On the algebraic immunity of weightwise perfectly balanced functions

Agnese Gini[0009−0001−9565−380X], Pierrick Méaux[0000−0001−5733−4341]

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

Abstract. In this article we study the Algebraic Immunity (AI) of Weightwise Perfectly Balanced (WPB) functions. After showing a lower bound on the AI of two classes of WPB functions from the previous literature, we prove that the minimal AI of a WPB n-variables function is constant, equal to 2 for $n \geq 4$. Then, we compute the distribution of the AI of WPB function in 4 variables, and estimate the one in 8 and 16 variables. For these values of n we observe that a large majority of WPB functions have optimal AI, and that we could not obtain a WPB function with AI 2 by sampling at random. Finally, we address the problem of constructing WPB functions with bounded algebraic immunity, exploiting a construction from [12]. In particular, we present a method to generate multiple WPB functions with minimal AI, and we prove that the WPB functions with high nonlinearity exhibited in [12] also have minimal AI. We conclude with a construction giving WPB functions with lower bounded AI, and give as example a family with all elements with AI at least $n/2 - \log(n) + 1$.

Keywords: Boolean functions, algebraic immunity, weightwise perfectly balanced functions, FLIP.

1 Introduction.

Among the different criteria of Boolean functions analyzed during the last years, those targeting Boolean functions with restricted input sets have been increasingly studied after the work of Carlet, Méaux, and Rotella [6]. The authors introduced cryptographic criteria of Boolean functions with restricted input for the cryptanalysis of FLIP stream cipher [22], whose specificity is that its filter function is evaluated on sets of Boolean vectors having constant Hamming weight. Therefore, considering functions with good properties also when restricted is crucial for investigating its security. Properties on sets of constant Hamming weight arise also in other contexts, such as side channel attacks where it is common to obtain information on the Hamming weight of inputs (*e.g.* [18,32]).

One property of main interest is the balancedness, as in most cryptographic contexts using balanced functions prevents biased output distributions, it is desirable for applications like FLIP to work with functions balanced when restricted to the slices $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$ of the Boolean hypercube $\mathbb{F}_2^n$. In this context Carlet *et al.* [6] presented the concept of Weightwise Perfectly Balanced (WPB) functions, $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, such that $|\{x \in \mathsf{E}_{k,n} \,|\, f(x) = 0\}| = |\{x \in \mathsf{E}_{k,n} \,|\, f(x) = 1\}|$ for each $1 \leq k \leq n-1$, f globally balanced, and $f(0_n) = 0$. These functions are at maximal distance from the set of symmetric functions, deeply studied in the context of cryptography *e.g.* [1,2,3], analogously to the bent functions (*e.g.* [24,30]) from the set of affine functions. Diverse methods for constructing WPB functions have been proposed since 2017 *e.g.* [10,11,12,13,14,15,17,19,25,26,27,33,34,35,37]. The main cryptographic properties that have been studied on WPB functions so far are the weightwise nonlinearity (*i.e.* nonlinearity restricted on the slices) such as in [10,15,27], and more recently the (global) nonlinearity such as in [12,17]. Other relevant cryptographic properties on Boolean functions have not been studied deeply on the set of WPB functions, such as the algebraic immunity.

The concept of Algebraic Immunity (AI) appeared in [7] in the context of algebraic attacks on stream ciphers. In the attack described by Courtois and Meier, instead of focusing on the system of equations given by a filter function f (a Boolean function in n variables), they consider a system of equations potentially simpler to solve, obtained by the annihilators of f. They show that even if f has a high degree (close to n), f or $f+1$ always admits an annihilator of degree at most $\lceil (n+1)/2 \rceil$, allowing the attacker to reduce the attack to solving an algebraic system of the annihilator's degree. The notion of algebraic immunity has been formalized later in [23], as $\mathsf{AI}(f) = \min_{g\neq 0}\{\mathsf{deg}(g) \mid fg = 0 \text{ or } (f+1)g = 0\}$. Since then, the algebraic immunity has been thoroughly studied since it applies to the contexts of filtered linear shift back registers [7], and more recently (improved) filtered permutators [?, 22], group filter permutators [?], local PseudoRandom Generators (PRG) such as Goldreich's PRG [?] (see [?]) or variants [?], and conceptually simple weak pseudorandom functions [?, ?]. For WPB functions the AI is only known for a few constructions. The family exhibited by Tang and Liu [33], and later the families from [26, 27] are designed to have optimal AI. Then, all the other results are experimental, computing the AI of WPB functions in 4, 8 or 16 variables such as in [11, 25, 35].

Hence, the goal of this article is to further study the algebraic immunity of WPB functions. First we investigate the extreme values of the AI inside the class of WPB functions, and the AI distribution in a small number of variables. Since families with optimal AI have been exhibited, we focus on the minimal value that can reach a WPB function, and show lower bounds for two former secondary constructions (from [6] and [37]). Contrarily to the degree that is at least $n/2$, we show that the minimal AI of a WPB function is constant, equal to 2 for $n \geq 4$. We compute the distribution of the AI of WPB functions in 4 variables, and estimate the one in 8 and 16 variables, following the model established by [10] for the weightwise nonlinearities. For these values of n we observe that a large majority of WPB functions have optimal AI, and that we could not obtain an WPB function with AI 2 by sampling at random. Then, we address the problem of constructing WPB functions with bounded algebraic immunity. We use the construction from [12] to build functions with upper bounded AI. In particular, we present a method to generate multiple WPB functions with minimal AI, and we prove that the WPB functions with high nonlinearity exhibited in [12] also have minimal AI. We finish with a construction giving WPB functions with lower bounded AI, and give as example a family with all elements with AI at least $n/2 - \log(n) + 1$.

2 Preliminaries

For readability we use the notation $+$ instead of $\oplus$ to denote the addition in $\mathbb{F}_2$ and $\sum$ instead of $\bigoplus$. 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 of $\mathbb{F}_2^n$ we denote $\mathsf{d_H}(v, w)$ the Hamming distance between v and w, that is $\mathsf{d_H}(v, w) = \mathsf{w_H}(v + w)$.

2.1 Boolean functions and weightwise considerations

In this part we recall general concepts on Boolean functions and their weightwise properties we use in this article. For a deeper introduction on Boolean functions and their cryptographic parameters we refer to the survey of [4] and to [6] for the weightwise properties, also called properties on the slices. For $k \in [0, n]$ we denote $\mathsf{E}_{k,n}$ the set $\{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$ and call it slice of the Boolean hypercube (of dimension n). 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 Boolean functions in n variables is denoted by $\mathcal{B}_n$, and we denote by $\mathcal{B}_n^*$ the set without the null function.*

To denote when a property or a definition is restricted to a slice we 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 denote $\mathsf{supp}_k(f)$ its support restricted to a slice, that is $\mathsf{supp}(f) \cap \mathsf{E}_{k,n}$.

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 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 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 $f(0, \ldots, 0) = 0$ and $f(1, \ldots, 1) = 1$. The set of WPB functions in 2^m variables is denoted $\mathcal{WPB}_m$.*
When n is not a power of 2, other weights $k \notin \{0, n\}$ give slices of odd cardinality, in this case we call $f \in \mathcal{B}_n$ Weightwise Almost Perfectly Balanced (WAPB) if $|\mathsf{supp}_k(f)| = (|\mathsf{E}_{k,n}| \pm (|\mathsf{E}_{k,n}| \mod 2))/2$. The set of WAPB functions in n variables is denoted $\mathcal{WAPB}_n$.

Definition 4 (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 $\mathcal{W}_{f,k}(a)$, and for $a = 0_n$ we denote $\mathcal{W}_{f,k}(a)$ by $\mathcal{W}_{f,k}(0)$.*

Definition 5 (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 $g(x) = a \cdot x + \varepsilon$, $a \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2$ (where $\cdot$ is an inner product in $\mathbb{F}_2^n$, any choice of inner product will give the same value of $\mathsf{NL}(f)$).*

Definition 6 (Non Perfect Balancedness ([12], Definition 11)). *Let $m \in \mathbb{N}^*$, $n = 2^m$, and f an n-variable Boolean function, the non perfect balancedness of f, denoted $\mathsf{NPB}(f)$ is defined as $\mathsf{NPB}(f) = \min_{g \in \mathcal{WPB}_m} \mathsf{d_H}(f, g)$.*

Property 1 (NPB and restricted Walsh transform ([12], Proposition 2))**.** *Let $m \in \mathbb{N}^*$, $n = 2^m$, and $f \in \mathcal{B}_n$, the following holds on its non perfect balancedness:*

$$\mathsf{NPB}(f) = \frac{2 - \mathcal{W}_{f,0}(0) + \mathcal{W}_{f,n}(0)}{2} + \sum_{k=1}^{n-1} \frac{|\mathcal{W}_{f,k}(0)|}{2}.$$

Definition 7 (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 $\mathsf{deg}(f)$ is either $\max\limits_{I \subseteq [1,n]}\{|I| \mid a_I = 1\}$ if f is not null, or $\mathsf{deg}(f) = 0$, otherwise.*

Property 2 ([6], Proposition 4)**.** *If f is a WPB Boolean function of n variables, then the ANF of f contains at least one monomial of degree $n/2$.*

Definition 8 (Algebraic Immunity). *The algebraic immunity of a Boolean function $f \in \mathcal{B}_n$ is*

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

where $\mathsf{deg}(g)$ is the algebraic degree of g. The function g is called an annihilator of f (or $f+1$). Additionally, we denote $\mathsf{AN}(f) = \min_{g \neq 0}\{\mathsf{deg}(g) \mid fg = 0\}$.

Property 3. *If $g \in \mathcal{B}_n^*$ is an annihilator of f and h another function such that $\mathsf{supp}(h) \subseteq \mathsf{supp}(g)$, then $hf = 0$.*

2.2 Families of WPB functions

In this section we recall families of WPB functions exhibited in former works, they will be used as examples or building blocks.

Definition 9 (CMR WAPB construction (adapted from [6], 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 $n \geq 3$:*

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

Re-indexing the variables the subfamily of WPB functions (when n is a power of 2) can be written as

$$f(x_1, x_2, \ldots, x_{2^m}) = \sum_{a=1}^{m} \sum_{i=1}^{2^{m-a}} \prod_{j=0}^{2^{a-1}-1} x_{i+j2^{m-a+1}}.$$

Definition 10 (TL WPB construction (adapted from [33], Construction 1 **)).** *Let $m \in \mathbb{N}^*$ and $n = 2^m \geq 4$ be an integer. A TL WPB Boolean function g on n-variable is such that:*

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

Remark 1. Despite Definition 10 may appear quite different respect the original paper, it is equivalent when applying the constrains from the definitions we consider. Namely, here we consider only the case where n is a power of two. Referring to Construction 1 of [33], this implies that the coefficients $c_1, \ldots, c_{k-1}$ must be zero. Moreover, in [33] $g(0_n) = 0$ and $g(1_n) = 1$ is not required for weightwise perfectly balancedness, differently from Definition 3. This implies that in this context we can only instantiate the construction with $(-1, 0, .., 0, 1)$ as input sequence, *i.e.* as in Definition 10.

Property 4 (TL WPB functions properties [33])**.** *Let $m \in \mathbb{N}^*$ and $n = 2^m$, a n-variable TL function g_n has optimal algebraic immunity $\mathsf{AI}(g_n) = \frac{n}{2}$.*

2.3 Symmetric Functions and Krawtchouk polynomials

The n-variable Boolean symmetric functions are those that are constant on each slice $\mathsf{E}_{k,n}$ for $k \in [0, n]$. This class has been thoroughly studied in the context of cryptography, see *e.g.* [1,2,3,5,20,29,31]. The set of n-variable symmetric functions is denoted $\mathcal{SYM}_n$, and $|\mathcal{SYM}_n| = 2^{n+1}$. In this article we mainly consider two families of symmetric functions, which are both bases of the symmetric functions' vector space:

Definition 11 (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.*

Definition 12 (Slice indicator functions). *Let $k \in [0, n]$, the indicator function of the slice of weight k is defined as: $\forall x \in \mathbb{F}_2^n$, $\varphi_{k,n}(x) = 1$ if and only if $\mathsf{w_H}(x) = k$.*

Property 5 (Properties of elementary symmetric functions)**.** *Let $n \in \mathbb{N}^*$, $d \in [0, n]$:*

- *The function $\sigma_{d,n}$ takes the value $\binom{k}{d} \mod 2$ on the elements of $\mathsf{E}_{k,n}$.*
- *The function $\sigma_{2,n}$ takes the value 1 only on the slices $\mathsf{E}_{k,n}$ such that $k = 2 \mod 4$ or $k = 3 \mod 4$.*
- *For n even the function $\sigma_{n/2,n}$ has algebraic immunity $n/2$ (e.g. [1, Theorem 9]).*

Property 6. *[11, Proposition 4] Let $n \in \mathbb{N}^*$, $k \in [0, n]$ and $f \in \mathcal{B}_n$, the following holds on $f + \varphi_{k,n}$: $\forall a \in \mathbb{F}_2^n, \forall i \in [0, n] \setminus \{k\}, \mathcal{W}_{f+\varphi_{k,n},i}(a) = \mathcal{W}_{f,i}(a)$, and $\mathcal{W}_{f+\varphi_{k,n},k}(a) = -\mathcal{W}_{f,i}(a)$.*

We give two results relatively to Krawtchouk polynomials we will use in the article. We refer to *e.g.* [16] for more details on these polynomials and their properties.

Definition 13 (Krawtchouk polynomials). *The Krawtchouk polynomial of degree k, with $0 \leq k \leq n$ is given by:* $\mathsf{K}_k(\ell, n) = \displaystyle\sum_{j=0}^{k} (-1)^j \binom{\ell}{j}\binom{n-\ell}{k-j}$.

Property 7 (Krawtchouk polynomials relations)**.** *Let $n \in \mathbb{N}^*$ and $k \in [0, n]$, the following relations hold:*

- $\mathsf{K}_k(\ell, n) = \sum_{x \in \mathsf{E}_{k,n}} (-1)^{a \cdot x}$, *where $a \in \mathbb{F}_2^n$ and $\ell = \mathsf{w_H}(a)$,*
- *[9, Proposition 5] For n even, $k \in [0, n]$ $\mathsf{K}_k(n/2, n) = (-1)^{k/2}\binom{n/2}{k/2}$ if k is even, and null otherwise.*

3 General results on the algebraic immunity of WPB functions

In this section we give general results on the algebraic immunity of weightwise perfectly balanced functions, and give constructions in Section 4. First, we discuss the bounds on the algebraic immunity known from former constructions. Then, we focus on lower bounds of the algebraic immunity. In Section 3.1 we show a lower bound on the algebraic immunity of a secondary constructions of WPB functions, that encompasses CMR WPB functions. The lower bound result is also extended to the construction of WAPB functions from [37]. Then, in Section 3.2 we study the minimal algebraic immunity a WPB function can take. Finally, in Section 3.3 we complete this general investigation by experimentally determining the AI of WPB functions chosen at random in a small number of variables.

The algebraic immunity of a WPB function can reach the optimal value (of an n-variable Boolean function, *i.e.* $n/2$). It has been proven by Tang and Liu in [33] where they gave the first construction of WPB functions with optimal algebraic immunity (see Property 4). Since then the constructions presented in [26,27] generalize this construction and also have optimal algebraic immunity. No lower bound have been exhibited so far, only experimental results show that not all WPB functions have optimal algebraic immunity. The algebraic immunity of constructions (following the idea of modifying low degree functions slightly weightwise unbalanced, as pioneered in [25]) in respectively 4, 8 and 16 variables are provided in [14, 34], reaching respectively an AI of 2, 3 and 3. In [11], the algebraic immunity of secondary constructions is provided in 8 and 16 variables. The secondary construction seeded with CMR functions result in functions of AI 3 in 8 variables and between 4 and 6 in 16 variables (the AI of f_8 itself is 3 and the one of f_{16} equals 4). The secondary construction seeded with Boolean functions from [15] give WPB functions with AI 4 and 7 in 8 and 16 variables respectively.

3.1 Lower bound on the algebraic immunity of secondary constructions

The experimental results inventoried above show that not all WPB functions have optimal algebraic immunity, and in particular for the first values of n the AI of CMR function grows logarithmically in n. In the following we show that $\mathsf{AI}(f_{2^m})$ is at least m. To do so we first specify a secondary construction, at the same time a subfamily of the secondary construction presented in [6] and encompassing CMR functions. The secondary constructions of WPB functions from [6] is the following:

Definition 14 (Adapted from [6], Theorem 2). *Let $m \in \mathbb{N}^*$, $n = 2^m$, f, f' and g be n-variable WPB functions and g' an arbitrary n-variable function. We define the $2n$ WPB function h as: $h(x, y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$ where $x, y \in \mathbb{F}_2^n$.*

We focus on the restriction where g' is the null function, and iterate the construction with WPB functions in a different number of variables.

Definition 15. *Let $m \in \mathbb{N}^*$, $n = 2^m$, f and g_0 be two n-variable WPB functions. Let $t \in \mathbb{N}$ and for $i \in [1, t]$ g_i be a 2^{m+i} WPB function. We define the 2^{m+t+1} WPB function $S(f, g_0, \ldots, g_t)$ as:*

$$S(f,g_0,\dots,g_t)(x,y^{(0)},\dots,y^{(t)}) = f(x) + g_0(y^{(0)}) + \prod_{j=1}^{n} y_j^{(0)} + \dots + g_t(y^{(t)}) + \prod_{j=1}^{2^{m+t}} y_j^{(t)},$$

where $x, y^{(0)} \in \mathbb{F}_2^n$, and for $i \in [1,t]$ $y^{(i)} \in \mathbb{F}_2^{2^{m+i}}$.

Note that CMR function, f_{2^m}, is obtained in [6] from this construction, taking $f_2 = x_1$ in 2 variables, $f = f_2 = g_0$ and iterating.

Contrarily to the secondary construction of Definition 14, the one from Definition 15 can be written as a direct sum of functions (that is, a sum of functions acting on different variables). We use this structure to give a lower bound on the algebraic immunity of any function built as $S(f,g_0,\dots,g_t)$, and an upper bound for CMR functions. We first recall a result on the algebraic immunity of direct sums from [21].

Property 8 (Adapted from [21], Lemma 6)**.** *Let $t \in \mathbb{N}^*$, and $f_1,\dots,f_t$ be t Boolean functions, if for $r \in [1,t]$ there exists r different indexes $i_1,\dots,i_r$ of $[1,t]$ such that $\forall j \in [1,r], \mathsf{deg}(f_{i_j}) \geq j$ then $\mathsf{AI}(\mathsf{DS}(f_1,\dots,f_t)) \geq r$, where $\mathsf{DS}(f_1,\dots,f_t)$ denotes the direct sum of f_1 to f_t.*

Proposition 1. *Let $m \in \mathbb{N}^*$, $n = 2^m$, f and g_0 be two n-variable WPB functions. Let $t \in \mathbb{N}$ and for $i \in [1,t]$ g_i be a 2^{m+i}-variable WPB function, then*

$$\mathsf{AI}(S(f,g_0,\dots,g_t)) \geq t+2.$$

Proof. First, we remark that $S(f,g_0,\dots,g_t)$ is the direct sum of $t+2$ functions, f and $g'_i = g_i + \prod_{j=0}^{2^{m+i}} y_j^{(i)}$ for i in $[0,t]$. f has degree at least 1 since it is a WPB function, and for all i in $[0,t]$ the function g'_i has degree 2^{m+i}. The latter comes from the fact that g_i has degree at most $2^{m+i}-1$ since it is WPB and therefore balanced, and then the addition with the degree 2^{m+i} monomial makes g'_i a 2^{m+i}-degree function. Then, for $i \in [0,t]$ we have $\mathsf{deg}(g'_i) = 2^{m+i} \geq 2+i$, it allows to apply Property 8 and to conclude $\mathsf{AI}(S(f,g_0,\dots,g_t)) \geq t+2$. □

We recall a result form [8] on the number of annihilators of f and $f+1$ when f is a direct sum with a linear part.

Property 9 (Adapted from [8], Proposition 9)**.** *Let $f \in \mathcal{B}_n$ be the direct sum of a linear function g in $k > 0$ variables and h in $n-k$ variables then: $\forall d \in [0,n]$, $\quad N_d^0 = N_d^1$, where N_d^ε for $\varepsilon \in \{0,1\}$ denotes the number of (linearly) independent annihilators of $f+\varepsilon$ of degree at most d.*

Proposition 2. *Let $m \in \mathbb{N}^*$, and f_{2^m} be the 2^m-variable CMR function (Definition 9), then $\mathsf{AI}(f_{2^m}) \geq m$, and for $m > 3$, $\mathsf{AI}(f_{2^m}) \leq 2^{m-2}$*

Proof. The bound $\mathsf{AI}(f_{2^m}) \geq m$ is a consequence of Proposition 1. Since $\mathsf{AI}(f_2) = 1$, $\mathsf{AI}(f_4) = 2$, and by construction for $m > 2$ we have $f_{2^{m+1}} = S(f_2,f_2,f_4,\dots,f_{2^m})$ and $\mathsf{AI}(S(f_2,f_2,f_4,\dots,f_{2^m})) \geq m+1$ by Proposition 1, a direct induction gives $\mathsf{AI}(f_{2^m}) \geq m$.

The bound $\mathsf{AI}(f_{2^m}) \leq 2^{m-2}$ comes from the upper bound on the algebraic immunity of a direct sum, the AI of the direct sum cannot be greater than the sum of the two AIs (*e.g.* [4], Section 9.1.4). We show the result by induction. For $m = 4$ since $\mathsf{AI}(f_m) = 4$, $\mathsf{AI}(f_{2^m}) \leq 2^{m-2}$ holds. Then for $m+1 > 4$ we can write $f_{2^{m+1}}$ as $S(f_{2^m}, f_{2^m})$ which is the direct sum of f_{2^m} and $g = f_{2^m} + \prod_{i=1}^{2^m} y_i$. By hypothesis $\mathsf{AI}(f_{2^m}) \leq 2^{m-2}$, and by construction g differs from f_{2^m} only in the value 1_{2^m} therefore an annihilator of f_{2^m} is also an annihilator of g since $f_{2^m}(1_{2^m}) = 1$ (since f is WPB). Since f_{2^m} can be written as the direct sum of the linear function f_2 and a 2^m-2 variable function, from Property 9 for each annihilator of f_{2^m} of degree d there is an annihilator of $1+f_{2^m}$ of the same degree, it guarantees that $\mathsf{AI}(g) \leq \mathsf{AI}(f_{2^m})$. Therefore, $\mathsf{AI}(f_{2^{m+1}}) \leq 2 \cdot \mathsf{AI}(f_{2^m}) \leq 2^{m-1}$. □

With a similar approach we can bound the algebraic immunity of the secondary construction of WAPB functions from Zhu and Su [37].

Definition 16 (Adapted from [37], Theorem 2)**.** *Let $t \in \mathbb{N}^*$ and $n_1,\dots,n_t$ be different powers of 2, and for $i \in [1,t]$, f_i be a WPB function in n_i variables. We call ZS construction the function f in $\sum_{i=1}^t n_i$ variables the direct sum $ZS(f_1,\dots,f_t) = \sum_{i=1}^t f_i$.*

Proposition 3. *Let $t \in \mathbb{N}^*$ and $n_1, \dots, n_t$ be different powers of 2, and for $i \in [1, t]$, f_i be a WPB function in n_i variables. The function $f = ZS(f_1, \dots, f_t)$ is such that:*

$$\mathsf{AI}(f) \geq \begin{cases} t-1 & \text{if } \exists j, k \in [1,t] \text{ such that } n_j = 1 \text{ and } n_k = 2, \\ t & \text{otherwise,} \end{cases}$$

and $\mathsf{AI}(f) \leq \left\lceil \sum_{i=1}^{t} n_i/2 \right\rceil$.

Proof. The upper bound comes from the fact that any n-variable function has its AI upper bounded by $\lceil n/2 \rceil$. Relatively to the lower bound, since an n-variable WPB function has algebraic degree at least $n/2$ (see Property 2), we can apply Property 8 on the f_i. When there are both an f_j in 1 variable and an f_k in 2 variables, we can only guarantee to find a chain of $t-1$ indexes r_1 to r_{t-1} such that $\mathsf{deg}(f_{r_i}) \geq i$ since both f_j and f_k could have degree 1. Since, apart from $n_j = 1$ and $n_k = 2$, the different powers of 2, n_i, ensure that the condition $\mathsf{deg}(f_{r_i}) \geq i$ can be fulfilled, we obtain $\mathsf{AI}(f) \geq t-1$. □

3.2 Minimal algebraic immunity of WPB functions

In the previous parts we showed that there exist WPB functions which algebraic immunity cannot be higher than 2^{m-2} (Proposition 2), and we saw examples close to $\log m$ or less for small values of m. In the following, we demonstrate that for $m \geq 2$ the minimal AI that a WPB function can reach is in fact a constant.

We begin by defining the minimal degree of annihilator (non null) a 2^m-variable WPB function (or its complement) can have, and give an alternative expression of this quantity.

Definition 17 (Minimal degree of annihilator reachable by a 2^m-variable WPB function). *Let $m \in \mathbb{N}^*$ and $\varepsilon \in \{0,1\}$, we denote d_m^ε the quantity:*

$$\mathsf{d}_m^\varepsilon = \min\{\mathsf{AN}(f+\varepsilon) \,|\, f \in \mathcal{WPB}_m\}.$$

Lemma 1. *Let $m \in \mathbb{N}^*$, $n = 2^m$ and $g \in \mathcal{B}_{2^m}^*$ such that $\mathcal{W}_{k,g}(0) \geq 0$ $\forall k \in [1, 2^m - 1]$.*

1. *If $\mathcal{W}_{n,g}(0) \geq 0$, then there exists $f \in \mathcal{WPB}_m$ such that g is an annihilator of f.*
2. *If $\mathcal{W}_{0,g}(0) \geq 0$, then there exists $f \in \mathcal{WPB}_m$ such that g is an annihilator of $1 + f$.*

Proof. Since $\mathcal{W}_{k,g}(0) \geq 0$ there are at least $\binom{n}{k}/2$ elements of Hamming weight k not in the support of g for $k \in [1, n-1]$. Therefore, we can build a function h such that $|\mathsf{supp}_k(h)| = \frac{\binom{n}{k}}{2}$ and $\mathsf{supp}_k(h) \supseteq \mathsf{supp}_k(g)$ for all $k \in [1, n-1]$. We have two cases:

a. Suppose $\mathcal{W}_{n,g}(0) \geq 0$. This implies that $g(1_n) = 0$. Then, we can set $h(1_n) = 0$ and $h(0_n) = 1$, in order to get a function $h \in \mathcal{B}_{2^m}^*$ such that $\mathsf{supp}(1+h) \subseteq \mathsf{supp}(1+g)$ and $(1+h) \in \mathcal{WPB}_m$.

b. Suppose $\mathcal{W}_{0,g}(0) \geq 0$. This implies that $g(0_n) = 0$. Then, that we can set $h(1_n) = 1$ and $h(0_n) = 0$, in order to get $\mathsf{supp}(1+h) \subseteq \mathsf{supp}(1+g)$ and $h \in \mathcal{WPB}_m$.

To conclude it is sufficient to notice that $1+g$ is an annihilator of g. Indeed, Property 3 implies that $g(h+1) = 0$, *i.e.* in both cases g is a non constant annihilator of $1+h$. Therefore, 1. and 2. follow by setting $f = 1+h$ and $f = h$, respectively. □

Proposition 4 (Equivalent characterization of d_m^ε). *Let $m \in \mathbb{N}^*$ and $\varepsilon \in \{0,1\}$. It holds*

$$\mathsf{d}_m^\varepsilon = \min\{\mathsf{deg}(f), f \in \mathcal{B}_{2^m}^* \,|\, \forall k \in [1-\varepsilon, 2^m - \varepsilon], \mathcal{W}_{k,f}(0) \geq 0\}.$$

Proof. We denote $n = 2^m$. First we prove $\mathsf{d}_m^\varepsilon \geq \min\{\mathsf{deg}(f), f \in \mathcal{B}_n^* \,|\, \forall k \in [1-\varepsilon, n-\varepsilon], \mathcal{W}_{k,f}(0) \geq 0\}$. We take $f \in \mathcal{WPB}_m$, and g an annihilator (not null) of f of degree d_m^0. Since f is WPB, f has exactly $|\mathsf{E}_{k,n}|/2$

elements of Hamming weight k (for $k \in [1, n-1]$) in its support and one in $\mathsf{E}_{n,n}$, therefore g takes the value 0 over all these elements. Consequently, $\forall k \in [1, 2^m]$:

$$\mathcal{W}_{k,g}(0) = \sum_{x \in \mathsf{E}_{k,n}} (-1)^{g(x)} = \sum_{\substack{x \in \mathsf{E}_{k,n} \\ g(x)=0}} 1 - \sum_{\substack{x \in \mathsf{E}_{k,n} \\ g(x)=1}} 1 \geq \frac{\binom{n}{k}}{2} - \sum_{\substack{x \in \mathsf{E}_{k,n} \\ g(x)=1}} 1 \geq 0.$$

Similarly, if we consider g an annihilator (not null) of $1+f$ of degree d_m^1. Since f is WPB $|\mathsf{supp}_k(f)| = |\mathsf{supp}_k(f+1)|$ for all $k \in [1, 2^m - 1]$ and $|\mathsf{supp}_0(1+f)| = 1$, we obtain that $\mathcal{W}_{k,g}(0) \geq 0$ for $k \in [0, 2^m - 1]$.

Then, we prove $\mathsf{d}_m^\varepsilon \leq \min\{\mathsf{deg}(f), f \in \mathcal{B}_n^* \,|\, \forall k \in [1-\varepsilon, n-\varepsilon], \mathcal{W}_{k,f}(0) \geq 0\}$. We take g_0, g_1 two 2^m-variable functions of minimum degree such that $\mathcal{W}_{k,g_\varepsilon}(0) \geq 0$ for all $k \in [1-\varepsilon, n-\varepsilon]$. From Lemma 1 we can build two functions f_ε for $\varepsilon \in \{0,1\}$, such that f_ε are WPB, and g_ε is a non null annihilator of $f_\varepsilon + \varepsilon$ by construction. This allows to conclude. □

As a first remark, since the algebraic immunity of a function f is the minimum between $\mathsf{AN}(f)$ and $\mathsf{AN}(f+1)$ (Definition 8), we have that $\min\left\{\mathsf{d}_m^0, \mathsf{d}_m^1\right\}$ is the minimal AI a WPB function can have. Then, since for any function f its complement $1+f$ is an annihilator, for each WPB function it gives an annihilator of the same degree, therefore d_m^ε is upper bounded by the minimal degree of a 2^m-variable WPB function, that is 2^{m-1} for $m \geq 1$ (see Property 2). In the following we show that $\mathsf{d}_1^\varepsilon = 1$, but $\mathsf{d}_m^\varepsilon > 1$ for $m > 1$.

Lemma 2. *Let $m \in \mathbb{N}^*$, $n = 2^m$ and $\varepsilon \in \{0,1\}$, the following holds on d_m^ε:*

$$\mathsf{d}_1^\varepsilon = 1 \qquad \textit{and} \qquad \textit{for } m > 1,\ \mathsf{d}_m^\varepsilon > 1.$$

Proof. We start with the particular case $m = 1$. In this context, denoting x_1 and x_2 the 2 variables, there are only two WPB functions: $f = x_1$ and $g = x_2$. They are respectively annihilated by the degree-1 function $1+x_1$ and $1+x_2$, and not by the constant function equal to 1, which allows to conclude $\mathsf{d}_1^0 = 1$. Furthermore, the two complementary functions of 2-variable WPB are $1+x_1$ and $1+x_2$, similarly annihilated by a degree 1 function and not by the constant function equal to one, so in this case $\mathsf{d}_1^1 = 1$. This implies that 1 is also the minimum on the algebraic immunity.

For $m > 1$, we show that no affine function f can satisfy the characterisation of d_m^ε from Proposition 4. If f is constant, f cannot be the null function by definition of d_m^ε, and the constant function equal to one is such that $\mathcal{W}_{k,f}(0) < 0$ for all $k \in [1, n]$. Then, any non constant affine function is balanced, therefore:

$$W_f(0) = 0 = \sum_{i=0}^{n} \mathcal{W}_{f,k}(0).$$

The condition in the definition of d_m^0 form Proposition 4 for $k = n$ forces $\mathcal{W}_{f,n}(0) = 1$ and therefore the restriction on the other coefficients can be only satisfied if

$$\mathcal{W}_{f,0}(0) = -1, \qquad \text{and} \qquad \forall k \in [1, n-1], \mathcal{W}_{f,k}(0) = 0.$$

This implies that f is balanced on all slices, and more precisely that $f+1$ is a weightwise perfectly balanced function. Similarly, if we consider the condition in the definition of d_m^1 form Proposition 4, we obtain that f should be a weightwise perfectly balanced function. Since a WPB function has degree at least 2^{m-1} by Property 2, both these cases are impossible. □

We show that in fact d_m^0 is constant in m, more precisely that for $m \geq 2$ there are always 2^m-variable WPB functions that are annihilated by quadratic functions.

Proposition 5. *Let $m \in \mathbb{N}$, for all $m \geq 2$, $\mathsf{d}_m^0 = 2$.*

Proof. We denote $n = 2^m$ for readability. We show that there exist degree-2 functions $g \in \mathcal{B}_n$ such that $\forall k \in [1, n]$, $\mathcal{W}_{g,k}(0) \geq 0$ or equivalently $\forall k \in [1, n]$, $|\mathsf{supp}_k(g)| \leq \binom{n}{k}/2$. More precisely we consider the functions with algebraic normal form $x_i x_j + x_i x_k$ where $i, j, k \in [1, n]$ and $i \neq j \neq k$, without lost of generality we take $g = x_1(x_2 + x_3)$. In the following we consider the size of the support of g on each slice.

- If $k \in [0,1]$, g takes only the value 0 hence $|\mathsf{supp}_k(g)| \leq \binom{n}{k}/2$.
- For $k = 2$, $g(x) = 1$ only when $x_1 = x_2 = 1$ or $x_1 = x_3 = 1$, therefore $|\mathsf{supp}_2(g)| = 2 \leq 2^{m-2}(2^m - 1) = \binom{n}{2}/2$.
- For $k \geq 3$, we split $x \in \mathbb{F}_2^n$ as (y, z) where $y \in \mathbb{F}_2^3$ and $z \in \mathbb{F}_2^{n-3}$, and determine the number of elements such that $g(x) = 1$ based on the value of y. The function g takes the value 1 only when $x_1(x_2 + x_3) = 1$ that is when $y = (1,1,0)$ or $y = (1,0,1)$, thereafter for $x \in \mathsf{E}_{k,n}$ it corresponds to 2/3 of the cases where $\mathsf{w_H}(y) = 2$ and none when $\mathsf{w_H}(y) \neq 2$. It allows us to get the cardinal of $\mathsf{supp}_k(g)$:

  $$|\mathsf{supp}_k(g)| = 2\binom{n-3}{k-2}.$$

  Then, we have to compare this value to $\binom{n}{k}/2$:

  $$\begin{aligned}2\binom{n-3}{k-2} \leq \frac{\binom{n}{k}}{2} &\Leftrightarrow \\ 4\binom{n-3}{k-2} &\leq \binom{n-3}{k-3} + 3\binom{n-3}{k-2} + 3\binom{n-3}{k-1} + \binom{n-3}{k}, \\ \Leftrightarrow \binom{n-3}{k-2} &\leq \binom{n-3}{k-3} + 3\binom{n-3}{k-1} + \binom{n-3}{k}.\end{aligned}$$

  Since $n-3$ is odd the binomial coefficient $\binom{n-3}{k-2}$ is lower than or equal to one of the two binomial coefficients $\binom{n-3}{k-1}$ and $\binom{n-3}{k-3}$, Therefore $|\mathsf{supp}_k(g)| \leq \binom{n}{k}/2$ that is $\mathcal{W}_{k,g}(0) \geq 0$.

It allows to conclude $\mathsf{d}_m^0 \leq 2$ from Proposition 4, and since for $m \geq 2$ $\mathsf{d}_m^0 > 1$ from Lemma 2, we obtain $\mathsf{d}_m^0 = 2$. □

Theorem 1. *Let $m \in \mathbb{N}$, for all $m \geq 2$, $\min\{\mathsf{AI}(f) \colon f \in \mathcal{WPB}_m\} = 2$.*

Proof. From Lemma 2 and Proposition 5 we have $\min\{\mathsf{AI}(f) \colon f \in \mathcal{WPB}_m\} = \min\left\{\mathsf{d}_m^0, \mathsf{d}_m^1\right\} = 2$. □

Corollary 1. *If $f \in \mathcal{WPB}_2$, then $\mathsf{AI}(f) = 2$.*

Proof. For every n-variable Boolean function f we have that $\mathsf{AI}(f) \leq \lceil n/2 \rceil$ and $\mathsf{AI}(f) \geq 2$ from Theorem 1. This implies $\mathsf{AI}(f) = 2$ for all $f \in \mathcal{WPB}_2$. □

Additionally, in Section 4.2 we give a construction to build WPB functions with minimal algebraic immunity, and study its properties.

3.3 Algebraic immunity distribution

To conclude this section we perform an experimental investigation on the algebraic immunity distribution for WPB functions in a small number of variables, following the same principle as in [10, 12]. Exhausting $\mathcal{WPB}_2$, we found that all the WPB function in 4 variables have algebraic immunity 2, it is indeed coherent with Corollary 1. For $m = 3$, we extrapolated an approximation of the algebraic immunity distribution from a sample of size larger than 2^{23} . As shown by Table 1, 8-variable WPB functions with non-optimal algebraic immunity are rare. In fact, for 16 variables we were not able to collect a sample sufficiently large to get at least a function with AI lower than 8.

4 Constructions of WPB functions with bounded algebraic immunity

In this section we exploit GM construction [12, Construction 1] in order to produce WPB functions with bounded algebraic immunity and prescribed nonlinearity. First, we focus on constructions with upper bounded

x	3	4
$\tilde{p}_{\mathsf{AI}}(x)\%$	0.004	99.996
#	353	8427167

Table 1. Approximation of the algebraic immunity distribution in $\mathcal{WPB}_3$ via sampling elements of $\mathcal{WPB}_3$ uniformly at random: $\tilde{p}_{\mathsf{AI}}(x) = \{f \in S \colon \mathsf{AI}(f) = x\} / |S|$ where S is a sample of size larger than 2^{23}.

AI in Section 4.1. More specifically, in Section 4.2 we construct WPB functions reaching the lowest algebraic immunity, the lower bound from Theorem 1. We refer to these particular functions with AI 2 as *porcelain* functions, since independently of their aesthetic, we do not advise to use them when implementing a cipher. Then, we prove that the WPB family of functions with almost optimal nonlinearity described in [12] has also minimal algebraic immunity. Finally, in Section 4.4 we show how to build WPB functions with lower bounded AI from GM construction. As an example we give a family of WPB functions with AI at least $2^{m-1} - m + 1$.

4.1 Construction with upper bounded AI

We describe here a method to construct WPB functions with upper bounded algebraic immunity and prescribed nonlinearity. The main idea is to construct a WPB function forcing a suitable function f of degree d to be an annihilator. We observed that we can efficiently built WPB functions as in Lemma 1 by seeding with certain functions the construction proposed by Gini and Méaux in [12] recalled in Construction 1. Indeed, their algorithm produces a WPB function from any Boolean function in 2^m variables by modifying the support of the input function on each slice to make it perfectly balanced, in such a manner that can be compatible with our method.

Construction 1 Construction 1 from [12]

```
Input: Let $m \in \mathbb{N}$, $m \geq 2$, $n = 2^m$ and $g$ a $n$-variable function.
Output: $h \in \mathcal{WPB}_m$.
Initiate the support of $h$ to $\mathsf{supp}(g)$.
If $0_n \in \mathsf{supp}(g)$ remove $0_n$ from $\mathsf{supp}(h)$.
If $1_n \notin \mathsf{supp}(g)$ add $1_n$ to $\mathsf{supp}(h)$.
for $k \leftarrow 1$ to $n-1$ do
    Compute $C_{k,n} = \mathcal{W}_{g,k}(0)/2$,
    if $C_{k,n} < 0$ then
        remove $|C_{k,n}|$ elements from $\mathsf{supp}_k(h)$,
    else
        if $C_{k,n} > 0$ then
            add $C_{k,n}$ new elements to $\mathsf{supp}_k(h)$,
        end if
    end if
end for
return $h$
```

We first summarize some useful properties of Construction 1 extending Theorem 2 of [12]:

Proposition 6. *Let $m \in \mathbb{N}$, $m \geq 2$ and $n = 2^m$. Any function h given by Construction 1 with input g is weightwise perfectly balanced. For $k \in [1, n-1]$:*

- *If $g \in \mathcal{B}_n^*$ is such that $\mathcal{W}_{k,g}(0) \leq 0$. Then $\mathsf{supp}_k(h) \subseteq \mathsf{supp}_k(g)$.*
- *If $g \in \mathcal{B}_n^*$ is such that $\mathcal{W}_{k,g}(0) \geq 0$. Then $\mathsf{supp}_k(h) \supseteq \mathsf{supp}_k(g)$.*

Additionally, $\mathsf{NL}(h) \geq \mathsf{NPB}(g) - \mathsf{NL}(g)$.

Proof. The first part (g is WPB) comes from Theorem 2 of [12]. Then, if for $k \in [1, n-1]$ $\mathcal{W}_{k,g}(0) \leq 0$, we get $C_{k,n} \leq 0$ in Construction 1. Hence, from step 7 we have that $\mathsf{supp}_k(h) \subseteq \mathsf{supp}_k(g)$. While, if $\mathcal{W}_{k,g}(0) \geq 0$, we get $C_{k,n} \geq 0$. Hence, from step 10 we have that $\mathsf{supp}_k(h) \supseteq \mathsf{supp}_k(g)$. Finally, for the nonlinearity, if a is an affine function, $\mathsf{NL}(g) \leq \mathsf{d_H}(g, a) \leq \mathsf{d_H}(g, h) + \mathsf{d_H}(h, a)$. This implies that $\mathsf{NL}(h) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$, since $\mathsf{d_H}(g, h) = \mathsf{NPB}(g)$ from Theorem 2 of [12]. □

Thus, combining Proposition 6 with arguments similar to Lemma 1 we obtain that seeding Construction 1 with suitable functions we can obtain WPB functions with upper bounded algebraic immunity.

Theorem 2. *Let $m \in \mathbb{N}$, $m \geq 2$ and $n = 2^m$. Let function $g \in \mathcal{B}_n^*$ such that $\mathcal{W}_{k,g}(0) \geq 0$ for all $k \in [1, n]$. Any function f given by Construction 1 seeded with $g + 1$ has the following properties:*

1. *$f \in \mathcal{WPB}_m$,*
2. *$\mathsf{AI}(f) \leq \mathsf{deg}(g)$,*
3. *$\mathsf{NL}(f) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$.*

Proof. From Proposition 6 we have that $f \in \mathcal{WPB}_m$, $\mathsf{NL}(f) \geq \mathsf{NL}(g+1) - \mathsf{NPB}(g+1) = \mathsf{NL}(f) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$ and $\mathsf{supp}_k(f) \subseteq \mathsf{supp}_k(1+g)$ for all $k \in [1, n-1]$. Moreover, since $\mathcal{W}_{n,g}(0) \geq 0$, $(1+g)(1_n) = 1$. This implies that $\mathsf{supp}(f) \subseteq \mathsf{supp}(1+g)$. Since $(1+g)$ is an annihilator of g, from Property 3 we obtain that $gf = 0$. Namely, g is a non constant annihilator of f. Therefore, $\mathsf{AI}(f) \leq \mathsf{deg}(g)$. □

Theorem 3. *Let $m \in \mathbb{N}$, $m \geq 2$ and $n = 2^m$. Let function $g \in \mathcal{B}_n^*$ such that $\mathcal{W}_{k,g}(0) \geq 0$ for all $k \in [0, n-1]$. Any function f given by Construction 1 seeded with g has the following properties:*

1. *$f \in \mathcal{WPB}_m$,*
2. *$\mathsf{AI}(f) \leq \mathsf{deg}(g)$,*
3. *$\mathsf{NL}(f) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$.*

Proof. From Proposition 6 we have that $f \in \mathcal{WPB}_m$, $\mathsf{NL}(f) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$ and $\mathsf{supp}_k(f) \supseteq \mathsf{supp}_k(g)$ for all $k \in [1, n-1]$. Moreover, since $\mathcal{W}_{n,g}(0) \geq 0$, $g(0_n) = 0$. This implies that $\mathsf{supp}(1+f) \subseteq \mathsf{supp}(1+g)$. Since $(1+g)$ is an annihilator of g, from Property 3 we obtain that $g(1+f) = 0$. Namely, g is a non constant annihilator of $1+f$. Therefore, $\mathsf{AI}(f) \leq \mathsf{deg}(g)$. □

4.2 Porcelain WPB functions

Using the characterization of d_m^0 in Section 3.2 we proved that for any $m \geq 2$ there exist WPB functions having algebraic immunity 2. Via Construction 1 we can explicitly construct many of them. We consider as primary material, for producing porcelain WPB functions, any *kaolin* function $\kappa_n = x_i(x_j + x_\ell)$ where i, j, ℓ are distinct. In fact, in the proof of Proposition 5 we showed that functions of this kind satisfy the hypotheses of Theorem 2. Thus, we have that any function h given by Construction 1 seeded by κ_n has the following properties: h is a WPB function and $\mathsf{AI}(h) \leq 2$, hence $\mathsf{AI}(h) = 2$. Moreover, we remark that kaolin functions are very peculiar, as their nonlinearity and their non perfect balancedness coincide:

Proposition 7. *Let $m \in \mathbb{N}$, $m \geq 2$ and $n = 2^m$, let $\kappa_n \in \mathcal{B}_n$ denote a function of the form $x_i(x_j + x_\ell)$ such that $i \neq j \neq \ell$. The following holds:*

$$\mathsf{NPB}(\kappa_n) = 2^{n-2}, \quad \textit{and} \quad \mathsf{NL}(\kappa_n) = 2^{n-2}.$$

Proof. We begin with the non perfect balancedness, using Property 1 we get:

$$\mathsf{NPB}(\kappa_n) = \frac{2 - \mathcal{W}_{\kappa_n,0}(0) + \mathcal{W}_{\kappa_n,n}(0)}{2} + \sum_{k=1}^{n-1} \frac{|\mathcal{W}_{\kappa_n,k}(0)|}{2}.$$

Following the proof of Proposition 5 we get:

- $\mathcal{W}_{\kappa_n,0}(0) = 1$ and $\mathcal{W}_{\kappa_n,1}(0) = n$ since $|\mathsf{supp}_k(\kappa_n)| = 0$ for $k \in [0,1]$,
- $\mathcal{W}_{\kappa_n,2}(0) = \binom{n}{2} - 4$ since $|\mathsf{supp}_2(\kappa_n)| = 2$ for $k \in [0,1]$,
- $\mathcal{W}_{\kappa_n,k}(0) = \binom{n}{k} - 4\binom{n-3}{k-2}$ for $k \in [3,n]$ since $|\mathsf{supp}_k(\kappa_n)| = 2\binom{n-3}{k-2}$.

Hence we obtain:

$$\begin{aligned}\mathsf{NPB}(\kappa_n) &= \frac{2-1+1}{2} + \frac{1}{2}\left(n + \binom{n}{2} - 4 + \sum_{k=3}^{n-1}\binom{n}{k} - 4\binom{n-3}{k-2}\right),\\ &= \frac{1}{2}\left(\sum_{k=0}^{n}\binom{n}{k} - 4\binom{n-3}{k-2}\right) = 2^{n-1} - 2\sum_{k=0}^{n}\binom{n-3}{k-2},\\ &= 2^{n-1} - 2^{n-2} = 2^{n-2}.\end{aligned}$$

Then, we determine the nonlinearity of κ_n. First we give the nonlinearity of κ_3. Since the function κ_3 has degree 2 it is not affine hence $\mathsf{NL}(\kappa_3) > 0$, its degree is not maximal hence the nonlinearity cannot be odd, and since κ_3 has weight 2 we can conclude $\mathsf{NL}(\kappa_3) = 2$. Then, in n variables κ_n can be written as the direct sum of κ_3 and the null function in $n-3$ variables, using the formula of the nonlinearity of direct sums (*e.g.* [4], Section 7.1.9.I.B), $\mathsf{NL}(\kappa_n) = \mathsf{NL}(\kappa_3)\cdot 2^{n-3} + \mathsf{NL}(0)\cdot 2^3 - 2\cdot\mathsf{NL}(0)\cdot\mathsf{NL}(\kappa_3) = 2\cdot 2^{n-3} + 0\cdot 2^3 - 2\cdot 0\cdot 2 = 2^{n-2}$. □

We compute now the number of porcelain WPB functions that can be generated by one kaolin function κ_n. Equation (9) from [12] gives the number of WPB functions that can be produced by Construction 1 for a fixed seed g:

$$\mathfrak{F}_n(g) = \prod_{k=1}^{n-1}\binom{\frac{1}{2}\binom{n}{k} + |C_{k,n}|}{|C_{k,n}|}, \tag{1}$$

where $C_{k,n} = \mathcal{W}_{g,k}(0_n)/2$. Notice that, although Corollary 1 of [12] is for a specific input, the proof of the value of $\mathfrak{F}_n$ holds in general. From the proof of Proposition 7 the following holds: $C_{k,n} = \mathcal{W}_{\kappa_n,k}(0_n)/2$. Namely,

$$\mathfrak{F}_n(\kappa_n) = \binom{n}{\frac{n}{2}}\binom{\binom{n}{2} - 2}{\frac{1}{2}\binom{n}{2} - 2}\prod_{k=3}^{n-1}\binom{\binom{n}{k} - 2\binom{n-3}{k-2}}{\frac{1}{2}\binom{n}{k} - 2\binom{n-3}{k-2}}$$

For instance, $\mathfrak{F}_8(\kappa_8) > 2^{152}$ and $\mathfrak{F}_{16}(\kappa_{16}) > 2^{44521}$.

4.3 WPB functions from [12]

The authors of [12] apply their construction to produce a family of WPB functions with high nonlinearity. The used seed function is $g_n = \sigma_{2,n} + \ell_{n/2}$, where $\ell_{n/2} = \sum_{i=1}^{n/2} x_i$. We now prove that this function satisfies the hypotheses of Theorem 3, which implies that all WPB functions from Construction 1 seeded with g_n have algebraic immunity 2 since the function g_n has degree 2.

Proposition 8. *Let $m \in \mathbb{N}$, $m \geq 2$ and $n = 2^m$. $\forall k \in [0, n-1]$, $\mathcal{W}_{k,g_n}(0) \geq 0$.*

Proof. First, we determine the values of $\mathcal{W}_{g_n,k}(0)$. Since $\ell_{n/2}$ is a linear function of $n/2$ terms using Property 7 Item 1 we have:

$$\mathcal{W}_{\ell_{n/2},k}(0) = \sum_{x \in \mathsf{E}_{k,n}} (-1)^{x\cdot(1_{n/2},0_{n/2})} = \mathsf{K}_k(n/2, n).$$

Then, using Property 7 Item 2 we obtain:

- For $k = 0 \mod 4$, $\mathcal{W}_{\ell_{n/2},k}(0) = \binom{n/2}{k/2} \geq 0$;
- for $k = 1 \mod 4$ and $k = 3 \mod 4$, $\mathcal{W}_{\ell_{n/2},k}(0) = 0$,
- for $k = 2 \mod 4$, $\mathcal{W}_{\ell_{n/2},k}(0) = -\binom{n/2}{k/2} \leq 0$.

Then, we can determine the sign of $\mathcal{W}_{g_n,k}(0)$ using Property 6, since $g_n = \ell_{n/2} + \sigma_{2,n}$ we get $\mathcal{W}_{g_n,k}(0) = \mathcal{W}_{\ell_{n/2},k}(0)$ when $\sigma_{2,n}$ takes the value 0 on $\mathsf{E}_{k,n}$ and $\mathcal{W}_{g_n,k}(0) = -\mathcal{W}_{\ell_{n/2},k}(0)$ when $\sigma_{2,n}$ takes the value 1 on $\mathsf{E}_{k,n}$. Using Property 5 Item 2, the sign changes only when $k = 2 \mod 4$ or $k = 3 \mod 4$. Therefore we obtain:

- For $k = 0 \mod 4$, $\mathcal{W}_{g_n,k}(0) = \mathcal{W}_{\ell_{n/2},k}(0) = \binom{n/2}{k/2} \geq 0$,
- for $k = 1 \mod 4$, $\mathcal{W}_{g_n,k}(0) = \mathcal{W}_{\ell_{n/2},k}(0) = 0$,
- for $k = 2 \mod 4$, $\mathcal{W}_{g_n,k}(0) = -\mathcal{W}_{\ell_{n/2},k}(0) = \binom{n/2}{k/2} \geq 0$,
- for $k = 3 \mod 4$, $\mathcal{W}_{g_n,k}(0) = -\mathcal{W}_{\ell_{n/2},k}(0) = 0$.

It allows us to conclude $\forall k \in [0, n-1]$, $\mathcal{W}_{k,g_n}(0) \geq 0$. □

4.4 Functions with lower bounded AI

We show how Construction 1 can be used to build WPB functions with lower bounded algebraic immunity. First we recall a result from Mesnager and Tang:

Property 10 (Adapted from [28], Proposition 12)**.** *Let $k, d \in \mathbb{N}$, let $f \in \mathcal{B}_n$ such that $\mathsf{AI}(f) = k$, and $h \in \mathcal{B}_n$ such that $\mathsf{w_H}(h) < \min(2^{n-k}, 2^{d+1} - 1)$, then $|\mathsf{AI}(f + h) - \mathsf{AI}(f)| \leq d$.*

This result shows that modifying few elements of the support has a limited impact on the algebraic immunity of the function. It allows to derive the following bound regarding Construction 1.

Theorem 4. *Let $m \in \mathbb{N}^*$, $m \geq 2$ and $n = 2^m$. Let $f \in \mathcal{B}_n$ such that $\mathsf{NPB}(f) < 2^{n/2}$. Any (WPB) function g given by Construction 1 seeded with f has the following property: $\mathsf{AI}(g) \geq \mathsf{AI}(f) - \lfloor \log(\mathsf{NPB}(f) + 1) \rfloor$.*

Proof. By construction g can be written as $f + h$ where $\mathsf{w_H}(h) = \mathsf{NPB}(f)$. Since $\mathsf{w_H}(h) < 2^{n/2}$ we have $\mathsf{w_H}(h) < 2^{n - \mathsf{AI}(f)} \leq 2^{n/2}$, and taking $d = \lfloor \log(\mathsf{NPB}(f) + 1) \rfloor$ we get $\mathsf{NPB}(f) < 2^{d+1} - 1$. Therefore, we can apply Property 10, $\mathsf{AI}(g) \geq \mathsf{AI}(f) - \lfloor \log(\mathsf{NPB}(f) + 1) \rfloor$. □

Accordingly to the theorem, seeding Construction 1 with functions with high algebraic immunity and low non perfect balancedness allows to get WPB functions with relatively high AI. In the next proposition, we show how low degree functions (hence functions with low AI) with low non perfect balancedness can also be used to produce WPB functions with lower bounded AI.

Proposition 9. *Let $m \in \mathbb{N}^*$, $m \geq 2$ and $n = 2^m$. Let $f \in \mathcal{B}_n$ such that $\mathsf{NPB}(f) < 2^{n/2}$ and $\mathsf{deg}(f) < n/2$. Any (WPB) function g given by Construction 1 seeded with $f + \sigma_{n/2,n}$ has the following property:*

$$\mathsf{AI}(g) \geq \frac{n}{2} - \mathsf{deg}(f) - \lfloor \log(\mathsf{NPB}(f) + 1) \rfloor.$$

Proof. Since the non perfect balancedness is not changed by the addition of a symmetric function null in 0 and 1_n (see Property 6), $\mathsf{NPB}(f + \sigma_{n/2,n}) = \mathsf{NPB}(f) < 2^{n/2}$. It allows to use Theorem 4, giving $\mathsf{AI}(g) \geq \mathsf{AI}(f + \sigma_{n/2,n}) - \lfloor \log(\mathsf{NPB}(f) + 1) \rfloor$.

Then, we bound the algebraic immunity of $f + \sigma_{n/2,n}$. Since $\mathsf{AI}(\sigma_{n/2,n}) = n/2$ (Property 5 Item 3) and since the algebraic immunity decreases by at most d when adding a degree-d function (*e.g.* [4], Proposition 139), we obtain $\mathsf{AI}(f + \sigma_{n/2,n}) \geq \frac{n}{2} - \mathsf{deg}(f)$. □

In particular, using Proposition 9 with low degree function with (known) low NPB allows to build WPB functions with relatively high AI. We illustrate it with the examples of truncated CMR functions, which weightwise support has been recently studied in [36].

Property 11 (Adapted from [36], Theorem 1)**.** *Let $m \in \mathbb{N}^*$, $m \geq 2$ and $n = 2^m$. Let $d \in \mathbb{N}^*$, $d < m$, and let $f_{d,m} \in \mathcal{B}_n$ the function which ANF contains only the terms of degree at most 2^{d-1} of the CMR function f_n (Definition 9), the following holds for $0 \leq k \leq n$:*

$$|\mathsf{supp}_k(f_{d,m})| = \begin{cases} \frac{1}{2}\binom{n}{k} & \text{if } k \not\equiv 0 \mod 2^d, \\ \frac{1}{2}\binom{n}{k} - \frac{(-1)^{k/2^d}}{2}\binom{2^{m-d}}{k/2^d} & \text{if } k \equiv 0 \mod 2^d. \end{cases}$$

Proposition 10. *Let $m \in \mathbb{N}^*$, $m \geq 2$ and $n = 2^m$. Let $d \in \mathbb{N}^*$, $d < m$, and let $f_{d,m} \in \mathcal{B}_n$ the function which ANF contains only the terms of degree at most 2^{d-1} of the CMR function f_n (Definition 9), any (WPB) function g given by Construction 1 seeded with $f_{d,m} + \sigma_{n/2,n}$ has the following property:*

$$\mathsf{AI}(g) \geq \frac{n}{2} - 2^{d-1} - m + d + 1.$$

Proof. First, we compute the NPB of $f_{d,m}$. Using Property 1, we get:

$$\mathsf{NPB}(f_{d,m}) = \frac{2 - \mathcal{W}_{f_{d,m},0}(0) + \mathcal{W}_{f_{d,m},n}(0)}{2} + \sum_{k=1}^{n-1} \frac{|\mathcal{W}_{f_{d,m},k}(0)|}{2}.$$

Using Property 11 since $\mathcal{W}_{f,k}(0) = |\mathsf{E}_{k,n}| - 2|\mathsf{supp}_k(f)|$ it gives:

$$\mathsf{NPB}(f_{d,m}) = \frac{2-1+1}{2} + \frac{1}{2}\sum_{t=1}^{2^{m-d}-1} \binom{2^{m-d}}{t} = 1 + 2^{m-d-1} - 1 = 2^{m-d-1}.$$

Then, since $2^{m-d-1} < 2^{n/2}$, we can apply Proposition 9, which gives

$$\mathsf{AI}(g) \geq \frac{n}{2} - \mathsf{deg}(f_{d,m}) - \lfloor \log(\mathsf{NPB}(f_{d,m}) + 1) \rfloor = 2^{m-1} - 2^{d-1} - m + d + 1.$$

□

In particular for $d = 1$ (in this case $f_{1,m}$ corresponds to $\ell_{n/2}$), it gives WPB functions with algebraic immunity at least $2^{m-1} - m + 1$.

5 Conclusion and open questions

In this article we performed the first study on the algebraic immunity of WPB function, the values it can take, and presented constructions reaching a low, or high value. In Section 3 we focused on the maximal and minimal values the AI can take inside this family, and the general distribution of this parameter. We showed a lower bound on the AI of two secondary constructions, and then proved the existence of WPB functions of AI only 2 for all m greater than 2. The experimental study that we performed in 8 and 16 variables showed that such functions are rare, whereas most WPB functions have optimal AI.

On the constructive side, in Section 4 we showed how GM Construction (Construction 1) can be used to generate WPB functions with bounded AI. In a first time we proved how to build WPB functions with lower bounded AI, one main example being the porcelain functions, an entire family with AI 2. We also demonstrated that the WPB functions with very high nonlinearity exhibited in [12] have in fact minimal AI. In a second time we used the construction to generate functions with upper bounded AI, together with an example of family with AI at least $2^{m-1} - m + 1$.

Different open questions arose from this study. First, since the GM construction allows to derive WPB functions with proven very high nonlinearity ([12]), but minimal AI or proven high AI when used with different seeds, it would be interesting to determine if the results can be combined to find seeds generating WPB functions with both proven high nonlinearity and AI. Then, we notice that in both cases the seeds used rely on a symmetric function with optimal nonlinearity in the first case and algebraic immunity in the second case. This leads to question if investigating the properties of WPB functions up to addition of symmetric functions could lead to WPB functions with good parameters for all the cryptographic criteria. Finally, the experimental tests and former results on WPB families show that WPB functions have high AI in general. It would be interesting to see if this property propagates to the criterion of weightwise algebraic immunity, AI_k, measuring the resistance to algebraic attacks when the Hamming weight is fixed.

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

References

AL18. Benny Applebaum and Shachar Lovett. Algebraic attacks against random local functions and their countermeasures. *SIAM J. Comput.*, pages 52–79, 2018.

BCG$^+$20. Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Correlated pseudorandom functions from variable-density lpn. In *61st FOCS*. IEEE Computer Society Press, 2020.

BIP$^+$18. Dan Boneh, Yuval Ishai, Alain Passelègue, Amit Sahai, and David J. Wu. Exploring crypto dark matter: - new simple PRF candidates and their applications. In *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*, pages 699–729, 2018.

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.

Car. Claude Carlet. On the degree, nonlinearity, algebraic thickness, and nonnormality of boolean functions, with developments on symmetric functions. *IEEE.*

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

CDM$^+$18. Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi, and Yann Rotella. On the concrete security of goldreich's pseudorandom generator. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part II*, volume 11273 of *Lecture Notes in Computer Science*, pages 96–124. Springer, 2018.

CHMS22. Orel Cosseron, Clément Hoffmann, Pierrick Méaux, and François-Xavier Standaert. Towards case-optimized hybrid homomorphic encryption - featuring the Elisabeth stream cipher. In *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III*, volume 13793 of *Lecture Notes in Computer Science*, pages 32–67. Springer, 2022.

CM03. Nicolas Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*. Springer, Heidelberg, May 2003.

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 Transactions on Information Theory*, pages 2791–2811, 2005.

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.

GJLS21. Romain Gay, Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from simple-to-state hard problems: New assumptions, new techniques, and simplification. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part III*, volume 12698 of *Lecture Notes in Computer Science*, pages 97–126. Springer, 2021.

GM22a. Agnese Gini and Pierrick Méaux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discrete Applied Mathematics*, 322:320–341, 2022.

GM22b. Agnese Gini and Pierrick Méaux. Weightwise almost perfectly balanced functions: Secondary constructions for all n and better weightwise nonlinearities. In Takanori Isobe and Santanu Sarkar, editors, *Progress in Cryptology - INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 492–514. Springer, 2022.

GM23. Agnese Gini and Pierrick Méaux. Weightwise perfectly balanced functions and nonlinearity. In Said El Hajji, Sihem Mesnager, and El Mamoun Souidi, editors, *Codes, Cryptology and Information Security*, pages 338–359, Cham, 2023. Springer Nature Switzerland.

Gol01. Oded Goldreich. *Foundations of Cryptography: Basic Tools*, volume 1. Cambridge University Press, Cambridge, UK, 2001.

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

LM19. Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *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.

MCJS19. Pierrick Méaux, Claude Carlet, Anthony Journault, and François-Xavier Standaert. Improved filter permutators for efficient FHE: better instances and implementations. In Feng Hao, Sushmita Ruj, and Sourav Sen Gupta, editors, *Progress in Cryptology - INDOCRYPT*, volume 11898 of *LNCS*, pages 68–91. Springer, 2019.

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

Méa22. Pierrick Méaux. On the algebraic immunity of direct sum constructions. *Discrete Applied Mathematics*, 320:223–234, 2022.

Mes16. Sihem Mesnager. *Bent functions*, volume 1. Springer, 2016.

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.

MKCL22. Sara Mandujano, Juan Carlos Ku Cauich, and Adriana Lara. Studying special operators fortheapplication ofevolutionary algorithms intheseek ofoptimal boolean functions forcryptography. In Obdulia Pichardo Lagunas, Juan Martínez-Miranda, and Bella Martínez Seis, editors, *Advances in Computational Intelligence*, pages 383–396, Cham, 2022. Springer Nature Switzerland.

MOP07. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks - revealing the secrets of smart cards.* Springer, 2007.

MPC04. Willi Meier, Enes Pasalic, and Claude Carlet. Algebraic attacks and decomposition of boolean functions. In Christian Cachin and Jan L. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, pages 474–491, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

MPJ$^+$22. Luca Mariot, Stjepan Picek, Domagoj Jakobovic, Marko Djurasevic, and Alberto Leporati. Evolutionary construction of perfectly balanced boolean functions. In *2022 IEEE Congress on Evolutionary Computation (CEC)*, page 18. IEEE Press, 2022.

MS78. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-holland Publishing Company, 2nd edition, 1978.

MS21. Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced boolean functions. *Cryptography and Communications*, 13:951–979, 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.

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

MT21. Sihem Mesnager and Chunming Tang. Fast algebraic immunity of boolean functions and LCD codes. *IEEE Transactions on Information Theory*, 67(7):4828–4837, 2021.

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.

Rot76. O.S Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, 1976.

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

Sta10. François-Xavier Standaert. Introduction to side-channel attacks. In Ingrid M. R. Verbauwhede, editor, *Secure Integrated Circuits and Systems*, Integrated Circuits and Systems, pages 27–42. Springer, 2010.

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.

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

ZLC$^+$23. Qinglan Zhao, Mengran Li, Zhixiong Chen, Baodong Qin, and Dong Zheng. A unified construction of weightwise perfectly balanced boolean functions. *Discrete Applied Mathematics*, 337:190–201, 2023.

ZS22. Linya Zhu and Sihong Su. A systematic method of constructing weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. *Discrete Applied Mathematics*, 314:181–190, 2022.

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