The Revisited Hidden Weight Bit Function

Pierrick Méaux[1], Tim Seuré(✉)[1], and Deng Tang[2]

[1] University of Luxembourg, Esch-sur-Alzette, Luxembourg
pierrick.meaux@uni.lu, tim.seure@uni.lu
[2] Shanghai Jiao Tong University, Shanghai, China
dengtang@sjtu.edu.cn

Abstract. The Hidden Weight Bit Function (HWBF) has drawn considerable attention for its simplicity and cryptographic potential. Despite its ease of implementation and favorable algebraic properties, its low nonlinearity limits its direct application in modern cryptographic designs. In this work, we revisit the HWBF and propose a new weightwise quadratic variant obtained by combining the HWBF with a bent function. This construction offers improved cryptographic properties while remaining computationally efficient. We analyze the balancedness, nonlinearity, and other criteria of this function, presenting theoretical bounds and experimental results to highlight its advantages over existing functions in similar use cases. The different techniques we introduce to study the nonlinearity of this function also enable us to bound the nonlinearity of a broad family of weightwise quadratic functions, both theoretically and practically. We believe these methods are of independent interest.

Keywords: Boolean functions · HWBF · Nonlinearity.

1 Introduction

The Hidden Weight Bit Function (HWBF) has attracted significant attention since its introduction by Bryant in 1991 [7]. It has been regarded as the simplest example of a function whose binary decision diagram has exponential size [5,7]. The ease of implementing this function across various computational models—owing to its reliance on computing the Hamming weight of the input and applying a simple linear function—combined with its relatively strong cryptographic properties as demonstrated in [46] (*e.g.*, balancedness, nonlinearity, degree, and algebraic immunity), has made it a noteworthy candidate for use as a filter function in stream cipher constructions.

Recent developments in stream ciphers have reignited interest in this function. The emergence of new applications for stream ciphers with filter functions on a larger number of variables—such as Hybrid Homomorphic Encryption (HHE) [40]—has further emphasized the relevance of such functions. HHE requires Boolean functions that can be efficiently evaluated in an input-oblivious algorithm. For instance, several new binary stream ciphers have been proposed since 2016, including Kreyvium [9], FLIP [37], Rasta [25], FiLIP [36], Dasta [4] and Fasta [19].

Currently, designs employing Boolean functions with more than one hundred variables as filters lead to HHE schemes with the best latency [1,20,28,39].

The HWBF, while efficient to compute, suffers from low nonlinearity, which limits its direct application as a filter function. Consequently, various generalizations have been explored to enhance this parameter while preserving or improving other cryptographically relevant properties, such as balancedness, algebraic degree, and algebraic immunity. Notable examples include functions introduced in [13,16] and [38]. The latter work considers functions obtained by computing the Hamming weight of the input and applying a quadratic Boolean function, so-called weightwise quadratic functions.

In this article, we propose a new generalization of the HWBF, a weightwise quadratic function constructed by XOR-ing the HWBF with a bent quadratic function. This leads to a family of Boolean functions that are computationally efficient and feature superior cryptographic properties compared to previous constructions. Additionally, the techniques we introduce to analyze nonlinearity have broader applicability and provide bounds on the maximum absolute Walsh spectrum for a wider class of weightwise quadratic functions. Our contributions are as follows:

- *Balancedness analysis* (Section 3): We define the revisited HWBF in n variables, hereafter denoted by f, and analyze its balancedness. This involves studying the (restricted) Walsh transform of specific quadratic functions over sets of fixed Hamming weights (called slices). By establishing recursive relations for these values, we determine for which values of n the function is balanced.
- *Nonlinearity bounds* (Section 4): We relate the maximum Walsh coefficients of the revisited HWBF to the coefficients of generating functions and employ complex analysis techniques to prove lower bounds on the nonlinearity of f. Unlike most studies on Boolean functions used in cryptography, this approach yields strong nonlinearity bounds for a broader class of functions in an even number of variables.
- *Experimental results and comparisons* (Section 5): For bounded values of n, we employ specific techniques to refine the nonlinearity bounds of f, providing tighter estimates up to $n = 80$. Through experiments, we compare these bounds with actual nonlinearity values for f and other weightwise quadratic functions, such as the majority function, the HWBF, and the two main examples in [38]. Our results highlight the revisited HWBF's superior nonlinearity relative to functions with similar computational costs.
- *Analysis of other cryptographic parameters* (Section 6): We evaluate other cryptographically relevant parameters of f, including degree, algebraic immunity, and fast algebraic immunity. Similar to the nonlinearity analysis, the revisited HWBF outperforms or matches other functions with comparable computational costs.

2 Preliminaries

Throughout this paper, $n \geqslant 0$ will always denote a non-negative integer. Further, our intervals will only contain integers, so that for instance $[0, n] = \{0, 1, \ldots, n\}$. The set of binary vectors of length n will be denoted by $\mathbb{F}_2^n$, with the zero vector written as 0_n. The canonical basis of $\mathbb{F}_2^n$ will be written as $\{e_1, \ldots, e_n\}$; therefore, $e_i \in \mathbb{F}_2^n$ is the vector which is zero everywhere except at position i. The entries of a binary vector $x \in \mathbb{F}_2^n$ will always be denoted by $x_1, \ldots, x_n$. Given a permutation $\pi : [1, n] \to [1, n]$ and a vector $x \in \mathbb{F}_2^n$, we define $\pi(x) = (x_{\pi(i)})_{i \in [1,n]} \in \mathbb{F}_2^n$. We write the scalar product of two binary vectors $x, y \in \mathbb{F}_2^n$ as $x \cdot y = \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_2$. The Hamming weight of a binary vector $x \in \mathbb{F}_2^n$ is denoted by $\mathsf{w_H}(x) = |\{i \in [1, n] : x_i = 1\}|$.

2.1 Boolean Functions and Cryptographic Parameters

In this part, we recall general concepts on Boolean functions and their cryptographic properties we use in this article. For a deeper introduction on Boolean functions and their cryptographic parameters, we refer to the book [12], and to [15] for properties on slices, so-called weightwise properties.

Definition 1 (Slice). *For any integer k, we introduce the set $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n : \mathsf{w_H}(x) = k\}$, and call it the k-th slice of the Boolean hypercube (of dimension n); note that if $k \notin [0, n]$, then $\mathsf{E}_{k,n} = \varnothing$.*

Definition 2 (Boolean function). *A Boolean function 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 this set without the null function by $\mathcal{B}_n^*$.*

Below, for a Boolean function $f \in \mathcal{B}_n$, we write $f + 1$ for the Boolean function $g \in \mathcal{B}_n$ which satisfies $g(x) = f(x) + 1$ for every $x \in \mathbb{F}_2^n$.

Definition 3 (Algebraic normal form, degree). *We call algebraic normal form of a Boolean function $f \in \mathcal{B}_n$ its unique representation as an element of the ring $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$, and we express it as $f(x_1, \ldots, x_n) = \sum_{I \subseteq [1,n]} a_I \left(\prod_{i \in I} x_i\right)$, where $a_I \in \mathbb{F}_2$. The (algebraic) degree of f is defined by $\mathsf{deg}(f) = 0$ in case f is the null function, and $\mathsf{deg}(f) = \max\{|I| : I \subseteq [1, n], a_I = 1\}$ otherwise.*

Definition 4 (Walsh transform). *The Walsh transform at $a \in \mathbb{F}_2^n$ of $f \in \mathcal{B}_n$ restricted to a subset $S \subseteq \mathbb{F}_2^n$ is defined as $\mathcal{W}_{f,S}(a) = \sum_{x \in S} (-1)^{f(x)+a \cdot x}$. The (unrestricted) Walsh transform of f is then defined as $\mathcal{W}_f = \mathcal{W}_{f,\mathbb{F}_2^n}$. For any integer k, we also set $\mathcal{W}_{f,k} = \mathcal{W}_{f,\mathsf{E}_{k,n}}$.*

Definition 5 (Balancedness). *A Boolean function $f \in \mathcal{B}_n$ is called balanced if $|\{x \in \mathbb{F}_2^n : f(x) = 0\}| = 2^{n-1} = |\{x \in \mathbb{F}_2^n : f(x) = 1\}|$. Equivalently, f is balanced if and only if $\mathcal{W}_f(0_n) = 0$.*

Definition 6 (Nonlinearity, *e.g.*, page 79 in [12]). *The nonlinearity* $\mathsf{NL}(f)$ *of a Boolean function* $f \in \mathcal{B}_n$ *is the minimum Hamming distance between* f *and all the affine functions in* $\mathcal{B}_n$*, that is,* $\mathsf{NL}(f) = \min\{\mathsf{d_H}(f,g) : g \in \mathcal{B}_n, \mathsf{deg}(g) \leqslant 1\}$*, where the Hamming distance between* f *and* g *is defined as* $\mathsf{d_H}(f,g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}|$*. Alternatively, the nonlinearity of* $f \in \mathcal{B}_n$ *can also be defined in terms of its Walsh transform:* $\mathsf{NL}(f) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} |\mathcal{W}_f(a)|$.

When n is even, the nonlinearity of a Boolean function in n variables can reach at most $2^{n-1} - 2^{n/2-1}$. Functions reaching this maximum are called bent functions. Due to their broad applications and importance, they have been the focus of multiple works, *e.g.*, [42,24,8,45,33]. The quadratic function $d_n \in \mathcal{B}_n$ given by $d_n(x) = \sum_{i=1}^{n/2} x_{2i-1}x_{2i}$ is an example for such a bent function.

The algebraic degree of multiples of a Boolean function is a crucial quantity for various attacks on stream ciphers that utilize a Boolean function as a filter. The well-known algebraic attack [22] and fast algebraic attack [21] on filtered LFSRs have motivated the study of cryptographic properties such as algebraic immunity and fast algebraic immunity, *e.g.*, [2,27,29]. Nowadays, these parameters are systematically determined for any function considered as a filter.

Definition 7 (Annihilator, algebraic immunity [32]). *Let* $f \in \mathcal{B}_n$ *be a Boolean function. Then a function* $g \in \mathcal{B}_n^*$ *is called an annihilator of* f *if it satisfies* $fg = 0$*. The algebraic immunity of* f *is then defined as* $\mathsf{AI}(f) = \min\{\mathsf{deg}(g) : g \in \mathcal{B}_n^*$ *is an annihilator of* f *or* $f+1\}$.

Definition 8 (Fast algebraic immunity, *e.g.*, [3,17,30]). *The fast algebraic immunity of* $f \in \mathcal{B}_n$ *is defined as* $\mathsf{FAI}(f) = \min\{2\mathsf{AI}(f), \min\{\mathsf{deg}(g) + \mathsf{deg}(fg) : g \in \mathcal{B}_n, 1 \leqslant \mathsf{deg}(g) < \mathsf{AI}(f)\}\}$.

2.2 Symmetric Functions, HWBF and Weightwise Degree-d Functions

Recall that the Boolean symmetric functions in n variables are those that are constant on the slice $\mathsf{E}_{k,n}$ for every $k \in [0,n]$. This class of functions has been thoroughly studied in the context of cryptography, see *e.g.*, [6,10,11,14,18,34,35,41,44]. In this article, the symmetric functions that we consider will mainly be the slice indicator function and the majority function.

Definition 9 (Slice Indicator Functions). *The indicator function of the slice of weight* $k \in [0,n]$ *is the function* $\varphi_{k,n} \in \mathcal{B}_n$ *defined by* $\varphi_{k,n}(x) = 1$ *if and only if* $\mathsf{w_H}(x) = k$.

Definition 10 (Majority function). *The majority function in* n *variables is the Boolean function* $\mathsf{Maj}_n \in \mathcal{B}_n$ *defined by* $\mathsf{Maj}_n(x) = 1$ *if and only if* $\mathsf{w_H}(x) \geqslant n/2$.

Bigger families of functions can be obtained by considering functions of bounded degree on each slice. This corresponds to the concept of weightwise degree-d functions introduced in [26] for $d = 1$ and [38] for the general case.

Definition 11 (Weightwise degree-*d* functions, Definition 12 in [38]). *A Boolean function $f \in \mathcal{B}_n^*$ is called weightwise degree-d if it can be written under the form $f = \sum_{k=0}^{n} f_k \varphi_{k,n}$ with $f_k \in \mathcal{B}_n$ of degree at most d. The set of weightwise degree-d functions is denoted by $\mathcal{WD}_n^d$. Additionally, a weightwise degree-d function $f = \sum_{k=0}^{n} f_k \varphi_{k,n}$ is called a cyclic weightwise degree-d function if for all $k \in [0, n]$ and all $x \in \mathbb{F}_2^n$, it holds that $f_k(x) = f_0(O^k(x))$, where $O^k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the cyclic shift by k positions, defined by $O^k(x_1, \ldots, x_n) = (x_{(1+k) \bmod n}, \ldots, x_{(n+k) \bmod n})$, the representatives modulo n being taken as integers in $[1, n]$.*

Various weightwise affine functions (*i.e.*, belonging to $\mathcal{WD}_n^1$) have been exhibited, such as in [15] where the bent functions in Propositions 1 and 2 are weightwise affine, or in [26] to show that no weightwise perfectly balanced function is weightwise affine for $n \geqslant 8$. The arguably best known example of weightwise affine function is the Hidden Weight Bit Function introduced in [7], the one obtained by fixing $f_0 = 0$ and $f_k = x_k$ for $k \in [1, n]$. The cryptographic properties of this function have been studied in [46], showing good algebraic properties for this function.

Definition 12 (Hidden Weight Bit Function). *We call Hidden Weight Bit Function (HWBF) the Boolean function $h \in \mathcal{B}_n$ defined as:*

$$h(x) = \sum_{k=1}^{n} x_k \varphi_{k,n}(x).$$

In [38], the parameters of different functions from $\mathcal{WD}_n^1$ and $\mathcal{WD}_n^2$ are studied experimentally for $n \leqslant 20$, and lower bounds are given for the nonlinearity for all n. These bounds focus on cyclic weightwise quadratic functions and involve sums of binomial coefficients. For simplicity, in the following, we provide only the nonlinearity values of the majority function and HWBF, as these bounds will be used for comparison.

Property 1.

- (*E.g.*, Theorem 3 and Theorem 2 in [23]) The majority function $\mathsf{Maj}_n \in \mathcal{B}_n$ satisfies $\mathsf{NL}(\mathsf{Maj}_n) = 2^{n-1} - \binom{n-1}{\frac{n}{2}}$ and $\deg(\mathsf{Maj}_n) = 2^{\lfloor \log_2(n) \rfloor}$ for even $n \geqslant 2$.
- (Theorem 3 and Theorem 1 in [46]) The HWBF $h \in \mathcal{B}_n$ satisfies $\mathsf{NL}(h) = 2^{n-1} - 2\binom{n-2}{\frac{n-2}{2}}$ for even $n \geqslant 2$ and $\deg(h) = n - 1$ for even $n \geqslant 4$.

2.3 Krawtchouk Polynomials

We use Krawtchouk polynomials and some of their properties to prove one of our main results. We give the necessary definition here and refer to [31] for more details, for instance.

Definition 13 (Krawtchouk polynomials). *The n-th Krawtchouk polynomial of degree $k \in \mathbb{Z}$ is given by $\mathsf{K}_k(x,n) = \sum_{j=0}^{k}(-1)^j \binom{x}{j}\binom{n-x}{k-j}$. Alternatively, the Krawtchouk polynomials can be characterized as the coefficients in the generating function for $(1+z)^{n-x}(1-z)^x$ in the variable z, that is, $(1+z)^{n-x}(1-z)^x = \sum_{k\in\mathbb{Z}} \mathsf{K}_k(x,n)z^k$.*

3 Revisited HWBF and Balancedness

In this part, we will formally define the revisited HWBF function and introduce a quantity that allows us to study its balancedness and nonlinearity.

3.1 Definition and Basic Properties

Definition 14 (Revisited Hidden Weight Bit Function). *For an even integer $n \geqslant 0$, we call revisited HWBF the Boolean function $f \in \mathcal{B}_n$ defined as:*

$$f(x) = \sum_{k=1}^{n} x_k \varphi_{k,n}(x) + \sum_{i=1}^{n/2}(x_i+1)x_{i+n/2}.$$

Since f is the sum of a quadratic function and a weightwise affine function, it is a weightwise quadratic function. Note that, while the HWBF can be computed by first computing the Hamming weight of the input and then applying a linear function, the revisited HWBF can be computed by first computing the Hamming weight of the input and then applying a quadratic function, leading to a similar computational cost for both.

Using the formalism of Definition 11, f is the weightwise quadratic function defined by $f_0(x) = 0$ and $f_k(x) = x_k + \sum_{i=1}^{n/2}(x_i+1)x_{i+n/2}$ for $k \in [1,n]$. This form allows to derive the restricted Walsh transform of f, which can be a useful tool to study the balancedness and bound the nonlinearity of a function.

Proposition 1. *Let $n \geqslant 0$ be an even integer, and let $f \in \mathcal{B}_n$ be the revisited HWBF. Consider any binary vector $a \in \mathbb{F}_2^n$ and any integer $k \in [1,n]$. Define $c = a + e_k + \sum_{i=n/2+1}^{n} e_i$. Then the restricted Walsh transform of f satisfies:*

$$\mathcal{W}_{f,k}(a) = \sum_{x\in\mathsf{E}_{k,n}} (-1)^{\sum_{i=1}^{n/2} x_i x_{i+n/2} + c\cdot x}.$$

Proof. By definition, we have $\mathcal{W}_{f,k}(a) = \sum_{x\in\mathsf{E}_{k,n}}(-1)^{x_k + \sum_{i=1}^{n/2}(x_i+1)x_{i+n/2} + a\cdot x}$. Therefore:

$$\begin{aligned}\mathcal{W}_{f,k}(a) &= \sum_{x\in\mathsf{E}_{k,n}} (-1)^{\sum_{i=1}^{n/2} x_i x_{i+n/2} + \left(x_k + \sum_{i=n/2+1}^{n} x_i + a\cdot x\right)} \\ &= \sum_{x\in\mathsf{E}_{k,n}} (-1)^{\sum_{i=1}^{n/2} x_i x_{i+n/2} + c\cdot x}.\end{aligned}$$

□

Accordingly, we can study the restricted Walsh transform of the revisited HWBF by analyzing the following Boolean function $d_n \in \mathcal{B}_n$.

Definition 15. *Let $n \geqslant 0$ be an even integer. Then we define the Boolean function $d_n \in \mathcal{B}_n$ by:*

$$d_n(x) = \sum_{i=1}^{n/2} x_{2i-1}x_{2i}.$$

Further, for an integer k and a binary vector $a \in \mathbb{F}_2^n$, we define:

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

The $\mathsf{D}_{k,n}(a)$ satisfy a recursive relation.

Proposition 2. *Let $n \geqslant 0$ be an even integer. Then for all integers k and all binary vectors $a \in \mathbb{F}_2^n$, the following hold:*

- *We have $\mathsf{D}_{0,0}(a) = 1$ and $\mathsf{D}_{k,0}(a) = 0$ if $k \neq 0$.*
- *If $n \geqslant 2$, then for $b = (a_1, \ldots, a_{n-2}) \in \mathbb{F}_2^{n-2}$, we have:*

$$\begin{aligned}\mathsf{D}_{k,n}(a) = \mathsf{D}_{k,n-2}(a) &+ \left((-1)^{a_{n-1}} + (-1)^{a_n}\right)\mathsf{D}_{k-1,n-2}(a)\\ &+ (-1)^{1+a_{n-1}+a_n}\mathsf{D}_{k-2,n-2}(a).\end{aligned}$$

Proof. We have that $\mathsf{D}_{0,0}(a) = (-1)^0 = 1$ since $\mathsf{E}_{0,0} = \{\varepsilon\}$ for the empty vector $\varepsilon = a \in \mathbb{F}_2^0$. That $\mathsf{D}_{k,0}(a) = 0$ if $k \neq 0$ follows from $\mathsf{E}_{k,0}$ being empty if $k \neq 0$. Assume now that $n \geqslant 2$. By considering binary vectors $x \in \mathbb{F}_2^n$ as $x = (y, x_{n-1}, x_n)$ for $y \in \mathbb{F}_2^{n-2}$, we get:

$$\begin{aligned}\mathsf{D}_{k,n}(a) &= \sum_{x \in \mathsf{E}_{k,n}} (-1)^{d_n(x)+a\cdot x}\\ &= \sum_{y \in \mathsf{E}_{k,n-2}} (-1)^{d_{n-2}(y)+b\cdot y} + \sum_{y \in \mathsf{E}_{k-1,n-2}} (-1)^{d_{n-2}(y)+b\cdot y+a_{n-1}}\\ &\quad + \sum_{y \in \mathsf{E}_{k-1,n-2}} (-1)^{d_{n-2}(y)+b\cdot y+a_n}\\ &\quad + \sum_{y \in \mathsf{E}_{k-2,n-2}} (-1)^{d_{n-2}(y)+b\cdot y+1+a_{n-1}+a_n}\\ &= \mathsf{D}_{k,n-2}(a) + \left((-1)^{a_{n-1}} + (-1)^{a_n}\right)\mathsf{D}_{k-1,n-2}(a)\\ &\quad + (-1)^{1+a_{n-1}+a_n}\mathsf{D}_{k-2,n-2}(a).\end{aligned}$$

□

Remark 1. We note that Proposition 2 gives three different cases depending on the values of the two last elements of a:

- if $a_{n-1} = 0 = a_n$, then $\mathsf{D}_{k,n}(a) = \mathsf{D}_{k,n-2}(a) + 2\mathsf{D}_{k-1,n-2}(a) - \mathsf{D}_{k-2,n-2}(a)$,
- if $a_{n-1} \neq a_n$, then $\mathsf{D}_{k,n}(a) = \mathsf{D}_{k,n-2}(a) + \mathsf{D}_{k-2,n-2}(a)$,
- if $a_{n-1} = 1 = a_n$, then $\mathsf{D}_{k,n}(a) = \mathsf{D}_{k,n-2}(a) - 2\mathsf{D}_{k-1,n-2}(a) - \mathsf{D}_{k-2,n-2}(a)$.

Remark 2. The recursive formula of Proposition 2 gives different cases depending on the values of the pair (a_{n-1}, a_n). However, the same reasoning applies to any pair of the form (a_{2i-1}, a_{2i}) for $i \in [1, n/2]$. Therefore, the value of $\mathsf{D}_{k,n}(a)$ depends only on the number of pairs (a_{2i-1}, a_{2i}) in a being $(0,0)$, $(1,1)$, $(0,1)$ or $(1,0)$. We give the values of $\mathsf{D}_{k,2}(a)$ for $n = 2$ in Table 1. These values together with Proposition 2 are sufficient to determine any $\mathsf{D}_{k,n}(a)$.

Table 1. Values of $\mathsf{D}_{k,2}(a)$.

a	$(0,0)$	$(0,1)$	$(1,1)$
$\mathsf{D}_{0,2}(a)$	1	1	1
$\mathsf{D}_{1,2}(a)$	2	0	-2
$\mathsf{D}_{2,2}(a)$	-1	1	-1

In the following, we show how the Walsh transform of the revisited HWBF $f \in \mathcal{B}_n$ can be written in terms of the $\mathsf{D}_{k,n}(a)$. Then, in Section 3.2, we use Proposition 2 to determine the balancedness of f, and in Section 4.1 we study the value of $\mathsf{D}_{k,n}(a)$ using generating functions.

Proposition 3. *Let $n \geqslant 0$ be an even integer, and let $f \in \mathcal{B}_n$ be the revisited HWBF. Denote by $\pi : [1,n] \to [1,n]$ the permutation sending the first $n/2$ elements to the odd positions and the $n/2$ last ones to the even positions. Let $a \in \mathbb{F}_2^n$ be a binary vector, and let $b = \pi^{-1}(a) + \sum_{i=1}^{n/2} e_{2i}$. Then the following holds true:*

$$\mathcal{W}_f(a) = 1 + \sum_{k=1}^{n} \mathsf{D}_{k,n}(a).$$

Proof. For every $k \in [1,n]$, we have by Proposition 1 that:

$$\begin{aligned}
\mathcal{W}_{f,k}(a) &= \sum_{x \in \mathsf{E}_{k,n}} (-1)^{f(x)+a\cdot x} \\
&= \sum_{\pi(x) \in \mathsf{E}_{k,n}} (-1)^{f(\pi(x))+a\cdot \pi(x)} \\
&= \sum_{\pi(x) \in \mathsf{E}_{k,n}} (-1)^{\sum_{i=1}^{n/2} x_{\pi(i)}x_{\pi(i+n/2)} + x_{\pi(k)} + a\cdot\pi(x) + \sum_{i=1}^{n/2} x_{\pi(i+n/2)}} \\
&= \sum_{\pi(x) \in \mathsf{E}_{k,n}} (-1)^{d_n(x) + x_{\pi(k)} + \pi^{-1}(a)\cdot x + \sum_{i=1}^{n/2} x_{2i}} \\
&= \sum_{x \in \mathsf{E}_{k,n}} (-1)^{d_n(x) + (b + \pi(e_k))\cdot x} \\
&= \mathsf{D}_{k,n}(a).
\end{aligned}$$

We conclude by applying $\mathcal{W}_f(a) = 1 + \sum_{k=1}^{n} \mathcal{W}_{f,k}(a)$. □

3.2 Balancedness of f

In this part, we determine for which values of n the revisited HWBF $f \in \mathcal{B}_n$ is balanced, using the expression of its Walsh transform in terms of the $\mathsf{D}_{k,n}(a)$ and the recursive relation of these quantities.

Theorem 1. *Let $n \geqslant 2$ be an even integer. Then the Walsh transform of the revisited HWBF $f \in \mathcal{B}_n$ at 0_n satisfies:*

$$\mathcal{W}_f(0_n) = \begin{cases} 0 & \text{if } n \equiv 0 \bmod 4, \\ -2\binom{(n-2)/2}{(n-2)/4} & \text{if } n \equiv 2 \bmod 4. \end{cases}$$

Accordingly, f is balanced if and only if $n \equiv 0 \bmod 4$.

Proof. We use Proposition 3, applying Remark 2 and that $\pi^{-1}(0_n) = 0_n$:

$$\begin{aligned} \mathcal{W}_f(0_n) &= 1 + \sum_{k=1}^{n} \mathsf{D}_{k,n}(a) \\ &= 1 + \sum_{k=1}^{n/2} \mathsf{D}_{k,n}(a) + \sum_{k=n/2+1}^{n} \mathsf{D}_{k,n}(a). \end{aligned}$$

Using the recursive relation from Proposition 2, we obtain:

$$\begin{aligned} \mathsf{D}_{k,n}(a) = \mathsf{D}_{k,n-2}(a) \\ + \mathsf{D}_{k-2,n-2}(a). \end{aligned}$$

By reapplying this $n/2 - 1$ times, we obtain:

$$\begin{aligned} \mathsf{D}_{k,n}(a) &= \sum_{i=0}^{n/2-1} \binom{n/2-1}{i} \mathsf{D}_{k-2i,2}(a) \\ &= \binom{n/2-1}{k/2} \mathsf{D}_{0,2}(a) + \binom{n/2-1}{(k-1)/2} \mathsf{D}_{1,2}(a) \\ &\quad + \binom{n/2-1}{k/2-1} \mathsf{D}_{2,2}(a) \\ &= \binom{n/2-1}{k/2} - 2\binom{n/2-1}{(k-1)/2} - \binom{n/2-1}{k/2-1}. \end{aligned}$$

We similarly get:

$$\mathsf{D}_{k,n}(a) = \binom{n/2-1}{k/2} + 2\binom{n/2-1}{(k-1)/2} - \binom{n/2-1}{k/2-1}.$$

Then, combining both, we obtain:

$$\begin{aligned}
\mathcal{W}_f(0_n) &= 1 + \sum_{k=1}^{n/2} \mathsf{D}_{k,n}(a) + \sum_{k=n/2+1}^{n} \mathsf{D}_{k,n}(a) \\
&= \sum_{k=0}^{n/2} \left(\binom{n/2-1}{k/2} - 2\binom{n/2-1}{(k-1)/2} - \binom{n/2-1}{k/2-1} \right) \\
&\quad + \sum_{k=n/2+1}^{n} \left(\binom{n/2-1}{k/2} + 2\binom{n/2-1}{(k-1)/2} - \binom{n/2-1}{k/2-1} \right) \\
&= \sum_{k=0}^{n} \left(\binom{n/2-1}{k/2} - \binom{n/2-1}{k/2-1} \right) \\
&\quad + 2 \left(\sum_{k=n/2+1}^{n} \binom{n/2-1}{(k-1)/2} - \sum_{k=0}^{n/2} \binom{n/2-1}{(k-1)/2} \right) \\
&= 0 + 2 \left(\sum_{k=n/2+1}^{n} \binom{n/2-1}{(k-1)/2} - \sum_{k=0}^{n/2} \binom{n/2-1}{(k-1)/2} \right) \\
&= 2 \left(\sum_{i=\lceil n/4 \rceil}^{n/2-1} \binom{n/2-1}{i} - \sum_{i=0}^{\lfloor (n-2)/4 \rfloor} \binom{n/2-1}{i} \right).
\end{aligned}$$

The result follows by applying that $\binom{n}{k} = \binom{n}{n-k}$ for all integers $n \geqslant 0$ and k. □

4 Extensive Study of the $\mathsf{D}_{k,n}(a)$ and Bounds on the Walsh Spectrum of f

This section examines the values of $\mathsf{D}_{k,n}(a)$ through the use of generating functions. To begin, in Section 4.1, we determine essential characteristics of these values. Subsequently, in Section 4.2, we employ Cauchy's estimate to bound the absolute value of the $\mathsf{D}_{k,n}(a)$. This approach allows us to also bound the absolute value of the Walsh transform of the revisited HWBF, thereby constraining the nonlinearity. Lastly, in Section 4.3, we illustrate how this result can be extended to bound the nonlinearity of a family of weightwise quadratic functions.

4.1 Study of the $\mathsf{D}_{k,n}(a)$ through Generating Functions

Definition 16. *Let $n \geqslant 0$ be an even integer. For $a \in \mathbb{F}_2^n$, we denote by $p = p(a)$ the number of $i \geqslant 1$ for which $(a_{2i-1}, a_{2i}) = (0,0)$, by $q = q(a)$ the number of $i \geqslant 1$ for which $(a_{2i-1}, a_{2i}) = (1,1)$, and by $r = r(a)$ the number of $i \geqslant 1$ for which $(a_{2i-1}, a_{2i}) \in \{(0,1),(1,0)\}$. We then have $p + q + r = n/2$. We further introduce the integer polynomial $P_a(z)$ given by the following expression:*

$$P_a(z) = (-z^2 + 2z + 1)^p \cdot (-z^2 - 2z + 1)^q \cdot (z^2 + 1)^r.$$

Proposition 4. *For every even integer $n \geqslant 0$ and every binary vector $a \in \mathbb{F}_2^n$, the following holds:*

$$\sum_{k\in\mathbb{Z}} \mathsf{D}_{k,n}(a)z^k = P_a(z).$$

Proof. We proceed by induction on even $n \geqslant 0$. For the base case $n = 0$, we consider the empty vector $a = \varepsilon \in \mathbb{F}_2^0$; it satisfies $P_a(z) = 1$, while $\mathsf{D}_{0,0}(a) = 1$ and $\mathsf{D}_{k,0}(a) = 0$ if $k \neq 0$ by Proposition 2. For the inductive step, let $n \geqslant 2$ be even, and assume that the corresponding formula holds for $n-2$. Using the recursive formula for $\mathsf{D}_{k,n}(a)$ from Proposition 2 with $b = (a_1, \ldots, a_{n-2}) \in \mathbb{F}_2^{n-2}$, we have:

$$\begin{aligned}
\sum_{k\in\mathbb{Z}} \mathsf{D}_{k,n}(a)z^k &= \sum_{k\in\mathbb{Z}} \mathsf{D}_{k,n-2}(a)z^k + \big((-1)^{a_{n-1}} + (-1)^{a_n}\big) \sum_{k\in\mathbb{Z}} \mathsf{D}_{k-1,n-2}(a)z^k \\
&\qquad + (-1)^{1+a_{n-1}+a_n} \sum_{k\in\mathbb{Z}} \mathsf{D}_{k-2,n-2}(a)z^k \\
&= P_b(z) + \big((-1)^{a_{n-1}} + (-1)^{a_n}\big) z P_b(z) + (-1)^{1+a_{n-1}+a_n} z^2 P_b(z) \\
&= P_b(z) \cdot \Big(z^2(-1)^{1+a_{n-1}+a_n} + z\big((-1)^{a_{n-1}} + (-1)^{a_n}\big) + 1\Big) \\
&= P_a(z).
\end{aligned}$$

□

Remark 3. We have already argued in Remark 2 that $\mathsf{D}_{k,n}(a)$ only depends on $p(a)$, $q(a)$ and $r(a)$. This observation can also be obtained from Proposition 4: since $P_a(z)$ only depends on $p(a)$, $q(a)$ and $r(a)$ (by definition), we deduce that also $\mathsf{D}_{k,n}(a)$ only depends on $p(a)$, $q(a)$ and $r(a)$. Therefore, for any $p, q, r \geqslant 0$ satisfying $p+q+r = n/2$, it makes sense to introduce the notation $\mathsf{D}_{k,n}^{p,q,r} = \mathsf{D}_{k,n}(a)$, where $a \in \mathbb{F}_2^n$ is any vector with $(p(a), q(a), r(a)) = (p, q, r)$. We will make use of this notation in Section 5.1.

Proposition 5. *For every even integer $n \geqslant 0$, for every binary vector $a \in \mathbb{F}_2^n$, and for every integer k, the following holds:*

$$\mathsf{D}_{n-k,n}(a) = (-1)^{p+q+k}\mathsf{D}_{k,n}(a).$$

Proof. We define the reverse polynomial $Q_a(z)$ as the degree n polynomial where each coefficient of z^k in $Q_a(z)$, for any k, is equal to the coefficient of z^{n-k} in $P_a(z)$. Then we have:

$$\begin{aligned}
Q_a(z) &= z^n P_a(1/z) \\
&= (z^2 + 2z - 1)^p \cdot (z^2 - 2z - 1)^q \cdot (z^2 + 1)^r \\
&= (-1)^{p+q}(-z^2 - 2z + 1)^p \cdot (-z^2 + 2z + 1)^q \cdot (z^2 + 1)^r \\
&= (-1)^{p+q} P_a(-z).
\end{aligned}$$

Therefore, the coefficient of z^k in $Q_a(z)$, which is $\mathsf{D}_{n-k,n}(a)$, is equal to the coefficient of z^k in $(-1)^{p+q}P_a(-z)$, which is $(-1)^{p+q+k}\mathsf{D}_{k,n}(a)$. □

Corollary 1. *Let $n \geqslant 0$ be an even integer, and let $a \in \mathbb{F}_2^n$ be a binary vector. If $r = r(a)$ is odd, then it holds that $\mathsf{D}_{n/2,n}(a) = 0$.*

Proof. By Proposition 5, it holds that $\mathsf{D}_{n/2,n}(a) = (-1)^{p+q+n/2}\mathsf{D}_{n/2,n}(a) = -\mathsf{D}_{n/2,n}(a)$ because $p+q+n/2$ is odd: $p+q+n/2 \equiv n/2-p-q \equiv r \equiv 1 \bmod 2$. □

Another immediate case for zero coefficients is the following.

Proposition 6. *Let $n \geqslant 0$ be an even integer, and let $a \in \mathbb{F}_2^n$ be a binary vector. If k is an odd integer and $p = q$, then it holds that $\mathsf{D}_{k,n}(a) = 0 = \mathsf{D}_{n-k,n}(a)$.*

Proof. If $p = q$, we have $P_a(z) = (z^4 - 6z^2 + 1)^p \cdot (z^2 + 1)^r$, which can be seen as a polynomial in z^2. Thus, the coefficient $\mathsf{D}_{k,n}(a)$ in $P_a(z)$ of z^k for odd k must be zero. It also follows that $\mathsf{D}_{n-k,n}(a) = 0$ by Proposition 5. □

Remark 4. We can also use Proposition 4 to obtain $\mathsf{D}_{k,n}(a)$ through differentiation and evaluation at $z = 0$, to get $k! \cdot \mathsf{D}_{k,n}(a) = \frac{\mathrm{d}^k}{\mathrm{d}^k z} P_a(z)|_{z=0}$. Using this formula, we can for instance use a computer algebra system to deduce $\mathsf{D}_{k,n}(a)$ for small values of k, see Table 2. Note that even though the expression for $\mathsf{D}_{3,n}(a)$ involves a division by 3, its evaluation at specific values for (p, q, r) will always yield integers. Indeed, either $p - q \equiv 0 \bmod 3$, or $(p - q)^2 \equiv 1 \bmod 3$, in which case $2(p - q)^2 + 7 \equiv 0 \bmod 3$.

Table 2. Values of $\mathsf{D}_{k,n}(a)$ for small values of k.

k	$\mathsf{D}_{k,n}(a)$
0	1
1	$2(p-q)$
2	$2(p-q)^2 - 3(p+q) + r$
3	$\frac{2}{3}(p-q)\left(2(p-q)^2 - 9(p+q) + 3r + 7\right)$

From differentiation, we can get more cases in which $\mathsf{D}_{k,n}(a) = 0$.

Proposition 7. *Let $n \geqslant 0$ be an even integer, and let $a \in \mathbb{F}_2^n$ be a binary vector.*

1. *For every integer $s \geqslant 0$, define $\ell_s = s(s-1)$. If $n = 16m$ and $\{p, q\} = \{m + \ell_s, m + \ell_{s+1}\}$ for integers $m, s \geqslant 0$, then $\mathsf{D}_{2,n}(a) = 0 = \mathsf{D}_{n-2,n}(a)$.*
2. *For every integer $s \geqslant 0$, define $\ell_s = \left(6s^2 + 6s + (-1)^s(2s+1) - 1\right)/8$. If $n = 16m + 2$ and $\{p, q\} = \{m + \ell_s, m + \ell_{s+2}\}$ for integers $m, s \geqslant 0$, then $\mathsf{D}_{3,n}(a) = 0 = \mathsf{D}_{k-3,n}(a)$.*
3. *For every integer $s \geqslant 0$, define $\ell_s = s^2$. If $n = 16m + 4$ and $\{p, q\} = \{m + \ell_s, m + \ell_{s+1}\}$ for integers $m, s \geqslant 0$, then $\mathsf{D}_{2,n}(a) = 0 = \mathsf{D}_{n-2,n}(a)$.*
4. *For every integer $s \geqslant 0$, define $\ell_s = \left(6s^2 + 6s - (-1)^s(2s+1) + 1\right)/8$. If $n = 16m + 6$ and $\{p, q\} = \{m + \ell_s, m + \ell_{s+2}\}$ for integers $m, s \geqslant 0$, then $\mathsf{D}_{3,n}(a) = 0 = \mathsf{D}_{n-3,n}(a)$.*

Proof. We use the expressions from Table 2, and replace p, q and r by their respective values. For instance, for the case $n = 16m$, we replace p, q and r by $m + s(s-1)$, $m + s(s+1)$ and $6m - 2s^2$, respectively, in the expression $\mathsf{D}_{2,n}(a) = 2(p-q)^2 - 3(p+q) + r$, which yields $\mathsf{D}_{2,n}(a) = 0$. This checking can be automatized by a computer algebra system, for which we provide a SageMath implementation.[3] □

Remark 5. There are other instances where $\mathsf{D}_{k,n}(a) = 0$ which have not been described by any of the previous results. For instance, we have $\mathsf{D}_{4,34}(a) = 0$ if $\{p, q\} = \{1, 2\}$.

Using Proposition 4, we can also deduce some sums involving the $\mathsf{D}_{k,n}(a)$.

Proposition 8. *Let $n \geqslant 0$ be an even integer, and let $a \in \mathbb{F}_2^n$ be a binary vector.*

1. *The sum and alternating sum over k of the $\mathsf{D}_{k,n}(a)$ are, respectively:*

$$\sum_{k\in\mathbb{Z}} \mathsf{D}_{k,n}(a) = (-1)^q 2^{n/2}, \qquad \sum_{k\in\mathbb{Z}} (-1)^k \mathsf{D}_{k,n}(a) = (-1)^p 2^{n/2}.$$

2. *The sum over the even and the odd k of the $\mathsf{D}_{k,n}(a)$ are, respectively:*

$$\sum_{k\in\mathbb{Z}} \mathsf{D}_{2k,n}(a) = 2^{n/2-1}\big((-1)^q + (-1)^p\big),$$
$$\sum_{k\in\mathbb{Z}} \mathsf{D}_{2k+1,n}(a) = 2^{n/2-1}\big((-1)^q - (-1)^p\big).$$

Proof. For the sum and the alternating sum, we compute $P_a(1)$ and $P_a(-1)$, respectively. The sum of the $\mathsf{D}_{k,n}(a)$ over the even (respectively, odd) k is obtained by adding (respectively, subtracting) these two sums and dividing by 2. □

4.2 Bounding the Walsh Transform of f using the Cauchy Estimate

We recall Cauchy's estimate on holomorphic functions.

Property 2 (Cauchy's estimate, e.g., Theorem 10.26 in [43]). Let w be a complex number, and let $R > 0$ be some radius. Let $D \subseteq \mathbb{C}$ be a set containing every complex number z satisfying $|z - w| \leqslant R$. Let $f : D \to \mathbb{C}$ be a holomorphic function, and let M_R be the maximum of the absolute value of f on the circle defined by $|z - w| = R$. Then for every integer $k \geqslant 0$, the k-th derivative of f evaluated at w can be bounded, in absolute value, by $\left|\frac{\mathrm{d}^k}{\mathrm{d}^k z} f(z)|_{z=w}\right| \leqslant \frac{k! \cdot M_R}{R^k}$.

Theorem 2. *Let $n \geqslant 0$ be an even integer, and let $a \in \mathbb{F}_2^n$ be a binary vector. Then, for every integer $k \in [0, n]$, it holds that:*

$$|\mathsf{D}_{k,n}(a)| \leqslant 2^{3n/4}.$$

[3] `https://github.com/se-tim/Revisited-HWBF.git`

Proof. From Remark 4 we have $k! \cdot \mathsf{D}_{k,n}(a) = \frac{\mathrm{d}^k}{\mathrm{d}^k z} P_a(z)|_{z=0}$. Choosing $f = P_a$, $w = 0$ and $R = 1$ in Property 2 then gives $|\mathsf{D}_{k,n}(a)| = \frac{1}{k!}\left|\frac{\mathrm{d}^k}{\mathrm{d}^k z} P_a(z)|_{z=0}\right| \leqslant M$, where M is the maximum of $|P_a(z)|$ on the complex circle $\mathsf{c}_1 = \{z \in \mathbb{C} : |z| = 1\}$. We claim, and prove below, that the maximum of $\left|-z^2 + 2z + 1\right|$ on c_1 is $2\sqrt{2}$. This implies that the maximum of $\left|-z^2 - 2z + 1\right|$ on c_1 is $2\sqrt{2}$ as well because $-z^2 - 2z + 1 = -(-z)^2 + 2(-z) + 1$. Since the maximum of $\left|z^2 + 1\right|$ on c_1 is $2 < 2\sqrt{2}$, it follows that $|\mathsf{D}_{k,n}(a)| \leqslant M \leqslant (2\sqrt{2})^{p+q} 2^r \leqslant (2\sqrt{2})^{n/2}$.

We prove that the maximum of $|-z^2 + 2z + 1|$ on c_1 is $2\sqrt{2}$ by showing that the one of $|-z^2 + 2z + 1|^2$ on c_1 equals 8. Using that $|w|^2 = w\overline{w}$ for every complex number w, we obtain for all $z \in \mathsf{c}_1$:

$$\left|-z^2 + 2z + 1\right|^2 = \left(z^2 - 2z - 1\right)\left(\overline{z}^2 - 2\overline{z} - 1\right) = 6 - \left(z^2 + \overline{z}^2\right) = 6 - 2\mathrm{Re}\left(z^2\right).$$

Since the minimum of $\mathrm{Re}\left(z^2\right)$ on c_1 is -1, we conclude that the maximum of $|-z^2 + 2z + 1|^2$ on c_1 is $6 - 2(-1) = 8$. □

Corollary 2. *Let $n \geqslant 0$ be an even integer, and let $f \in \mathcal{B}_n$ be the revisited HWBF. Then for every binary vector $a \in \mathbb{F}_2^n$, it holds that:*

$$|\mathcal{W}_f(a)| \leqslant 1 + n \cdot 2^{3n/4}.$$

Equivalently, it holds that $\mathsf{NL}(f) \geqslant 2^{n-1} - \frac{1}{2} - 2^{3n/4 + \log_2(n) - 1}$.

Proof. It is enough to prove the bound on $|\mathcal{W}_f(a)|$; the bound on the nonlinearity of f comes from the second expression of Definition 6. We have previously established in Proposition 3 that $\mathcal{W}_f(a) = 1 + \sum_{k=1}^{n} \mathsf{D}_{k,n}(a)$ for some vectors $b_k \in \mathbb{F}_2^n$. Then, applying the triangle inequality together with Theorem 2 yields $|\mathcal{W}_f(a)| \leqslant 1 + \sum_{k=1}^{n} |\mathsf{D}_{k,n}(a)| \leqslant 1 + n \cdot 2^{3n/4}$. □

4.3 Generalization to a Family of Weightwise Quadratic Functions

In this part, we generalize the results of Section 4.2 to all weightwise quadratic functions f such that, for every $k \in [1, n]$, the function f_k (as defined in Definition 11) contains exactly t quadratic terms with no shared variables. We skip the proofs of the following results; they are provided in the appendix, see Section A.

Definition 17. *For an even integer $n \geqslant 0$ and an integer $t \in [0, n/2]$, we define the Boolean function $d_{t,n} \in \mathcal{B}_n$ by:*

$$d_{t,n}(x) = \sum_{i=1}^{t} x_{2i-1} x_{2i}.$$

Further, for an integer k and a binary vector $a \in \mathbb{F}_2^n$, we define:

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

In particular, it holds that $d_{n/2,n}(x) = d_n(x)$ and $\mathsf{D}_{n/2,k,n}(a) = \mathsf{D}_{k,n}(a)$. We now focus on the $\mathsf{D}_{t,k,n}(a)$.

Proposition 9. *Let $n \geqslant 0$ be an even integer, and let $t \in [0, n/2]$. Let $a \in \mathbb{F}_2^n$ be a binary vector, and write $a = (b, c)$ with $b \in \mathbb{F}_2^{2t}$ and $c \in \mathbb{F}_2^{n-2t}$. Then the following holds for all integers k:*

$$\mathsf{D}_{t,k,n}(a) = \sum_{\ell=0}^{2t} \mathsf{D}_{\ell,2t}(a) \cdot \mathsf{K}_{k-\ell}(\mathsf{w}_\mathsf{H}(c), n-2t).$$

Definition 18. *Let $n \geqslant 0$ be an even integer, and let $t \in [0, n/2]$. Let $a = (b, c) \in \mathbb{F}_2^n$ be a binary vector with $b \in \mathbb{F}_2^{2t}$ and $c \in \mathbb{F}_2^{n-2t}$. By letting $u = u_t(a) = n - 2t - \mathsf{w}_\mathsf{H}(c)$ and $v = v_t(a) = \mathsf{w}_\mathsf{H}(c)$, we introduce the polynomial $P_{t,a}(z)$ given by the following expression:*

$$P_{t,a}(z) = P_b(z) \cdot (1+z)^u \cdot (1-z)^v.$$

Proposition 10. *For every even integer $n \geqslant 0$, every integer $t \in [0, n/2]$ and every binary vector $a \in \mathbb{F}_2^n$, the following holds:*

$$\sum_{k \in \mathbb{Z}} \mathsf{D}_{t,k,n}(a) z^k = P_{t,a}(z).$$

This result can in turn be used to bound the $\mathsf{D}_{t,k,n}(a)$. The following result is a direct generalization of Theorem 2.

Theorem 3. *Let $n \geqslant 0$ be an even integer, and let $t \in [0, n/2]$. We define $\lambda = t/n$, as well as:*

$$\mu = \mu(\lambda) = \begin{cases} \frac{\lambda+1}{2} + \frac{1}{2}\log_2\left(\frac{\left(-\lambda^2+2\lambda+\lambda\sqrt{\lambda^2-4\lambda+2}\right)^\lambda}{\left(1-\lambda+\sqrt{\lambda^2-4\lambda+2}\right)^{2\lambda-1}}\right) & \text{if } \lambda > \frac{1}{6}, \\ 1-\lambda & \text{if } \lambda \leqslant \frac{1}{6}. \end{cases}$$

Then, for all $a \in \mathbb{F}_2^n$ and all $k \in [0, n]$, the following hold:

$$|\mathsf{D}_{t,k,n}(a)| \leqslant 2^{\mu n}, \qquad |\mathcal{W}_{d_{t,n}}(a)| \leqslant 1 + n \cdot 2^{\mu n}.$$

The curve of $\lambda \mapsto \mu(\lambda)$ defined in the above Theorem 3 is represented in Figure 1. Observe that $\mu(1/2) = 3/4$, which corresponds to Theorem 2.

5 Experiments and Comparisons

In this section, we establish a tighter bound on the absolute value of the Walsh transform of the revisited HWBF for even $n \in [1, 80]$. We then compare the nonlinearity of this function to that of other functions suited to similar use cases, such as the HWBF or the weightwise cyclic functions from [38].

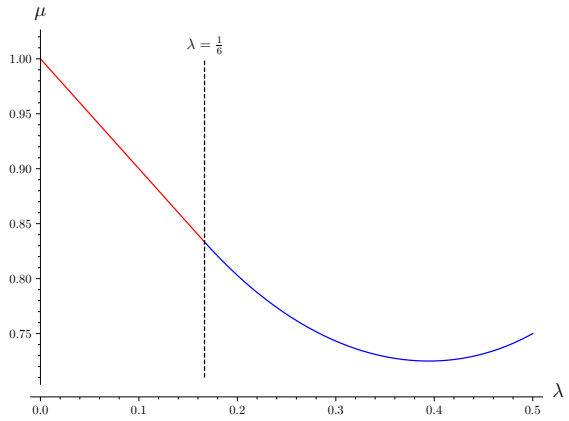

Fig. 1. The curve of $\lambda \mapsto \mu(\lambda)$ with $0 \leqslant \lambda \leqslant \frac{1}{2}$ from Theorem 3.

5.1 Experimentally Bounding the Walsh Transform of f

Following Corollary 2, we deduce that $|\mathcal{W}_f(a)| \leqslant 1 + n \cdot 2^{3n/4}$ for every even integer $n \geqslant 0$ and every binary vector $a \in \mathbb{F}_2^n$, where $f \in \mathcal{B}_n$ denotes the revisited HWBF. This is a somewhat pessimistic bound. In this part, we discuss how a tighter bound on $|\mathcal{W}_f(a)|$ can be obtained in polynomial time in n.

This method is based on the identity given in Proposition 3. For this, consider a vector $b \in \mathbb{F}_2^n$; we write $(p, q, r) = (p(b), q(b), r(b))$. Also, for $k \in [1, n]$, let $b_k = b + \pi(e_k)$ and $(p_k, q_k, r_k) = (p(b_k), q(b_k), r(b_k))$, where $\pi : [1, n] \to [1, n]$ is again the permutation sending the first $n/2$ elements to the odd positions and the $n/2$ last ones to the even positions. Notice first that for every integer $k \in [1, n]$, it holds that $(p_k, q_k, r_k) \in \{(p \pm 1, q, r \mp 1), (p, q \pm 1, r \mp 1)\}$. Furthermore, observe that if $k \in [0, n/2]$ and $(p_k, q_k, r_k) = (p + \alpha, q + \beta, r + \gamma)$ for $\{\alpha, \beta, \gamma\} = \{0, \pm 1\}$ with $\gamma \neq 0$, then we have $(p_{k+n/2}, q_{k+n/2}, r_{k+n/2}) = (p+\alpha', q+\beta', r+\gamma')$ for some $\{\alpha', \beta', \gamma'\} = \{0, \pm 1\}$ with $\gamma' \neq 0$, where α',β' and γ' only depend on α, β and γ. Explicitly, we have $(\alpha', \beta', \gamma') = (\alpha, \beta, \gamma)$ if $\gamma = 1$ and $(\alpha', \beta', \gamma') = (\beta, \alpha, \gamma)$ if $\gamma = -1$.

In the following discussion, we outline a method to determine an upper bound on $\max_{a \in \mathbb{F}_2^n} \mathcal{W}_f(a)$. A similar approach can be applied to find a lower bound on $\min_{a \in \mathbb{F}_2^n} \mathcal{W}_f(a)$, and by utilizing both, we can also obtain an upper bound on $\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_f(a)|$ by making use of the following identity:

$$\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_f(a)| = \max\left(\max_{a \in \mathbb{F}_2^n} \mathcal{W}_f(a), -\min_{a \in \mathbb{F}_2^n} \mathcal{W}_f(a) \right).$$

For each $k \in [1, n/2]$, we select $\{\alpha_k, \beta_k, \gamma_k\} = \{0, \pm 1\}$ with $\gamma_k \neq 0$ such that the following expression, based on the notation introduced in Remark 3, is defined and maximized:

$$B_k^{p,q,r} = \mathsf{D}_{k,n}^{p+\alpha_k, q+\beta_k, r+\gamma_k} + \mathsf{D}_{k+n/2,n}^{p+\alpha'_k, q+\beta'_k, r+\gamma'_k}.$$

This implies that $\mathsf{D}_{k,n}(a) + \mathsf{D}_{k+n/2,n}(a) \leqslant B_k^{p,q,r}$ for every $k \in [1, n/2]$, leading to the conclusion that $\sum_{k=1}^{n} \mathsf{D}_{k,n}(a) \leqslant \sum_{k=1}^{n/2} B_k^{p,q,r}$. As a result, we derive the following upper bound:

$$\max_{a \in \mathbb{F}_2^n} \mathcal{W}_f(a) \leqslant 1 + \max_{p+q+r=n/2} \sum_{k=1}^{n/2} B_k^{p,q,r}. \tag{1}$$

Under the assumption that the values of $\mathsf{D}_{k,n}^{p,q,r}$ have already been computed for all $k \in [1, n]$ and for all triplets (p, q, r) satisfying $p + q + r = n/2$, the bound in equation (1) can be determined with a computational complexity of $\mathcal{O}(n^3)$. This is because there are $\mathcal{O}(n^2)$ possible triplets (p, q, r) that meet the condition $p + q + r = n/2$, and the summation itself can be computed in $\mathcal{O}(n)$ steps.

We consider now the complexity involved in computing the values of $\mathsf{D}_{k,n}^{p,q,r}$ for all $k \in [1, n]$ and all triplets (p, q, r) satisfying $p + q + r = n/2$. We claim that this computation has a complexity of $\mathcal{O}(n^3 \log n)$. Towards this, it is sufficient to expand $(-z^2 + 2z + 1)^p \cdot (-z^2 - 2z + 1)^q \cdot (z^2 + 1)^r$ for all triplets (p, q, r) such that $p + q + r = n/2$; this is due to Proposition 4.

To achieve this, we first precompute the expanded polynomial $(-z^2 + 2z + 1)^p$ for each $p \in [0, n/2]$. This can be done recursively using the formula $(-z^2 + 2z + 1)^{p+1} = (-z^2 + 2z + 1) \cdot (-z^2 + 2z + 1)^p$. For each p, this requires $\mathcal{O}(n)$ arithmetic computations. Performing this for every p results in a total complexity of $\mathcal{O}(n^2)$. The same approach can be used to expand the polynomials $(-z^2 - 2z + 1)^q$ and $(z^2 + 1)^r$, resulting in an overall complexity of $\mathcal{O}(n^2)$ for all $p, q, r \in [0, n/2]$.

Finally, for each triplet (p, q, r) satisfying $p + q + r = n/2$, we multiply the three expanded polynomials $(-z^2 + 2z + 1)^p$, $(-z^2 - 2z + 1)^q$ and $(z^2 + 1)^r$. These two multiplications are performed in $\mathcal{O}(n \log n)$ operations by using the fast Fourier transform. Given that there are $\mathcal{O}(n^2)$ triplets (p, q, r) to consider, we conclude that precomputing the values $\mathsf{D}_{k,n}^{p,q,r}$ for all $k \in [1, n]$ and all triplets (p, q, r) has a complexity of $\mathcal{O}(n^3 \log n)$, making the overall complexity of the procedure also $\mathcal{O}(n^3 \log n)$.

In Table 3, we compare the exact values of $\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_f(a)|$ for small values of n (calculated using SageMath) to the bound B_n obtained through the above method and to the bound from Corollary 2. Additionally, Table 4 provides the values of the bound B_n for all even values of $n \in [1, 80]$. The method described above offers a tighter bound compared to Corollary 2. Its polynomial complexity makes it possible to extend the analysis well beyond the limitations imposed by a full computation of the Walsh spectrum, which requires a complexity of $\mathcal{O}(n2^n)$. We provide a SageMath implementation to obtain the bound B_n.[4]

5.2 Comparison of the Nonlinearity

In this part, we compare the nonlinearity of the revisited HWBF with other weightwise quadratic functions considered for similar use-cases, such as the majority function, the HWBF and the cyclic weightwise functions studied in [38].

[4] `https://github.com/se-tim/Revisited-HWBF.git`

Table 3. The actual $\max_{a\in\mathbb{F}_2^n} |\mathcal{W}_f(a)|$ compared to the bound B_n and the theoretical bound from Corollary 2.

n	$\max_a \lvert\mathcal{W}_f(a)\rvert$	B_n	$\lfloor 1 + n \cdot 2^{3n/4} \rfloor$
2	2	2	6
4	8	8	33
6	20	28	136
8	52	76	513
10	108	212	1 811
12	292	596	6 145
14	700	1 828	20 275
16	2 176	5 196	65 537
18	4 964	14 668	208 535
20	14 968	41 468	655 361
22	34 232	118 544	2 039 002
24	109 648	325 188	6 291 457

Table 4. Approximate values of B_n for various values of n.

n	$\approx B_n$
2	$2.00 \cdot 10^0$
4	$8.00 \cdot 10^0$
6	$2.80 \cdot 10^1$
8	$7.60 \cdot 10^1$
10	$2.12 \cdot 10^2$
12	$5.96 \cdot 10^2$
14	$1.83 \cdot 10^3$
16	$5.20 \cdot 10^3$
18	$1.47 \cdot 10^4$
20	$4.15 \cdot 10^4$

n	$\approx B_n$
22	$1.19 \cdot 10^5$
24	$3.25 \cdot 10^5$
26	$9.59 \cdot 10^5$
28	$2.68 \cdot 10^6$
30	$7.65 \cdot 10^6$
32	$2.14 \cdot 10^7$
34	$6.25 \cdot 10^7$
36	$1.76 \cdot 10^8$
38	$5.03 \cdot 10^8$
40	$1.40 \cdot 10^9$

n	$\approx B_n$
42	$4.01 \cdot 10^9$
44	$1.12 \cdot 10^{10}$
46	$3.21 \cdot 10^{10}$
48	$8.91 \cdot 10^{10}$
50	$2.56 \cdot 10^{11}$
52	$7.12 \cdot 10^{11}$
54	$2.05 \cdot 10^{12}$
56	$5.73 \cdot 10^{12}$
58	$1.65 \cdot 10^{13}$
60	$4.59 \cdot 10^{13}$

n	$\approx B_n$
62	$1.32 \cdot 10^{14}$
64	$3.66 \cdot 10^{14}$
66	$1.05 \cdot 10^{15}$
68	$2.93 \cdot 10^{15}$
70	$8.40 \cdot 10^{15}$
72	$2.33 \cdot 10^{16}$
74	$6.71 \cdot 10^{16}$
76	$1.87 \cdot 10^{17}$
78	$5.39 \cdot 10^{17}$
80	$1.51 \cdot 10^{18}$

In Figure 2, we compare bounds for the values of $\max_{a\in\mathbb{F}_2^n} |\mathcal{W}_f(a)|$ for various functions $f \in \mathcal{B}_n$, where a smaller maximum indicates better nonlinearity, see Definition 6. We present values for n up to 80, which is sufficient for examining the asymptotic behavior of the different bounds. The bound on the cyclic weightwise linear functions stems from [38]. With the notation from Definition 11, these functions f satisfy $f_0(x) = b \cdot x$ for $\mathsf{w_H}(b)$ odd; therefore, this represents, for instance, an upper bound for the HWBF. The bound also applies to the cyclic weightwise quadratic function f defined by $f_0(x) = x_1 + x_2x_3$. Next, the bound for the majority function and the HWBF comes from Property 1; we use a single curve here because the nonlinearity difference between these two functions is too small to be distinguished on a logarithmic scale. The theoretical and experimental bounds for the revisited HWBF come from Corollary 2 and Section 5.1, respectively.

The revisited HWBF demonstrates significantly better performance compared to the majority function, the original HWBF and the functions studied in [38]. Its theoretical bound on $\max_{a\in\mathbb{F}_2^n} |\mathcal{W}_f(a)|$ reveals an asymptotic slope of 3/4 on a logarithmic scale, contrasting with the slope of 1 for the majority function, the HWBF, and the bounds proven in [38]. Notably, the two curves for the revisited HWBF appear to share this asymptotic slope of 3/4, supporting the effectiveness of Corollary 2 and the stronger Theorem 3 in capturing asymptotic behavior.

We also compare in Table 5 the precise nonlinearity values of the functions under consideration. Among the various weightwise quadratic functions studied

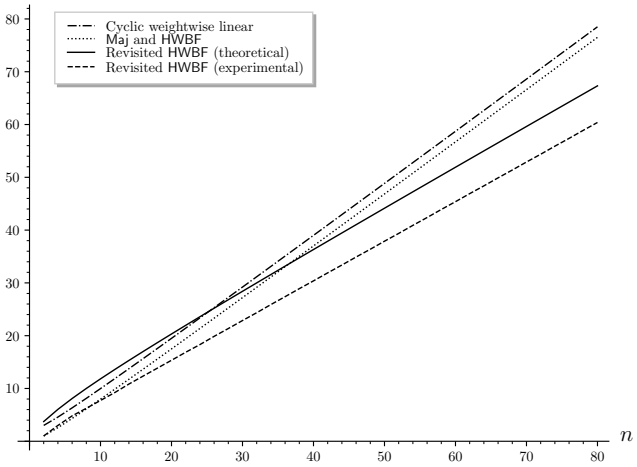

Fig. 2. Bounds on $\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_f(a)|$ for various functions $f \in \mathcal{B}_n$ for even n, shown on a logarithmic scale. The bound for the cyclic weightwise linear functions stems from [38]. The bound for the majority function and the HWBF comes from Property 1. The theoretical bound for the revisited HWBF is from Corollary 2, and the experimental bound is from Section 5.1.

so far, we observe that the revisited HWBF has the highest nonlinearity from $n = 10$ onward.

Table 5. Comparison of the nonlinearity.

n	4	6	8	10	12	14	16
HWBF	4	20	88	372	1 544	6 344	25 904
Majority	5	22	93	386	1 586	6 476	26 333
t [38]	4	22	96	404	1 672	6 854	27 884
u [38]	4	24	104	456	1 888	7 816	31 616
Revisited HWBF	4	22	102	458	1 902	7 842	31 680

6 Other Parameters

In this section, we present additional cryptographic parameters for the revisited HWBF. While Theorem 1 describes its balancedness and Sections 4.2 and 5 thoroughly explore its nonlinearity, our focus here will be on its algebraic characteristics. Specifically, we will examine the degree, the algebraic immunity, and the fast algebraic immunity, and offer comparisons with other weightwise quadratic functions.

Proposition 11. *Let $n \geqslant 4$ be even, and let $f \in \mathcal{B}_n$ be the revisited HWBF. Then $\mathsf{deg}(f) = n - 1$.*

Proof. We write $f = q + h$, where $q \in \mathcal{B}_n$ is given by $q(x) = \sum_{i=1}^{n/2}(x_i + 1)x_{i+n/2}$ and $h \in \mathcal{B}_n$ is the HWBF. The function h has degree $n-1 \geqslant 3$ by Property 1, and the function q has no monomial of degree higher than 2, so $\mathsf{deg}(f) = \mathsf{deg}(h) = n - 1$. □

In Table 6, we display the algebraic degree of different weightwise quadratic functions. We observe that the revisited HWBF has the highest degree along with the original HWBF when n is not a power of 2. However, when n is a power of 2, the majority function has a degree that is one higher than that of the other two functions, as explained by Property 1 and Proposition 11.

Table 6. Comparison of the degree and algebraic immunity.

n	4	6	8	10	12	14	16
HWBF	3, 2	5, 3	7, 4	9, 4	11, 5	13, 5	15, 6
Majority	4, 2	4, 3	8, 4	8, 5	8, 6	8, 7	16, 8
t [38]	2, 2	5, 3	6, 4	9, 5	11, 5	13, 6	14, 7
u [38]	2, 2	4, 3	6, 4	8, 5	10, 6	12, 6	14, 7
Revisited HWBF	3, 2	5, 3	7, 4	9, 5	11, 6	13, 6	15, 7

Proposition 12. *Let $n \geqslant 4$ be even, let $f \in \mathcal{B}_n$ be the revisited HWBF, and let $h \in \mathcal{B}_n$ be the HWBF. Then $\mathsf{AI}(f) \geqslant \mathsf{AI}(h) - 2$.*

Proof. Let $q \in \mathcal{B}_n$ be given by $q(x) = \sum_{i=1}^{n/2}(x_i + 1)x_{i+n/2}$, so that $h = f + q$. Let $g \in \mathcal{B}_n^*$ with $\mathsf{deg}(g) = \mathsf{AI}(f)$ be an annihilator of $f + \varepsilon$ for some $\varepsilon \in \{0, 1\}$. Then the following holds:

$$\begin{aligned} g \cdot (q+1) \cdot (h+\varepsilon) &= g \cdot (q+1) \cdot (f+q+\varepsilon) \\ &= g \cdot (q+1) \cdot (f+\epsilon) + g \cdot (q+1) \cdot q \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Hence, $g \cdot (q + 1)$ is an annihilator of $h + \varepsilon$. If $g \cdot (q + 1) \neq 0$, it follows that $\mathsf{AI}(h) \leqslant \mathsf{deg}(g \cdot (q+1)) \leqslant \mathsf{deg}(g) + \mathsf{deg}(q+1)$, and therefore that $\mathsf{AI}(f) = \mathsf{deg}(g) \geqslant \mathsf{AI}(h) - \mathsf{deg}(q+1) = \mathsf{AI}(h) - 2$. If $g \cdot (q+1) = 0$, then $0 = g \cdot (f + \epsilon + q + 1) = g \cdot (h + \epsilon + 1)$, showing that $\mathsf{AI}(f) = \mathsf{deg}(g) \geqslant \mathsf{AI}(h)$. □

From Theorem 4 in [46], the algebraic immunity of the HWBF is at least $\lfloor n/3 \rfloor + 1$, which leads to $\lfloor n/3 \rfloor - 1$ for the revisited HWBF. In Table 6, we present the algebraic immunity of various weightwise quadratic functions. We observe that the revisited HWBF demonstrates the best performance after the majority function; the latter is known to achieve optimal algebraic immunity.

Lastly, we also considered the fast algebraic immunity of the revisited HWBF f. In Table 7, we give the best couples (d, e) encountered for the function f, where $\mathsf{deg}(g) = d$ and $\mathsf{deg}(h) = e$ for functions g and h satisfying $fg = h$.

These various results on the algebraic properties of the revisited HWBF suggest that it possesses strong resistance against standard attacks. Furthermore, its high nonlinearity makes it a well-suited candidate for use as a filter function in contexts such as filtered LFSRs or in homomorphically-friendly schemes like FLIP and FiLIP. For example, the best current FiLIP filters in HHE [1,20,39] are XOR-threshold functions—the sum of a k-variable linear function and an m-variable threshold function (generalizing majority). By Proposition 7 in [14], their nonlinearity is at most $2^{k+m-1} - 2^k \cdot M$, where $M = \binom{m-1}{\frac{m-1}{2}}$ if M is odd, and $M = (1/2) \cdot \binom{m}{\frac{m}{2}}$ if M is even. This is similar to the majority function, whereas the revisited HWBF achieves higher nonlinearity for the same size, offering better resistance to correlation-like attacks with fewer variables.

Table 7. Lowest possible values of (d, e) for different values of n.

n	4	6	8	10	12	14	16	18
(d, e)	$(1, 2)$	$(1, 3)$	$(1, 5)$	$(1, 7)$	$(1, 9)$	$(1, 11)$	$(1, 13)$	$(1, 15)$
			$(2, 4)$	$(2, 6)$	$(2, 8)$	$(2, 10)$	$(2, 12)$	$(2, 14)$
				$(3, 5)$	$(3, 6)$	$(3, 9)$	$(3, 11)$	$(3, 13)$
							$(4, 9)$	$(4, 11)$
								$(5, 10)$

7 Conclusion and Open Questions

In this work, we introduced the revisited Hidden Weight Bit Function, a weightwise quadratic Boolean function with improved cryptographic properties over existing constructions. We analyzed its balancedness, and using generating functions in combination with complex analysis, we derived interesting lower bounds on its nonlinearity, demonstrating that the revisited HWBF achieves superior nonlinearity compared to other functions with similar computational costs. We further examined other cryptographic parameters such as degree, algebraic immunity, and fast algebraic immunity, confirming that the revisited HWBF matches or outperforms comparable functions in these aspects.

Our approach utilizes generating functions and Cauchy's estimate to establish lower bounds on the nonlinearity of weightwise quadratic functions. This naturally raises the question: can the employed techniques, particularly the use of Cauchy's estimate, be extended to other families of Boolean functions? Specifically, this approach appears feasible for other weightwise-degree-d functions f where the f_k are direct sums. Investigating this could potentially lead to the discovery of new functions with comparable computational costs and even better cryptographic properties.

Acknowledgments. Pierrick Méaux was funded by the European Research Council (ERC) under the Advanced Grant program (reference number: 787390). Tim Seuré acknowledges the support of the Luxembourgish "Fonds National de la Recherche" (FNR) through an Individual Grant (reference number: 17936291). The work of Deng

Tang was supported in part by the National Natural Science Foundation of China (NSFC, reference number: 62272303). We would also like to thank Claude Carlet for discussing the function introduced in this work with Deng Tang some years ago.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

A Proofs for Section 4.3

In this section, we provide the missing proofs for Section 4.3.

Proof of Proposition 9. By considering binary vectors $x \in \mathbb{F}_2^n$ as $x = (y, z)$ with $y \in \mathbb{F}_2^{2t}$ and $z \in \mathbb{F}_2^{n-2t}$, we get:

$$\begin{aligned}
\mathsf{D}_{t,k,n}(a) &= \sum_{x \in \mathsf{E}_{k,n}} (-1)^{d_{t,n}(x)+a\cdot x} \\
&= \sum_{(y,z) \in \mathsf{E}_{k,n}} (-1)^{d_{t,2t}(y)+b\cdot y+c\cdot z} \\
&= \sum_{\ell=0}^{2t} \sum_{\substack{y \in \mathsf{E}_{\ell,2t} \\ z \in \mathsf{E}_{k-\ell,n-2t}}} (-1)^{d_{t,2t}(y)+b\cdot y+c\cdot z} \\
&= \sum_{\ell=0}^{2t} \left(\sum_{y \in \mathsf{E}_{\ell,2t}} (-1)^{d_{2t}(y)+b\cdot y} \right) \left(\sum_{z \in \mathsf{E}_{k-\ell,n-2t}} (-1)^{c\cdot z} \right) \\
&= \sum_{\ell=0}^{2t} \mathsf{D}_{\ell,2t}(a) \cdot \mathsf{K}_{k-\ell}(\mathsf{w}_\mathsf{H}(c), n-2t).
\end{aligned}$$

□

Proof of Proposition 10. Applying Proposition 9, we get:

$$\begin{aligned}
\sum_{k \in \mathbb{Z}} \mathsf{D}_{t,k,n}(a) z^k &= \sum_{\ell=0}^{2t} \mathsf{D}_{\ell,2t}(a) z^\ell \sum_{k \in \mathbb{Z}} \mathsf{K}_{k-\ell}(\mathsf{w}_\mathsf{H}(c), n-2t) z^{k-\ell} \\
&= \left(\sum_{\ell=0}^{2t} \mathsf{D}_{\ell,2t}(a) z^\ell \right) \cdot (1+z)^u \cdot (1-z)^v \\
&= P_b(z) \cdot (1+z)^u \cdot (1-z)^v \\
&= P_{t,a}(z).
\end{aligned}$$

□

Lastly, we provide a proof for Theorem 3. We start with a preliminary result that will be required for the proof.

Lemma 1. *Let $N \geqslant 1$ be an integer and $D \subseteq \mathbb{C}$ a set of complex numbers. For every $i \in [1, N]$, consider integers $m_i \geqslant 0$ and $k_i \geqslant 1$, as well as complex functions*

$f_{i,1}, \ldots, f_{i,k_i} : D \to \mathbb{C}$. Assume that the following maximum exists (which holds for instance if the functions $f_{i,j}$ are continuous and D is topologically compact):

$$M = \max_{\substack{\forall i \in [1,N]:\, p_{i,1}+\cdots+p_{i,k_i}=m_i \\ z \in D}} \left| \prod_{i=1}^{N} \prod_{j=1}^{k_i} f_{i,j}(z)^{p_{i,j}} \right|.$$

Then there exist integers $j_1, \ldots, j_N$ with $j_i \in [1, k_i]$ such that the following holds:

$$M = \max_{z \in D} \left| \prod_{i=1}^{N} f_{i,j_i}(z)^{m_i} \right|.$$

Proof. Let us choose the integers $p_{i,j} \geqslant 0$ satisfying $\sum_{j=1}^{k_i} p_{i,j} = m_i$ for every $i \in [1, N]$ together with the complex number $z \in D$ to maximize the quantity $\left| \prod_{i=1}^{N} \prod_{j=1}^{k_i} f_{i,j}(z)^{p_{i,j}} \right|$. Next, for every $i \in [1, N]$, choose $j_i \in [1, k_i]$ such that $|f_{i,j_i}(z)| \geqslant |f_{i,j}(z)|$ for every $j \in [1, k_i]$. Then we have:

$$\begin{aligned} M &= \left| \prod_{i=1}^{N} \prod_{j=1}^{k_i} f_{i,j}(z)^{p_{i,j}} \right| \\ &\leqslant \left| \prod_{i=1}^{N} \prod_{j=1}^{k_i} f_{i,j_i}(z)^{p_{i,j}} \right| \\ &= \left| \prod_{i=1}^{N} f_{i,j_i}(z)^{\sum_{j=1}^{k_i} p_{i,j}} \right| \\ &= \left| \prod_{i=1}^{N} f_{i,j_i}(z)^{m_i} \right| \\ &\leqslant M. \end{aligned}$$

□

Proof of Theorem 3. To begin, we observe that the inequality $|\mathcal{W}_{d_{t,n}}(a)| \leqslant 1 + n \cdot 2^{\mu n}$ will follow from the inequality $|\mathsf{D}_{t,k,n}(a)| \leqslant 2^{\mu n}$ using precisely the arguments of the proof of Corollary 2, so that we are only required to prove the first inequality. Also, since the case $\lambda = 1/2$ corresponds to Theorem 2, we will henceforth assume $\lambda < 1/2$.

Similarly to the proof of Theorem 2, we want to bound the maximum of $|P_{t,a}(z)|$ on $\mathsf{c}_1 = \{z \in \mathbb{C} : |z| = 1\}$ for $a \in \mathbb{F}_2^n$, and this will then be an upper bound on $|\mathsf{D}_{t,k,n}(a)|$ for every $k \in [0, n]$. We write $a = (b, c)$ with $b \in \mathbb{F}_2^{2t}$ and $c \in \mathbb{F}_2^{n-2t}$, and define $(p, q, r) = (p(b), q(b), r(b))$, and further consider $u = n - 2t - \mathsf{w}_\mathsf{H}(c)$ and $v = \mathsf{w}_\mathsf{H}(c)$ as in Definition 18. To find a bound for $|P_{t,a}(z)|$ on c_1 that applies to all $a \in \mathbb{F}_2^n$, we would like to bound the quantity $\max_{a \in \mathbb{F}_2^n, z \in \mathsf{c}_1} |P_{t,a}(z)|$. Moving through all $a \in \mathbb{F}_2^n$ is equivalent to moving through all tuples $(p, q, r; u, v)$ of non-negative integers which satisfy $p + q + r = t$ and $u + v = n - 2t$. It follows from Lemma 1 that it is enough to consider only the cases for which only one of

p, q, r is non-zero, and for which only one of u, v is non-zero. This leaves us with the following cases to consider for $(p, q, r; u, v)$:

$$(t, 0, 0; n-2t, 0), \quad (0, t, 0; n-2t, 0), \quad (0, 0, t; n-2t, 0),$$
$$(t, 0, 0; 0, n-2t), \quad (0, t, 0; 0, n-2t), \quad (0, 0, t; 0, n-2t).$$

Since simultaneously replacing (p, q) by (q, p) and (u, v) by (v, u) has the same effect as replacing z by $-z$ in $P_{t,a}(z)$ and therefore does not change the maximum of $|P_{t,a}(z)|$ on c_1, we can restrict ourselves to the following tuples for $(p, q, r; u, v)$:

$$(t, 0, 0; n-2t, 0), \quad (0, t, 0; n-2t, 0), \quad (0, 0, t; n-2t, 0).$$

Let us start by bounding $|P_{t,a}(z)|$ on c_1 in the case $(p, q, r; u, v) = (t, 0, 0; n - 2t, 0)$. Since $t = \lambda n$, we can write:

$$P_{t,a}(z) = \left((-z^2 + 2z + 1)^{\lambda}(1+z)^{1-2\lambda}\right)^n.$$

Writing $z = \mathrm{e}^{\mathrm{i}\alpha}$ and $z^2 = \mathrm{e}^{2\mathrm{i}\alpha}$ for $\alpha \in [-\pi, \pi]$, and using that $|w|^2 = w\overline{w}$ for every complex number w, we get:

$$|-z^2 + 2z + 1|^2 = \left(-\mathrm{e}^{2\mathrm{i}\alpha} + 2\mathrm{e}^{\mathrm{i}\alpha} + 1\right)\left(-\mathrm{e}^{-2\mathrm{i}\alpha} + 2\mathrm{e}^{-\mathrm{i}\alpha} + 1\right).$$

Expanding yields $|-z^2 + 2z + 1|^2 = 6 - \mathrm{e}^{2\mathrm{i}\alpha} - \mathrm{e}^{-2\mathrm{i}\alpha} = 6 - 2\cos(2\alpha)$ because $\mathrm{e}^{2\mathrm{i}\alpha} = \cos(2\alpha) + \mathrm{i}\sin(2\alpha)$. We similarly obtain that $|1+z|^2 = 2 + 2\cos\alpha$. Combining both, we get:

$$\begin{aligned} P_{t,a}(z)|^2 &= \left(\left|-z^2 + 2z + 1\right|^{2\lambda} |1+z|^{2(1-2\lambda)}\right)^n \\ &= \left((6 - 2\cos(2\alpha))^{\lambda}(2 + 2\cos\alpha)^{1-2\lambda}\right)^n. \end{aligned}$$

The goal will be to prove that the maximum of the function $g(\alpha) = g^{(\lambda)}(\alpha) = (6 - 2\cos(2\alpha))^{\lambda}(2 + 2\cos\alpha)^{1-2\lambda}$ for $\alpha \in [-\pi, \pi]$ is equal to $2^{2\mu}$; the maximum of $|P_{t,a}(z)|$ on c_1 will then be $\left(2^{2\mu}\right)^{n/2} = 2^{\mu n}$. Note that g is an even function, so it is enough to focus on the interval $\alpha \in [0, \pi]$; the function g is represented for several values of $0 \leqslant \lambda < 1/2$ in Figure 3.

Writing $g(\alpha) = g_1(\alpha)^{\lambda} g_2(\alpha)^{1-2\lambda}$ for $g_1(\alpha) = 6 - 2\cos(2\alpha)$ and $g_2(\alpha) = 2 + 2\cos\alpha$, we compute the first derivative of g, and apply the double angle formulas $\cos(2\alpha) = 2\cos^2\alpha - 1$ and $\sin(2\alpha) = 2\cos\alpha\sin\alpha$:

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}\alpha} g(\alpha) &= g_1(\alpha)^{\lambda-1} g_2(\alpha)^{-2\lambda} \left(\lambda g_2(\alpha) \frac{\mathrm{d}}{\mathrm{d}\alpha} g_1(\alpha) + (1-2\lambda) g_1(\alpha) \frac{\mathrm{d}}{\mathrm{d}\alpha} g_2(\alpha)\right) \\ &= g_1(\alpha)^{\lambda-1} g_2(\alpha)^{-2\lambda} (\lambda(2 + 2\cos\alpha) \cdot 4\sin(2\alpha) \\ &\quad + (1-2\lambda)(6 - 2\cos(2\alpha))(-2\sin\alpha)) \\ &= g_1(\alpha)^{\lambda-1} g_2(\alpha)^{-2\lambda} \big(\lambda(2 + 2\cos\alpha) \cdot 4 \cdot 2\cos\alpha\sin\alpha \\ &\quad + (1-2\lambda)\left(8 - 4\cos^2\alpha\right)(-2\sin\alpha)\big) \\ &= 8 g_1(\alpha)^{\lambda-1} g_2(\alpha)^{-2\lambda} \sin\alpha \big(2\lambda\cos\alpha(1 + \cos\alpha) \\ &\quad - (1-2\lambda)\left(2 - \cos^2\alpha\right)\big) \\ &= 8 g_1(\alpha)^{\lambda-1} g_2(\alpha)^{-2\lambda} \sin\alpha \left(\cos^2\alpha + 2\lambda\cos\alpha + 4\lambda - 2\right). \end{aligned}$$

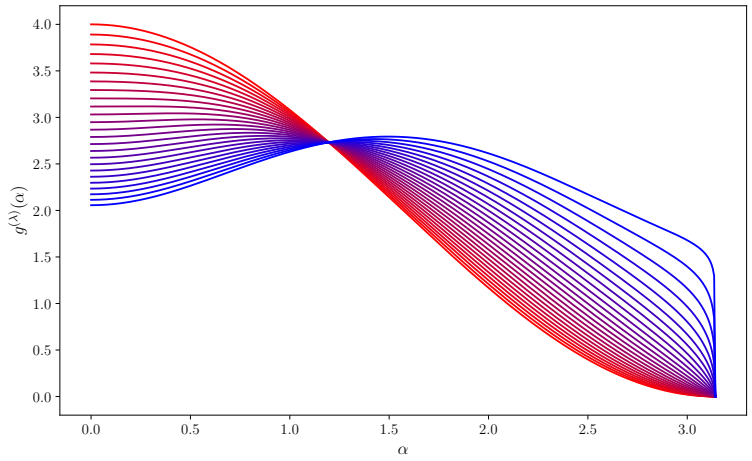

Fig. 3. The curves of $\alpha \mapsto g^{(\lambda)}(\alpha)$ for the values $\lambda = \frac{i}{50}$ from $i = 0$ (the curve with the highest value at $\alpha = 0$) to $i = 24$ (the curve with the lowest value at $\alpha = 0$).

The only interesting zeros of $\frac{\mathrm{d}}{\mathrm{d}\alpha} g(\alpha)$ are those of the last factor $\cos^2\alpha + 2\lambda\cos\alpha + 4\lambda - 2$: the factor $8g_1(\alpha)^{\lambda-1} g_2(\alpha)^{-2\lambda}$ has none, and those for $\sin\alpha$ are $\alpha = 0$ and $\alpha = \pi$, with corresponding values $g(0) = 2^{2-2\lambda}$ and $g(\pi) = 0$.

Our first claim is that the equation $\mathcal{E} : \cos^2\alpha + 2\lambda\cos\alpha + 4\lambda - 2 = 0$ has a unique solution $\cos\alpha = -\lambda + \sqrt{\lambda^2 - 4\lambda + 2}$ if $\lambda \geqslant 1/6$ and has no solution $\cos\alpha$ otherwise. To see this, we consider $\mathcal{E}$ as an equation of second degree in $\cos\alpha$, which leads to the two solution candidates $\cos\alpha = -\lambda \pm \sqrt{\lambda^2 - 4\lambda + 2}$.

We can exclude the solution $\cos\alpha = -\lambda - \sqrt{\lambda^2 - 4\lambda + 2}$ since $\cos\alpha \in [-1, 1]$ and $\lambda \in [0, 1/2)$. The other solution needs to be excluded for the same reason if $\lambda < 1/6$.

Our second claim is that $\frac{\mathrm{d}^2}{\mathrm{d}^2\alpha} g(\alpha)|_{\alpha=0}$ has the same sign as $6\lambda - 1$. To see why, we apply the definition of the second derivative:

$$\begin{aligned}
\frac{\mathrm{d}^2}{\mathrm{d}^2\alpha} g(\alpha)|_{\alpha=0} &= \lim_{\alpha\to 0} \frac{\frac{\mathrm{d}}{\mathrm{d}\alpha} g(\alpha)}{\alpha} \\
&= \lim_{\alpha\to 0} 8(6 - 2\cos(2\alpha))^{\lambda-1}(2 + 2\cos\alpha)^{-2\lambda} \\
&\qquad \cdot \frac{\sin\alpha}{\alpha} \cdot \left(\cos^2\alpha + 2\lambda\cos\alpha + 4\lambda - 2\right) \\
&= 8 \cdot 4^{\lambda-1} \cdot 4^{-2\lambda} \cdot 1 \cdot (6\lambda - 1) \\
&= 2^{1-2\lambda}(6\lambda - 1).
\end{aligned}$$

Therefore, in case $\lambda < 1/6$, we can conclude from the two claims that $g(\alpha)$ reaches its maximum at $\alpha_0 = 0$, and this maximum is then equal to $2^{2-2\lambda} = 2^{2\mu}$, as required. For $\lambda = 1/6$, the solution to the equation $\mathcal{E}$ is $\cos\alpha = 1$, again implying that $g(\alpha)$ reaches its maximum at $\alpha_0 = 0$, and we obtain the same

maximum of $2^{2\mu}$. In case $\lambda > 1/6$, the two claims imply that $g(\alpha)$ reaches its maximum at the unique $\alpha_0 \in [0, \pi]$ for which $\cos\alpha_0 = -\lambda + \sqrt{\lambda^2 - 4\lambda + 2}$. For this α_0, the double angle formula for the cosine implies that $\cos(2\alpha_0) = 4\lambda^2 - 8\lambda + 3 - 4\lambda\sqrt{\lambda^2 - 4\lambda + 2}$. If we replace $\cos\alpha_0$ and $\cos(2\alpha_0)$ by their respective values, we obtain that the maximum of $g(\alpha)$ for $\alpha \in [0, \pi]$ is given by the following value:

$$g(\alpha_0) = \frac{\left(-8\lambda^2 + 16\lambda + 8\lambda\sqrt{\lambda^2 - 4\lambda + 2}\right)^{\lambda}}{\left(2 - 2\lambda + 2\sqrt{\lambda^2 - 4\lambda + 2}\right)^{2\lambda - 1}} = 2^{2\mu}.$$

With this, we have covered the case $(p, q, r; u, v) = (t, 0, 0; n - 2t, 0)$ entirely. Similarly, it can be proven that $|P_{t,a}(z)|$ is also bounded by $2^{\mu n}$ on c_1 for the remaining two cases of $(p, q, r; u, v)$. For $(p, q, r; u, v) = (0, t, 0; n - 2t, 0)$, one can proceed in exactly the same way, and for $(p, q, r; u, v) = (0, 0, t; n - 2t, 0)$, it is enough to replace $g(\alpha)$ by $h(\alpha) = (2 + 2\cos(2\alpha))^{\lambda}(2 + 2\cos\alpha)^{1-2\lambda}$, whose maximum is bounded by the maximum of $g(\alpha)$ since $0 \leqslant h(\alpha) \leqslant g(\alpha)$. □

References

1. Aranha, D.F., Guimarães, A., Hoffmann, C., Méaux, P.: Secure and Efficient Transciphering for FHE-Based MPC. IACR Cryptology ePrint Archive (2024)
2. Armknecht, F.: Improving Fast Algebraic Attacks. In: Fast Software Encryption. Springer (2004)
3. Armknecht, F., Carlet, C., Gaborit, P., Künzli, S., Meier, W., Ruatta, O.: Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks. In: Advances in Cryptology – EUROCRYPT 2006. Springer (2006)
4. Beierle, C., Leander, G.: 4-Uniform Permutations with Null Nonlinearity. Cryptography and Communications **12** (2020)
5. Bollig, B., Löbbing, M., Sauerhoff, M., Wegener, I.: On the Complexity of the Hidden Weighted Bit Function for Various BDD Models. RAIRO Theoretical Informatics and Applications **33**(2) (1999)
6. Braeken, A., Preneel, B.: On the Algebraic Immunity of Symmetric Boolean Functions. In: Progress in Cryptology – INDOCRYPT 2005. Springer (2005)
7. Bryant, R.E.: On the Complexity of VLSI Implementations and Graph Representations of Boolean Functions with Application to Integer Multiplication. IEEE Transactions on Computers **40**(2) (1991)
8. Budaghyan, L., Carlet, C., Helleseth, T.: On Bent Functions Associated to AB Functions. In: IEEE Information Theory Workshop 2011. IEEE (2011)
9. Canteaut, A., Carpov, S., Fontaine, C., Lepoint, T., Naya-Plasencia, M., Paillier, P., Sirdey, R.: Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression. Journal of Cryptology **31**(3) (2018)
10. Canteaut, A., Videau, M.: Symmetric Boolean Functions. IEEE Transactions on Information Theory (2005)
11. Carlet, C.: On the Degree, Nonlinearity, Algebraic Thickness, and Nonnormality of Boolean Functions, with Developments on Symmetric Functions. IEEE Transactions on Information Theory (2004)
12. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press (2021)

13. Carlet, C.: A Wide Class of Boolean Functions Generalizing the Hidden Weight Bit Function. IEEE Transactions on Information Theory **68**(2) (2022)
14. Carlet, C., Méaux, P.: A Complete Study of Two Classes of Boolean Functions: Direct Sums of Monomials and Threshold Functions. IEEE Transactions on Information Theory (2021)
15. Carlet, C., Méaux, P., Rotella, Y.: Boolean Functions with Restricted Input and Their Robustness; Application to the FLIP Cipher. IACR Transactions on Symmetric Cryptology **2017** (2017)
16. Carlet, C., Sarkar, P.: Constructions of Efficiently Implementable Boolean Functions Possessing High Nonlinearity and Good Resistance to Algebraic Attacks. IACR Cryptology ePrint Archive (2024)
17. Carlet, C., Tang, D.: Enhanced Boolean Functions Suitable for the Filter Model of Pseudo-Random Generator. Designs, Codes and Cryptography **76**(3) (2015)
18. Chen, Y., Lu, P.: Two Classes of Symmetric Boolean Functions with Optimum Algebraic Immunity: Construction and Analysis. IEEE Transactions on Information Theory **57** (2011)
19. Cid, C., Indrøy, J.P., Raddum, H.: FASTA – A Stream Cipher for Fast FHE Evaluation. In: Topics in Cryptology – CT-RSA 2022. Springer (2022)
20. Cong, K., Das, D., Park, J., Pereira, H.V.L.: SortingHat: Efficient Private Decision Tree Evaluation via Homomorphic Encryption and Transciphering. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. ACM (2022)
21. Courtois, N.T.: Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Advances in Cryptology – CRYPTO 2003. Springer (2003)
22. Courtois, N.T., Meier, W.: Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Advances in Cryptology – EUROCRYPT 2003. Springer (2003)
23. Dalai, D.K., Maitra, S., Sarkar, S.: Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. Designs, Codes and Cryptography (2006)
24. Dobbertin, H.: Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity. In: Fast Software Encryption. Springer (1995)
25. Dobraunig, C., Eichlseder, M., Grassi, L., Lallemand, V., Leander, G., List, E., Mendel, F., Rechberger, C.: Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit. In: Advances in Cryptology – CRYPTO 2018. Springer (2018)
26. Gini, A., Méaux, P.: On the Weightwise Nonlinearity of Weightwise Perfectly Balanced Functions. Discrete Applied Mathematics **322** (2022)
27. Hawkes, P., Rose, G.G.: Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers. In: Advances in Cryptology – CRYPTO 2004. Springer (2004)
28. Hoffmann, C., Méaux, P., Ricosset, T.: Transciphering, Using FiLIP and TFHE for an Efficient Delegation of Computation. In: Progress in Cryptology – INDOCRYPT 2020. Springer (2020)
29. Jiao, L., Zhang, B., Wang, M.: Establishing Equations: The Complexity of Algebraic and Fast Algebraic Attacks Revisited. In: Information Security. Springer (2013)
30. Liu, M., Lin, D., Pei, D.: Fast Algebraic Attacks and Decomposition of Symmetric Boolean Functions. IEEE Transactions on Information Theory **57**(7) (2011)
31. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company (1978)
32. Meier, W., Pasalic, E., Carlet, C.: Algebraic Attacks and Decomposition of Boolean Functions. In: Advances in Cryptology – EUROCRYPT 2004. Springer (2004)

33. Mesnager, S.: Bent Functions. Springer (2016)
34. Méaux, P.: On the Fast Algebraic Immunity of Majority Functions. In: Progress in Cryptology – LATINCRYPT 2019. Springer (2019)
35. Méaux, P.: On the Fast Algebraic Immunity of Threshold Functions. Cryptography and Communications **13** (2021)
36. Méaux, P., Carlet, C., Journault, A., Standaert, F.X.: Improved Filter Permutators for Efficient FHE: Better Instances and Implementations. In: Progress in Cryptology – INDOCRYPT 2019. Springer (2019)
37. Méaux, P., Journault, A., Standaert, F.X., Carlet, C.: Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. In: Advances in Cryptology – EUROCRYPT 2016. Springer (2016)
38. Méaux, P., Ozaim, Y.: On the Cryptographic Properties of Weightwise Affine and Weightwise Quadratic Functions. Discrete Applied Mathematics **355** (2024)
39. Méaux, P., Park, J., Pereira, H.V.L.: Towards Practical Transciphering for FHE with Setup Independent of the Plaintext Space. IACR Communications in Cryptology **1**(1) (2024)
40. Naehrig, M., Lauter, K.E., Vaikuntanathan, V.: Can Homomorphic Encryption Be Practical? In: Proceedings of the 3rd ACM Cloud Computing Security Workshop (CCSW 2011). ACM (2011)
41. Qu, L., Feng, K., Liu, F., Wang, L.: Constructing Symmetric Boolean Functions with Maximum Algebraic Immunity. IEEE Transactions on Information Theory (2009)
42. Rothaus, O.S.: On "Bent" Functions. Journal of Combinatorial Theory, Series A **20** (1976)
43. Rudin, W.: Real and Complex Analysis. McGraw-Hill Book Company (1987)
44. Sarkar, P., Maitra, S.: Balancedness and Correlation Immunity of Symmetric Boolean Functions. Discrete Mathematics (2007)
45. Tokareva, N.: Bent Functions: Results and Applications to Cryptography. Academic Press (2015)
46. Wang, Q., Carlet, C., Stanica, P., Tan, C.H.: Cryptographic Properties of the Hidden Weighted Bit Function. Discrete Applied Mathematics **174** (2014)