# On the cryptographic properties of weightwise affine and weightwise quadratic functions.

Pierrick Méaux[0000−0001−5733−4341], Yassine Ozaim

University of Luxembourg, Luxembourg
pierrick.meaux@uni.lu, yassine.ozaim@gmail.com

**Abstract.** Weightwise degree-d functions are Boolean functions that take the values of a function of degree at most d on each set of fixed Hamming weight. The class of weightwise affine functions encompasses both the symmetric functions and the Hidden Weight Bit Function (HWBF). The good cryptographic properties of the HWBF, except for the nonlinearity, motivates to investigate a larger class with functions that share the good properties and have a better nonlinearity. Additionally, the homomorphic friendliness of symmetric functions exhibited in the context of hybrid homomorphic encryption and the recent results on homomorphic evaluation of Boolean functions make this class of functions appealing for efficient privacy-preserving protocols.
In this article we realize the first study on weightwise degree-d functions, focusing on weightwise affine and weightwise quadratic functions. We show some properties on these new classes of functions, in particular on the subclass of cyclic weightwise functions. We provide balanced constructions and prove nonlinearity lower bounds for all cyclic weightwise affine functions and for a family of weightwise quadratic functions. We complement our work with experimental results, they show that other cyclic weightwise linear functions than the HWBF have better cryptographic parameters, and considering weightwise quadratic functions allows to reach higher algebraic immunity and substantially better nonlinearity.

**Keywords:** Boolean functions, cryptography, symmetric functions, HWBF

## 1 Introduction.

Weightwise affine functions have been introduced in [GM22], they are Boolean functions that are affine on each subset of $\mathbb{F}_2^n$ with vectors with fixed Hamming weight, also called slices $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \mid \mathsf{w_H}(x) = k\}$. More generally, we call *weightwise degree-$d$ functions* the Boolean functions that take the same values as a function of degree at most $d$ on each slice (potentially a different function on each slice). Weightwise degree-$0$ and weightwise degree-$1$ functions have been studied in various research domains such as cryptography, with a different formalism. The weightwise degree-$0$ functions, constant on all slices, are the intensively studied symmetric functions *e.g.* [Car04, CV05, BP05, SM07, CL11, CM19, Méa19, Méa21, CM22].

One weightwise degree-$1$ function have received a lot of attention since its introduction by Bryant in [Bry91], the Hidden Weight Bit Function (HWBF). This function takes the value $x_k$ on each slice $\mathsf{E}_{k,n}$ for $k \in [1, n]$ (and $0$ in $0_n$), it has been considered as the simplest example of function with binary decision diagram of exponential size [Bry91, BLSW99]. Since both computing the Hamming weight and applying an affine function are cheap in different models of computation, the HWBF can be implemented efficiently and has been considered in different contexts. For example, the cryptographic properties of HWBF have been investigated in [WCST14], showing good algebraic properties for this function, but a nonlinearity insufficient to use it alone as filter in a stream cipher design. Since then, various generalizations of the HWBF have been proposed to conserve the good cryptographic properties and improve the nonlinearity, such as in [WTS14] and recently in [Car22].

Generalizing symmetric functions and the HWBF to weightwise degree-$d$ functions for small values of $d$ allows to obtain a bigger class of functions that are still efficiently computable and with potentially better cryptographic parameters. In particular, in the context of hybrid homomorphic encryption [NLV11],

private key ciphers such as LowMC [ARS+15], Kreyvium [CCF+16], FLIP [MJSC16], Rasta [DEG+18] and FiLIP [MCJS19] have been designed to be homomorphic friendly, that is, with components that can be efficiently evaluated homomorphically. Moreover, the homomorphic evaluation of symmetric functions can be made very efficient as demonstrated in [HMR20, CDPP22, MPP23]. The efficient evaluation of multiplexers for homomorphic schemes like FHEW [DM15] and TFHE [CGGI16] allows to evaluate the Hamming weight of an input as shown in [HMR20] and therefore enable to efficiently evaluate weightwise low degree functions. The homomorphic evaluation of Boolean functions is a growing research topic, leading to better and better performances as shown recently by [BCBS23, BSS+23, TCBS23, BOS23, BPR23].

In this article we realize the first study on the cryptographic properties of weightwise affine and weightwise degree-2 functions:

- In Section 3 we give general properties on the class of weightwise degree-$d$ functions and provide balanced constructions.
- We focus on the subfamily of cyclic weightwise functions in Section 4, defining them and showing some particular characteristics.
- In Section 5 we prove lower bounds on the nonlinearity of all weightwise affine functions, and on a family of weightwise quadratic function. The techniques we use allow to find differently the result on the nonlinearity of the HWBF and to derive bounds on some generalizations.
- We perform experiments on weightwise affine and quadratic functions up to 16 variables and summarize the results in Section 6. These experiments show that other weightwise linear functions and mostly weightwise quadratic functions allow to obtain better cryptographic parameters than the HWBF, in particular relatively to the nonlinearity.

## 2 Preliminaries.

We denote $[n]$ the subset of all integers between 1 and $n$: $\{1, \ldots, n\}$. For readability we use the notation $+$ instead of $\oplus$ for the addition in $\mathbb{F}_2$. For a vector $v \in \mathbb{F}_2^n$ we denote $\mathsf{w_H}(v)$ its Hamming weight $\mathsf{w_H}(v) = |\{i \in [n] \,|\, v_i = 1\}|$. For two vectors $v$ and $w$ of $\mathbb{F}_2^n$ we denote $\mathsf{d_H}(v, w)$ the Hamming distance between $v$ and $w$, $\mathsf{d_H}(v, w) = \mathsf{w_H}(v + w)$.

### 2.1 Generalities on Boolean functions

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

**Definition 2 (Equivalences Notions (adapted from [Car21], Definition 5)).** *Two $n$-variable Boolean functions $f$ and $a_0 + f \circ L + g$ where:*

$$L : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n) \times \mathbf{M} + (a_1, \ldots, a_n), \text{ are called:}$$

- *extended affine equivalent if $a_0 \in \mathbb{F}_2$, $L$ is an affine automorphism of $\mathbb{F}_2^n$, $\mathbf{M}$ being an $n \times n$ nonsingular matrix over $\mathbb{F}_2$, $(a_1, \ldots, a_n) \in \mathbb{F}_2^n$, and $g$ is an affine $n$-variable Boolean function.*
- *linear equivalent if $a_0 = 0$ and $L$ is a linear automorphism of $\mathbb{F}_2^n$, $\mathbf{M}$ being an $n \times n$ nonsingular matrix over $\mathbb{F}_2$, $(a_1, \ldots, a_n) = 0_n$, $g$ is null.*
- *permutation equivalent if they are linear equivalent with $\mathbf{M}$ having exactly one $1$ by row and by column.*

**Definition 3 (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 $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$):*

$$f(x) = \sum_{I \subseteq [n]} a_I \left( \prod_{i \in I} x_i \right) = \sum_{I \subseteq [n]} a_I x^I,$$

*where $a_I \in \mathbb{F}_2$.*

- *The algebraic degree of $f$ is: $\mathsf{deg}(f) = \max_{\{I \mid a_I = 1\}} |I|$ (with the convention that $\mathsf{deg}(0) = 0$).*
- *Any term $\prod_{i \in I} x_i$ in such an ANF is called a monomial and its degree equals $|I|$.*

### 2.2 Cryptographic criteria of Boolean functions

For more details on the criteria of Boolean function used in cryptography we refer to [Car21].

**Definition 4 (Balancedness).** *A Boolean function $f \in \mathcal{B}_n$ is said to be balanced if and only if $|\mathsf{supp}(f)| = |\mathsf{supp}(f + 1)| = 2^{n-1}$, where the support of $f$ denotes the set $\{x \in \mathbb{F}_2^n, \text{ such that } f(x) = 1\}$.*

**Definition 5 (Resilience).** *A Boolean function $f \in \mathcal{B}_n$ is called $m$-resilient if any of its restrictions obtained by fixing at most $m$ of its coordinates is balanced. We denote by $\mathsf{res}(f)$ the maximum resilience (also called resilience order) of $f$ and set $\mathsf{res}(f) = -1$ if $f$ is unbalanced.*

**Definition 6 (Nonlinearity).** *The nonlinearity $\mathsf{NL}(f)$ of a Boolean function $f \in \mathcal{B}_n$, where $n$ is a positive integer, is the minimum Hamming distance between $f$ and all the affine functions in $\mathcal{B}_n$:*

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

*with $d_H(f, g) = \#\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}$ the Hamming distance between $f$ and $g$, and $g(x) = a \cdot x + \varepsilon$; $a \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2$ (where $\cdot$ is an inner product in $\mathbb{F}_2^n$).*

**Definition 7 (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:*

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

**Property 1** (Nonlinearity, resilience and Walsh transform, *e.g.* [Car21])**.** *Let $n \in \mathbb{N}^*$, for every $n$-variable Boolean function $f$:*

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

*A function $f$ is balanced if and only if $W_f(0_n) = 0$.*

**Definition 8 (Algebraic Immunity, [MPC04]).** *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 $f + 1$).*

### 2.3 Slices and symmetric functions

**Definition 9 (Slices of the Boolean hypercube).** *For $k \in [0, n]$ we call slice of the Boolean hypercube (of dimension $n$) the set $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \mid \mathsf{w_H}(x) = k\}$.*

Following Definition 9 the Boolean hypercube is partitioned into $n + 1$ slices where the elements have the same Hamming weight. For properties holding on the slices we use the adjective *weightwise*.

**Definition 10 (Restricted Walsh transform, [CMR17]).** *Let $f \in \mathcal{B}_n$ be a Boolean function and $S \subset \mathbb{F}_2^n$, 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 $\mathcal{W}_{f,k}(a)$.*

The $n$-variable Boolean symmetric functions are the functions that are constant on each slice.

**Definition 11 (Symmetric Functions).** *Let $n \in \mathbb{N}^*$, the Boolean symmetric functions are the functions which are constant on each $\mathsf{E}_{k,n}$ for $k \in [0, n]$. The set of $n$ variable symmetric functions is denoted $\mathcal{SYM}_n$ and $|\mathcal{SYM}_n| = 2^{n+1}$. We distinguish families of symmetric functions:*

- *Elementary symmetric functions. Let $i \in [0, n]$, the elementary symmetric function of degree $i$ in $n$ variables, denoted $\sigma_{i,n}$, is the function which ANF contains all monomials of degree $i$ and no monomials of other degrees.*
- *Threshold Functions. Let $d \in [0, n]$, the threshold function of threshold $d$ is defined as:*

$$\forall x \in \mathbb{F}_2^n, \quad \mathsf{T}_{d,n}(x) = \begin{cases} 0 & \text{if } \mathsf{w_H}(x) < d, \\ 1 & \text{otherwise.} \end{cases}$$

- *Slice indicator functions. Let $k \in [0, n]$, the indicator function of the slice of weight $k$ is defined as:*

$$\forall x \in \mathbb{F}_2^n, \quad \varphi_{k,n}(x) = \begin{cases} 1 & \text{if } \mathsf{w_H}(x) = k, \\ 0 & \text{otherwise.} \end{cases}$$

The $n + 1$ $n$-variable symmetric functions of each family form a basis of $\mathcal{SYM}_n$ (that is every element of $\mathcal{SYM}_n$ can be written as a linear combination of these $n + 1$ functions).

**Definition 12 (Weightwise degree-$d$ functions).** *Let $n \in \mathbb{N}^*$ and for $k \in [0, n]$ $\varphi_{k,n}$ denotes the indicator function of $\mathsf{E}_{k,n}$. An $n$-variable Boolean function $f$, written as $f = \sum_{k=0}^{n} f_k \varphi_{k,n}$, is called weightwise degree-$d$ if and only if for each $k \in [0, n]$ $f_k$ coincide with a function of degree at most $d$ over $\mathsf{E}_{k,n}$.*

*The set of weightwise degree-$d$ functions is denoted by $\mathcal{WD}_n^d$.*

In [GM22] the authors study the relationship between weightwise perfectly balanced functions (functions balanced on all the slices, see for example [CMR17, LM19, TL19, MSL21, MKCL22, ZLC+23, YCL+23, GM23]) and weightwise affine functions *i.e.* weightwise degree-1 functions. In fact weightwise degree-1 and degree-0 functions have been studied for their cryptographic properties in many works, without the same formalism. The weightwise constant functions ($\mathcal{WD}_n^0$) are the symmetric functions that have been extensively studied (*e.g.* [Car04, CV05, BP05, SM07, CL11, CM19, Méa19, Méa21, CM22]). Thereafter, the hidden weight bit function introduced in [Bry91] is a weightwise degree-1 function, the one obtained by fixing $f_0 = 0$ and $f_k = x_k$ for $k \in [n]$. The cryptographic properties of this function have been studied in [WCST14], showing good algebraic properties for this function. In [CMR17], the bent functions in Propositions 1 and 2 are weightwise affine.

### 2.4 Spherically Punctured Reed-Muller Codes

Reed Muller codes $\mathsf{RM}(r,n)$ are binary codes of length $2^n$ whose codewords are the evaluations of all Boolean functions of algebraic degree at most $r$ in $n$ variables on their $2^n$ entries. Fixing the Hamming weight to the entries to $k$ gives the spherically punctured Reed-Muller codes studied by Kapralova and Dumer [DK13, DK17]. The properties of these codes are connected to Boolean functions with fixed weight entries.

**Definition 13 (Spherically punctured Reed Muller codes of order-$d$).** *For all $n \in \mathbb{N}^*$, $k, d \in [0,n]$, we denote by $\mathsf{P}_{k,n,d}$ the punctured order-$d$ Reed Muller code of length $\binom{n}{k}$ obtained by puncturing all entries of Hamming weight different from $k$.*

**Property 2** (Dimension of $\mathsf{P}_{n,k,d}$, [DK13] Corollary 3)**.** *Let $n \in \mathbb{N}^*$, $k, d \in [0,n]$, the dimension of $\mathsf{P}_{n,k,d}$ is:*

$$\begin{cases} \binom{n}{d} & \text{if } k \in [d, n-d], \\ \binom{n}{k} & \text{otherwise.} \end{cases}$$

### 2.5 Krawtchouk polynomials

We recall the definition of Krawtchouk polynomials and some of their properties. They naturally appear when we study the restriction of the Walsh transform on a slice for an affine function. We refer to *e.g.* [MS78] for more details on these polynomials and their properties.

**Definition 14 (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 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 $\ell = \mathsf{w_H}(a)$,*
- $\mathsf{K}_k(n-\ell, n) = (-1)^k \mathsf{K}_k(\ell, n)$,
- *[DMS06] (adapted from Lemma 5), $\forall k \in [0,n] \setminus \{\frac{n}{2}\}$ and $\ell \in [1, n-1] \setminus \{\frac{n}{2}\}$, $|\mathsf{K}_k(1,n)| \geq |\mathsf{K}_k(\ell,n)|$.*
- *[DMS06] (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.*
- $\binom{n}{\ell}\mathsf{K}_k(\ell, n) = \binom{n}{k}\mathsf{K}_\ell(k, n)$.

## 3 Generalities on weightwise degree-$d$ functions

In this part we focus on the general properties of the set of weightwise degree-$d$ functions, introduced in Definition 12. First, we determine the cardinal of these functions and introduce the notion of weightwise degree. Then, we provide constructions of balanced weightwise degree-$d$ functions, by exhibiting sufficient conditions on the $f_k$ components of the weightwise degree-$d$ function $f$.

### 3.1 Cardinality and weightwise degree

**Proposition 1 (Number of weightwise degree-$d$ functions).** *Let $n \in \mathbb{N}^*$ and $d \in \mathbb{N}$ such that $0 \leq d \leq n$, the $\mathbb{F}_2$-vector space of Boolean functions from the set $\mathcal{WD}_n^d$ has dimension $D$ where:*

$$D = \sum_{k \in [0,d] \cup [n-d,n]} \binom{n}{k} + \sum_{k=d+1}^{n-d-1} \binom{n}{d}, \quad \textit{and} \quad |\mathcal{WD}_n^d| = 2^D.$$

*Proof.* First, note that if $f \in \mathcal{B}_n$ and $g \in \mathcal{B}_n$ are both in the set $\mathcal{WD}_n^d$ then there exist functions of degree at most $d$ $f_i$ and $g_i$ for all $i \in [0, n]$ such that $f = \sum_{i=0}^n f_i \varphi_{i,n}$ and $g = \sum_{i=0}^n g_i \varphi_{i,n}$. Thereafter, any $\mathbb{F}_2$-linear combination of $f$ and $g$ can be written as $a \cdot f + b \cdot g = \sum_{i=0}^n (a \cdot f_i + b \cdot g_i)\varphi_{i,n}$, and for all $i$ the function $a \cdot f_i + b \cdot g_i$ has degree at most $d$, therefore $a \cdot f + b \cdot g \in \mathcal{WD}_n^d$.

Then, we determine the dimension of the vector space, using Property 2. The $n$-variable Boolean functions of degree up to $d$ are in bijection with the Reed Muller code $\mathsf{RM}(d, n)$ (each function being identified uniquely by its truth table). For $i \in [0, n]$ the truth table of $f_i \varphi_{i,n}$ is equal to 0 on all slices different from $i$, therefore the dimension of $< \varphi_{i,n} f_i, f_i \in \mathcal{B}_n \,|\, 0 \leq \mathsf{deg}(f_i) \leq d >$ is the dimension of the code $\mathsf{P}_{n,i,d}$. Since for all $i \neq j$ we have $\mathsf{supp}(\varphi_{j,n}) \cap \mathsf{supp}(\varphi_{i,n}) = \emptyset$ we get:

$$\dim(\mathcal{WD}_n^d) = \sum_{i=0}^{n} \dim(\mathsf{P}_{n,i,d}) = \sum_{k=0}^{d} \binom{n}{k} + \sum_{k=d+1}^{n-d-1} \binom{n}{d} + \sum_{k=n-d}^{n} \binom{n}{k},$$

where the last equality comes from Property 2.

□

From this result we can derive the dimension of $\mathcal{SYM}_n$, weightwise affine and weightwise quadratic functions, the main focuses of this work.

**Corollary 1.** *Let $n \in \mathbb{N}^*$, for the first values of $d$ the set $\mathcal{WD}_n^d$ (as $\mathbb{F}_2$-vector space) has the following dimension:*

$$\dim(\mathcal{WD}_n^0) = n + 1, \quad \dim(\mathcal{WD}_n^1) = n^2 - n + 2, \quad \textit{and } \dim(\mathcal{WD}_n^2) = \frac{n^3 - 4n^2 + 7n + 4}{2}.$$

A natural question coming with the representation of a Boolean function as a weightwise degree-$d$ function is to determine the minimal $d$ such that the function belongs to $\mathcal{WD}_n^d$. We formalize this notion as weightwise degree and show that such $d$ is bounded by $\lfloor n/2 \rfloor$.

**Definition 15 (Weightwise degree).** *Let $n \in \mathbb{N}^*$, we call weightwise degree of the function $f$ the smallest integer $d$ such that $f \in \mathcal{WD}_n^d$, and we denote it by* $\mathsf{wdeg}(f)$.

**Proposition 2.** *Let $n \in \mathbb{N}^*$, for all $f \in \mathcal{B}_n$, there exists $d \in [0, \lfloor n/2 \rfloor]$ such that $f \in \mathcal{WD}_n^d$.*

*Proof.* Using Proposition 1 we have $|\mathcal{WD}_n^d| = 2^D$ where

$$D = \sum_{k \in [0,d] \cup [n-d,n]} \binom{n}{k} + \sum_{k=d+1}^{n-d-1} \binom{n}{d}.$$

Since for $d = \lfloor n/2 \rfloor$ for all $n \in \mathbb{N}$ it holds $[d+1, n-d+1] = \emptyset$, the formula gives $D = \sum_{k=0}^{n} \binom{n}{k} = 2^n$. Hence, on one hand, $|\mathcal{WD}_n^{\lfloor n/2 \rfloor}| = 2^D = 2^{2^n} = |\mathcal{B}_n|$, and on the other hand $\mathcal{WD}_{\lfloor n/2 \rfloor}^n \subset \mathcal{B}_n$ so $\mathcal{WD}_n^{\lfloor n/2 \rfloor} = \mathcal{B}_n$. By Definition 12, since a weightwise degree $d$ function is also a weightwise degree-$t$ function for $t \geq d$ we have $\mathcal{WD}_n^0 \subset \mathcal{WD}_n^1 \subset \ldots \subset \mathcal{WD}_n^{\lfloor n/2 \rfloor - 1} \subset \mathcal{WD}_n^{\lfloor n/2 \rfloor}$. It allows to conclude: for all $f \in \mathcal{B}_n$, there exists $d \in [0, \lfloor n/2 \rfloor]$ such that $f \in \mathcal{WD}_n^d$.

□

### 3.2 Conditions for balancedness

We exhibit two sufficient conditions on the $f_i$ functions to have the associated function $f$ balanced.

**Proposition 3.** *Let $n \in \mathbb{N}^*$, and $f_i \in \mathcal{B}_n$ for all $i$ such that $0 \leq i < n/2$. The weightwise degree-$d$ function $f = \sum_{i=0}^{n} f_i \varphi_{i,n}$ obtained by taking:*

- *$f_{n-i}(x) = 1 + f_i(1_n + x)$ for $i \in [0, (n-1)/2]$, if $n$ is odd,*
- *$f_{n-i}(x) = 1 + f_i(1_n + x)$ for $i \in [0, n/2 - 1]$, and $f_{n/2}$ a function balanced on $\mathsf{E}_{n/2,n}$ if $n$ is even,*

*is balanced.*

*Proof.* Let n be an odd number, $f = \sum_{i=0}^{n} f_i \varphi_{i,n}$. We know that $W_f(0_n) = \sum_{i \in [0,n]} \sum_{x \in \mathsf{E}_{i,n}} (-1)^{f_i(x)}$. So, for $i \in [0, (n-1)/2]$, we have:

$$\sum_{x \in \mathsf{E}_{n-i,n}} (-1)^{f_{n-i}(x)} = \sum_{x \in \mathsf{E}_{n-i,n}} (-1)^{1+f_i(1_n+x)} = \sum_{x \in \mathsf{E}_{i,n}} (-1)^{1+f_i(x)}.$$

Hence,

$$\sum_{x \in \mathsf{E}_{i,n}} (-1)^{f_i(x)} + \sum_{x \in \mathsf{E}_{n-i,n}} (-1)^{f_{n-i}(x)} = \sum_{x \in \mathsf{E}_{i,n}} (-1)^{f_i(x)} + (-1)^{1+f_i(x)} = 0.$$

Since it holds for all $i \in [0, (n-1)/2]$, we obtain $W_f(0_n) = 0$, hence $f$ is balanced by Property 1.

For $n$ even, we can argue the same way for all $i \in [0, n/2 - 1]$, and the sum $\sum_{i \in \mathsf{E}_{n/2,n}} (-1)^{f_i(x)}$ is equal to 0 by hypothesis. It allows to conclude, $f$ is balanced. □

**Proposition 4.** *Let $n \in \mathbb{N}^*$, Let $P_i$ for $i \in [0, n]$ $n+1$ permutations from $\mathbb{S}_n$. The function $g \in \mathcal{B}_n$ is balanced if and only if the weightwise degree-$d$ function $f$ defined by $f_i = g(P_i(x))$ is balanced.*

*Proof.* Let us define the function $f$ as $f = \sum_{i=0}^{n} f_i \varphi_{i,n}$ with $f_i(x) = g(P_i(x))$, where g is a given function and $P_i$ is such that:

$$\begin{aligned} P_i : \mathsf{E}_{i,n} &\to \mathsf{E}_{i,n} \\ x &\mapsto P_i(x) = (x_{\pi_i(1)}, x_{\pi_i(2)}, \cdots, x_{\pi_i(n)}), \end{aligned}$$

where $\pi_i \in \mathbb{S}_n$ for $i \in [0, n]$. Our goal is to demonstrate the equivalence between $f$ being balanced and $g$ being balanced, respectively. On the one hand $x$ and $P_i(x)$ have the same Hamming weight, for every

$x \in \mathbb{F}_2^n$ and $P_i$. Then, we have:

$$\begin{aligned} W_f(0_n) &= \sum_{x \in \mathsf{E}_{0,n}} (-1)^{f_0(x)} + \cdots + \sum_{x \in \mathsf{E}_{n,n}} (-1)^{f_n(x)} \\ &= \sum_{x \in \mathsf{E}_{0,n}} (-1)^{g(P_0(x))} + \cdots + \sum_{x \in \mathsf{E}_{n,n}} (-1)^{g(P_n(x))} \end{aligned}$$

On the other hand we have that $P_i$ is a bijection over $\mathsf{E}_{i,n}$ for all $i \in [0, n]$ since $\pi_i \in \mathbb{S}_n$. So, $\sum_{x \in \mathsf{E}_{i,n}} (-1)^{g(P_i(x))} = \sum_{x \in \mathsf{E}_{i,n}} (-1)^{g(x)}$, and therefore $W_f(0_n) = \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x)} = W_g(0_n)$.

□

## 4 Subfamily of interest: cyclic weightwise functions

We focus our study on a particular family of weightwise degree-$d$ functions, defined by $f_1 = g$ and then the other $f_i$ are defined as $g$ applied on a cyclic shift of $x$.

### 4.1 Definition

**Definition 16 (Cyclic weightwise degree-$d$ function).**
*Let $n \in \mathbb{N}^*$, and $g \in \mathcal{B}_n$, we call cyclic weightwise degree-$d$ function associated to $g$ the weightwise degree-$\mathsf{deg}(g)$ function defined by:*

- $f_1 = g$,
- *for $i \in [0, n] \setminus \{1\}$, $f_i(x) = g(\mathsf{O}^{i-1}(x))$, where $\mathsf{O}^i$ denotes the cyclic shift by $i$ positions: $\mathsf{O}^i(x_1, \ldots, x_n) = (x_{1+i \mod n}, \ldots, x_{n+i \mod n})$, the representative modulo being taken as the integer between 1 and $n$.*

*We denote by $\mathcal{CWD}_n^d$ the set of cyclic weightwise degree-$d$ function.*

*Example 1.* For $n = 4$ and $g(x_1, x_2, x_3, x_4) = x_1 + x_2x_3$ the associated cyclic weightwise quadratic function is:

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= \sum_{i=0}^{4} g(\mathsf{O}^{i-1}(x))\varphi_{i,4}(x), \\ &= (x_1 + x_2x_3)\varphi_{1,4}(x) + (x_2 + x_3x_4)\varphi_{2,4}(x) + (x_3 + x_1x_4)\varphi_{3,4}(x) + (x_4 + x_1x_2)\varphi_{4,4}(x), \\ &= x_1 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4. \end{aligned}$$

The interests of Cyclic Weightwise (CW) functions are their easiness of implementation among the weightwise degree-$d$ functions (cyclic shifts for each $f_i$), and that we expect this subfamily to be general enough to contain functions with good cryptographic parameters. For example, note that the HWBF is a CW function, the one defined by $g(x) = x_1$.

### 4.2 Properties

In the following we first remark some direct properties of $\mathcal{CWD}_n^d$, then we show the equivalence of functions from $\mathcal{CWD}_n^1$. The latter allows us to restrict our experimental study in Section 6.

**Property 4.** *Let $n \in \mathbb{N}^*$, the following holds:*

- $\forall i \in [0, n], \mathcal{CWD}_n^d \subset \mathcal{WD}_n^d$,
- $|\mathcal{CWD}_n^d| \leq 2^D$ *where* $D = \sum_{i=0}^{d} \binom{n}{i}$.

In this part we focus on functions in $\mathcal{CWD}_n^1$, more particularly on the cyclic weightwise linear functions; the ones such that $g$ is linear. In this case, $g(x) = a \cdot x$ and the $2^n$ linear functions can be represented by the $2^n$ elements of $\mathbb{F}_2^n$ (seen as length-$n$ vectors). For $a \in \mathbb{F}_2^n$ we denote by $f_a$ the function in $\mathcal{CWD}_n^1$ defined by $g(x) = a \cdot x$. First, we show that if $a$ and $b$ are such that $\mathsf{O}^i(b) = a$ for an $i$ in $[0, n]$ (that is, if they are in the same orbit) then $f_a$ and $f_b$ are permutation equivalent functions (see Definition 2). Then, we show that if $a$ and $b$ are such that $a + b = 1_n$ then $f_a$ and $f_b$ are extended affine equivalent. Since permutation equivalent functions have the same cryptographic parameters, and extended affine equivalent functions have the same nonlinearity (and degree and algebraic immunity differing by at most one), we can restrict our study (Section 6) to one representative of each orbit where the elements have Hamming weight at most $n/2$.

**Proposition 5.** *Let $n \in \mathbb{N}^*$ and $a, b \in \mathbb{F}_2^n$, if there exists $i \in [0, n]$ such that $\mathsf{O}^i(b) = a$ then $f_a$ and $f_b$ are permutation equivalent functions.*

*Proof.* We denote $j$ the integer such that $\mathsf{O}^j(b) = a$. Then:

$$f_a = \sum_{i=0}^{n} \varphi_{i,n}\, a \cdot \mathsf{O}^{i-1}(x) = \sum_{i=0}^{n} \varphi_{i,n}\, \mathsf{O}^j(b) \cdot \mathsf{O}^{i-1}(x) = \sum_{i=0}^{n} \varphi_{i,n}\, b \cdot \mathsf{O}^{n-j+i-1}(x).$$

We define the permutation of indices: $\forall i \in [1, n], x_i \mapsto x_{j+i \mod n}$, and the associated matrix $\mathbf{M}$. Therefore:

$$f_a(x \times \mathbf{M}) = \sum_{i=0}^{n} \varphi_{i,n}(x \times \mathbf{M}) b \cdot \mathsf{O}^{n-j+i-1}(x \times \mathbf{M}) = \sum_{i=0}^{n} \varphi_{i,n}(x) b \cdot \mathsf{O}^{i-1}(x) = f_b(x),$$

which proves that $f_a$ and $f_b$ are permutation equivalent (see Definition 2).

□

**Proposition 6.** *Let $n \in \mathbb{N}^*$ and $a, b \in \mathbb{F}_2^n$, if $a + b = 1_n$ then $f_a$ and $f_b$ are extended affine equivalent functions.*

*Proof.* We rewrite $f_a$:

$$\begin{aligned}
f_a(x) &= \sum_{i=0}^{n} \varphi_{i,n}(x)\, a \cdot \mathsf{O}^{i-1}(x) = \sum_{i=0}^{n} \varphi_{i,n}(x) \left( b \cdot \mathsf{O}^{i-1}(x) + 1_n \cdot \mathsf{O}^{i-1}(x) \right), \\
&= \sum_{i=0}^{n} \varphi_{i,n}(x)\, b \cdot \mathsf{O}^{i-1}(x) + \sum_{i=0}^{n} \varphi_{i,n}(x)\, 1_n \cdot \mathsf{O}^{i-1}(x), \\
&= \sum_{i=0}^{n} \varphi_{i,n}(x) b \cdot \mathsf{O}^{i-1}(x) + (\mathsf{wH}(x) \mod 2), \\
&= f_b(x) + \sigma_{1,n}(x).
\end{aligned}$$

Accordingly, $f_b$ and $f_a$ are extended affine equivalent (see Definition 2) since $\sigma_{1,n}(x) = \sum_{i=1}^{n} x_i = \mathsf{w_H}(x) \mod 2$ is linear. □

## 5 On the nonlinearity of weightwise cyclic functions.

In this part we show lower bounds on the nonlinearity of some cyclic weightwise functions. First, we derive a bound on the nonlinearity of any cyclic affine weightwise function, it generalizes the result of [WCST14] giving the nonlinearity of the HWBF function. Then, we give a lower bound on the weightwise quadratic function given by $g(x) = x_1 + x_2x_3$. We obtain both bounds by studying the Walsh transform restricted to the slices, and using properties of Krawtchouk polynomials.

### 5.1 Lower bound on the nonlinearity of CW linear functions

**Lemma 1.** *Let $n \in \mathbb{N}^*$, $b \in \mathbb{F}_2^n \setminus \{0_n\}$ and $f$ be the CW linear function associated to $g = b \cdot x$, the following holds on its Walsh transform:*

$$W_f(a) = \sum_{k=0}^{n} \mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b) + a), n).$$

*Proof.* We prove the expression of $W_f(a)$ in terms of Krawtchouk polynomials:

$$\begin{aligned} W_f(a) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x} = \sum_{k=0}^{n} \sum_{x \in \mathsf{E}_{k,n}} (-1)^{f(x)+a\cdot x} \\ &= \sum_{k=0}^{n} \sum_{x \in \mathsf{E}_{k,n}} (-1)^{g(\mathsf{O}^{k-1}(x))+a\cdot x} = \sum_{k=0}^{n} \sum_{x \in \mathsf{E}_{k,n}} (-1)^{(\mathsf{O}^{1-k}(b)+a)\cdot x} \\ &= \sum_{k=0}^{n} \mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b) + a), n), \end{aligned}$$

where the equality comes from Property 3 Item 1.

□

**Lemma 2.** *Let $n \in \mathbb{N}^*$, $b \in \mathbb{F}_2^n \setminus \{0_n\}$ and $f$ be the CW linear function associated to $g = b \cdot x$. We denote $B_{a,b}$ the bound on $|W_f(a)|$ given by $B_{a,b} = \sum_{k=0}^{n} |\mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b) + a), n)|$. Then:*

$$B_{a,b} \leq \sum_{k \in [0,n] \setminus \{\frac{n}{2}\}} |\mathsf{K}_k(1, n)| + |\mathsf{K}_{\frac{n}{2}}(\mathsf{w_H}(\mathsf{O}^{1-k}(b)+a), n)| + \sum_{\substack{k \in [0,n] \setminus \{\frac{n}{2}\} \\ \mathsf{w_H}(\mathsf{O}^{1-k}(b)+a) \in \{0, \frac{n}{2}, n\}}} |\mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b)+a), n)|.$$

*Proof.* We give the upper bound on $|W_f(a)|$ using Lemma 1:

$$|W_f(a)| = |\sum_{k=0}^{n} \mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b) + a), n)| \leq \sum_{k=0}^{n} |\mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b) + a), n)| = B_{a,b}.$$

From Property 3 Item 3 we can bound $B_{a,b}$ since $|\mathsf{K}_k(1, n)|$ is higher than the other absolute values in most cases:

$$B_{a,b} \leq \sum_{k \in [0,n] \setminus \{\frac{n}{2}\}} |\mathsf{K}_k(1, n)| + |\mathsf{K}_{\frac{n}{2}}(\mathsf{w_H}(\mathsf{O}^{1-n/2}(b)+a), n)| + \sum_{\substack{k \in [0,n] \setminus \{\frac{n}{2}\} \\ \mathsf{w_H}(\mathsf{O}^{1-k}(b)+a) \in \{0, \frac{n}{2}, n\}}} |\mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b)+a), n)|.$$

□

**Lemma 3.** *Let $n \in \mathbb{N}^*$, $b \in \mathbb{F}_2^n \setminus \{0_n\}$ and $f$ be the CW linear function associated to $g = b \cdot x$. For all $a \in \mathbb{F}_2^n, B_{a,b} = B_{a+1_n,b}$*

*Proof.* First, we write the Walsh transform of $W_f(a + 1_n)$ using Lemma 1:

$$\begin{aligned} W_f(a+1_n) &= \sum_{k=0}^{n} \mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b)+a+1_n), n) \\ &= \sum_{k=0}^{n} \mathsf{K}_k(n - \mathsf{w_H}(\mathsf{O}^{1-k}(b)+a), n) \\ &= \sum_{k=0}^{n} (-1)^k \mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b)+a), n), \end{aligned}$$

where the last equality comes from Property 3 Item 2.

Since $B_{a,b} = \sum_{k=0}^{n} |\mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b)+a), n)|$, we obtain $B_{a,b} = B_{a+1_n,b}$ □

From Lemma 3 we can use the same bound of $B_{a,b}$ for $a$ and $a + 1_n$, therefore we restrict our study to the vectors $a$ of Hamming weight at most $n/2$.

**Lemma 4.** *Let $n \in \mathbb{N}^*$, $b \in \mathbb{F}_2^n \setminus \{0_n\}$ and $f$ be the CW linear function associated to $g = b \cdot x$, the following holds on its Walsh transform:*

$$B_{a,b} \leq 2\binom{n-1}{\lceil \frac{n}{2} \rceil - 1} + C_{a,b}, \quad \textit{where}$$

$$C_{a,b} = |\mathsf{K}_{\frac{n}{2}}(\mathsf{w_H}(\mathsf{O}^{1-n/2}(b)+a), n)| + \sum_{\substack{k \in [0,n] \setminus \{\frac{n}{2}\} \\ \mathsf{w_H}(\mathsf{O}^{1-k}(b)+a) \in \{0, \frac{n}{2}, n\}}} |\mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b)+a), n)|.$$

*Proof.* Using Lemma 2 we have: $B_{a,b} \leq C_{a,b} + \sum_{k \in [0,n] \setminus \{\frac{n}{2}\}} |\mathsf{K}_k(1, n)|$. Then, we bound the sum:

$$\begin{aligned} \sum_{k \in [0,n] \setminus \{\frac{n}{2}\}} |\mathsf{K}_k(1,n)| &= \sum_{k < \frac{n}{2}} \binom{n-1}{k} - \binom{n-1}{k-1} + \sum_{k > \frac{n}{2}} \binom{n-1}{k-1} - \binom{n-1}{k} \\ &= 2 \sum_{k < \frac{n}{2}} \binom{n-1}{k} - \binom{n-1}{k-1} = 2\binom{n-1}{\lceil \frac{n}{2} \rceil - 1}, \end{aligned}$$

where the first equality comes from the definition of Krawtchouk polynomials (Definition 14). It allows to conclude.

□

Note that we want to bound the term $C_{a,b}$, which mostly comes from the part where $\mathsf{w_H}(\mathsf{O}^{1-i}(b)+a)$ belongs to the set $\{0, \frac{n}{2}, n\}$. To bound these contributions to the sum we can consider two approaches, first we can bound the number of cases where such Hamming weight is possible, then we can bound the sum of that number of contributions, since for all $\ell$ the maximum absolute value of $\mathsf{K}_k(\ell, n)$ is bounded by the binomial coefficient $\binom{n}{k}$. We introduce two quantities to study these bounds. First, we denote $\mathsf{ord}(b) = \min_{i \in [1,n]} \{i \mid \mathsf{O}^i(b) = b\}$ the order of an element $b \in \mathbb{F}_2^n$. The other quantity is the maximal value a sum of $i$ different binomial coefficients can take, we denote it by $M(i, n)$.

**Definition 17 (Sum of different binomial coefficients).** *Let $n \in \mathbb{N}^*$ and $i \in \mathbb{N}$ such that $i \leq n$, we define $M(i,n)$ as:*

$$M(i,n) = \max\Big\{ \sum_{j=1}^{i} \binom{n}{k_j}, \quad \textit{where } 1 \leq k_1 < \cdots < k_i \leq n \Big\}.$$

Due to the properties of the binomial coefficients, the following property holds on $M(i,n)$

**Property 5.** *Let $n \in \mathbb{N}^*$ and $i \in \mathbb{N}$ such that $i \leq n$, the value of $M(i,n)$ is given by:*

$$M(i,n) = \begin{cases} 0 & \textit{if } i = 0, \\ \binom{n}{\frac{n}{2}} + 2\sum_{j=1}^{(i-1)/2} \binom{n}{\frac{n}{2}-j} & \textit{if } n \textit{ is even, and } i-1 \textit{ is even}, \\ \binom{n}{\frac{n}{2}} + \binom{n}{\frac{n}{2}-\lceil \frac{i-1}{2} \rceil} + 2\sum_{j=1}^{\lfloor (i-1)/2 \rfloor} \binom{n}{\frac{n}{2}-j} & \textit{if } n \textit{ is even, and } i-1 \textit{ is odd}, \\ 2\sum_{j=1}^{i/2} \binom{n}{\lceil \frac{n}{2} \rceil - j} & \textit{if } n \textit{ is odd, and } i \textit{ is even}, \\ \binom{n}{\lceil \frac{n}{2} \rceil - \lceil i/2 \rceil} + 2\sum_{j=1}^{\lfloor i/2 \rfloor} \binom{n}{\lceil \frac{n}{2} \rceil - j} & \textit{if } n \textit{ is odd, and } i \textit{ is odd}. \end{cases}.$$

With these notations we can give the main theorem.

**Theorem 1 (Nonlinearity bound of weightwise cyclic linear functions).** *Let $n \in \mathbb{N}$, $n \geq 2$, $b \in \mathbb{F}_2^n$ such that $\mathsf{w_H}(b) \in [1, n/2]$ and $f$ be the CW linear function associated to $g = b \cdot x$, the following holds on its Walsh transform:*

$$\mathsf{NL}(f) \geq \begin{cases} 2^{n-1} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - \frac{1}{2}\left( \max\left\{ M\left(\frac{n}{\mathsf{ord}(b)} - 1, n\right) + 2, M\left(\frac{n}{\mathsf{ord}(b)}, n\right) \right\} \right) & \textit{if } n \textit{ is odd}, \\ 2\left( \sum_{i=0}^{(n-3)/2} \binom{n-1}{i} \right) - \frac{1}{2}\binom{n}{(n-1)/2} & \textit{if } n \textit{ is odd, and } \mathsf{ord}(b) = n, \\ 2^{n-1} - \frac{1}{2}\binom{n}{n/2} - 2^{n/2-1} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - \frac{1}{2}\left( \max\left\{ M\left(\frac{n}{\mathsf{ord}(b)} - 1, n\right) + 2, M\left(\frac{n}{\mathsf{ord}(b)}, n\right) \right\} \right) & \textit{if } n \textit{ is even, and } \mathsf{w_H}(b) \neq n/2, \\ 2^{n-1} - \binom{n}{n/2} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - 2^{n/2-1} & \textit{if } n \textit{ is even, } \mathsf{w_H}(b) \neq n/2, \textit{ and } \mathsf{ord}(b) = n, \\ 2^{n-1} - \frac{1}{2}\binom{n}{n/2} - 2^{n/2-1} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - \left( M\left(\frac{n}{\mathsf{ord}(b)}, n\right) + 1 \right) & \textit{if } n \textit{ is even and } \mathsf{w_H}(b) = n/2. \end{cases}.$$

*Proof.* We bound the nonlinearity by bounding the absolute value of the Walsh transform, to do so we bound the term $C_{a,b}$ for all $a \in \mathbb{F}_2^n$. From Lemma 4 we have that $C_{a,b}$ is a bound on $B_{a,b}$ and therefore on $|W_f(a)|$ by Lemma 2. Using Lemma 3 we know we can restrict our study to the vectors $a$ such that $\mathsf{w_H}(a) \leq n/2$.

First we take care of the cases where $n$ is **odd**. In this case the first part of $C_{a,b}$ is null ($\mathsf{K}_{n/2}(k,n)$ is not defined for $n$ odd), then the terms in the summation comes only from the cases where $\mathsf{O}^{1-k}(b) + a$ is equal to 0 or $n$. Since for $n$ odd we restrict our study to the vectors $a$ and $b$ such that $\mathsf{w_H}(a) < n/2$ and $\mathsf{w_H}(b) < n/2$, $\mathsf{O}^{1-k}(b) + a$ cannot have Hamming weight $n$. Hence, we need to bound the contributions to the sum only when $\mathsf{w_H}(\mathsf{O}^{1-k}(b) + a) = 0$, that is when $\mathsf{O}^{1-k}(b) = a$. It means that $b$ is in the orbit of $a$ (using the vocabulary of group action, considering the group action where the group is the group of cyclic

permutations, acting on the set of length-$n$ binary vectors), and the maximum number of weights $k$ between 0 and $n$ such that $\mathsf{O}^{1-k}(b) = a$ depends on the order of $b$. On a period (of size $n$) $\mathsf{O}^i(b)$ equals $a$ $n/\mathsf{ord}(b)$ times, therefore at most $n/\mathsf{ord}(b) + 1$ times for the weights between 0 and $n$ since $\mathsf{O}^0(b) = \mathsf{O}^n(b)$. We denote $S(a, b)$ the set defined as $S(a, b) = \{i \in [0, n-1] \,|\, \mathsf{O}^{1-i}(b) = a\}$, we have:

$$|S(a,b)| = \begin{cases} 0 & \text{if } b \text{ is not in the orbit of } a, \\ \frac{n}{\mathsf{ord}(b)} & \text{otherwise.} \end{cases}.$$

Accordingly, the number of weights $k \in [0, n]$ such that $\mathsf{O}^{1-k}(b) = a$ is 0 if $b$ is not in the orbit of $a$, $n/\mathsf{ord}(b)$ if $\mathsf{O}^{1-0}(b) = \mathsf{O}^{1-n}(b) \neq a$ and $n/\mathsf{ord}(b) + 1$ otherwise. Since $|\mathsf{K}_k(0, n)| = |\mathsf{K}_k(n, n)| = \binom{n}{k}$, we can bound $C_{a,b}$ using $M(i, n)$ the bound on the sum of $i$ different binomial coefficients. Thereafter, we get the following bounds on $C_{a,b}$:

$$C_{a,b} \leq \begin{cases} 0 & \text{if } b \text{ is not in the orbit of } a, \\ M(\frac{n}{\mathsf{ord}(b)} - 1, n) + 2 & \mathsf{O}^1(b) = a\,, \\ M(\frac{n}{\mathsf{ord}(b)}, n) & \text{otherwise.} \end{cases}.$$

For the second case, we use the bound $M(\frac{n}{\mathsf{ord}(b)} - 1, n) + 2$ instead of $M(\frac{n}{\mathsf{ord}(b)} + 1, n)$ since the rotation of $b$ equals $a$ on the slices of weight 0 and $n$ where $\binom{n}{k} = 1$. It allows to conclude for the case $n$ odd, taking the maximum over all vectors $a \in \mathbb{F}_2^n$:

$$\begin{aligned} \mathsf{NL}(f) &= 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_a| \\ &\geq 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left( 2 \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} + C_{a,b} \right) \\ &\geq 2^{n-1} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - \frac{1}{2} \left( \max \left\{ M\left( \frac{n}{\mathsf{ord}(b)} - 1, n \right) + 2, M\left( \frac{n}{\mathsf{ord}(b)}, n \right) \right\} \right), \end{aligned}$$

where the first line is obtained using Property 1, the second one applying Lemma 4 and the third one using the bound on $C_{a,b}$ right above.

In particular, for elements $b$ of maximal order ($\mathsf{ord}(b) = n$), for all $a$ we get $C_{a,b} \leq \max\left(2, \binom{n}{(n-1)/2}\right)$. For $n > 1$ it gives the bound:

$$\mathsf{NL}(f) \geq 2^{n-1} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - \frac{1}{2} \binom{n}{(n-1)/2} = 2 \left( \sum_{i=0}^{(n-3)/2} \binom{n-1}{i} \right) - \frac{1}{2} \binom{n}{(n-1)/2}.$$

Then, we consider the case when $n$ is **even**. In this case $C_{a,b}$ has potentially more non null terms than in the $n$ odd case: the term $T = |\mathsf{K}_{\frac{n}{2}}(\mathsf{w_H}(\mathsf{O}^{1-n/2}(b) + a), n)|$, and the ones in the sum where the weight of $\mathsf{O}^{1-k}(b) + a)$ equals $n/2$ or $n$ (from Lemma 4). First, we bound $T$ using Property 3 Item 5:

$$T = |\mathsf{K}_{\frac{n}{2}}(\mathsf{w_H}(\mathsf{O}^{1-n/2}(b) + a), n)| \leq \max_{\ell \in [0,n]} |\mathsf{K}_{\frac{n}{2}}(\ell, n)| = \max_{\ell \in [0,n]} |\binom{n}{n/2} \binom{n}{\ell}^{-1} \mathsf{K}_\ell(n/2, n)|.$$

Then, using Property 3 Item 4 it gives:

$$T \leq \max_{\substack{\ell \in [0,n] \\ \ell \text{ even}}} |\binom{n}{n/2} \binom{n}{\ell}^{-1} \binom{n/2}{\ell/2}|.$$

Since for all $\ell$ even $\binom{n/2}{\ell/2} \leq \binom{n}{\ell}$ (using Pascal's relation the latter binomial can be written as a sum containing the former) we obtain $T \leq \binom{n}{n/2}$.

In the following we consider the contributions to the sum coming from the cases where the weight of $\mathsf{O}^{1-k}(b)+a)$ equals $n/2$ or $n$. First, we consider the case $\mathsf{w_H}(b) < n/2$, in this context since we restricted our study to vectors $a$ of Hamming weight at most $n/2$ (since we can derive the associated bound on the absolute value of the Walsh spectrum in $a + 1_n$ using Lemma 3), $\mathsf{O}^{1-k}(b) + a$ cannot reach the weight $n$. Hence, we need to bound only the cases where $\mathsf{w_H}(\mathsf{O}^{1-k}(b) + a)) = n/2$ (for an Hamming weight equal to 0, we will use the bound already derived from case $n$ odd). Since $|\mathsf{K}_k(n/2, n)|$, is relatively small we consider the bound taking the sum over all $k \in [0, n]$, rather than on limited number of weights as before. From Property 3 Item 4 we obtain:

$$\begin{aligned} D_{a,b} &= \sum_{\substack{k\in[0,n]\setminus\{\frac{n}{2}\} \\ \mathsf{w_H}(\mathsf{O}^{1-k}(b)+a)=\frac{n}{2}}} |\mathsf{K}_k(\mathsf{w_H}(\mathsf{O}^{1-k}(b)+a), n)| \\ &\leq \sum_{k\in[0,n]} |\mathsf{K}_k(n/2, n)| = \sum_{k'\in[0,n/2]} |(-1)^{k'}\binom{n/2}{k'}| = 2^{n/2} = U. \end{aligned}$$

Thereafter, adding the bound on the contributions when $\mathsf{w_H}(\mathsf{O}^{1-k}(b) + a)) = 0$, for $n$ even and $b$ such that $\mathsf{w_H}(b) < n/2$ we obtain:

$$\begin{aligned} \mathsf{NL}(f) &\geq 2^{n-1} - \frac{T}{2} - \frac{U}{2} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - \frac{1}{2}\left(\max\left\{M\left(\frac{n}{\mathsf{ord}(b)} - 1, n\right) + 2, M\left(\frac{n}{\mathsf{ord}(b)}, n\right)\right\}\right) \\ &\geq 2^{n-1} - \frac{1}{2}\binom{n}{\frac{n}{2}} - 2^{\frac{n}{2}-1} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - \frac{1}{2}\left(\max\left\{M\left(\frac{n}{\mathsf{ord}(b)} - 1, n\right) + 2, M\left(\frac{n}{\mathsf{ord}(b)}, n\right)\right\}\right). \end{aligned}$$

In particular, when $\mathsf{ord}(b) = n$ it gives:

$$\begin{aligned} \mathsf{NL}(f) &\geq 2^{n-1} - \frac{1}{2}\binom{n}{n/2} - 2^{n/2-1} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - \frac{1}{2}\left(\max\left\{2, \binom{n}{n/2}\right\}\right) \\ &\geq 2^{n-1} - \binom{n}{n/2} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - 2^{n/2-1}. \end{aligned}$$

Finally, we consider the case $\mathsf{w_H}(b) = n/2$. In this case the element $\mathsf{O}^{1-k}(b) + a$ can have Hamming weight $n$, which means that $\mathsf{O}^{1-k}(b)+a = 1_n$. As for the case $\mathsf{O}^{1-k}(b)+a = 0_n$, it is possible only $n/\mathsf{ord}(b)$ times on a period of $n$, therefore we can bound this contribution to the sum by $M(n/\mathsf{ord}(b), n)+1$ as before. It allows to conclude for this case:

$$\mathsf{NL}(f) \geq 2^{n-1} - \frac{1}{2}\binom{n}{n/2} - 2^{n/2-1} - \binom{n-1}{\lceil \frac{n}{2} \rceil - 1} - \left(M\left(\frac{n}{\mathsf{ord}(b)}, n\right) + 1\right).$$

□

*Remark 1.* From Remark 1 of [WCST14] the exact value of the nonlinearity of the $n$-variable HWBF is $2\left(\sum_{i=0}^{(n-3)/2}\binom{n-1}{i}\right)$. This function corresponds to $\mathsf{w_H}(b) = 1$ that has then maximal order. We remark that for $n$ odds the general bound of Theorem 1 adds only a term $\frac{1}{2}\binom{n}{(n-1)/2}$, and $\binom{n}{n/2} + 2^{n/2-1}$ when $n$ is even.

Theorem 1 gives bounds on the nonlinearity valid for all CW linear functions, but it can be tighten in many cases. For example, when the bound on $C_{a,b}$ is computed the contribution to the sum from the weight $k$ such that $\mathsf{O}^{1-k}(b) + a = 0_n$ is added without removing $|\mathsf{K}_k(1,n)|$ from the sum. For $n$ even, the bound have an extra contribution for all even weights that could be removed for a tighter bound.

### 5.2 Lower bound on the nonlinearity of a CW quadratic function

In this part we bound the nonlinearity of the CW quadratic function given by $g = x_1 + x_2 \cdot x_3$. First, we study the absolute value of a particular sum appearing when computing the Walsh transform of such functions.

**Proposition 7.** *Let $n \in \mathbb{N}^*$, $k, \ell \in \mathbb{N}$ such that $k \in [0,n]$, $\ell \in [0, n-2]$ and let $\mu, \nu \in \{0,1\}$, we denote by $A_{k,\ell,\mu,\nu}$ the quantity:*

$$A_{k,\ell,\mu,\nu} = \sum_{x \in \mathsf{E}_{k,n}} (-1)^{x_1 x_2 + \mu x_1 + \nu x_2 + b \cdot y},$$

*where $y = (x_3, \ldots, x_n)$ and $b \in \mathsf{E}_{\ell,n-2}$.*

*For all $\mu, \nu \in \{0,1\}^2$ the following hold:*

$$|A_{k,\ell,\mu,\nu}| \leq |\mathsf{K}_k(\ell, n-2)| + 2|\mathsf{K}_{k-1}(\ell, n-2)| + |\mathsf{K}_{k-2}(\ell, n-2)|.$$

*Proof.* First we consider the case $\mu = \nu = 0$, we get:

$$\begin{aligned}
|A_{k,\ell,\mu,\nu}| &= |\sum_{x \in \mathsf{E}_{k,n}} (-1)^{x_1 x_2 + b \cdot y}| \\
&= |\sum_{y \in \mathsf{E}_{k,n-2}} (-1)^{0 + b \cdot y} + 2 \sum_{y \in \mathsf{E}_{k-1,n-2}} (-1)^{0 + b \cdot y} + \sum_{y \in \mathsf{E}_{k-2,n-2}} (-1)^{1 + b \cdot y}| \\
&= |\mathsf{K}_k(\ell, n-2) + 2\mathsf{K}_{k-1}(\ell, n-2) - \mathsf{K}_{k-2}(\ell, n-2)| \\
&\leq |\mathsf{K}_k(\ell, n-2)| + 2|\mathsf{K}_{k-1}(\ell, n-2)| + |\mathsf{K}_{k-2}(\ell, n-2)|,
\end{aligned}$$

where the second equality is obtained by partitioning on the possible values of $x_1$ and $x_2$.

Similarly, for the other possible values of $\mu$ and $\nu$ only the signs before the $4$ terms $\mathsf{K}_k(\ell, n-2)$, $\mathsf{K}_{k-1}(\ell, n-2)$, $\mathsf{K}_{k-1}(\ell, n-2)$ and $\mathsf{K}_{k-2}(\ell, n-2)$ change. Therefore the same bound applies.

□

**Theorem 2 (Nonlinearity bound of a weightwise cyclic quadratic function).** *Let $n \in \mathbb{N}$, $n \geq 3$, and $f$ be the CW quadratic function associated to $g = x_1 + x_2 x_3$, the following holds on its nonlinearity:*

$$\mathsf{NL}(f) \geq \begin{cases} 2^{n-1} - 2\left(2\binom{n-3}{\lceil \frac{n}{2} \rceil - 2} + \binom{n-2}{\lceil \frac{n}{2} \rceil - 1} + 1\right) & \text{if } n \text{ is odd}, \\ 2^{n-1} - 2\left(2\binom{n-3}{\frac{n}{2}-2} + \binom{n-2}{n/2-1} + 2^{n/2-1} + \binom{n-2}{\frac{n}{2}-1} + 1\right) & \text{if } n \text{ is even}. \end{cases}.$$

*Proof.* The proof follows the main ideas of the one of Theorem 1. First, as for CW linear functions we bound the nonlinearity by bounding the absolute value of the Walsh spectrum:

$$\begin{aligned}
W_f(a) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+a\cdot x} = \sum_{k=0}^{n} \sum_{x\in\mathsf{E}_{k,n}} (-1)^{\mathsf{O}^{k-1}(x_1+x_2x_3)+a\cdot x}.\\
|W_f(a)| &\leq \sum_{k=0}^{n} |\sum_{x\in\mathsf{E}_{k,n}} (-1)^{\mathsf{O}^{k-1}(x_1+x_2x_3)+a\cdot x}| \leq \sum_{k=0}^{n} |A_{k,\ell_k,\mu_k,\nu_k}|\\
&\leq \sum_{k=0}^{n} \left(|\mathsf{K}_k(\ell_k, n-2)| + 2|\mathsf{K}_{k-1}(\ell_k, n-2)| + |\mathsf{K}_{k-2}(\ell_k, n-2)|\right),
\end{aligned}$$

where for the second line we use that $\mathsf{O}^{k-1}(x_1+x_2x_3)+a\cdot x = x_{(k \mod n)} + x_{(k+1 \mod n)}x_{(k+2 \mod n)} + a\cdot x$ (using the cyclic shift definition from Definition 16). This expression can be written as:

$$x_{(k+1 \mod n)}x_{(k+2 \mod n)} + \mu x_{(k+1 \mod n)} + \nu x_{(k+2 \mod n)} + b\cdot y,$$

where $\mu = a_{(k+1 \mod n)}$, $\nu = a_{(k+1 \mod n)}$, $b$ is the $(n-2)$-length vector obtained from $a$ by removing the indices $(k+1 \mod n)$ and $(k+2 \mod n)$. For each $k$ in the sum we define such $\mu$, $\nu$ and $\ell = \mathsf{w_H}(b)$ and index them with $k$. The last equation comes from Proposition 7.

Then, we bound the sums of absolute value of Krawtchouk polynomials similarly as is in the proofs of Section 5.1. Recall that using Property 3 Item 3, $|\mathsf{K}_k(1,n)|$ is greater than the others values unless $k = n/2$ or $\ell \in \{0, n/2, n\}$. As previously, we bound by considering the sum of all Krawtchouk polynomials with $k = 1$ plus the limited number of special cases where this upper bound does not apply.

As in the proof of Theorem 1, for $|\mathsf{K}_k(\ell_k, n-2)|$ we can neglect the case $\ell_k = n-2$ since the bound on $|W_f(a)|$ and $|W_f(a+1_n)|$ is the same. Accordingly, we can restrict the study to $a \in \mathbb{F}_2^n$, $\mathsf{w_H}(a) \leq n/2$.

The case $k = n/2-1$ can be treated separately as before, since the maximal possible contribution from this part is small. Using Property 3 Item 4 it gives:

$$\max_{\ell\in[0,n-2]} |\mathsf{K}_{n/2-1}(\ell, n-2)| \leq \max_{\substack{\ell\in[0,n-2]\\ \ell \text{ even}}} |\binom{n-2}{n/2-1}\binom{n-2}{\ell}^{-1}\binom{n/2-1}{\ell/2}| \leq \binom{n-2}{n/2-1}.$$

The cases $\ell_k = n/2-1$ can be handled as previously since the sum is small, using Property 3 Item 4 we obtain:

$$\sum_{k\in[0,n-2]} |\mathsf{K}_k(n/2-1, n-2)| = \sum_{k'\in[0,n/2-1]} |(-1)^{k'}\binom{n/2-1}{k'}| = 2^{n/2-1}.$$

The last special cases are the ones such that $\ell_k = 0$, we can bound their contribution using $M(i, n-2)$ introduced in Definition 17 as before, counting the maximum number of times $a$ and $x_1 + x_2x_3$ can coincide on the linear part restricted to $y$ along an orbit. This is equivalent to the cardinal $C = |\{i \in [n], \mathsf{supp}(\mathsf{O}^i(a)) \subset [3] \text{ and } \mathsf{O}^i(a)_1 = 1\}|$. We consider the different cases based on the Hamming weight of $a$. When $\mathsf{w_H}(a) = 0$ the set is empty. When $\mathsf{w_H}(a) = 1$, $C = 1$. For $\mathsf{w_H}(a) \in \{2,3\}$ $C \leq 1$ since if $a$ is a rotation of $1_20_{n-2}$ or $1010_{n-3}$ or $1110_{n-3}$ once per orbit it coincides. When $\mathsf{w_H}(a) > 3$, $C = 0$.

Summing up we obtain the following bound:

$$\begin{aligned}|W_f(a)| &\leq \sum_{k=0}^{n} \left(|\mathsf{K}_k(\ell_k, n-2)| + 2|\mathsf{K}_{k-1}(\ell_k, n-2)| + |\mathsf{K}_{k-2}(\ell_k, n-2)|\right) \\ &\leq 4\left(\sum_{k\in[0,n-2]\setminus\{n/2-1\}} |\mathsf{K}_k(1, n-2)| + \binom{n-2}{n/2-1} + 2^{n/2-1} + M(1, n-2) + 1\right) \\ &\leq 4\left(2\binom{n-3}{\lceil \frac{n}{2}\rceil - 2} + \binom{n-2}{n/2-1} + 2^{n/2-1} + \binom{n-2}{\lceil \frac{n}{2}\rceil - 1} + 1\right).\end{aligned}$$

The last equation is obtained by summing (over $k$) the values $|\mathsf{K}_k(1, n-2)|$ as in the proof of Lemma 4, and plugging the value of $M(1, n-2)$ using Property 5.

Using Property 1 we can conclude on the bound on the nonlinearity of such functions. When $n$ is even

$$\mathsf{NL}(f) \geq 2^{n-1} - 2\left(2\binom{n-3}{\frac{n}{2}-2} + \binom{n-2}{n/2-1} + 2^{n/2-1} + \binom{n-2}{\frac{n}{2}-1} + 1\right).$$

When $n$ is odd:

$$\mathsf{NL}(f) \geq 2^{n-1} - 2\left(2\binom{n-3}{\lceil \frac{n}{2}\rceil - 2} + \binom{n-2}{\lceil \frac{n}{2}\rceil - 1} + 1\right).$$

□

## 6 Experimental results

In this part we summarize the results of our experiments on cyclic weightwise affine and quadratic functions, up to 16 variables.

### 6.1 Cyclic weightwise linear and quadratic functions in 8 variables

In Table 1 we give the cryptographic parameters of the 8-variable CW linear functions. Based on Proposition 5 and Proposition 6 we give only on representative of each orbit, for the elements of Hamming weight at most 4. We remark that the second row corresponds to the HWBF (in red), we observe that almost all other functions have equal or better nonlinearity. Additionally, some functions with $\mathsf{w_H}(a) \in \{3, 4\}$ have strictly better nonlinearity, with the same degree, algebraic immunity and resilience order.

Still in 8 variables, we give the cryptographic parameters of some 8-variable CW quadratic functions in Table 2. We observe that the nonlinearity of this functions is at least as good as the best one for a CW linear function.

| $a$ | degree | algebraic immunity | nonlinearity | resilience |
|---|---|---|---|---|
| $(0,0,0,0,0,0,0,0)$ | 0 | 0 | 0 | $-1$ |
| $(1,0,0,0,0,0,0,0)$ | 7 | 4 | 88 | 0 |
| $(1,1,0,0,0,0,0,0)$ | 7 | 3 | 92 | 0 |
| $(1,0,1,0,0,0,0,0)$ | 5 | 4 | 88 | 0 |
| $(1,0,0,1,0,0,0,0)$ | 7 | 3 | 92 | 0 |
| $(1,0,0,0,1,0,0,0)$ | 3 | 3 | 96 | 0 |
| $(1,1,1,0,0,0,0,0)$ | 7 | 4 | 88 | 0 |
| $(1,1,0,1,0,0,0,0)$ | 7 | 4 | 96 | 0 |
| $(1,1,0,0,1,0,0,0)$ | 7 | 4 | 88 | 0 |
| $(1,1,0,0,0,1,0,0)$ | 7 | 4 | 88 | 0 |
| $(1,1,0,0,0,0,1,0)$ | 7 | 4 | 96 | 0 |
| $(1,0,1,0,1,0,0,0)$ | 7 | 4 | 88 | 0 |
| $(1,0,1,0,0,1,0,0)$ | 7 | 4 | 88 | 0 |
| $(1,1,1,1,0,0,0,0)$ | 5 | 3 | 88 | 0 |
| $(1,1,1,0,1,0,0,0)$ | 7 | 4 | 92 | 0 |
| $(1,1,1,0,0,1,0,0)$ | 5 | 4 | 88 | 0 |
| $(1,1,1,0,0,0,1,0)$ | 7 | 4 | 92 | 0 |
| $(1,1,0,1,1,0,0,0)$ | 5 | 4 | 88 | 0 |
| $(1,1,0,0,1,1,0,0)$ | 3 | 2 | 64 | 0 |
| $(1,1,0,1,0,1,0,0)$ | 7 | 4 | 92 | 0 |
| $(1,1,0,1,0,0,1,0)$ | 5 | 3 | 88 | 0 |
| $(1,1,0,0,1,0,1,0)$ | 7 | 4 | 92 | 0 |
| $(1,0,1,0,1,0,1,0)$ | 1 | 1 | 0 | 3 |

**Table 1.** Cryptographic parameters of the 8-variable CW linear functions $f_a$.

| $g$ | degree | algebraic immunity | nonlinearity | resilience |
|---|---|---|---|---|
| $x_1 + x_2x_3$ | 6 | 4 | 96 | 0 |
| $x_1 + x_3x_4$ | 7 | 4 | 102 | 0 |
| $x_1 + x_4x_5$ | 6 | 4 | 104 | 0 |
| $x_1 + x_5x_6$ | 7 | 4 | 98 | 0 |
| $x_1 + x_6x_7$ | 6 | 4 | 100 | 0 |
| $x_1 + x_7x_8$ | 7 | 4 | 98 | 0 |
| $x_1 + x_2x_4$ | 7 | 4 | 98 | 0 |
| $x_1 + x_3x_5$ | 7 | 4 | 102 | 0 |
| $x_1 + x_2x_3 + x_4x_5$ | 7 | 4 | 102 | 0 |
| $x_1 + x_2x_3 + x_4x_5 + x_6x_7$ | 7 | 4 | 104 | 0 |

**Table 2.** Cryptographic parameters of some 8-variable CW quadratic functions.

### 6.2 Properties of cyclic weightwise linear and quadratic functions in 16 variables

For $n = 16$ we give the degree, nonlinearity and resilience order of some examples of both CW linear and CW quadratic functions in Table 3, the HWBF function corresponds to the first row (in red). As for $n = 8$ we observe that CW quadratic functions have nonlinearity sensibly better than CW linear functions.

| $g$ | degree | nonlinearity | resilience |
|---|---|---|---|
| $x_1$ | 15 | 25904 | 0 |
| $x_1 + x_2$ | 15 | 25772 | 0 |
| $x_1 + x_2 + x_3$ | 15 | 25888 | 0 |
| $x_1 + x_2 + x_3 + x_4$ | 13 | 25864 | 0 |
| $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8$ | 9 | 25840 | 0 |
| $x_1 + x_9$ | 7 | 26432 | 0 |
| $x_1 + x_5 + x_9$ | 15 | 25904 | 0 |
| $x_1 + x_3 + x_5 + x_7 + x_9 + x_{11} + x_{13} + x_{15}$ | 1 | 0 | 7 |
| $x_1 + x_2x_3$ | 14 | 27884 | 0 |
| $x_1 + x_2 + x_2x_3$ | 15 | 28412 | 0 |
| $x_1 + x_2 + x_3x_4$ | 15 | 28266 | 0 |
| $x_1 + x_2x_3 + x_4x_5$ | 15 | 29554 | 0 |
| $x_1 + x_2x_3 + x_4x_5 + x_6x_7$ | 14 | 30736 | 0 |
| $x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_8x_9$ | 15 | 31346 | 0 |
| $x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_8x_9 + x_{10}x_{11}$ | 14 | 31600 | 0 |
| $x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_8x_9 + x_{10}x_{11} + x_{12}x_{13}$ | 15 | 31490 | 0 |
| $x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_8x_9 + x_{10}x_{11} + x_{12}x_{13} + x_{14}x_{15}$ | 14 | 31616 | 0 |

**Table 3.** Cryptographic parameters of some 16-variable CW functions.

### 6.3 Comparisons of cyclic weightwise functions up to 16 variables

We compare the parameters of 4 CW functions in 4 to 16 variables. First we consider to CW linear functions, the HWBF in Table 4 and the one given by $g = x_1 + x_2$ in Table 5 we call $s$. Then, we consider the CW quadratic function given by $g = x_1 + x_2 \cdot x_3$ in Table 6, which nonlinearity is bounded by Theorem 2. Finally we consider the CW quadratic function given by $g(x) = x_1 + \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} x_{2i}x_{2i+1}$ in Table 7. For readability we denote $t$ and $u$ these functions.

| $n$ | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Degree | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| AI | 2 | 3 | 3 | 3 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 6 | 6 |
| Nonlinearity | 4 | 10 | 22 | 44 | 88 | 186 | 372 | 772 | 1544 | 3172 | 6344 | 12952 | 25904 |
| Resilience | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table 4.** Cryptographic parameters of the HWBF in $n$ variables, for $n \in [4, 16]$.

| $n$ | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Degree | 3 | 4 | 5 | 6 | 5 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 13 |
| AI | 2 | 2 | 3 | 3 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 6 | 6 |
| Nonlinearity | 4 | 10 | 22 | 44 | 88 | 188 | 376 | 784 | 1568 | 3226 | 6452 | 13172 | 26344 |
| Resilience | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table 5.** Cryptographic parameters of the CW linear function $s$ given by $g = x_1 + x_2$ in $n$ variables, for $n \in [4, 16]$.

| $n$ | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Degree | 2 | 4 | 5 | 6 | 6 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 14 |
| AI | 2 | 3 | 3 | 3 | 4 | 4 | 5 | 5 | 5 | 6 | 6 | 6 | 7 |
| Nonlinearity | 4 | 10 | 22 | 46 | 96 | 196 | 404 | 816 | 1672 | 3358 | 6854 | 13722 | 27884 |
| Resilience | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table 6.** Cryptographic parameters of the CW quadratic function $t$ given by $g = x_1 + x_2x_3$ in $n$ variables, for $n \in [4, 16]$.

| $n$ | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Degree | 2 | 4 | 4 | 6 | 6 | 8 | 8 | 10 | 10 | 12 | 12 | 14 | 14 |
| AI | 2 | 3 | 3 | 3 | 4 | 4 | 5 | 5 | 6 | 6 | 6 | 6 | 7 |
| Nonlinearity | 4 | 10 | 24 | 48 | 104 | 220 | 456 | 924 | 1888 | 3862 | 7816 | 15748 | 31616 |
| Resilience | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table 7.** Cryptographic parameters of the CW quadratic function $u$ given by $g = x_1 + \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} x_{2i}x_{2i+1}$ in $n$ variables, for $n \in [4, 16]$.

From these experiments we observe the following for the different criteria:

- **Degree**. The degree of the HWBF is $n-1$ (as proven in former works), we observe the same trend for $s$ and $t$ except when $n$ is a power of 2. The one of $u$ equals $n-1$ when $n$ is odd and $n-2$ otherwise.
- **Algebraic immunity**. For all these values we observe the following relation: $\mathsf{AI}(HWBF) \leq \mathsf{AI}(s) \leq \mathsf{AI}(t) \leq \mathsf{AI}(u)$.
- **Nonlinearity**. The HWBF is the one with the lowest nonlinearity, its is overreached by the one of $u$ since $n = 6$, the one of $t$ since $n = 7$ and the one of $s$ since $n = 9$. We also have the relation $\mathsf{NL}(HWBF) \leq \mathsf{NL}(s) \leq \mathsf{NL}(t) \leq \mathsf{NL}(u)$ for all values of $n$ we tried.
- **Resilience**. The resilience order is 0 for all these functions, they are all balanced but not 1-resilient.

The nonlinearity of $u$ is way higher than for the other functions, based in the experimental values we conjecture the following:

$$\forall \ell \in \mathbb{N}^*, \quad \mathsf{NL}(u_{4\ell}) = 2^{4\ell-1} - 2^{2\ell-1} - 2^{3\ell-2}.$$

## 7 Conclusion and open questions

In this article we realized the first study on weightwise degree-$d$ functions. First, we defined this notion and explained how it generalizes different classes of functions already studied in the context of cryptography. After determining their cardinality and exhibiting some balanced constructions, we focused on the subfamily of cyclic weightwise functions that are motivated by efficient implementation. Then, for this class of functions we investigated their nonlinearity, deriving lower bounds. Our techniques based on sum of absolute values of Krawtchouk polynomials allowed to generalize the result known only for the HWBF to any CW affine function, and also on a family of CW quadratic functions. Finally, we presented experimental results for Boolean function up to 16 variables. This experiment shows that other CW linear functions have better cryptographic parameters than the HWBF. More importantly, we can observe that CW quadratic functions allow to get a substantially higher nonlinearity, the main weakness that prevent HWBF to be considered in stream cipher designs.

Different open questions arose during this work, we highlight the following ones:

- First, the nonlinearity bounds of Section 5 are not tight. It would be interesting to improve these bounds or determine exactly the nonlinearity as in the case of the HWBF since we can see from Section 6.3 that the real values are far better than the bounds. The proofs could also be adapted to other subfamilies, for example to generalize the results to all CW quadratic functions.
- Then, an engaging direction consists in determining or bounding the degree and algebraic immunity of specific CW families. From Section 6.3 we can observe that $t$ and $u$ functions have AI better than or equal to the HWBF, it would be interesting to prove or refute that the AI is strictly higher for $n$ big enough.
- In Section 6.3 we conjecture the exact nonlinearity of the function $u$, it is appealing to prove it, or the exact value for another family with at least this nonlinearity. This family is the one with best nonlinearity we observed in the experimental part of this work, it is interesting to exhibit balanced CW quadratic functions with better nonlinearity.
- Finally, one future direction consists in designing a stream cipher using a CW quadratic function as filter function. The main challenges are determining the number of variables necessary to have a strong enough filter, and how to use the cyclic properties to gain in efficiency.

## References


ARS+15. Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. Ciphers for MPC and FHE. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 430–454. Springer, Heidelberg, April 2015.

BCBS23. Adda-Akram Bendoukha, Pierre-Emmanuel Clet, Aymen Boudguiga, and Renaud Sirdey. Optimized stream-cipher-based transciphering by means of functional-bootstrapping. In Vijayalakshmi Atluri and Anna Lisa Ferrara, editors, *Data and Applications Security and Privacy XXXVII*, pages 91–109, Cham, 2023. Springer Nature Switzerland.

BLSW99. Beate Bollig, Martin Löbbing, Martin Sauerhoff, and Ingo Wegener. On the complexity of the hidden weighted bit function for various BDD models. *RAIRO Theor. Informatics Appl.*, 33(2):103–116, 1999.

BOS23. Thibault Balenbois, Jean-Baptiste Orfila, and Nigel P. Smart. Trivial transciphering with trivium and TFHE. *IACR Cryptol. ePrint Arch.*, page 980, 2023.

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.

BPR23. Nicolas Bon, David Pointcheval, and Matthieu Rivain. Optimized homomorphic evaluation of boolean functions. Cryptology ePrint Archive, Paper 2023/1589, 2023.

Bry91. Randal E. Bryant. On the complexity of VLSI implementations and graph representations of boolean functions with application to integer multiplication. *IEEE Trans. Computers*, 40(2):205–213, 1991.

BSS+23. Adda-Akram Bendoukha, Oana Stan, Renaud Sirdey, Nicolas Quero, and Luciano Freitas. Practical homomorphic evaluation of block-cipher-based hash functions with applications. Cryptology ePrint Archive, Paper 2023/480, 2023.

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

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

Car22. Claude Carlet. A wide class of boolean functions generalizing the hidden weight bit function. *IEEE Trans. Inf. Theory*, 68(2):1355–1368, 2022.

CCF+16. Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. Stream ciphers: A practical solution for efficient homomorphic-ciphertext compression. In Thomas Peyrin, editor, *FSE 2016*, volume 9783 of *LNCS*. Springer, Heidelberg, March 2016.

CDPP22. Kelong Cong, Debajyoti Das, Jeongeun Park, and Hilder V.L. Pereira. Sortinghat: Efficient private decision tree evaluation via homomorphic encryption and transciphering. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, page 563–577. Association for Computing Machinery, 2022.

CGGI16. Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 3–33. Springer, Heidelberg, December 2016.

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

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

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

CMR17. Claude Carlet, Pierrick Méaux, and Yann Rotella. Boolean functions with restricted input and their robustness; application to the FLIP cipher. *IACR Trans. Symmetric Cryptol.*, 2017(3), 2017.

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

DEG+18. Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Eik List, Florian Mendel, and Christian Rechberger. Rasta: A cipher with low anddepth and few ands per bit. In *CRYPTO 2018*, pages 662–692, 2018.

DK13. Ilya Dumer and Olga Kapralova. Spherically punctured biorthogonal codes. *IEEE Trans. Information Theory*, 59(9):6010–6017, 2013.

DK17. Ilya Dumer and Olga Kapralova. Spherically punctured reed-muller codes. *IEEE Trans. Information Theory*, 63(5):2773–2780, 2017.

DM15. Léo Ducas and Daniele Micciancio. FHEW: Bootstrapping homomorphic encryption in less than a second. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 617–640. Springer, Heidelberg, April 2015.

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.

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

GM23. Agnese Gini and Pierrick Méaux. On the algebraic immunity of weightwise perfectly balanced functions. In Abdelrahaman Aly and Mehdi Tibouchi, editors, *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*, volume 14168 of *Lecture Notes in Computer Science*, pages 3–23. Springer, 2023.

HMR20. Clément Hoffmann, Pierrick Méaux, and Thomas Ricosset. Transciphering, using filip and TFHE for an efficient delegation of computation. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 39–61. Springer, 2020.

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

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.

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

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

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

MKCL22. Sara Mandujano, Juan Carlos Ku Cauich, and Adriana Lara. Studying special operators for the application of evolutionary algorithms in the seek of optimal boolean functions for cryptography. In Obdulia Pichardo Lagunas, Juan Martínez-Miranda, and Bella Martínez Seis, editors, *Advances in Computational Intelligence*, pages 383–396, Cham, 2022. Springer Nature Switzerland.

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.

MPP23. Pierrick Méaux, Jeongeun Park, and Hilder V. L. Pereira. Towards practical transciphering for fhe with setup independent of the plaintext space. Cryptology ePrint Archive, Paper 2023/1531, 2023.

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

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.

NLV11. Michael Naehrig, Kristin Lauter, and Vinod Vaikuntanathan. Can homomorphic encryption be practical? In *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, CCSW '11, page 113–124, New York, NY, USA, 2011. Association for Computing Machinery.

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

TCBS23. Daphné Trama, Pierre-Emmanuel Clet, Aymen Boudguiga, and Renaud Sirdey. At last! A homomorphic AES evaluation in less than 30 seconds by means of TFHE. 2023.

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

WCST14. Qichun Wang, Claude Carlet, Pantelimon Stanica, and Chik How Tan. Cryptographic properties of the hidden weighted bit function. *Discret. Appl. Math.*, 174:1–10, 2014.

WTS14. Qichun Wang, Chik How Tan, and Pantelimon Stanica. Concatenations of the hidden weighted bit function and their cryptographic properties. *Adv. Math. Commun.*, 8(2):153–165, 2014.

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

ZLC+23. Qinglan Zhao, Mengran Li, Zhixiong Chen, Baodong Qin, and Dong Zheng. A unified construction of weightwise perfectly balanced boolean functions. Cryptology ePrint Archive, Paper 2023/460, 2023.