - 2]$. Similarly, we identify $\mathbb{F}_2^r$ to $\mathbb{F}_{2^r}$ and define the order using the consecutive powers of α, as in the following definition:

Definition 13 (field order). *Let $r \in \mathbb{N}^*$, for $s \in \mathbb{N}$ such that $s \leq 2^r - 2$ and α a primitive element of $\mathbb{F}_2^r$, we call field order defined by α and s the total order over $\mathbb{F}_2^r$ given by: $\alpha^s \prec \alpha^{s-1} \prec \ldots \prec \alpha^{2^r-2} \prec 0 \prec 1 \prec \ldots \prec \alpha^{s-2} \prec \alpha^{s-1}$.*

For WPB functions we use field orders for r powers of two only. In Table 5 we give the parameters of some 8-variable WPB functions obtained from the field representation. For these experiments (using Sage math) we took α the root of $X^4 + X + 1$ to build $\mathbb{F}_{16}$ and β the root of $X^2 + X + 1$ to build $\mathbb{F}_4$. The value t corresponds to the choice for the order used on the strings of length 2, and s for the one of length 4.

Value t	Value s	res	deg	NL	AI	NL_2	NL_3	NL_4	NL_5	NL_6	AI_2	AI_3	AI_4	AI_5	AI_6
0	0	0	7	78	4	6	13	20	18	8	1	2	3	2	2
0	4	0	7	92	4	4	8	20	12	8	1	2	2	2	2
0	6	0	7	88	4	6	15	20	18	6	2	2	2	2	2
1	1	0	7	90	4	6	12	24	18	8	1	2	2	2	2

Table 5. Cryptographic parameters of Construction 1 with the field representation, $n = 8$.

u	t	s	res	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}
0	0	0	0	30196	26	161	634	1770	3518	5062	5822	5185	3540	1848	725	196	34
0	0	128	0	30306	40	204	765	1814	3484	5138	5875	5158	3514	1819	743	182	35
1	11	111	0	30332	38	219	758	1887	3511	5041	5699	5105	3601	1879	702	189	36

u	t	s	deg	AI	AI_2	AI_3	AI_4	AI_5	AI_6	AI_7	AI_8	AI_9	AI_{10}	AI_{11}	AI_{12}	AI_{13}	AI_{14}
0	0	0	15	8	1	2	3	4	5	6	6	6	5	4	3	2	2
0	0	128	15	8	2	3	4	4	5	6	6	6	5	4	3	2	2
1	11	111	15	8	2	3	3	4	5	6	6	6	5	4	3	2	2

Table 6. Cryptographic parameters of Construction 1 with the field representation, $n = 16$.

From Table 5 and 6 we observe that the obtained functions have optimal degree ($n - 1$ for a balanced function) and optimal algebraic immunity ($\lceil n/2 \rceil$). Their weightwise algebraic immunities are at least as good as the ones of the functions built in Section 4.1 and Section 4.2, with a neat improvement for the medium weights in 16 variables. We display in green the values that reach the upper bound on the weightwise algebraic immunity $\min\{e \in \mathbb{N} \,|\, 2\binom{n}{e} > \binom{n}{k}\}$ ([4], Corollary 9), we observe that the weightwise AI of the function we test are optimal on the medium weights (from 6 to 10) in 16 variables. Regarding the nonlinearity and weightwise nonlinearities, in 8 variables there is always a function from Table 5 with a better value than the functions with parameters exhibited in Section 4.1 and 4.2. In 16 variables, the 3 WPB functions with parameters displayed in Table 6 always have better nonlinearity and weightwise nonlinearities than the other functions.

To compare the properties of these functions to the state of the art, we summarize in Table 7 and 8 the best parameters obtained with our construction from the field representation and the best known parameters for WPB functions. In 8 variables, all the functions exhibited so far have resilience order 0, the degree is 7 for more than half of them (see [12]) and cannot be more. The maximum nonlinearity comes from [13], the algebraic immunity can be optimal, 4 in this case. The maxima for the NLk come from the functions in [21] except for $k = 4$ which comes from [38], the maxima for the AIk come from this work. In 16 variables, all the functions exhibited so far have resilience order 0 and the maximal degree is 15. The best known nonlinearity comes from [13]. For the NLk, the best parameters are from h_{16} [10] or the one reached by the functions in Table 8. The maxima for the AIk come from this work.

From these tables, we can conclude that the newly built functions reach the highest parameters exhibited for all the algebraic properties and resilience. Regarding nonlinearity, the functions from this section reach a lower value than a random WPB function (see the experiments in [9], but a value sufficient for functions used in the context of FLIP [26] or FiLIP [25] based on their security analyses. The NLk for the 16-variable functions is the best exhibited for most of the values, but there are only a handful of articles to compare with. To conclude, the experimental findings suggest that utilizing order-based construction with field representations stands out as a very promising approach for generating WPB functions with good cryptographic parameters.

	res	deg	NL	AI	NL_2	NL_3	NL_4	NL_5	NL_6	AI_2	AI_3	AI_4	AI_5	AI_6
Table 5	0	7	92	4	6	15	24	18	8	2	2	3	2	2
SOTA	0	7	116	4	9	22	28	22	9	2	2	3	2	2

Table 7. Best known parameters of WPB functions, $n = 8$.

	res	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}
Table 6	0	30196	40	219	765	1887	3518	5138	5875	5185	3601	1879	743	196	36
SOTA	0	32598	40	219	765	1887	3629	5138	5875	5185	3625	1884	743	196	36

	deg	AI	AI_2	AI_3	AI_4	AI_5	AI_6	AI_7	AI_8	AI_9	AI_{10}	AI_{11}	AI_{12}	AI_{13}	AI_{14}
Table 6	15	8	2	3	4	4	5	6	6	6	5	4	3	2	2
SOTA	15	8	2	3	4	4	5	6	6	6	5	4	3	2	2

Table 8. Best known parameters of WPB functions, $n = 16$.

5 Generalization to WAPB constructions

We generalize the recursive order-based construction to build WAPB functions, and we exhibit the parameters of some of them. There are a few secondary constructions for building WAPB functions as illustrated in [10, 43]. However, most constructions are primarily focused on WPB functions and do not extend to WAPB functions.

5.1 An order-based WAPB construction

We propose the following construction of WAPB functions for any value of $n \geq 1$.

Definition 14 (Construction 3). *Let $n \in \mathbb{N}$, $n \geq 2$ and for $i \in [1, \lfloor \log_2(n) \rfloor]$ $\preceq_{\lfloor n/(2^i) \rfloor}$ be a total order on the set of $\lfloor n/(2^i) \rfloor$-length binary strings. Let f_n be the n-variable function defined recursively as:*

- *if $n = 1$, $f_1(0) = 0$ and $f_1(1) = 1$,*
- *if n is odd, $f_n(x_1, \ldots, x_n) = f_{n-1}(x_1, \ldots, x_{n-1})$*
-
$$f_n(x, y) = \begin{cases} f_{\lfloor n/2 \rfloor}(x) & \text{if } x = y, \\ 0 & \text{if } x \prec_{n/2} y, \\ 1 & \text{if } y \prec_{n/2} x, \end{cases}$$

  where $x, y \in \mathbb{F}_2^{n/2}$.

Theorem 5. *Let f_n defined as in Definition 14, f_n is WAPB.*

Proof. We prove the result by recursion. First, if $n = 1$, $f_1(0) = 0$ and $f_1(1) = 1$ hence $f_1 = x_1$ is WAPB by definition. Then, we assume that f_i is WAPB for all $i \in [1, n-1]$ such that f_i is defined. We consider two cases, n odd and n even.

If n is odd, by construction $f_n(x_1, \ldots, x_n) = f_{n-1}(x_1, \ldots, x_{n-1})$. In this case f_n can be written using Siegenthaler's construction as:

$$f_n = x_n \cdot f_{n-1}(x_1, \ldots, x_{n-1}) + (1 + x_n) \cdot f_{n-1}(x_1, \ldots, x_{n-1}).$$

Using [10] Proposition 2 we have the following relation on the restricted Walsh transform of f_n for all $k \in [0, n]$: $\mathcal{W}_{f_n,k}(0_n) = \mathcal{W}_{f_{n-1},k}(0_n) + \mathcal{W}_{f_{n-1},k-1}(0_n)$. Using Property 1 since f_{n-1} is WAPB we have that both $\mathcal{W}_{f_{n-1},k}(0_n)$ and $\mathcal{W}_{f_{n-1},k-1}(0_n)$ have absolute value no greater than 1. Since $n-1$ is even, at least one of the binomial coefficients between $\binom{n-1}{k}$ and $\binom{n-1}{k-1}$ is even ($\binom{m}{r}$ with m even and r odd is even using Lucas' theorem), hence $\mathcal{W}_{f_n,k}(0_n) \in \{-1, 0, 1\}$, and f_n is WAPB by Property 1.

If n is even, we rewrite $\mathcal{W}_{f_n,k}(0_n)$: $\mathcal{W}_{f_n,k}(0_n) = \mathcal{W}_{f_n,A}(0_n) + \mathcal{W}_{f_n,B}(0_n)$, where $A = \{\mathsf{E}_{k,n} \cap \{(x, y), x \in \mathbb{F}_2^{n/2}, y \in \mathbb{F}_2^{n/2}, x = y\}\}$ and $B = \{\mathsf{E}_{k,n} \cap \{(x, y), x \in \mathbb{F}_2^{n/2}, y \in \mathbb{F}_2^{n/2}, x \neq y\}\}$. Since $f_{\lfloor n/2 \rfloor}(x) = 0$ if $x \prec_{n/2} y$ and 1 if $y \prec_{n/2} x$, we get $W_{f_n,B}(0_n) = 0$. Then, note that $W_{f_n,A}(0_n) = W_{f_{n/2},\frac{n}{2}}(0_{n/2})$, and since $f_{n/2}$ is WAPB by assumption, $W_{f_{n/2},\frac{n}{2}}(0_{n/2}) \in \{-1, 0, 1\}$ hence $W_{f_n,k}(0_n) \in \{-1, 0, 1\}$ which allows to conclude that f_n is WAPB in this case and it finishes the proof.

□

Remark 3. Note that when $\mathsf{E}_{k,n}$ has an odd parity the value of -1 or $+1$ of $\mathcal{W}_{f,k}$ circles back to the values of f_1, which leads to having one extra 0 for slices such that $k < n/2$ and an extra 1 for $k > n/2$. Accordingly, the functions generated by Construction 3 are Special WAPB functions (as introduced in [10]).

We also remark that for m a power of 2, the functions created are the same WPB functions as the ones from Construction 1 (only the index of the orders differ, between 0 and $m-1$ for Construction 1 corresponding to 2^0 to 2^{m-1} for Construction 3).

Note also that Construction 3 can be generalized to give other WAPB functions. Defining $f_n(x_1, \ldots, x_n)$ as $f_{n-1}(x_1, \ldots, x_{n-1})$ when n is odd corresponds to ignoring the last variable to keep even-length bit-strings, it allows to consider an order comparing the two (same-length) halves. Similarly, any of the n variables can be ignored at each step where n is odd, giving different WAPB constructions. Additionally the values of f in 0_n and 1_n can also be defined differently at each step to generalize the construction.

5.2 Order-based WAPB construction and experimental results

In this section, we present the parameters of WAPB functions derived from Construction 3, based on orders previously outlined in Section 4. Notably, for an odd number n, the function f_n is equivalent to f_{n-1} but includes an additional mute variable. Consequently, the characteristics of f_n can be deduced from those of f_{n-1} (for instance, by applying the properties related to the direct sum of f_{n-1} and the 1-variable null function, see for example [26] Lemma 3). Therefore, our analysis primarily concentrates on functions with an even number of variables. Detailed parameters for WAPB functions with 10 variables are provided in Table 9. Subsequently, we delve into the functions with 12 variables in Table 10 and those with 14 variables in Table 11.

In the tables, “Lex” denotes the lexicographic order applied in Construction 3 across various lengths: $1, 2, 5$ for $n = 10$; $1, 3, 6$ for $n = 12$; and $1, 3, 7$ for $n = 14$. “Cool” signifies the cool order, detailed in Definition 8. The terms “HWlex” and “HWcool” are used for weightwise orders as described in Section 4.2. “Fields0” and “FieldsHalf” represent the field orders from Definition 13, where for the biggest length, the order is determined with $s = 0$ or $2^{n/2-1}$ respectively, with 0 used for the remaining lengths.

Function	res	deg	NL	AI	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8	AI_2	AI_3	AI_4	AI_5	AI_6	AI_7	AI_8
Lex	0	7	248	2	9	32	45	56	45	32	9	1	2	2	2	2	2	1
Cool	0	9	396	4	9	20	61	62	71	28	10	1	2	3	3	3	2	2
HWlex	0	9	322	5	9	20	53	50	53	20	9	1	2	2	3	2	2	1
HWcool	0	9	354	5	9	20	69	50	65	20	9	1	2	2	3	2	2	1
Fields0	0	9	406	5	9	32	71	90	79	44	13	1	2	3	3	3	3	2
FieldsHalf	0	9	420	5	14	34	81	82	81	34	10	2	2	3	3	3	2	1

Table 9. Cryptographic parameters of Construction 3 in 10 variables.

Function	res	NL	NL$_2$	NL$_3$	NL$_4$	NL$_5$	NL$_6$	NL$_7$	NL$_8$	NL$_9$	NL$_{10}$
Lex	0	1008	12	56	123	186	204	186	123	56	12
Cool	0	1650	12	30	147	202	320	200	173	50	14
HWlex	0	1362	12	40	143	180	258	180	143	40	12
HWcool	0	1430	12	40	163	180	278	180	156	40	14
Fields0	0	1728	14	65	168	216	372	316	180	81	19
FieldsHalf	0	1730	20	64	179	322	384	330	195	71	14

Function	deg	AI	AI$_2$	AI$_3$	AI$_4$	AI$_5$	AI$_6$	AI$_7$	AI$_8$	AI$_9$	AI$_{10}$
Lex	10	2	1	2	2	2	2	2	2	2	1
Cool	11	5	1	2	3	3	4	3	3	2	2
HWlex	11	6	1	2	2	3	3	3	2	2	1
HWcool	11	6	1	2	2	3	3	3	2	2	1
Fields0	11	6	1	2	3	4	4	4	3	2	2
FieldsHalf	11	6	2	2	3	4	4	4	3	2	1

Table 10. Cryptographic parameters of Construction 3 in 12 variables.

Function	res	NL	NL$_2$	NL$_3$	NL$_4$	NL$_5$	NL$_6$	NL$_7$	NL$_8$	NL$_9$	NL$_{10}$	NL$_{11}$	NL$_{12}$
Lex	0	4064	19	94	275	506	699	792	699	506	275	94	19
Cool	0	6600	19	42	289	532	1103	924	1089	520	354	82	20
HWlex	0	5656	19	70	315	490	893	884	893	490	315	70	19
HWcool	0	5810	19	70	319	490	941	884	931	490	332	70	21
Fieds0	0	6894	21	106	339	704	1233	1452	1314	823	384	122	22
FieldsHalf	0	6976	25	90	384	834	1259	1414	1221	837	407	138	28

Function	deg	AI	AI$_2$	AI$_3$	AI$_4$	AI$_5$	AI$_6$	AI$_7$	AI$_8$	AI$_9$	AI$_{10}$	AI$_{11}$	AI$_{12}$
Lex	11	2	1	2	2	2	2	2	2	2	2	2	1
Cool	12	6	1	2	3	3	4	4	4	3	3	2	2
HWlex	12	7	1	2	2	3	3	4	3	3	2	2	1
HWcool	13	7	1	2	2	3	3	4	3	3	2	2	1
Fieds0	13	7	1	2	3	4	5	5	5	4	3	2	2
FieldsHalf	13	7	2	2	3	4	5	5	5	4	3	2	2

Table 11. Cryptographic parameters of Construction 3 in 14 variables.

The outcomes for WAPB functions mirror those observed in the previous section for 8-variable and 16-variable WPB functions. We note that across various cryptographic parameters, WAPB functions utilizing field-based ordering achieve superior outcomes, particularly in terms of nonlinearities and algebraic immunities. Specifically, the two field-based constructions significantly outperform others in nonlinearity and weightwise nonlinearities, followed by those based on the cool order, which in turn exhibit better parameters than the remaining constructions. To the best of our knowledge, no other studies have presented parameters for WAPB constructions in more than 8 variables, making it difficult to compare the values reached by these functions beyond between themselves. In terms of algebraic properties, the degree and AI for the Fields0 and FieldsHalf constructions are consistently optimal. Highlighted in green are the values that achieve the upper bound of the weightwise algebraic immunity, indicating that, particularly for mid-range weights, the field-based functions reach the optimum. It is important to note that this upper bound may not always be attainable, suggesting that other values presented in the tables could also be optimal.

6 Conclusion

In this article, we presented two WPB constructions and one WAPB construction based on the concept of order. Unlike previous approaches for constructing these functions, we anticipate that these W(A)PB functions will be easier to implement and will lead to more efficient computations when used in the context of stream ciphers. Indeed, the ease of implementation and efficiency largely depend on how effectively the order between two inputs, x and y, can be determined. This, in turn, hinges on the orders chosen to define the function

In this article, we first demonstrated the general properties of order-based WPB functions. We introduced two constructions: a recursive one that utilizes multiple orders (one for each power of 2 up to $n/2$), and a second one that employs only two orders. We then counted the WPB functions in these two families and examined their nonlinearities. Specifically, we provided a lower bound for the nonlinearity and the weightwise nonlinearities for all functions within these two families.

Subsequently, we concentrated on specific orders that are commonly used: lexicographic and cool. We also examined weightwise orders, as well as those based on field representation. We demonstrated that within these constructions, some functions, such as those using the lexicographic order, exhibit the lowest possible algebraic immunity. Conversely, all functions employing weightwise orders achieve optimal algebraic immunity.

We provided experimental results detailing the parameters of WPB functions in 8 and 16 variables, along with WAPB functions for $n \in \{10, 12, 14\}$. We presented the outcomes for global parameters—such as resilience order, nonlinearity, degree, and algebraic immunity—as well as weightwise parameters, specifically NL_k and AI_k. This more comprehensive experimental study illustrates that order-based W(A)PB functions can possess robust cryptographic parameters. Notably, those based on field orders exhibit optimal degree, strong algebraic immunity, and favorable weightwise algebraic immunities and nonlinearities.

We outline two open questions arising from this work:

- The bound on nonlinearity from Theorem 3 assures that these functions achieve a nonlinearity that is at least half that of bent functions. It would be interesting to determine if a better bound could be established for the entire family or for a specific subfamily of order-based WPB functions.
- In the tables presented in Sections 4.3 and 5, we highlight instances where functions based on field orders achieve the upper bound of the AI_k parameter.

This parameter may be optimal for additional values of k, given that the upper bound is not proven to be tight. Further investigation into this criterion is warranted, as currently, very little is known about this variant of algebraic immunity. To date, the values achieved by W(A)PB functions have only been exhibited in a limited number of studies, such as [12, 37].

7 Acknowledgments

The author was supported by the ERC Advanced Grant no. 787390.

References

1. Belaïd, S., Fouque, P.A., Gérard, B.: Side-channel analysis of multiplications in gf(2128). In: Advances in Cryptology – ASIACRYPT 2014. pp. 306–325. Springer Berlin Heidelberg (2014)
2. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press (2021). https://doi.org/10.1017/9781108606806
3. Carlet, C., Feng, K.: An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In: Advances in Cryptology - ASIACRYPT 2008. pp. 425–440 (2008)
4. Carlet, C., Méaux, P., Rotella, Y.: Boolean functions with restricted input and their robustness; application to the FLIP cipher. IACR Trans. Symmetric Cryptol. **2017**(3) (2017)
5. Dachman-Soled, D., Ducas, L., Gong, H., Rossi, M.: LWE with side information: Attacks and concrete security estimation. In: Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II. Lecture Notes in Computer Science, vol. 12171, pp. 329–358. Springer (2020)
6. Dalai, D.K., Mallick, K.: A class of weightwise almost perfectly balanced boolean functions with high weightwise nonlinearity. BFA 2023 (2023)
7. Dalai, D.K., Mallick, K.: A class of weightwise almost perfectly balanced boolean functions. Advances in Mathematics of Communications **18**(2), 480–504 (2024)
8. Duval, S., Méaux, P., Momin, C., Standaert, F.X.: Exploring crypto-physical dark matter and learning with physical rounding: Towards secure and efficient fresh rekeying. IACR Transactions on Cryptographic Hardware and Embedded Systems **2021**(1), 373–401 (2020). https://doi.org/10.46586/tches.v2021.i1.373-401
9. Gini, A., Méaux, P.: On the weightwise nonlinearity of weightwise perfectly balanced functions. Discret. Appl. Math. **322**, 320–341 (2022). https://doi.org/10.1016/j.dam.2022.08.017
10. Gini, A., Méaux, P.: Weightwise almost perfectly balanced functions: Secondary constructions for all n and better weightwise nonlinearities. In: Isobe, T., Sarkar, S. (eds.) Progress in Cryptology - INDOCRYPT 2022 - 23rd International Conference on Cryptology in India, Kolkata, India, December 11-14, 2022, Proceedings. Lecture Notes in Computer Science, vol. 13774, pp. 492–514. Springer (2022)
11. Gini, A., Méaux, P.: On the algebraic immunity of weightwise perfectly balanced functions. In: Aly, A., Tibouchi, M. (eds.) Progress in Cryptology - LATINCRYPT 2023 - 8th International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2023, Quito, Ecuador, October 3-6, 2023,

Proceedings. Lecture Notes in Computer Science, vol. 14168, pp. 3–23. Springer (2023). https://doi.org/10.1007/978-3-031-44469-2_1

12. Gini, A., Méaux, P.: S0-equivalent classes, a new direction to find better weightwise perfectly balanced functions, and more. IACR Cryptol. ePrint Arch. p. 1101 (2023), `https://eprint.iacr.org/2023/1101`
13. Gini, A., Méaux, P.: Weightwise perfectly balanced functions and nonlinearity. In: Hajji, S.E., Mesnager, S., Souidi, E.M. (eds.) Codes, Cryptology and Information Security - 4th International Conference, C2SI 2023, Rabat, Morocco, May 29-31, 2023, Proceedings. Lecture Notes in Computer Science, vol. 13874, pp. 338–359. Springer (2023). https://doi.org/10.1007/978-3-031-33017-9_21
14. Guo, X., Su, S.: Construction of weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. Discrete Applied Mathematics **307**, 102–114 (2022)
15. Hoffmann, C., Méaux, P., Momin, C., Rotella, Y., Standaert, F.X., Udvarhelyi, B.: Learning with physical rounding for linear and quadratic leakage functions. In: Advances in Cryptology – CRYPTO 2023. pp. 410–439 (2023)
16. Joye, M., Olivier, F.: Side-channel analysis. In: van Tilborg, H.C.A. (ed.) Encyclopedia of Cryptography and Security. Springer (2005)
17. Li, J., Carlet, C., Zeng, X., Li, ., Hu, L., Shan, J.: Two constructions of balanced boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks. Designs, Codes and Cryptography **76** (03 2014)
18. Li, J., Su, S.: Construction of weightwise perfectly balanced boolean functions with high weightwise nonlinearity. Discret. Appl. Math. **279**, 218–227 (2020)
19. Limniotis, K., Kolokotronis, N.: Boolean functions with maximum algebraic immunity: further extensions of the carlet–feng construction. DCC **86**, 1685–1706 (2018)
20. Limniotis, K., Kolokotronis, N., Kalouptsidis, N.: Secondary constructions of boolean functions with maximum algebraic immunity. Cryptography and Communications **5** (09 2013)
21. Liu, J., Mesnager, S.: Weightwise perfectly balanced functions with high weightwise nonlinearity profile. Des. Codes Cryptogr. **87**(8), 1797–1813 (2019)
22. MacWilliams, F., Sloane, N.: The Theory of Error-Correcting Codes. North-holland Publishing Company, 2nd edn. (1978)
23. Mandujano, S., Ku Cauich, J.C., Lara, A.: Studying special operators for the application of evolutionary algorithms in the seek of optimal boolean functions for cryptography. In: Pichardo Lagunas, O., Martínez-Miranda, J., Martínez Seis, B. (eds.) Advances in Computational Intelligence. pp. 383–396. Springer Nature Switzerland, Cham (2022)
24. Mariot, L., Picek, S., Jakobovic, D., Djurasevic, M., Leporati, A.: Evolutionary construction of perfectly balanced boolean functions. In: 2022 IEEE Congress on Evolutionary Computation (CEC). p. 1–8. IEEE Press (2022)
25. Méaux, P., Carlet, C., Journault, A., Standaert, F.: Improved filter permutators for efficient FHE: better instances and implementations. In: Hao, F., Ruj, S., Gupta, S.S. (eds.) Progress in Cryptology - INDOCRYPT. LNCS, vol. 11898, pp. 68–91. Springer (2019)
26. Méaux, P., Journault, A., Standaert, F.X., Carlet, C.: Towards stream ciphers for efficient FHE with low-noise ciphertexts. In: Advances in Cryptology – EUROCRYPT 2016. pp. 311–343 (2016)
27. Mesnager, S., Su, S.: On constructions of weightwise perfectly balanced boolean functions. Cryptography and Communications (2021)

28. Mesnager, S., Su, S., Li, J.: On concrete constructions of weightwise perfectly balanced functions with optimal algebraic immunity and high weightwise nonlinearity. Boolean Functions and Applications (2021)
29. Mesnager, S., Su, S., Li, J., Zhu, L.: Concrete constructions of weightwise perfectly balanced (2-rotation symmetric) functions with optimal algebraic immunity and high weightwise nonlinearity. Cryptogr. Commun. **14**(6), 1371–1389 (2022)
30. Mesnager, S., Zhou, Z., Ding, C.: On the nonlinearity of boolean functions with restricted input. Cryptogr. Commun. **11**(1), 63–76 (2019)
31. Oren, Y., Renauld, M., Standaert, F., Wool, A.: Algebraic side-channel attacks beyond the hamming weight leakage model. In: Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7428, pp. 140–154. Springer (2012)
32. Renauld, M., Standaert, F.: Algebraic side-channel attacks. In: Bao, F., Yung, M., Lin, D., Jing, J. (eds.) Information Security and Cryptology - 5th International Conference, Inscrypt 2009, Beijing, China, December 12-15, 2009. Revised Selected Papers. Lecture Notes in Computer Science, vol. 6151, pp. 393–410. Springer (2009)
33. Rizomiliotis, P.: On the resistance of boolean functions against algebraic attacks using univariate polynomial representation. IEEE Trans. on Inf. Theory **56**(8), 4014–4024 (2010)
34. Ruskey, F., Williams, A.: The coolest way to generate combinations. Discrete Mathematics **309**(17), 5305–5320 (2009)
35. Standaert, F.: Introduction to side-channel attacks. In: Verbauwhede, I.M.R. (ed.) Secure Integrated Circuits and Systems, pp. 27–42. Integrated Circuits and Systems, Springer (2010)
36. Stevens, B., Williams, A.: The coolest order of binary strings. In: Kranakis, E., Krizanc, D., Luccio, F.L. (eds.) Fun with Algorithms - 6th International Conference, FUN 2012, Venice, Italy, June 4-6, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7288, pp. 322–333. Springer (2012)
37. Tang, D., Liu, J.: A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity. Cryptogr. Commun. **11**(6), 1185–1197 (2019)
38. Yan, L., Cui, J., Liu, J., Xu, G., Han, L., Jolfaei, A., Zheng, X.: Iga: An improved genetic algorithm to construct weightwise (almost) perfectly balanced boolean functions with high weightwise nonlinearity. In: Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security. p. 638–648. ASIA CCS '23, Association for Computing Machinery, New York, NY, USA (2023)
39. Zeng, X., Carlet, C., Shan, J., Hu, L.: More balanced boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks. IEEE Transactions on Information Theory **57**(9), 6310–6320 (2011)
40. Zhang, R., Su, S.: A new construction of weightwise perfectly balanced boolean functions. Adv. Math. Commun. **17**(4), 757–770 (2023). https://doi.org/10.3934/AMC.2021020
41. Zhao, Q., Jia, Y., Zheng, D., Qin, B.: A new construction of weightwise perfectly balanced functions with high weightwise nonlinearity. Mathematics **11**(5) (2023)
42. Zhao, Q., Li, M., Chen, Z., Qin, B., Zheng, D.: A unified construction of weightwise perfectly balanced boolean functions. Discrete Applied Mathematics **337**, 190–201 (2023)
43. Zhu, L., Su, S.: A systematic method of constructing weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. Discrete Applied Mathematics **314**, 181–190 (2022)