From at Least $n/3$ to at Most $3\sqrt{n}$: Correcting the Algebraic Immunity of the Hidden Weight Bit Function

Algebraic Immunity Upper Bounds on Weightwise Degree-d Functions and Their Implications

Pierrick Méaux[0000−0001−5733−4341]

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

Abstract. Weightwise degree-d functions are Boolean functions that, on each set of fixed Hamming weight, coincide with a function of degree at most d. They generalize both symmetric functions and the Hidden Weight Bit Function (HWBF), which has been studied in cryptography for its favorable properties. In this work, we establish a general upper bound on the algebraic immunity of such functions, a key security parameter against algebraic attacks on stream ciphers like filtered Linear Feedback Shift Registers (LFSRs). We construct explicit low-degree annihilators for WWdd functions with small d, and show how to generalize these constructions. As an application, we prove that the algebraic immunity of the HWBF is upper bounded by $3\sqrt{n}$ disproving a result from 2011 that claimed a lower bound of $n/3$. We then apply our technique to several generalizations of the HWBF proposed since 2021 for homomorphically friendly constructions and LFSR-based ciphers, refining or refuting results from six prior works.

Keywords: Boolean functions, algebraic immunity, symmetric functions, HWBF

1 Introduction.

1.1 Weightwise degree-d functions, a unifying perspective

Weightwise degree-d functions are Boolean functions that, when restricted to each set of inputs of fixed Hamming weight—called a slice—coincide with a function of algebraic degree at most d. This notion, introduced in [GM22], was originally used to study the relationship between weightwise affine functions (the case $d = 1$) and weightwise perfectly balanced functions, *i.e.* , functions that are balanced on every slice [CMR17]. Although the definition is recent, weightwise constant and affine functions—corresponding to the cases $d = 0$ and $d = 1$—have appeared in many earlier works, often under different names. For instance, symmetric Boolean functions (WWd0), which depend only on the Hamming weight of their input, have been extensively studied for their cryptographic relevance *e.g.* [Car04, CV05, BP05, SM07]. The most known example of a weightwise affine function is the Hidden Weight Bit Function (HWBF) [Bry91], which outputs the k-th bit of the input when the Hamming weight is k, and 0 on the all-zero vector. It has drawn attention both for its exponential binary decision diagram size [BLSW99] and for its main cryptographic parameters, studied in [WCST14]. While efficiently computable, the HWBF lacks sufficient nonlinearity to be used directly as a cryptographic filter in stream ciphers, leading to generalizations that aim to preserve its efficiency while improving its cryptographic strength [WTS14, Car22].

In recent years, weightwise degree-d functions—particularly for small values of d—have gained renewed attention, both through their emergence in modern applications and their revival in classical cipher design. One primary motivation comes from the field of Hybrid Homomorphic Encryption (HHE) [NLV11], where components of symmetric ciphers must be efficiently evaluable under homomorphic encryption. Multiple symmetric ciphers have been developed with this constraint in mind, including LowMC [ARS+15],

Kreyvium [CCF+16], FLIP [MJSC16], Rasta [DEG+18], and FiLIP [MCJS19]. In this context, weightwise low-degree functions offer a good trade-off between structural simplicity and algebraic complexity, making them attractive for homomorphically friendly design. This direction is supported by ongoing advances in the homomorphic evaluation of Boolean functions. Notably, the efficient homomorphic computation of Hamming weight [HMR20] and the use of fast multiplexer circuits in schemes such as FHEW [DM15] and TFHE [CGGI16] have enabled the practical evaluation of symmetric and WWdd functions on encrypted inputs. Recent implementations demonstrate HHE evaluation with latency under 10ms per bit [CDPP22, MPP24], further underscoring the practicality of these function classes. A second motivation stems from the renewed interest in stream cipher constructions based on filtered Linear Feedback Shift Registers (LFSRs), a classical paradigm originally explored in the late 1990s and early 2000s. In this setting, WWdd functions—especially those related to the HWBF—have been proposed as filtering functions due to their low implementation cost and presumed resistance to algebraic attacks. This line of work has reemerged in recent designs such as [MO24,CS24,CMA25], where the structured nature of WWdd functions is leveraged to combine simplicity with cryptographic strength.

1.2 Algebraic immunity and annihilators

Algebraic attacks are among the most powerful techniques for cryptanalyzing stream ciphers. These attacks consist in deriving, from the observed keystream, a system of algebraic equations in the secret key bits, and then solving this system of multivariate equations over $\mathbb{F}_2$. In the case of a filtered LFSR, the adversary obtains equations of degree equal to that of the Boolean filtering function. However, the algebraic attack introduced by Courtois and Meier [CM03] showed that one can exploit annihilators of the filtering function to obtain an even lower-degree system. Specifically, instead of using the function f directly, the attacker considers a nonzero Boolean function g of low degree such that $f \cdot g = 0$. To quantify a function's resistance to such attacks, the notion of Algebraic Immunity (AI) was formalized in [MPC04]. It is defined as the minimal degree of a nonzero annihilator of a Boolean function f or its complement $f + 1$. A high AI is generally considered a key requirement for any Boolean function used as a filtering component in a stream cipher.

While the concept is well defined, computing or bounding the AI of a function is notoriously difficult. In most cases, known results focus on specific functions or restricted classes, and rely on ad hoc techniques. Only a few Boolean functions families are known to achieve optimal algebraic immunity (*i.e.* , ceiling of $n/2$ for n variables), such as the majority function [DGM05] and the Carlet–Feng functions [CF08]. However, these functions suffer from drawbacks: the majority function has low nonlinearity, and Carlet–Feng functions are difficult to implement efficiently, as they are defined via their support over $\mathbb{F}_{2^n}$. As a result, functions with suboptimal but sufficiently high AI are often preferred in practice.

In this article, we adopt a different strategy for analyzing the algebraic immunity of the HWBF and its generalizations. Rather than relying on case-specific constructions, we leverage the structure of weightwise degree-d functions to build low-degree annihilators in a more systematic way. The key idea is that when a function has low algebraic degree on each Hamming weight slice, one can combine this slice-wise structure with symmetric functions that vanish on most slices to derive global annihilators of remarkably low degree. This approach allows us to obtain new upper bounds on the AI of a broad class of functions—including many recently proposed for cryptographic use. In particular, we show that viewing a function through the lens of weightwise degree-d structure can reveal weaknesses not captured before. In the next part, we present our main contributions, which include both theoretical results on annihilator construction and concrete applications to functions recently introduced in symmetric cryptography and homomorphic-friendly designs.

1.3 Contributions

The first part of this work is devoted to developing a general method for constructing low-degree annihilators for Boolean functions based on their representation as weightwise degree-d functions. Our starting point is the observation that certain low-degree symmetric functions vanish on most slices. This property makes them ideal candidates to multiply with functions annihilating the functions taken by the target function on the remaining slices.

We formalize this idea in our main theorem: if a Boolean function is weightwise degree-d and has no constant term on any slice, then it admits an annihilator of degree at most $\sqrt{nd}(\sqrt{2}+1)$. This yields a nontrivial upper bound on the algebraic immunity of a broad class of functions, including symmetric, weightwise linear, and many HWBF-like constructions. In some cases, refining our approach allows the construction of even lower-degree annihilators, by targeting multiple remaining slices simultaneously.

Beyond the class of WWdd functions, we also show how this methodology can be generalized to other settings. The key idea is to replace the weight slices with any partition of $\mathbb{F}_2^n$ satisfying two conditions:

i. there exists a low-degree function that vanishes on most parts of the partition, and
ii. the target function coincides with low-degree functions on the remaining parts.

Under these conditions, similar upper bounds on the degree of annihilators can be obtained, extending the scope of our approach beyond the WWdd framework.

In the second part of this work, we demonstrate the effectiveness of our method by applying it to several Boolean functions that have been proposed in the cryptographic literature. Our first result concerns the hidden weight bit function. While [WCST14] claimed that the HWBF has algebraic immunity of at least $n/3$, we show that it actually admits an annihilator of degree at most $\sqrt{n}(\sqrt{2}+1)$ for sufficiently large n, thereby disproving the previously accepted bound. This gap between the expected and actual algebraic immunity has important consequences. Over the past decade, a number of works have used the HWBF or closely related functions under the assumption that they offer strong resistance to algebraic attacks. Our results challenge this assumption and provide new upper bounds that refine or invalidate claims in these works.

In particular, we revisit six works in which HWBF-like functions play a central role:

- We address the original result of [WCST14] by disproving its claim on the algebraic immunity of the HWBF. We show that the first value where our technique gives an explicit annihilator that contradicts the claimed bound from [WCST14] is $n = 27$ and we provide such an example.
- In [MO24], cyclic weightwise quadratic functions are introduced for efficient homomorphic evaluation. We prove that the algebraic immunity of these functions also scales proportionally to $\sqrt{n}$, and we provide explicit annihilators for the two main functions highlighted in the article.
- In [CS24], Boolean functions based on the HWBF and the Maiorana–McFarland construction are studied as potential filtering functions. Although these functions are not strictly weightwise quadratic, they can be analyzed in a similar manner by considering the Hamming weight of one half of the input. We establish upper bounds on the algebraic immunity for two families introduced in the paper and determine for which values of n these bounds contradict the conjectured AI.
- In [MST24], a generalization of the HWBF with higher nonlinearity is proposed. We apply our method to this function and derive an upper bound on its algebraic immunity.
- In [CMA25], filtered LFSRs are revisited with large parameters, using weightwise quadratic functions as filters. We show that these functions also fall within the scope of our general bound, without contradicting the conjectured AI stated in that work.

– In [CS25], the authors continue this line of research with new functions based on Maiorana-McFarland construction. Unlike the functions in [CS24], the main function studied here has algebraic immunity of at least $n/4$. We explain why our method does not yield annihilators of degree proportional to $\sqrt{n}$ in this case, and we establish an upper bound on the AI of this family.

In each case, we either disprove a conjecture, correct a previously stated bound, or offer new insight into the function's actual algebraic immunity.

2 Preliminaries.

We denote by $[1, n]$ the set of all integers from 1 to n, *i.e.* $\{1, \ldots, n\}$. For readability, we use the notation $+$ instead of $\oplus$ for addition in $\mathbb{F}_2$. For a vector $v \in \mathbb{F}_2^n$, we denote its Hamming weight by $\mathsf{w_H}(v)$, defined as $\mathsf{w_H}(v) = |\{i \in [n] \mid v_i = 1\}|$. Throughout this article, $\log$ denotes the base-2 logarithm.

2.1 Generalities on Boolean functions and cryptographic criteria

In this section, we review fundamental concepts of Boolean functions and define their key cryptographic properties. For a more in-depth discussion on Boolean functions and their cryptographic properties, we refer to the book [Car21].

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 (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 $|I|$.*

In this article, we study the algebraic immunity of various functions. Below, we provide its definition. Algebraic immunity is, among other things, the main parameter used to estimate the complexity of the algebraic attack [CM03] on filtered linear feedback shift registers. We then recall the concepts of balancedness and nonlinearity, which are the other key cryptographic criteria to consider for Boolean functions used in stream ciphers.

Definition 3 (Algebraic Immunity, [MPC04]). *The algebraic immunity of a Boolean function $f \in \mathcal{B}_n$, denoted as $\mathsf{AI}(f)$, is defined as:*

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

The function g is called an annihilator of f (or $f + 1$).

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 (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 $\mathbb{F}_2^n$).

2.2 Slices, symmetric functions and weightwise degree-d functions

Definition 6 (Slices of the Boolean hypercube). *For $k \in [0,n]$, we define the k-th slice of the n-dimensional Boolean hypercube as the set $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \mid \mathsf{w_H}(x) = k\}$.*

According to Definition 6, the Boolean hypercube is partitioned into $n+1$ slices, where each slice consists of vectors sharing the same Hamming weight. We refer to properties that hold slice-wise as weightwise properties. The n-variable symmetric Boolean functions are precisely those that are constant on each slice.

Definition 7 (Symmetric Functions). *Let $n \in \mathbb{N}^*$. A Boolean function in n variables is said to be symmetric if it is constant on each slice $\mathsf{E}_{k,n}$ for $k \in [0,n]$. The set of symmetric functions in n variables is denoted by $\mathcal{SYM}_n$, and we have $|\mathcal{SYM}_n| = 2^{n+1}$.*

We distinguish the following notable families of symmetric functions:

- ***Elementary symmetric functions.*** *For $i \in [0,n]$, the elementary symmetric function of degree i, denoted $\sigma_{i,n}$, is the Boolean function whose ANF contains all monomials of degree i, and none of other degrees.*
- ***Slice indicator functions.*** *For $k \in [0,n]$, the indicator function of the k-th slice is defined as*

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

- ***Threshold functions.*** *For $d \in [0,n]$, the threshold function of threshold d is defined as*

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

In particular, the majority function MAJ_n is the threshold function with $d = \lceil n/2 \rceil$.

The $n+1$ functions in each of the three families above form a basis for $\mathcal{SYM}_n$—that is, every symmetric Boolean function can be written as a linear combination of these $n+1$ functions.

We recall a property of elementary symmetric functions that will be useful in the sequel.

Property 1. *Let $n \in \mathbb{N}^*$ and $d \in [0,n]$. The elementary symmetric function $\sigma_{d,n}$ satisfies:*

$$\sigma_{d,n}(x) = \binom{k}{d} \bmod 2 \quad \text{for all } x \in \mathsf{E}_{k,n}.$$

We now recall the definition of weightwise degree-d functions:

Definition 8 (Weightwise degree-d functions ([GM22])). *Let $n \in \mathbb{N}^*$. For $k \in [0, n]$, let $\varphi_{k,n}$ denote the indicator function of the slice $\mathsf{E}_{k,n}$.*

A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, written as $f = \sum_{k=0}^{n} f_k \varphi_{k,n}$, is called weightwise degree-d *(WWdd) if and only if, for each $k \in [0, n]$, the restriction f_k coincides with a function of degree at most d over $\mathsf{E}_{k,n}$.*

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

The notion was introduced in [GM22], where the authors studied the relationship between weightwise perfectly balanced functions (*i.e.* functions that are balanced on every slice—see, for example, [CMR17, TL19, LM19, LS20, MS21, MPJ+22, MKCL22, DM24]) and weightwise affine functions—that is, functions of weightwise degree-1.

Weightwise degree-0 and degree-1 functions have been studied for their cryptographic properties in many works, although not under the formalism introduced in [GM22]. Weightwise constant functions (*i.e.* $\mathcal{WD}_n^0$) correspond to symmetric Boolean functions (Definition 7), which have been extensively studied (see, *e.g.* [Car04, CV05, BP05, SM07, CL11, Méa19, CM21]). The hidden weight bit function, introduced in [Bry91], is a notable example of a weightwise degree-1 function. It is defined by setting $f_0 = 0$ and $f_k = x_k$ for $k \in [1, n]$. Its cryptographic properties were analyzed in [WCST14]. In [CMR17], the bent functions presented in Propositions 1 and 2 are shown to be weightwise affine.

Weightwise quadratic functions have also been studied more recently, starting in [MO24] and continuing in [CS24, MST24, CMA25]. In this article, we rely on the formalism of weightwise degree-d functions to derive bounds on their algebraic immunity.

2.3 Properties on binomial coefficients

We recall some results on binomial coefficients used in a few proofs in the article.

Property 2 (Lucas' Theorem, *e.g.* [Fin47])**.** *Let $a, b, p \in \mathbb{N}$ be integers such that $a > b$ and p is a prime. Consider their p-adic expansions $a = \sum_{j=0}^{q} a_j p^j$ and $b = \sum_{j=0}^{q} b_j p^j$ such that $0 \leq a_j < p$ and $0 \leq b_j < p$ for each $j \in [0, q]$ and $a_q \neq 0$. Then*

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

Property 3 (Properties on binomial coefficients)**.** *Let $n \in \mathbb{N}$, the following hold on the binomial coefficients:*

- $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.
- $\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1}$.

3 Algebraic immunity upper bound

In this section, we construct low-degree symmetric functions and show how they can be used to build annihilators for weightwise degree-d functions.

In Section 3.1, we present low-degree symmetric functions that vanish on most slices of the Boolean hypercube. These functions are then used in our main result, Theorem 1, to derive an upper bound on the algebraic immunity of weightwise degree-d functions whose components f_k have no constant term.

In Section 3.2, we explore generalizations of this result. First, we show that other symmetric functions can also be used to construct low-degree annihilators for WWdd functions. We then discuss how even lower-degree annihilators can be obtained. Finally, we explain how these techniques can be extended to partitions beyond the slice decomposition and provide an illustrative example.

3.1 Low-degree symmetric functions with low weight

First, in this part we introduce a family of symmetric functions and show they take the value 1 only on a fraction of the slices.

Proposition 1. *Let $n \in \mathbb{N}^*$, and $r \in [0, \lfloor \log(n) \rfloor]$, we define the Boolean symmetric function $\psi_{r,n}$ as:*

$$\psi_{r,n} = \sum_{i=0}^{2^r-1} \sigma_{i,n}.$$

$\psi_{r,n}$ has the following properties:

- $\mathsf{deg}(\psi_{r,n}) = 2^r - 1$,
- $\psi_{r,n}(x) = 1 \Leftrightarrow x \in \mathsf{E}_{k,n}$ *with* $k \equiv 0 \mod 2^r$.

Proof. The degree of $\psi_{r,n}$ is $2^r - 1$ since it is the sum of homogeneous functions of different degrees, with maximum degree $2^r - 1$.

Then, we focus on the value of $\psi_{r,n}$ on a slice $\mathsf{E}_{k,n}$ (since $\psi_{r,n}$ is symmetric, it takes the same value on all elements of a slice). We denote e_k this value, using Property 1 we obtain:

$$e_k \equiv \sum_{d=0}^{2^r-1} \binom{k}{d} \mod 2.$$

From Lucas' theorem (Property 2), for all $k \in [0, n]$ we have that $\binom{k}{d} \equiv \binom{u}{d} \mod 2$ where $u \in [0, 2^r - 1]$ denotes the rest of the Euclidean division of k by 2^r. Accordingly, using Property 3:

$$e_k = \sum_{d=0}^{2^r-1} \binom{u}{d} \equiv \sum_{d=0}^{u} \binom{u}{d} \equiv 2^u \mod 2 \equiv \begin{cases} 1 & \text{if } u = 0, \\ 0 & \text{otherwise.} \end{cases}$$

□

These function can be used to build annihilators of weightwise degree-d functions. We focus on the case where each restriction on the slice, f_k, has no constant component (*i.e.* $a_\emptyset = 0$ in its ANF).

Theorem 1. *Let $n \in \mathbb{N}^*$, and $f \in \mathcal{WD}_n^d$, where all restriction on the slices, f_k, are degree-d functions with no constant term, then the following holds on f:*

$$\mathsf{AI}(f) \leq \min_{0 \leq r \leq \lfloor \log(n) \rfloor} 2^r - 1 + d \cdot \left\lfloor \frac{n}{2^r} \right\rfloor.$$

Proof. We prove the upper bound on the algebraic immunity by exhibiting non trivial annihilators of f of degree $2^r - 1 + d \cdot \left\lfloor \frac{n}{2^r} \right\rfloor$ for each $r \in \lfloor \log(n) \rfloor$.

We consider the function g_r defined as:

$$g_r = \psi_{r,n} \cdot \prod_{i=1}^{\lfloor n/2^r \rfloor} (1 + f_{2^r \cdot i}).$$

Then, for all $x \in \mathbb{F}_2^n$ we get $f \cdot g_r = 0$. From Proposition 1, $\psi_{r,n}$ takes the value 0 on all slices where $k \not\equiv 0 \mod 2^r$, hence g_r and $f \cdot g_r = 0$ on these slices. On the remaining slices, we have on $\mathsf{E}_{k,n}$ $f \cdot g_r =$

$f_k \cdot \prod_{i=1}^{\lfloor n/2^r \rfloor}(1 + f_{2^r \cdot i})$ which is null since there is a product $f_k \cdot (1 + f_k) = 0$. Accordingly, g_r is an annihilator of f.

Since g_r is the product of functions taking the value 1 in 0_n (by definition of $\psi_{r,n}$ and the restrictions of f on the slices), we get $g_r(0_n) = 1$, hence g_r is not the null function. Furthermore, since $\deg(\psi_{r,n}) = 2^r - 1$ and the $\lfloor n/2^r \rfloor$ functions $1 + f_i$ have degree d, g_r has degree at most $2^r - 1 + d \cdot \left\lfloor \frac{n}{2^r} \right\rfloor$. We conclude using that the algebraic immunity is the minimum degree aver all non trivial annihilators of f and $f + 1$.

□

Remark 1. The restriction in Theorem 1 that the functions f_k do not contain a constant term arises from the construction of the annihilator of f (see g_r in the proof). If two slices, f_k and $f_{k'}$, satisfy $f_k = 1 + f_{k'}$, then the annihilator constructed in the proof could be a multiple of $f_k \cdot (1 + f_{k'}) = 0$, resulting in the trivial annihilator. Consequently, the restriction in the theorem is sufficient to ensure that the constructed annihilator is nontrivial for all such functions.

Furthermore, we note that Theorem 1 does not apply to majority or (non-constant) threshold functions, as these functions necessarily have at least one slice f_k that corresponds to the constant function 1.

3.2 Towards generalizations

The proof of Theorem 1 relies on the functions $\psi_{r,n}$, which are nonzero only on slices where k is congruent to 0 modulo 2^r. This choice is motivated by its simplicity and the applications studied in Section 4. Nevertheless, the same proof techniques can be applied using other low-degree symmetric functions that take the value 1 on exactly one slice out of every 2^r. In the following theorem, we establish the existence and degree of such functions.

Theorem 2. *Let $n \in \mathbb{N}^*$, $r \in [0, \lfloor \log(n) \rfloor]$ and $k \in [0, 2^r - 1]$, the n-variable Boolean symmetric function:*

$$f = \sum_{\substack{i=0 \\ i \equiv k \mod 2^r}}^{n} \varphi_{i,n},$$

is such that $\deg(f) = 2^r - 1$.

Proof. First, since the family of n-variable elementary symmetric functions forms a basis for the space of n-variable symmetric functions, it follows that f can be expressed as a linear combination of the σ_i. Using Property 1, for all $d \geq 2^r$, the function σ_d evaluates to 0 on all slices $\mathsf{E}_{k,n}$ where $k \in [0, 2^r - 1]$. Consequently, the linear combination of σ_i representing f must involve elementary symmetric functions of degree strictly less than 2^r. Next, by applying Property 1 and Property 2, since for any $d < 2^r$, the function σ_d takes the same value on all slices $\mathsf{E}_{k,n}$ that share the same congruence modulo 2^r, the linear combination of σ_i that matches f on slices of weight in the range $[0, 2^r - 1]$ also maintains the same values as f across all slices. This allows us to conclude that f has degree at most $2^r - 1$.

To show that f has exactly degree $2^r - 1$, we argue by contradiction. Since f takes the value 1 an odd number of times in the range $[0, 2^r - 1]$, the function σ_{2^r-1} must be present in the linear combination defining f. Suppose, for contradiction, that $\deg(f) < 2^r - 1$. Then, f would be a sum of symmetric functions that take the value 1 on an even number of slices in the range $[0, 2^r - 1]$. Indeed, for $d \in [0, 2^r - 2]$, the function σ_d takes the value $\binom{k}{d} \mod 2$ on the slice $\mathsf{E}_{k,n}$ (by Property 1). Moreover, using Property 3, Item 2, we obtain:

$$\sum_{k=0}^{2^r-1} \binom{k}{d} = \sum_{k=d}^{2^r-1} \binom{k}{d} = \binom{2^r}{d+1} \equiv 0 \mod 2,$$

where the congruence modulo 2 follows from Property 2, since $d+1 \in [1, 2^r-1]$. Since all such σ_i functions take the value 1 an even number of times on the slices in the range $[0, 2^r - 1]$, the same must hold for any linear combination of these functions. Consequently, if $\mathsf{deg}(f) < 2^r - 1$, then f would take the value 1 on an even number of slices in the range $[0, 2^r - 1]$, contradicting the definition of f. This contradiction confirms that $\deg(f) = 2^r - 1$. □

Using Theorem 2, there exist cases where nonzero annihilators of degree lower than the bound given in Theorem 1 can be constructed. Let us call r' the value of r leading to the minimum in Theorem 1. If there exists $i \in [0, 2^{r'} - 1]$ such that a function g annihilates all the f_k with $k \equiv i \mod 2^{r'}$ and has degree lower than $d \cdot \lfloor n/2^{r'} \rfloor$, then g is a candidate for constructing an annihilator of lower degree than the upper bound. If g is nonzero on one of the slice $\mathsf{E}_{k,n}$ where $k \equiv i \mod 2^{r'}$, then it is sufficient to obtain an annihilator with the desired property.

It provides a more general perspective on the underlying mechanism behind the results of Section 3.1 for bounding the algebraic immunity. To establish an upper bound on the AI of a function f, we rely on the following facts:

1. There exists a partition $\mathcal{P}$ of $\mathbb{F}_2^n$, $\mathcal{P} = \{P_1, \ldots, P_t\}$ that allows f to be expressed as:
$$f = \sum_{i=1}^{t} f_i \cdot \mathbb{1}_{P_i},$$
where each f_i has low degree.
2. There exists a low degree function g such that g is null on most of the P_i, specifically on all P_i such that $i \in I \subsetneq [1, t]$.
3. There exists a low degree function h such that $h \cdot f_i = 0$ (at least over P_i) for all $i \in [1, t] \setminus I$.
4. The product $g \cdot h$ is nonzero.

We emphasize that the low-degree condition in item 1 is not strictly necessary. In the case of weightwise degree-d functions, it was precisely this property that allowed us to construct a low-degree function h. Generalizing these techniques to upper-bound the algebraic immunity of other families of functions ultimately reduces to identifying partitions where: a low-degree function evaluates to zero on most of the parts, another low-degree function annihilates all remaining terms on the parts where they are defined, and the product of these two functions is nonzero.

For illustration we provide the following example.

Example 1. Let $\mathcal{P}$ be the partition of $\mathbb{F}_2^n$ defined by:

- $P_1 = \{x \in \mathbb{F}_2^n \mid x_1 = 1\}$,
- for $i \in [2, n]$, $P_i = \{x \in \mathbb{F}_2^n \mid x_i = 1, x_1 = \cdots = x_{i-1} = 0\}$,
- $P_{n+1} = \{0_n\}$.

Any function $f \in \mathcal{B}_n$ can be expressed as:
$$f = \sum_{i=1}^{n+1} f_i \cdot \mathbb{1}_{P_i} = f_{n+1} \cdot \mathbb{1}_{0_n} + \sum_{i=1}^{n} f_i \cdot x_i \prod_{j=1}^{i-1}(1 + x_j).$$

We observe that for $j \in [1, n]$ the linear function x_j is null over P_i for $i \in [j+1, n+1]$. Thus it can serve as the function g. Then, an annihilator h of f_i for all $i \in [1, j]$ not null on the set $\{x \in \mathbb{F}_2^n \mid x_j = 1\}$ allows us to build the non null annihilator $x_j \cdot h$ of f, with degree $1 + \mathsf{deg}(h)$ which can be as low as $1 + \sum_{i=1}^{j} \mathsf{deg}(f_i)$.

4 AI bound on already studied functions

In this section, we apply the methodology developed in Section 3 to derive upper bounds on the algebraic immunity of various Boolean functions proposed in the cryptographic literature. We present six cases where our approach is applicable. In each instance, we either disprove a conjecture, revise a previously stated bound, or provide new insight into the true algebraic immunity of the function under study.

4.1 Hidden weight bit function

The hidden weight bit function was introduced in [Bry91] and is considered the simplest example of a function whose binary decision diagram has exponential size [Bry91, BLSW99]. Its cryptographic properties, such as balancedness, nonlinearity, algebraic degree, and algebraic immunity, have been analyzed in [WCST14]. The function's relatively strong parameters have contributed to recent interest in its generalization, particularly towards achieving higher nonlinearity. Another reason for this interest is its computational efficiency.

We begin by recalling the definition of the HWBF, both as presented in [WCST14] and as a WWdd function.

Definition 9 (Hidden weight bit function). *The hidden weight bit function in n variables, $h \in \mathcal{B}_n$ is defined as follows:*

$$h(x) = \begin{cases} 0 & \text{if } x = 0_n, \\ x_{\mathsf{wH}(x)} & \text{otherwise.} \end{cases}$$

It is a weightwise linear function, that can be written as $h = \sum_{k=0}^{n} h_k \varphi_{k,n}$ where:

$$h_0 = 0, \quad \text{and } \forall k \in [1, n] \quad h_k = x_k.$$

In [WCST14], Theorem 4 states that the HWBF has an algebraic immunity of at least $\lfloor \frac{n}{3} \rfloor + 1$, based on a lengthy proof involving case disjunctions and induction. In the following, we demonstrate that this result is incorrect and show that the algebraic immunity of the HWBF does not exceed $3\sqrt{n}$.

Theorem 3 (Upper bound on the algebraic immunity of the HWBF).
Let $n \in \mathbb{N}^*$, the algebraic immunity of the n-variable HWBF h satisfies the relation:

$$\begin{aligned} \mathsf{AI}(h) &\leq \min(2^{\lfloor \frac{\log n}{2} \rfloor} + \lfloor 2^{\log(n) - \lfloor \frac{\log n}{2} \rfloor} \rfloor, 2^{\lceil \frac{\log n}{2} \rceil} + \lfloor 2^{\log(n) - \lceil \frac{\log n}{2} \rceil} \rfloor) - 1 \\ &\leq \sqrt{n}(\sqrt{2} + 1) - 1. \end{aligned}$$

Proof. Since h is weightwise linear, we can apply Theorem 1 to obtain an upper bound on its algebraic immunity. The minimum is attained for $r = \lfloor \log n/2 \rfloor$ or $r = \lceil \log n/2 \rceil$, yielding the first bound. We then proceed by case disjunction. First, we assume that $(\log n)/2 - \lfloor (\log n)/2 \rfloor \leq 0.5$ and denote this quantity by ε. In this case, the bound obtained by taking $r = \lfloor \log n/2 \rfloor$ gives:

$$\begin{aligned} \mathsf{AI}(h) &\leq 2^{\lfloor \frac{\log n}{2} \rfloor} + \lfloor 2^{\log(n) - \lfloor \frac{\log n}{2} \rfloor} \rfloor - 1 \\ &\leq 2^{\frac{\log n}{2}} + 2^{\frac{\log n}{2} + \varepsilon} - 1 \leq \sqrt{n} + \sqrt{n} \cdot 2^{\varepsilon} - 1 \\ &\leq (1 + \sqrt{2})\sqrt{n} - 1. \end{aligned}$$

Otherwise, if $0.5 < (\log n)/2 - \lfloor (\log n)/2 \rfloor < 1$, we define $\varepsilon' = \lceil (\log n)/2 \rceil - (\log n)/2$, which satisfies $\varepsilon' \leq 0.5$. In this case, the bound obtained by taking $r = \lceil \log n/2 \rceil$ gives:

$$\mathsf{AI}(h) \leq 2^{\lceil \frac{\log n}{2} \rceil} + \lfloor 2^{\log(n) - \lceil \frac{\log n}{2} \rceil} \rfloor - 1 \leq 2^{\frac{\log n}{2} + \varepsilon'} + 2^{\frac{\log n}{2}} - 1 \leq (\sqrt{2}+1)\sqrt{n} - 1.$$

We can conclude from the two cases: $\mathsf{AI}(h) \leq \sqrt{n}(\sqrt{2}+1) - 1$.

□

We note that the inconsistency between the statement in [WCST14] and Theorem 3 cannot be observed for small values of n, as computing the algebraic immunity of a function with 20 variables is already computationally demanding in terms of time and resources. In Table 1, we compare the two bounds for several values of n. We observe that the first value of n for which the two bounds become incompatible is $n = 27$. In this case, h admits the following degree-9 annihilator (which can be verified using a computer algebra system such as Sage):

$$(1 + \sigma_{1,n} + \sigma_{2,n} + \sigma_{3,n})(1 + x_4)(1 + x_8)(1 + x_{12})(1 + x_{16})(1 + x_{20})(1 + x_{24}).$$

Bound	5	10	15	20	25	26	27	28	29	30	35	40	50	60
[WCST14], Theorem 4	2	4	6	7	9	9	10	10	10	11	12	14	17	21
Our result, Theorem 3	3	5	6	8	9	9	9	10	10	10	11	12	13	14

Table 1. Comparison of the AI bounds of the HWBF .

The algebraic immunity of the HWBF is significantly lower than previously thought; its value, being less than $3\sqrt{n}$ rather than greater than $n/3$, may undermine its suitability for stream ciphers susceptible to algebraic attacks [CM03, Cou03].

4.2 Weightwise quadratic functions from [MO24]

The WeightWise Quadratic (WWQ) functions introduced in [MO24] are cyclic WWdd functions designed for efficient computation using input-oblivious algorithms, a key requirement for homomorphic evaluation. One of the primary motivations for the functions proposed in [MO24] is their potential application in stream ciphers for hybrid homomorphic encryption [NLV11].

We begin by recalling the notion of cyclic WWdd function introduced in [MO24].

Definition 10 (Cyclic weightwise degree-d function [MO24] Definition 16). *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 O^i denotes the cyclic shift by i positions: $\mathsf{O}^i(x_1, \ldots, x_n) = (x_{1+i \bmod n}, \ldots, x_{n+i \bmod n})$, the representative modulo n being taken as the integer between 1 and n.*

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

In particular, [MO24] investigates the properties of two cyclic WWQ functions, specifically those defined by $g = x_1 + x_2x_3$ and $g = x_1 + \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} x_{2i}x_{2i+1}$, which we denote by t and u, respectively. The following proposition provides an upper bound on the algebraic immunity of cyclic WWQ functions. We omit the proof, as it follows directly from applying Theorem 1 with $d = 2$.

Proposition 2. *Let $n \in \mathbb{N}^*$, and $f \in \mathcal{CWD}_n^2$, associated to g of degree 2 and with no constant term (i.e. $g(0_n) = 0$), then the following holds on f:*

$$\mathsf{AI}(f) \leq \min(2^{\lfloor \frac{(\log n)+1}{2} \rfloor} + 2\lfloor 2^{\log(n)-\lfloor \frac{\log n+1}{2} \rfloor} \rfloor, 2^{\lceil \frac{(\log n)+1}{2} \rceil} + 2\lfloor 2^{\log(n)-\lceil \frac{(\log n)+1}{2} \rceil} \rfloor) - 1.$$

We provide examples of annihilators for t and u when $n = 2^{2k+1}$.

Example 2. Let $k \in \mathbb{N}^*$ and $n = 2^{2k+1}$. In Table 2, we present the values of the bound obtained from Proposition 2 for the first few values of k and provide examples of annihilators for t and u of degree $2^{r+1} - 1 = 2^{\frac{(\log n)+3}{2}} - 1$.

k	n	r	AI bound
1	8	2	≤ 7
2	32	3	≤ 15
3	128	4	≤ 31
4	512	5	≤ 63

Table 2. Algebraic immunity upper bound from Proposition 2 on cyclic WWQ functions in 2^{2k+1} variables.

In particular for t we have the annihilators of degree $2\sqrt{2n} - 1$:

$$\left(\sum_{i=0}^{2^r-1} \sigma_{i,n}\right) \cdot \prod_{j=1}^{2^k} \mathsf{O}^{j\cdot 2^r-1}(1 + x_1 + x_2x_3), \text{ and } \left(\sum_{i=0}^{2^r-1} \sigma_{i,n}\right) \cdot \prod_{j=1}^{2^k} \mathsf{O}^{j\cdot 2^r-1}((1 + x_1)(1 + x_2)).$$

The function u admits the following annihilator:

$$\left(\sum_{i=0}^{2^r-1} \sigma_{i,n}\right) \cdot \prod_{j=1}^{2^k} \mathsf{O}^{j\cdot 2^r-1}(1 + x_1 + \sum_{\ell=1}^{\lfloor \frac{n-1}{2} \rfloor} x_{2\ell}x_{2\ell+1}).$$

Remark 2. We observe that the annihilators derived using the technique behind the proof of Theorem 1 have a higher degree for the functions studied in [MO24] compared to those for the HWBF. This difference arises from the fact that, in this case, we rely solely on the parameter d of the WWdd function, which leads to annihilators of degree close to $2\sqrt{nd}$. Formally, adapting the arguments from the proof of Theorem 3, we obtain the bound $\mathsf{AI} \leq \sqrt{nd}(\sqrt{2} + 1) - 1$.

4.3 Maiorana McFarland subclass from [CS24]

In [CS24], the authors investigate various constructions of Boolean functions aimed at achieving better cryptographic properties than the state of the art and/or facilitating easier implementation. They begin by

examining a specific instance of the Maiorana–McFarland construction, which we will first recall, followed by a modification to ensure balancedness. Their instantiation of the Maiorana–McFarland construction involves WWdd functions, an n-to-n permutation where each coordinate function is affine-equivalent to the HWBF, and the majority function.

Definition 11 (Maiorana-McFarland class). *Let $n \in \mathbb{N}^*$, let $\pi : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ be a bijection, $\pi_1, \ldots, \pi_n$ be the coordinate functions of π, and $h \in \mathcal{B}_n$, let $x \in \mathbb{F}_2^n$, $x = (x_1, \ldots, x_n)$ and $y \in \mathbb{F}_2^n$, $y = (y_1, \ldots, y_n)$. The $2n$-variable Boolean function MM_{2n} is defined as:*

$$\mathsf{MM}_{2n}(x, y) = \pi(x) \cdot y + h(x) = h(x) + \sum_{i=1}^{n} \pi_i(x) y_i,$$

where $\pi(x) \cdot y$ denotes the inner product between $\pi(x)$ and y.

To instantiate π, the authors of [CS24] first examine certain cyclic weightwise degree-d functions for small values of d. They then instantiate π by defining each coordinate function as a cyclic shift of the HWBF. We now recall the definitions of the two main constructions they consider in $2n$ variables:

Definition 12 (MM and Bal instances from [CS24]). *Let $n \in \mathbb{N}^*$. We define the following two families of functions:*

- $$\mathsf{MM\text{-}CS}_{2n}(x, y) = \mathsf{Rot\text{-}HWBF}(x) \cdot y + \mathsf{MAJ}_n(x),$$

  where Rot-HWBF denotes the bijection over $\mathbb{F}_2^n$ in which the i-th coordinate is the HWBF applied to $\mathsf{O}^{i-1}(x)$.
- $$\mathsf{Bal\text{-}CS}_{2n}(x, y) = \mathsf{MM\text{-}CS}_{2n}(x, y) + f(y) \cdot \prod_{i=1}^{n} (1 + x_i),$$

  where $f \in \mathcal{B}_n$.

  In [CS24], Conjecture 1 states the following for even $n \geq 6$:

$$\lfloor \frac{n}{3} \rfloor \leq \mathsf{AI}(\mathsf{MM\text{-}CS}_n) \leq \mathsf{AI}(\mathsf{Bal\text{-}CS}_n) \leq 1 + \lfloor \frac{n}{3} \rfloor.$$

  We disprove the conjecture with the following theorem:

Theorem 4. *Let $n \in \mathbb{N}^*$. The functions $\mathsf{MM\text{-}CS}_{2n}$ and $\mathsf{Bal\text{-}CS}_{2n}$, as defined in Definition 12, satisfy:*

$$\mathsf{AI}(\mathsf{MM\text{-}CS}_{2n}) \leq \sqrt{2n}(\sqrt{2} + 1) - 1, \quad \textit{and} \quad \mathsf{AI}(\mathsf{Bal\text{-}CS}_{2n}) \leq \sqrt{2n}(\sqrt{2} + 1).$$

Proof. First, we rewrite $\mathsf{MM\text{-}CS}_{2n}$ in a way the Hamming weight of x appears:

$$\begin{aligned} \mathsf{MM\text{-}CS}_{2n}(x, y) &= \mathsf{Rot\text{-}HWBF}(x) \cdot y + \mathsf{MAJ}_n(x) = \mathsf{MAJ}_n(x) + y \cdot \mathsf{O}^{\mathsf{w_H}(x)-1}(x) \\ &= \sum_{i=1}^{n} \varphi_{i,n}(x) f_i(x, y), \end{aligned}$$

where:

$$f_i(x, y) = \begin{cases} y \cdot \mathsf{O}^{i-1}(x) = \sum_{j=1}^{n} y_j (\mathsf{O}^{i-1}(x))_j & \text{if } i < n/2, \\ 1 + y \cdot \mathsf{O}^{i-1}(x) = 1 + \sum_{j=1}^{n} y_j (\mathsf{O}^{i-1}(x))_j & \text{otherwise.} \end{cases}$$

The functions $f_i(x, y)$ are quadratic. However, since their expression in terms of $\varphi_{i,n}(x)$ depends only on the weight of the first part of the input, this does not allow us to conclude that $\mathsf{MM\text{-}CS}_{2n}(x, y)$ is WWQ. However, this expression is sufficient to determine low-degree annihilators using Proposition 1 and ideas from the proof of Theorem 1. For $r \in [1, \dots, \lceil \log n \rceil]$ we consider the function g_r defined as:

$$g_r(x, y) = \left(\sum_{i=1}^{2^r-1} \sigma_{i,n}(x) \right) \prod_{j=1}^{\lfloor n/(2^r) \rfloor} (1 + f_{j2^r}(x, y)).$$

The function g_r has degree at most $2^r - 1 + 2\lfloor \frac{n}{2^r} \rfloor$ by construction and serves as an annihilator of $\mathsf{MM\text{-}CS}_{2n}(x, y)$. This follows from the fact that $\sum_{i=1}^{2^r-1} \sigma_{i,n}(x)$ evaluates to 0 for all (x, y) such that $\mathsf{w_H}(x) \not\equiv 0 \mod 2^r$. Additionally, for all values of $\mathsf{w_H}(x)$ congruent to $0 \mod 2^r$ within the range $[2^r, n]$, the term $(1 + f_{j2^r}(x, y))$ in the product ensures that the overall expression evaluates to 0.

To use g_r to bound the algebraic immunity, we need to show that it is not the null function. To do so, we demonstrate the existence of an element $(u, v) \in \mathbb{F}_2^{2n}$ such that $g_r(u, v) = 1$. First, for the component $u \in \mathbb{F}_2^n$, we define $u_i = 1 \Leftrightarrow i \in [2^r, 2 \cdot 2^r - 1]$. Since u has Hamming weight $\mathsf{w_H}(u) = 2^r$, Proposition 1 ensures that $\sum_{i=1}^{2^r-1} \sigma_{i,n}(u) = 1$. Next, we observe that for each $j \in [1, \lfloor n/2^r \rfloor]$, the equation $1 + f_{j2^r}(u, y) = 1$ depends only on 2^r variables y_i:

$$\begin{aligned} 1 + f_{j2^r}(u, y) = 1 &\Leftrightarrow \varepsilon_j + y \cdot \mathsf{O}^{j2^r-1}(u) = 1 \\ &\Leftrightarrow \varepsilon_j + \sum_{i=1}^{2^r} y_{i+n-(j-1)2^r} = 1, \end{aligned}$$

where $\varepsilon_j \in \mathbb{F}_2$. In the $m = \lfloor n/2^r \rfloor$ equations, each variable y_i appears at most once and in an affine equation. Hence, we can find an assignment $v \in \mathbb{F}_2^n$ that satisfies all m equations. Therefore, (u, v) is such that $g_r(u, v) \neq 0$, proving that g_r is a non-null annihilator of $\mathsf{MM\text{-}CS}_{2n}$.

By choosing $r = \lfloor \frac{\log(n)+1}{2} \rfloor$ or $r = \lceil \frac{\log(n)+1}{2} \rceil$ and applying the same arguments as in Theorem 3, we obtain: $\mathsf{AI}(\mathsf{MM\text{-}CS}_{2n}) \leq \sqrt{2n}(\sqrt{2} + 1) - 1$. For $\mathsf{Bal\text{-}CS}_{2n}$, we note that for all $i \in [1, n]$, the following holds:

$$x_i \prod_{j=1}^{n} (1 + x_j) = 0.$$

By selecting any $i \in [2^r, 2 \cdot 2^r - 1]$, we obtain $\mathsf{deg}(x_i \cdot g_r) \leq \mathsf{deg}(g_r) + 1$, ensuring that $x_i \cdot g_r(u, v) = 1$, and:

$$\begin{aligned} (x_i \cdot g_r) \cdot \mathsf{Bal\text{-}CS}_{2n}(x, y) &= (x_i \cdot g_r) \cdot (\mathsf{MM\text{-}CS}_{2n}(x, y) + f(y) \cdot \prod_{i=1}^{n} (1 + x_i)) \\ &= x_i \cdot (g_r \cdot (\mathsf{MM\text{-}CS}_{2n}(x, y)) + g_r \cdot x_i \left(\prod_{i=1}^{n} (1 + x_i) \right) \cdot f(y) \\ &= x_i \cdot 0 + g_r \cdot 0 \cdot f(y) = 0. \end{aligned}$$

Accordingly, $x_i \cdot g_r$ is a non-null annihilator of $\mathsf{Bal\text{-}CS}_{2n}$, regardless of the choice of $f(y)$, allowing us to conclude. □

In Figure 1, we illustrate the difference between the algebraic immunity expected from the conjecture in [CS24], the proven bound from Theorem 4, and the more precise bound derived from the constructed

annihilators. We observe that for $n \geq 72$, the conjecture does not hold. Consequently, MM-CS$_n$ and Bal-CS$_n$ should not be used for this number of variables in contexts where the algebraic immunity needs to be as high as $n/3$.

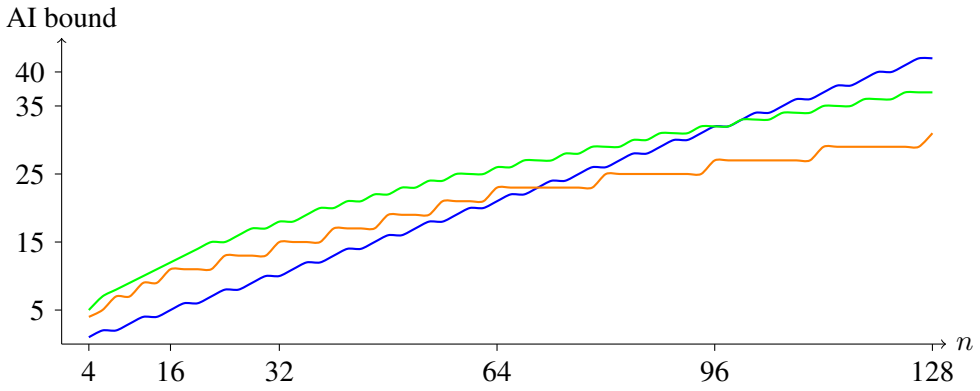

Fig. 1. Comparison of the conjecture of [CS24] and the AI upper bound of MM-CSn for n even. In blue the bound from Conjecture 1, in orange the precise degree of the built annihilators, and in green the upper bound from Theorem 4.

4.4 Revisited HWBF [MST24]

The revisited HWBF, introduced in [MST24], is a variant of the HWBF with significantly higher nonlinearity. We recall its definition:

Definition 13 (Revisited HWBF [MST24], Definition 14). *For an even integer $n \geq 0$, we call revisited HWBF the Boolean function $f \in \mathcal{B}_n$ defined as:*

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

Rewriting this function as a WWdd function, we have $f_0 = 0$, and for $k \in [1, n]$,

$$f_k = x_k + \sum_{i=1}^{n/2} (x_i + 1) x_{i+n/2},$$

which classifies it as a WWQ function. Consequently, we can apply Theorem 1 with $d = 2$, obtaining the same upper bound as in Proposition 2.

In [MST24], it is proven that the AI of the revisited HWBF is at least that of the HWBF minus two. However, this does not result in an AI close to $n/3$, as initially expected based on claims about the HWBF ([WCST14]). Instead, it leads to an AI of at most $\sqrt{n}(\sqrt{2}+1)+1$, as shown in the following proposition. This upper bound is more restrictive than the general bound for WWQ functions.

Proposition 3. *Let $n \in \mathbb{N}^*$ be even, and let f be the n-variable revisited HWBF. Then, we have:*

$$\mathsf{AI}(f) \leq \sqrt{n}(\sqrt{2}+1) + 1.$$

Proof. Using Theorem 3, the n-variable HWBF function h has an algebraic immunity of at most $\sqrt{n}(\sqrt{2}+1)+1$. From the proof of Theorem 1, the annihilators used to establish this bound are annihilators of h (rather than $h+1$), where each subfunction involved takes the value 1 in 0_n. Explicitly, these annihilators of h have the form:

$$g_r = (1+\sigma_1+\cdots+\sigma_{2^r-1}) \prod_{i=1}^{\lfloor n/2^r \rfloor} (1+x_{2^r \cdot i}).$$

Moreover, the quadratic function $q = 1 + \sum_{i=1}^{n/2}(x_i+1)x_{i+n/2}$ also takes the value 1 in 0_n. Let g be the function corresponding to an index r such that $\deg(g_r) \leq \sqrt{n}(\sqrt{2}+1)-1$. Then, the product $g \cdot q$ in not the null function and has degree at most $\sqrt{n}(\sqrt{2}+1)+1$. Denoting by f the n-variable revisited HWBF we obtain:

$$g \cdot q \cdot f = g \cdot q \cdot h + g \cdot q \cdot \sum_{i=1}^{n/2}(x_i+1)x_{i+n/2} = q \cdot 0 + g \cdot 0 = 0,$$

which allows us to conclude. □

4.5 Weightwise quadratic functions from [CMA25]

In [CMA25], the authors propose revisiting the design of filtered linear feedback shift registers, using larger parameters than those typically employed in the 2000s, with a design tailored towards the use case of hybrid homomorphic encryption. The proposed cipher uses, as a filter, a WWQ function f in 128 variables, defined as:

$$f_k = x_k + \sum_{i=1}^{\lfloor \frac{n}{3} \rfloor} x_{k-i}x_{k+2i-1}.$$

Applying Theorem 1 with $n = 128$ and $d = 2$, we obtain the bound $\mathsf{AI}(f) \leq 31$. In [CMA25], the family of functions f (indexed by n) is conjectured to have algebraic immunity at least $\min(\lfloor n/3 \rfloor, 2\sqrt{n})$, which is not contradicted by our results.

Since the function used is WWQ, we also obtain the same general bound as in Proposition 2 (Section 4.2). In particular, Remark 2 gives:

$$\mathsf{AI}(f) \leq \sqrt{2n}(\sqrt{2}+1)+1.$$

4.6 Maiorana McFarland subclass from [CS25]

As a continuation of [CS24], the authors focus on a specific instantiation of the Maiorana–McFarland construction and its balanced variant, and propose filtered LFSRs that use this function as the filtering function. In contrast to MM-CS (Definition 12), the permutation π is replaced with the reverse-order permutation, defined by $\pi_i(x) = x_{n+1-i}$. We denote this variant by MM-CSrev.

In [CS24], Theorem 1 guarantees that when π is a bit permutation, the algebraic immunity of MM_{2n} is at least that of h. In particular, for MM-CSrev, Proposition 4 states that for even $n \geq 4$, we have $\mathsf{AI}(\text{MM-CSrev}) \geq \lceil n/4 \rceil$. For small values of n, the authors observed that $\mathsf{AI}(\text{MM-CSrev})$ takes the value $1 + \lfloor n/4 \rfloor$. In the following, we explain why the algebraic immunity of MM-CSrev is significantly better than that of MM-CS, which grows proportionally to $\sqrt{n}$ as shown in Theorem 4, and we establish an upper bound on its algebraic immunity.

Similarly to the approach used in the proof of Theorem 4, we can rewrite MM-CSrev in terms of the Hamming weight of the first n bits, as follows:

$$\mathsf{MM\text{-}CSrev}_{2n}(x,y) = \pi(x)\cdot y + \mathsf{MAJ}_n(x) = \sum_{i=1}^{n} \varphi_{i,n}(x) f_i(x,y),$$

$$\text{where:} \quad f_i(x,y) = \begin{cases} y\cdot\pi(x) = \sum_{j=1}^{n} y_j x_{n+1-j} & \text{if } i < n/2, \\ 1 + y\cdot\pi(x) = 1 + \sum_{j=1}^{n} y_j x_{n+1-j} & \text{otherwise.} \end{cases}$$

We observe that the function f_i is the same for all $i < n/2$, which we denote by g, and likewise, the function f_i is the same for all $i \geq n/2$, which we denote by h. The functions g and h are complementary (*i.e.* $g = 1 + h$), meaning that their product is identically zero. Consequently, any annihilator constructed using the methodology from the proof of Theorem 4 with two f_i functions results in the null annihilator. This explains why this construction does not yield an annihilator of degree proportional to $\sqrt{n}$, nor does it for any π that is a bit permutation.

The following proposition gives an upper bound on $\mathsf{AI}(\mathsf{MM\text{-}CSrev})$:

Proposition 4. *Let $n \in \mathbb{N}$, $n \geq 4$ be even, the following holds on $\mathsf{MM\text{-}CSrev}_n$:*

$$\mathsf{AI}(\mathsf{MM\text{-}CSrev}_n) \leq 2^{\lceil \log(n/4) \rceil} + 1.$$

Proof. The $\mathsf{MM\text{-}CSrev}_n$ function can be rewritten as $\sum_{i=1}^{n/2} \varphi_{i,n/2}(x)(\varepsilon_i + \sum_{j=1}^{n/2} y_j x_{n/2+1-j})$ where $\varepsilon_i = 0$ for $i < n/4$ and 1 otherwise. We take $r = \lceil \log(n/4) \rceil$, the function:

$$g(x,y) = \left(\sum_{i=0}^{2^r-1} \sigma_{i,n/2}(x)\right) \cdot \left(\sum_{j=1}^{n/2} y_j x_{n/2+1-j}\right)$$

is an annihilator of $\mathsf{MM\text{-}CSrev}_n$ of degree at most $2^{\lceil \log(n/4) \rceil} + 1$. Indeed, by Proposition 1, the first part vanishes on all inputs where x has Hamming weight different from $0 \mod 2^{\lceil \log(n/4) \rceil}$. The second part serves as an annihilator of the function $1 + \sum_{j=1}^{n/2} y_j x_{n/2+1-j}$, which is the value taken by $\mathsf{MM\text{-}CSrev}_n$ when $\mathsf{wH}(x) \geq n/4$. By construction, $g(x,y)$ is not the zero function: take $u \in \mathbb{F}_2^{n/2}$ to be the vector consisting of $2^{\lceil \log(n/4) \rceil}$ consecutive ones followed by zeros, and let $v \in \mathbb{F}_2^{n/2}$ be the vector with $n/2 - 1$ consecutive zeros and a single one. Then we have $g(u,v) = 1$.

□

In Figure 2, we illustrate the bounds on the algebraic immunity of MM-CSrev for even values of n, showing the proven lower bound from [CS25], the extrapolated values based on small n from the same work, and our proven upper bound from Proposition 4.

In [CS25], the functions MM-CS and Bal-CS are proposed in the appendix as alternative filters, as their algebraic immunity appears to be better—estimated around $n/3$ based on extrapolated values—but they are more costly to implement in the model considered. However, as shown in Section 4.3, this extrapolation is not valid, and for functions in more than 75 variables (as suggested for the filtered LFSR instances), the actual AI is lower.

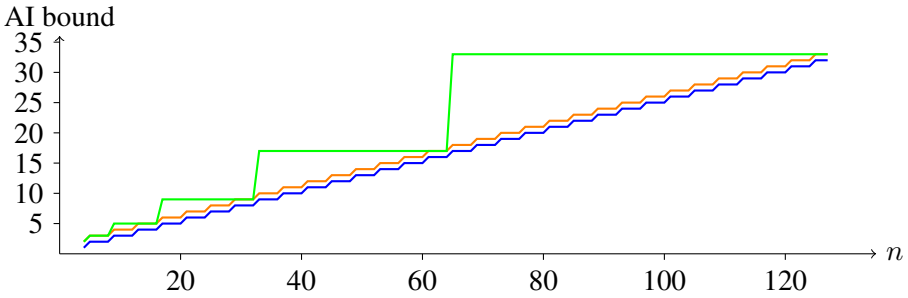

Fig. 2. Bound on the algebraic immunity of MM-CSrev for n even. In blue the proven lower bound from [CS25] in orange the extrapolated value from the experimental results for $n \in [4, 20]$ and in green the upper bound proven in Proposition 4.

5 Conclusions and open questions

In this article, we studied the algebraic immunity of weightwise degree-d functions and presented methods to construct low-degree annihilators for Boolean functions expressed in this form.

We began by showing that certain low-degree symmetric functions vanish on most slices of the Boolean hypercube. We then demonstrated how such functions can be used to construct low-degree annihilators for Boolean functions that coincide with low-degree functions on each slice. This approach was further generalized by combining annihilators across different slices to produce annihilators of even lower degree. More importantly, we showed that the same methodology can be extended to partitions beyond those defined by the slices.

In the second part of the article, we examined the impact of this method on various constructions proposed for cryptographic applications. We first showed that the previously assumed lower bound on the algebraic immunity of the HWBF was incorrect, and our result corrects the misleading belief in the high AI of HWBF and its generalizations. The upper bound we established—proportional to $\sqrt{dn}$ for a WWdd function—enabled us to correct or refine results concerning functions studied in six prior works.

These results open several directions for future work. First, while we demonstrated how the technique can be extended beyond slices, it remains an open question whether it can be generalized to other natural partitions of the Boolean hypercube—such as those arising from rotation symmetric or dihedral symmetric Boolean functions. Second, it would be interesting to investigate whether this framework could be further extended to characterize all annihilators of a given Boolean function. Such a characterization could potentially lead to new lower bounds on the algebraic immunity, complementing the upper bounds established in this work.

6 Acknowledgments

The author was funded by the European Research Council (ERC) under the Advanced Grant program (reference number: 787390).

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, 2015.

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.

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.

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.

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, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 313–333. Springer, 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.

CF08. Claude Carlet and Keqin Feng. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. In Josef Pieprzyk, editor, *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings*, volume 5350 of *Lecture Notes in Computer Science*, pages 425–440. Springer, 2008.

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, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 3–33, 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.

CM03. Nicolas T. Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 345–359. Springer, 2003.

CM21. Claude Carlet and Pierrick Méaux. A complete study of two classes of boolean functions: direct sums of monomials and threshold functions. *IEEE Transactions on Information Theory*, pages 1–1, 2021.

CMA25. Nabil Chacal, Pierrick Méaux, and AnonymousBeforeAcceptance. Nostalgia cipher: can filtered lfsrs be secure again? ORBilu Archive, 2025.

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.

Cou03. Nicolas T. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 176–194. Springer, 2003.

CS24. Claude Carlet and Palash Sarkar. Constructions of efficiently implementable boolean functions possessing high nonlinearity and good resistance to algebraic attacks. *IACR Cryptol. ePrint Arch.*, page 1305, 2024. https://eprint.iacr.org/archive/2024/1305/20240821:123900.5.

CS25. Claude Carlet and Palash Sarkar. The nonlinear filter model of stream cipher redivivus. Cryptology ePrint Archive, Paper 2025/160, 2025.

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 Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 662–692. Springer, 2018.

DGM05. Deepak Kumar Dalai, Kishan Chand Gupta, and Subhamoy Maitra. Cryptographically significant boolean functions: Construction and analysis in terms of algebraic immunity. In Henri Gilbert and Helena Handschuh, editors, *Fast*

Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers, volume 3557 of *Lecture Notes in Computer Science*, pages 98–111. Springer, 2005.

DM15. Léo Ducas and Daniele Micciancio. FHEW: bootstrapping homomorphic encryption in less than a second. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 617–640. Springer, 2015.

DM24. Deepak Kumar Dalai and Krishna Mallick. A class of weightwise almost perfectly balanced boolean functions. *Advances in Mathematics of Communications*, 18(2):480–504, 2024.

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

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

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.

LS20. Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced boolean functions with high weightwise nonlinearity. *Discret. Appl. Math.*, 279:218–227, 2020.

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

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.

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, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 311–343. Springer, 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.

MO24. Pierrick Méaux and Yassine Ozaim. On the cryptographic properties of weightwise affine and weightwise quadratic functions. *Discret. Appl. Math.*, 355:13–29, 2024.

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

MPJ+22. Luca Mariot, Stjepan Picek, Domagoj Jakobovic, Marko Djurasevic, and Alberto Leporati. Evolutionary construction of perfectly balanced boolean functions. In *2022 IEEE Congress on Evolutionary Computation (CEC)*, page 1–8. IEEE Press, 2022.

MPP24. Pierrick Méaux, Jeongeun Park, and Hilder V. L. Pereira. Towards practical transciphering for FHE with setup independent of the plaintext space. *IACR Commun. Cryptol.*, 1(1):20, 2024.

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

MST24. Pierrick Méaux, Tim Seuré, and Deng Tang. The revisited hidden weight bit function. *IACR Cryptol. ePrint Arch.*, page 2022, 2024. To appear at Selected Areas in Cryptography – SAC 2025.

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.

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.