



Article

# Near-Bent Boolean Functions Are Insufficient for Correlation-Robust Hashing: A Spectral Obstruction and an Information-Theoretic Frontier

Guillermo Sosa-Gómez <sup>1,2</sup>

<sup>1</sup> Facultad de Ciencias Económicas y Empresariales, Universidad Panamericana, Álvaro del Portillo 49, Zapopan 45010, Jalisco, Mexico; gsosag@up.edu.mx

<sup>2</sup> Laboratory for Reputation Management in Education, HSE University Saint-Petersburg, Griboedova Embankment 123, Office 502, Saint Petersburg 190068, Russia

## Abstract

Oblivious Transfer (OT) extension, in particular, the construction of Ishai, Kilian, Nissim, and Petrank (CRYPTO 2003) requires a hash function  $H$  that is correlation-robust (CR). All practical instantiations model  $H$  as a random oracle or an ideal cipher, leaving CR with no quantifiable reduction to a structural property of the deployed hash. It is natural to ask whether the most nonlinear balanced Boolean functions available on an odd number of variables, the near-bent functions of the Maiorana–McFarland (MM) class, furnish an algebraic, standard-model CR candidate. We prove that they do not, and we identify precisely why. First, we keep a correct spectral fact: a balanced  $H : \{0, 1\}^n \rightarrow \{0, 1\}$  is  $\varepsilon$ -CR if and only if  $\max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \leq 4\varepsilon \cdot 2^n$ , reducing CR to an autocorrelation bound. Against this criterion we establish three obstructions: (i) The MM-doubling family  $\mathcal{NB}_k$  on  $n = 2k + 1$  variables has autocorrelation supported only on the directions  $(a, 0, 1)$ , where it equals  $2^{k+1}W_a$  with  $\sum_{a \neq 0} W_a^2 = 2^{2k}$ ; hence  $\varepsilon \geq \frac{1}{4}(2^k - 1)^{-1/2}$ , a factor  $\geq 2^{k/2}$  above the value one would need, and an exhaustive search over all balanced members for  $k \leq 2$  returns the maximal  $\varepsilon = \frac{1}{4}$  in every case. (ii) Near-bentness controls the Walsh maximum (nonlinearity), not autocorrelation: every near-bent function satisfies  $\sum_{\Delta \neq 0} \mathcal{A}_f(\Delta)^2 = 2^{2n}$ , so  $\max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \geq 2^n(2^n - 1)^{-1/2}$  and no near-bent function is even approximately CR. (iii) A deterministic  $\mathbf{H} : \{0, 1\}^\kappa \rightarrow \{0, 1\}^\ell$  admits the support bound  $\mathbf{SD}((\mathbf{H}(x), \mathbf{H}(x \oplus \Delta)), (U_\ell, U_\ell)) \geq 1 - 2^{\kappa - 2\ell}$ , so statistical multi-output CR is impossible for  $\ell > \kappa/2$  and in particular at the IKNP regime  $\ell \approx \kappa$ . Together, these results close the near-bent route to standard-model CR and clarify which design objective (low absolute indicator, not high nonlinearity) and which parameter regime ( $\ell \leq \kappa/2$ ) a viable algebraic candidate would have to target.



Academic Editor: Josef Pieprzyk

Received: 1 June 2026

Revised: 24 June 2026

Accepted: 24 June 2026

Published: 26 June 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

**Keywords:** correlation-robust hashing; near-bent Boolean functions; autocorrelation; absolute indicator; oblivious transfer extension; standard model; impossibility; Maiorana–McFarland construction

**MSC:** 94A60; 06E30; 11T71

## 1. Introduction

Oblivious Transfer (OT) is complete for secure two-party and multi-party computation [1,2]: given an OT oracle, any function can be evaluated securely. Garbled circuits, Private Set Intersection, and arithmetic MPC frameworks all consume OTs in bulk, and each

OT, run from scratch, needs a public-key operation. The construction of Ishai, Kilian, Nisim, and Petrank [3], universally abbreviated IKNP, removes this cost at scale: it amplifies  $\kappa$  base OTs into  $m \gg \kappa$  extended OTs using only symmetric primitives, namely a constant number of evaluations of a hash function  $H$  per extended transfer. IKNP and its descendants [4–6] are the workhorse of practical MPC.

The security of IKNP rests entirely on one property of  $H$ , called correlation robustness. Informally, for a fixed but unknown offset  $\Delta$ , the receiver should be unable to distinguish  $H(x \oplus \Delta)$  from fresh randomness, even after seeing  $H$  evaluated at many related points. The original analysis [3], and every refinement since, supplies this property by modeling  $H$  as an idealized object: a random oracle, an ideal cipher, or a random permutation [7,8]. In such a model  $H$  carries no structure, the adversary's advantage is bounded by counting oracle queries, and the security parameter is not a function of any computable feature of the concrete hash that is actually deployed. This is a comfortable engineering situation and a slightly uncomfortable theoretical one: the proof lives outside the standard model, and the quantitative guarantee attaches to an idealization rather than to SHA-256 or AES that runs in production.

There are two known ways to leave the idealized models behind. One replaces the information-theoretic ambition with a computational assumption: Silent OT obtains sublinear communication under the Learning-Parity-with-Noise (LPN) assumption [9], and there are OT constructions from DDH and LWE [10] in the standard model. The other, more speculative, route asks for an explicit algebraic function whose correlation robustness can be read off a structural invariant, with no unproven hardness assumption at all. The appeal of the second route is obvious: a CR bound that is a theorem about the Walsh spectrum of a named function would make the security of OT extension as transparent as the nonlinearity of an S-box.

The natural first candidate for such a function is the most nonlinear balanced object available. On an even number of variables, this is the bent function, whose autocorrelation vanishes identically off the origin; bent functions are, however, never balanced, which disqualifies them as hash outputs. On an odd number of variables,  $n = 2k + 1$ , the analog is the near-bent function, whose Walsh–Hadamard spectrum takes only the two magnitudes 0 and  $2^{(n+1)/2}$  and which attains the maximal nonlinearity  $2^{n-1} - 2^{(n-1)/2}$  of balanced functions in odd dimension [11]. Near-bent functions are explicit, efficiently evaluable through the Maiorana–McFarland (MM) construction [12], and they are as close to “perfectly nonlinear” as a balanced function can be. It is therefore tempting to conjecture that a doubled MM near-bent family yields an algebraic, assumption-free CR hash, and to push that conjecture all the way to a concrete IKNP instantiation with an explicit statistical security bound.

This paper shows that the conjecture is false and, more usefully, explains two independent reasons why, thereby pointing toward what a viable construction would actually require. We do not merely exhibit a gap in a particular proof; we prove that the entire near-bent strategy cannot work for any choice of the underlying permutation and any setting of the parameters, and we separately prove an information-theoretic barrier that no choice of Boolean function can cross.

Our starting point is one correct and useful fact, which we retain. For a balanced scalar function, the correlation-robustness condition is exactly an autocorrelation bound:  $H$  is  $\varepsilon$ -CR if and only if  $\max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \leq 4\varepsilon \cdot 2^n$ , where  $f = (-1)^H$  (Theorem 1). This reduces a cryptographic question to a combinatorial one and is the lens through which the rest of the analysis is conducted. The crucial observation is what this lens reveals: correlation robustness is governed by autocorrelation, a propagation property, whereas near-bentness is a statement about the Walsh maximum, a nonlinearity property. These

two quantities coincide only for bent functions; for balanced functions in odd dimensions, they are essentially unrelated, and the near-bent strategy conflates them.

The first obstruction is specific to the construction. For the MM-doubling family  $\mathcal{NB}_k$ , we compute the autocorrelation in closed form: it is supported only on the directions  $\Delta = (a, 0, 1)$ , where it equals  $2^{k+1}W_a$  for a cross-correlation coefficient  $W_a$  satisfying the Parseval identity  $\sum_{a \neq 0} W_a^2 = 2^{2k}$  (Lemma 2). The identity forces a large coefficient: some nonzero direction has  $|\mathcal{A}_f(\Delta)| \geq 2^{2k+1}(2^k - 1)^{-1/2}$ , hence  $\varepsilon \geq \frac{1}{4}(2^k - 1)^{-1/2}$  (Theorem 2). This already exceeds the value one would need by a factor of at least  $2^{k/2}$ , so the family cannot be CR in any asymptotically meaningful sense. An exhaustive enumeration of *all* balanced members for  $k \leq 2$  sharpens the picture dramatically: every one of them achieves the worst possible  $\varepsilon = \frac{1}{4}$ , because the construction's  $b$ -linear term endows  $f$  with a near-linear structure that drives one autocorrelation coefficient to the extreme value  $\pm 2^n$ .

The second obstruction is generic to the near-bent class and independent of the MM structure. Every near-bent function satisfies the sum-of-squares identity  $\sum_{\Delta \neq 0} \mathcal{A}_f(\Delta)^2 = 2^{2n}$  (Lemma 3), which is exactly twice the bent minimum. A fixed second moment over  $2^n - 1$  directions forces  $\max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \geq 2^n(2^n - 1)^{-1/2} > 2^{n/2}$  (Theorem 4): no near-bent function, however its support is arranged, can be perfectly correlation-robust. The maximum nonlinearity of a near-bent function purchases nothing for CR.

The third obstruction is information-theoretic and concerns the multi-output setting that IKNP actually needs. For any deterministic  $\mathbf{H} : \{0, 1\}^\kappa \rightarrow \{0, 1\}^\ell$  and any offset, the pair  $(\mathbf{H}(x), \mathbf{H}(x \oplus \Delta))$  ranges over at most  $2^\kappa$  values as  $x$  varies, while two independent uniform  $\ell$ -bit strings range over  $2^{2\ell}$ ; hence the statistical distance is at least  $1 - 2^{\kappa-2\ell}$  (Theorem 5). For  $\ell > \kappa/2$  this is overwhelming, and at the IKNP regime  $\ell \approx \kappa$  it is essentially 1. The row-index tweak in the protocol leaves  $\ell$  unchanged and does not help. Statistical, standard-model, multi-output correlation robustness at IKNP parameters is therefore impossible for *every* deterministic hash, near-bent or not, a separation that is implicit in the random-oracle analyses but, to our knowledge, has not been stated as a clean frontier.

### 1.1. Contributions

1. A self-contained, corrected proof that  $\varepsilon$ -correlation-robustness of a balanced scalar function is equivalent to the autocorrelation bound  $\max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \leq 4\varepsilon \cdot 2^n$  (Section 4).
2. A closed-form autocorrelation analysis of the MM-doubling family  $\mathcal{NB}_k$  showing  $\varepsilon \geq \frac{1}{4}(2^k - 1)^{-1/2}$  unconditionally, together with an exhaustive verification that every balanced member for  $k \leq 2$  attains the maximal  $\varepsilon = \frac{1}{4}$  (Section 5).
3. A generic lower bound  $\max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \geq 2^n(2^n - 1)^{-1/2}$  for all near-bent functions, establishing that high nonlinearity is the wrong design objective for CR (Section 6).
4. An information-theoretic impossibility for statistical multi-output CR,  $\mathbf{SD} \geq 1 - 2^{\kappa-2\ell}$ , ruling out the IKNP regime  $\ell \approx \kappa$  for any deterministic hash (Section 7).
5. A delineation of what a viable algebraic CR candidate would need: a low absolute indicator rather than high nonlinearity, and an output length  $\ell \leq \kappa/2$  for the statistical multi-output setting (Section 8); and an explicit account of where the spectral/statistical language certifies security and where it must hand off to a computational assumption or an idealized model (Section 8.3).

### 1.2. Organization

Section 2 surveys related work. Section 3 fixes notation. Section 4 proves the spectral characterization of CR. Section 5 analyzes  $\mathcal{NB}_k$  and proves the construction-specific obstruction. Section 6 proves the generic near-bent lower bound and separates nonlinearity

from autocorrelation. Section 7 proves the multi-output impossibility. Section 8 discusses what would be needed and lists open problems.

## 2. Related Work

### 2.1. Oblivious Transfer and Its Extension

Rabin [13] introduced Oblivious Transfer; the 1-out-of-2 formulation is due to Even, Goldreich, and Lempel [14]. Kilian [1] and Goldreich, Micali, and Wigderson [2] established OT's completeness for secure computation. Beaver [15] showed OT extension is possible in principle; IKNP [3] made it efficient. Asharov, Lindell, Schneider, and Zohner [4] optimized IKNP and introduced the circular variant of CR; Keller, Orsini, and Scholl [5] added active security; Kolesnikov and Kumaresan [6] gave a coding-theoretic refinement for short secrets. Boyle et al. [9] obtained sublinear communication (Silent OT) under LPN, moving the trust from an idealized hash to a computational assumption.

### 2.2. Correlation Robustness

Correlation robustness was defined in [3] and strengthened to circular CR in [4]. Guo, Katz, Wang, and Yu [7] built efficient CR (and tweakable CR) hashes from block ciphers modeled as random permutations; Chen and Tessaro [8] sharpened the bounds using sum-capture theorems, achieving degradation of order  $(p + q)q/2^n$ . Both analyses are in an ideal-permutation model. No construction with a CR guarantee in the standard model reduced to a structural property of a concrete function and free of computational assumptions was previously known, and the present work explains why the most natural algebraic attempt cannot supply one.

### 2.3. Standard-Model and Assumption-Based OT

There are OT constructions from DDH and LWE [10] in the standard model; Peikert, Vaikuntanathan, and Waters [10] from LWE. These provide computational security. Our negative results concern the orthogonal goal of statistical (information-theoretic) CR from an explicit function, and one of them (Section 7) shows that this goal is unreachable in the multi-output IKNP regime regardless of the function, which is exactly the gap that computational assumptions fill.

### 2.4. Bent, Near-Bent, and Plateaued Functions

Bent functions were introduced by Rothaus [16] and Dillon [17]; the Maiorana–McFarland class [12]  $g(x, y) = \langle x, \pi(y) \rangle \oplus h(y)$  provides explicit constructions. Carlet and Mesnager [11] and Tokareva [18] treat near-bent (strictly, two-valued-spectrum) functions in odd dimensions; Carlet's monograph [19] and survey [20] give the general theory.

The quantity relevant to correlation robustness is not the Walsh maximum but the autocorrelation, equivalently, the propagation behavior and the absolute indicator  $\max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)|$  and the sum-of-squares indicator  $\sigma_f = \sum_{\Delta} \mathcal{A}_f(\Delta)^2$  of Zhang and Zheng [21]. Bent functions minimize these indicators and are, for balanced functions, in tension with both balancedness and the existence of algebraic structure. The literature on highly nonlinear functions has long recognized that nonlinearity and autocorrelation are distinct and not jointly optimizable for balanced functions in odd dimensions; our contribution clarifies this distinction by identifying the load-bearing observation in the CR setting and quantifying it for the MM-doubling family.

### 2.5. The Gap This Work Addresses

The open question we settle is whether near-bent functions, the natural odd-dimension analog of bent functions, yield an algebraic standard-model CR hash. The answer is no,

for two independent reasons a spectral obstruction and an information-theoretic barrier and the proof identifies the design target (low absolute indicator) and parameter regime ( $\ell \leq \kappa/2$ ) that any future candidate must respect.

### 3. Preliminaries

#### 3.1. Boolean Functions and the Walsh–Hadamard Transform

A Boolean function is a map  $H : \{0, 1\}^n \rightarrow \{0, 1\}$ ; we write  $f = (-1)^H$  for its  $\pm 1$  encoding. The inner product on  $\{0, 1\}^n$  is  $\langle \omega, x \rangle = \bigoplus_{i=1}^n \omega_i x_i$ .

**Definition 1** (Walsh–Hadamard transform).  $\hat{f}(\omega) = \sum_{x \in \{0, 1\}^n} f(x) (-1)^{\langle \omega, x \rangle}$ ,  $\omega \in \{0, 1\}^n$ .

**Definition 2** (Autocorrelation and indicators). The autocorrelation of  $f$  at  $\Delta$  is  $\mathcal{A}_f(\Delta) = \sum_x f(x) f(x \oplus \Delta)$ . The absolute indicator is  $\Delta_f = \max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)|$ , and the sum-of-squares indicator is  $\sigma_f = \sum_{\Delta} \mathcal{A}_f(\Delta)^2$ .

**Proposition 1** (Standard identities; see Chapter 6, [19]). For  $f = (-1)^H$ : (a)  $\sum_{\omega} \hat{f}(\omega)^2 = 2^{2n}$  (Parseval); (b)  $\hat{f}(0) = 0$  iff  $H$  is balanced; (c)  $\mathcal{A}_f(\Delta) = 2^{-n} \sum_{\omega} \hat{f}(\omega)^2 (-1)^{\langle \omega, \Delta \rangle}$  (Wiener–Khinchin); (d)  $\sigma_f = \sum_{\Delta} \mathcal{A}_f(\Delta)^2 = 2^{-n} \sum_{\omega} \hat{f}(\omega)^4$ .

**Proof.** (a)–(c) are classical [19]. For (d), (c) writes  $2^n \mathcal{A}_f$  as the Fourier transform of  $\hat{f}^2$ ; Parseval applied to  $\hat{f}^2$  gives  $\sum_{\Delta} (2^n \mathcal{A}_f(\Delta))^2 = 2^n \sum_{\omega} \hat{f}(\omega)^4$ , and dividing by  $2^{2n}$  yields (d).  $\square$

**Definition 3** (Nonlinearity; near-bent functions).  $\text{nl}(H) = 2^{n-1} - \frac{1}{2} \max_{\omega} |\hat{f}(\omega)|$ . For  $n = 2k + 1$  odd,  $H$  is near-bent (strict sense) if  $|\hat{f}(\omega)| \in \{0, 2^{(n+1)/2}\}$  for every  $\omega$  [11]; then  $\text{nl}(H) = 2^{n-1} - 2^{(n-1)/2}$ , the maximum over balanced functions on an odd number of variables. By Parseval the support  $S = \{\omega : \hat{f}(\omega) \neq 0\}$  has size  $|S| = 2^{n-1}$ .

#### 3.2. Correlation Robustness

**Definition 4** (Scalar correlation robustness [3]). A balanced  $H : \{0, 1\}^n \rightarrow \{0, 1\}$  is  $\varepsilon$ -correlation-robust ( $\varepsilon$ -CR) if for every  $\Delta \in \{0, 1\}^n \setminus \{0\}$ ,

$$\max_{(a,b) \in \{0,1\}^2} \left| \Pr_{x \leftarrow U_n} [H(x) = a, H(x \oplus \Delta) = b] - \frac{1}{4} \right| \leq \varepsilon. \quad (1)$$

**Definition 5** (Multi-output/IKNP correlation robustness [3,4]).  $\mathbf{H} : \{0, 1\}^{\kappa} \rightarrow \{0, 1\}^{\ell}$  is statistically  $\varepsilon$ -CR if, for a uniformly random offset  $s$  and any distinct query points, the values  $\mathbf{H}(\cdot \oplus s)$  are jointly  $\varepsilon$ -close to uniform; the pairwise case ( $m = 2$ ) requires  $(\mathbf{H}(x), \mathbf{H}(x \oplus \Delta))$  to be  $\varepsilon$ -close to  $(U_{\ell}, U_{\ell})$  for  $x \leftarrow U_{\kappa}$  and every nonzero  $\Delta$ .

**Remark 1.** The semi-honest IKNP protocol [3] reduces sender privacy to  $H$  being  $\varepsilon$ -CR with offset equal to the receiver’s secret  $s$ ; the hybrid argument over  $m$  rows accumulates the per-row CR error. Definition 5 is the property the reduction consumes; Definition 4 is its scalar restriction, which we analyze spectrally.

### 4. The Spectral Characterization of Correlation Robustness

We retain the one positive fact that the autocorrelation lens provides. It is exact for balanced scalar functions and underlies every negative result below.

**Lemma 1** (Moments). Let  $H$  be balanced and  $\Delta \neq 0$ , and write  $C_{\alpha, \beta}(\Delta) = \mathbb{E}_x [(-1)^{\alpha H(x) + \beta H(x \oplus \Delta)}]$ . Then  $C_{1,0}(\Delta) = C_{0,1}(\Delta) = 0$  and  $C_{1,1}(\Delta) = 2^{-n} \mathcal{A}_f(\Delta)$ .

**Proof.**  $C_{1,0} = 2^{-n} \widehat{f}(0) = 0$  and  $C_{0,1} = 0$  by balancedness (Proposition 1(b)). For  $C_{1,1}$ ,  $\mathbb{E}[f(x)f(x \oplus \Delta)] = 2^{-n} \mathcal{A}_f(\Delta)$  by definition.  $\square$

**Theorem 1** (CR  $\Leftrightarrow$  autocorrelation bound). *A balanced  $H : \{0,1\}^n \rightarrow \{0,1\}$  is  $\varepsilon$ -CR if and only if  $\max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \leq 4\varepsilon \cdot 2^n$ .*

**Proof.** By Fourier inversion on  $\mathbb{Z}_2^2$ ,  $\Pr[H(x) = a, H(x \oplus \Delta) = b] = \frac{1}{4} \sum_{\alpha, \beta} (-1)^{\alpha a + \beta b} C_{\alpha, \beta}(\Delta)$ , and  $C_{0,0} = 1$ . The deviation of this probability from  $\frac{1}{4}$  is therefore  $\frac{1}{4}$  times a signed sum of the three nontrivial moments. By Lemma 1 only  $C_{1,1}(\Delta)$  survives, and its contribution to each cell is  $\pm \frac{1}{4} C_{1,1}(\Delta)$ . Hence the maximal cell deviation is  $\frac{1}{4} |C_{1,1}(\Delta)| = \frac{1}{4} \cdot 2^{-n} |\mathcal{A}_f(\Delta)|$ , and the  $\varepsilon$ -CR condition is exactly  $\max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \leq 4\varepsilon \cdot 2^n$ .  $\square$

**Corollary 1.** *Bent functions have  $\mathcal{A}_f(\Delta) = 0$  for all  $\Delta \neq 0$  and hence would be 0-CR by the criterion above; they are excluded because they are unbalanced, so the hypothesis of Theorem 1 fails. This is the structural reason the problem moves to odd dimensions and to near-bent functions in the first place.*

## 5. The Construction-Specific Obstruction in $\mathcal{NB}_k$

### 5.1. The Maiorana–McFarland Doubling Family

Let  $n = 2k + 1$ , let  $g(x, y) = \langle x, \pi(y) \rangle \oplus h(y)$  be an MM bent function on  $\mathbb{F}_2^{2k}$  with  $\pi$  a permutation of  $\mathbb{F}_2^k$  and  $h : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ , and fix  $v = (v_x, v_y) \in \mathbb{F}_2^k \times \mathbb{F}_2^k \setminus \{0\}$ .

**Definition 6** (Family  $\mathcal{NB}_k$ ).

$$H_{g,v}(x, y, b) = g(x, y) \oplus b \cdot (\langle v_x, x \rangle \oplus \langle v_y, y \rangle), \quad x, y \in \mathbb{F}_2^k, b \in \{0, 1\}. \quad (2)$$

Every  $H_{g,v}$  is near-bent: summing over  $b$  gives  $\widehat{f}(\omega_x, \omega_y, \beta) = 2 \sum_{\langle v_x, x \rangle \oplus \langle v_y, y \rangle = \beta} (-1)^{g(x,y) \oplus \langle \omega_x, x \rangle \oplus \langle \omega_y, y \rangle}$ , and a case analysis on the MM structure yields  $|\widehat{f}| \in \{0, 2^{k+1}\} = \{0, 2^{(n+1)/2}\}$ . So the family realizes the maximal nonlinearity. The defect is entirely in its autocorrelation.

Balancedness is *not* automatic: for  $k = 1$ ,  $g(x, y) = xy$ ,  $\pi = \text{id}$ ,  $h = 0$ ,  $v = (1, 0)$ , the function  $H(x, y, b) = xy \oplus bx$  takes the value 1 only at  $(1, 1, 0)$  and  $(1, 0, 1)$  weight 2 of 8. We therefore restrict to the balanced sub-family  $v_x = 0$ ,  $v_y \neq 0$  (the largest sub-family for which balancedness holds uniformly); the obstruction below is established for exactly this sub-family, and an unbalanced function fails CR a fortiori.

### 5.2. Closed-Form Autocorrelation

**Lemma 2** (Autocorrelation of  $\mathcal{NB}_k$ ). *Let  $H_{g,v} \in \mathcal{NB}_k$  with  $v_x = 0$ ,  $v_y \neq 0$ . Then for every  $\Delta \neq 0$ ,  $\mathcal{A}_f(\Delta) = 0$  unless  $\Delta = (a, 0, 1)$  with  $a \neq 0$ , in which case*

$$\mathcal{A}_f(a, 0, 1) = 2^{k+1} W_a, \quad W_a = \sum_{y \in \mathbb{F}_2^k} (-1)^{\langle a, \pi(y) \rangle \oplus \langle v_y, y \rangle}, \quad (3)$$

and the coefficients satisfy

$$\sum_{a \in \mathbb{F}_2^k} W_a^2 = 2^{2k}, \quad W_0 = 0. \quad (4)$$

**Proof.** Write  $G(x, y) = (-1)^{g(x,y)}$  and  $\lambda(x, y) = (-1)^{\langle v_y, y \rangle}$ , so  $f(x, y, b) = G(x, y) \lambda(x, y)^b$  (using  $v_x = 0$ ). Fix  $\Delta = (a, c, \delta)$  and set  $(x', y') = (x \oplus a, y \oplus c)$ . Because  $\langle v_y, y \rangle \oplus \langle v_y, y' \rangle = \langle v_y, c \rangle$ ,  $\lambda(x, y) \lambda(x', y') = (-1)^{\langle v_y, c \rangle}$ .

Case  $\delta = 0$ .  $\mathcal{A}_f(\Delta) = \sum_{x,y} G(x, y) G(x', y') (1 + (-1)^{\langle v_y, c \rangle})$ . This vanishes if  $\langle v_y, c \rangle = 1$ ; if  $\langle v_y, c \rangle = 0$  it equals  $2 \mathcal{A}_G(a, c)$ , which is 0 for  $(a, c) \neq 0$  because  $g$  is bent.

Case  $\delta = 1$ .  $\mathcal{A}_f(\Delta) = \sum_{x,y} G(x,y)G(x',y')(\lambda(x,y) + \lambda(x',y')) = \sum_{x,y} G(x,y)G(x',y')\lambda(x,y)(1 + (-1)^{\langle v_y, c \rangle})$ , which again vanishes for  $\langle v_y, c \rangle = 1$ . For  $\langle v_y, c \rangle = 0$ ,  $\mathcal{A}_f(\Delta) = 2 \sum_{x,y} (-1)^{g(x,y) \oplus g(x',y') \oplus \langle v_y, y \rangle}$ . The exponent's  $x$ -dependence is  $\langle x, \pi(y) \oplus \pi(y \oplus c) \rangle$ , so summing over  $x$  gives  $2^k \mathbf{1}[\pi(y) = \pi(y \oplus c)] = 2^k \mathbf{1}[c = 0]$  since  $\pi$  is a bijection. Hence  $\mathcal{A}_f(\Delta) = 0$  for  $c \neq 0$ , and for  $c = 0$  the residual exponent is  $\langle a, \pi(y) \rangle \oplus \langle v_y, y \rangle$  (the  $h$  terms cancel and the  $x$ -sum contributes  $2^k$ ), giving  $\mathcal{A}_f(a, 0, 1) = 2 \cdot 2^k W_a = 2^{k+1} W_a$ . The case  $a = 0$  gives  $W_0 = \sum_y (-1)^{\langle v_y, y \rangle} = 0$  because  $v_y \neq 0$ .

Finally, expanding the square and using that  $\pi$  is a bijection,  $\sum_a W_a^2 = \sum_{y,y'} (-1)^{\langle v_y, y \oplus y' \rangle} \sum_a (-1)^{\langle a, \pi(y) \oplus \pi(y') \rangle} = 2^k \sum_{y,y'} (-1)^{\langle v_y, y \oplus y' \rangle} \mathbf{1}[y = y'] = 2^k \cdot 2^k = 2^{2k}$ .  $\square$

### 5.3. The Obstruction

**Theorem 2** ( $\mathcal{NB}_k$  is not correlation-robust). For every balanced  $H_{g,v} \in \mathcal{NB}_k$  ( $v_x = 0, v_y \neq 0$ ),

$$\Delta_f = \max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \geq \frac{2^{2k+1}}{\sqrt{2^k - 1}}, \quad \text{equivalently} \quad \varepsilon \geq \frac{1}{4\sqrt{2^k - 1}}. \quad (5)$$

Consequently  $\mathcal{NB}_k$  cannot achieve any  $\varepsilon = o(2^{-k/2})$ ; in particular it falls short of the optimistic target  $\varepsilon = \frac{1}{4} 2^{-(n-1)/2} = \frac{1}{4} 2^{-k}$  by a factor at least  $2^{k/2} \rightarrow \infty$ .

**Proof.** By Lemma 2,  $\Delta_f = 2^{k+1} \max_{a \neq 0} |W_a|$  and  $\sum_{a \neq 0} W_a^2 = 2^{2k}$  over  $2^k - 1$  indices. Averaging,  $\max_{a \neq 0} W_a^2 \geq 2^{2k} / (2^k - 1)$ , so  $\max_{a \neq 0} |W_a| \geq 2^k / \sqrt{2^k - 1}$  and  $\Delta_f \geq 2^{k+1} \cdot 2^k / \sqrt{2^k - 1} = 2^{2k+1} / \sqrt{2^k - 1}$ . Dividing by  $4 \cdot 2^n = 4 \cdot 2^{2k+1}$  (Theorem 1) gives  $\varepsilon \geq 1 / (4\sqrt{2^k - 1})$ .  $\square$

**Theorem 3** (Exhaustive worst case). For  $k \in \{1, 2\}$ , every balanced member of  $\mathcal{NB}_k$  attains the maximal  $\varepsilon = \frac{1}{4}$ , i.e., there exists  $\Delta$  with  $|\mathcal{A}_f(\Delta)| = 2^n$ .

**Proof (exhaustive verification).** We enumerate all  $(\pi, h, v)$  with  $v_x = 0, v_y \neq 0$  and retain the balanced functions: 4 members for  $k = 1$  ( $n = 3$ ) and 576 members for  $k = 2$  ( $n = 5$ ). For each, the autocorrelation spectrum is computed directly. In every case the unique nonzero magnitude off the origin is  $|\mathcal{A}_f| = 2^n$  (i.e.,  $|W_a| = 2^k$  for some  $a$ , saturating Lemma 2), giving  $\varepsilon = 2^n / (4 \cdot 2^n) = \frac{1}{4}$ .  $\square$

**Remark 2** (Why the construction saturates). The coefficient  $W_a$  equals  $\pm 2^k$  precisely when  $y \mapsto \langle a, \pi(y) \rangle \oplus \langle v_y, y \rangle$  is constant, i.e., when the linear form  $\langle v_y, \cdot \rangle$  factors through  $\pi$  as  $\langle a, \pi(\cdot) \rangle$ . The  $b$ -linear term  $b \langle v_y, y \rangle$  of Definition 6 is exactly what creates this alignment: it gives  $f$  a direction  $(a, 0, 1)$  behaving as a (near-)linear structure, where the autocorrelation reaches its extreme  $\pm 2^n$ . The very ingredient that keeps the function near-bent in the Walsh sense ruins it in the autocorrelation sense. For  $k \leq 2$  the alignment is unavoidable; for  $k \geq 3$  a minority of members avoid full saturation but, by Theorem 2, none escapes  $\varepsilon \geq 1 / (4\sqrt{2^k - 1})$ .

## 6. Why Maximal Nonlinearity Does Not Help

The previous obstruction might be blamed on the MM doubling. It cannot: the next bound is generic to the near-bent class and shows that no near-bent function, however, can have its spectral support arranged to be even approximately correlation-robust.

**Lemma 3** (Sum-of-squares of a near-bent function). If  $H$  is near-bent on  $n$  variables then  $\sigma_f = 2^{2n+1}$  and hence  $\sum_{\Delta \neq 0} \mathcal{A}_f(\Delta)^2 = 2^{2n}$ .

**Proof.** By Definition 3,  $\hat{f}(\omega)^2 \in \{0, 2^{n+1}\}$  on a support of size  $2^{n-1}$ , so  $\sum_{\omega} \hat{f}(\omega)^4 = 2^{n-1} \cdot (2^{n+1})^2 = 2^{3n+1}$ . Proposition 1(d) gives  $\sigma_f = 2^{-n} \cdot 2^{3n+1} = 2^{2n+1}$ . Subtracting  $\mathcal{A}_f(0)^2 = 2^{2n}$  leaves  $\sum_{\Delta \neq 0} \mathcal{A}_f(\Delta)^2 = 2^{2n}$ .  $\square$

**Theorem 4** (No approximate CR from near-bent functions). *Every near-bent  $H$  satisfies  $\Delta_f = \max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)| \geq 2^n / \sqrt{2^n - 1} > 2^{n/2}$ , and is therefore not  $\varepsilon$ -CR for any  $\varepsilon < 2^{-n/2-2}$ . The bent value  $\Delta_f = 0$  is unattainable in odd dimensions.*

**Proof.** By Lemma 3, the  $2^n - 1$  nonzero autocorrelation values have squared sum  $2^{2n}$ , so the largest satisfies  $\Delta_f^2 \geq 2^{2n} / (2^n - 1)$ . Then  $\varepsilon = \Delta_f / (4 \cdot 2^n) \geq 1 / (4\sqrt{2^n - 1}) > 2^{-n/2-2}$  by Theorem 1.  $\square$

**Remark 3** (Nonlinearity and autocorrelation are independent). *Near-bentness pins the Walsh maximum and hence the nonlinearity, but Lemma 3 only pins the second moment of the autocorrelation; its maximum is free to lie anywhere from  $\approx 2^{n/2}$  (when the excess  $2^{2n}$  is spread evenly) to  $2^n$  (when it is concentrated on a single linear structure). Section 5 shows the MM family sits at the bad extreme. The general lesson is that high nonlinearity is simply the wrong invariant for correlation robustness: the right one is the absolute indicator  $\Delta_f$ , a propagation quantity that maximal nonlinearity does not control. Bent functions minimize both invariants simultaneously, which is exactly why they are unbalanced and hence unavailable.*

## 7. An Information-Theoretic Frontier for Multi-Output CR

The two obstructions above concern the scalar setting. IKNP needs the multi-output property of Definition 5, and there a barrier applies that no Boolean-function design can cross.

**Theorem 5** (Support bound). *Let  $\mathbf{H} : \{0, 1\}^\kappa \rightarrow \{0, 1\}^\ell$  be any deterministic function and  $\Delta \neq 0$  any offset. For  $x \leftarrow U_\kappa$ ,*

$$\mathbf{SD}(\mathbf{H}(x), \mathbf{H}(x \oplus \Delta)), (U_\ell, U_\ell) \geq 1 - 2^{\kappa-2\ell}. \quad (6)$$

*In particular, for  $\ell = \kappa$  the distance is at least  $1 - 2^{-\kappa}$ , and for any  $\ell > \kappa/2$  it tends to 1.*

**Proof.** The map  $x \mapsto (\mathbf{H}(x), \mathbf{H}(x \oplus \Delta))$  takes at most  $2^\kappa$  distinct values, so the induced distribution  $P$  is supported on a set  $T$  with  $|T| \leq 2^\kappa$ . The uniform distribution  $Q = (U_\ell, U_\ell)$  assigns total mass  $|T|/2^{2\ell}$  to  $T$ . Hence  $\mathbf{SD}(P, Q) \geq P(T) - Q(T) = 1 - |T|/2^{2\ell} \geq 1 - 2^{\kappa-2\ell}$ .  $\square$

**Corollary 2** (Impossibility at IKNP parameters). *No deterministic hash  $\mathbf{H} : \{0, 1\}^\kappa \rightarrow \{0, 1\}^\ell$  with  $\ell > \kappa/2$  is statistically  $\varepsilon$ -CR in the pairwise sense for any  $\varepsilon < 1 - 2^{\kappa-2\ell}$ . The IKNP regime  $\ell \approx \kappa$  (e.g.,  $\kappa = \ell = 128$ ) is therefore unreachable in the standard model by any fixed function. The row-index tweak  $\tilde{\mathbf{H}}(j, x) = \mathbf{H}(x \oplus \phi(j))$  leaves the output length  $\ell$  unchanged and does not affect the bound.*

**Remark 4.** *The barrier is information-theoretic, not computational. In the random-oracle or ideal-cipher model the pair  $(\mathbf{H}(x), \mathbf{H}(x \oplus \Delta))$  is treated as a fresh sample and the support obstruction is bypassed by fiat; a concrete deterministic function cannot do the same. This is precisely the role those models play, and it explains why a standard-model statistical guarantee in this regime is not available from any algebraic construction near-bent or otherwise. Statistical multi-output CR is confined to short outputs  $\ell \leq \kappa/2$ , where it becomes a (still nontrivial) two-source-extractor-type requirement rather than a nonlinearity requirement.*

## 8. Discussion and Open Problems

### 8.1. What a Viable Candidate Would Need

Theorems 2–4 relocate the design target. Correlation robustness in the scalar setting is governed by the absolute indicator  $\Delta_f = \max_{\Delta \neq 0} |\mathcal{A}_f(\Delta)|$ , not by nonlinearity. A useful algebraic CR candidate must therefore minimize  $\Delta_f$  among balanced functions, a propagation/SAC objective in the spirit of [21], and the present results show that maximizing nonlinearity is, if anything, counterproductive, since the constructions that achieve it (MM doubling) introduce linear structure and push  $\Delta_f$  to its extreme. Plateaued functions with a controlled absolute indicator, or functions designed directly for low autocorrelation, are the natural next object of study; whether any balanced family attains  $\Delta_f = o(2^{n/2})$  with explicit structure is open.

### 8.2. What No Candidate Can Do

Theorem 5 caps the ambition: statistical multi-output CR with  $\ell > \kappa/2$  is impossible for every deterministic hash. Any standard-model construction aiming at IKNP-scale outputs must either (i) accept short outputs  $\ell \leq \kappa/2$  and meet a two-source-extractor-type bound, (ii) move to computational security under an assumption such as LPN [9], or (iii) remain in an idealized model [7,8]. The information-theoretic, assumption-free, IKNP-scale target does not exist.

### 8.3. From Spectral Structure to Cryptographic Security: What the Statistical Language Can and Cannot Certify

The results above sit on a boundary that is easy to cross without noticing, and we draw it explicitly here, both because it is the conceptual content of the paper and because it clarifies what a spectral invariant can be trusted to prove.

A Walsh–Hadamard or autocorrelation bound is a statement about the distribution of the outputs of a fixed function. By Theorem 1 it certifies, exactly and with no computational assumption, the statistical correlation robustness of a balanced scalar function: the pair  $(H(x), H(x \oplus \Delta))$  is within the stated distance of uniform over the choice of  $x$ . This is a genuine, model-free guarantee. It is the part of the picture for which the spectral language is the right tool, and the present paper uses it to its limit.

The reach of that guarantee, however, ends at a precise threshold. The distribution of  $(H(x), H(x \oplus \Delta))$  for a deterministic  $H : \{0, 1\}^\kappa \rightarrow \{0, 1\}^\ell$  is supported on at most  $2^\kappa$  points (Theorem 5), so a statistical certificate can exist only while  $2^{2\ell} \lesssim 2^\kappa$ , that is for short outputs  $\ell \leq \kappa/2$ . Below the threshold, the spectral language certifies a real (if hard to achieve) extractor-type property; at and above it in particular at the IKNP regime  $\ell \approx \kappa$  no statistical certificate exists for any function, because the required entropy is not present in a fixed deterministic map. There is nothing a cleverer spectral invariant could recover here: the obstruction is information-theoretic, not analytic.

This is exactly the point at which cryptographic practice introduces a computational assumption or an ideal model, and the support bound explains why it must. When  $H$  is modeled as a random oracle or an ideal cipher, the pair  $(H(x), H(x \oplus \Delta))$  is treated as a fresh sample drawn from the full  $2^{2\ell}$ -point space; the model supplies, by fiat, the independence that a concrete function provably cannot have at these lengths. The ideal object is the “reference mirror” against which a real instantiation is judged, and its role is not decorative: it manufactures precisely the entropy that Theorem 5 forbids a deterministic hash from carrying. A computational assumption plays an analogous role in the standard model, asserting that no efficient distinguisher can exploit the small support even though it exists.

The lesson for a reader importing spectral tools into a security argument is therefore specific. A structural invariant can certify statistical indistinguishability of outputs, and only

that; it cannot, by itself, certify the computational security of a concrete instantiation, and it cannot certify even statistical security once the output length exceeds half the input length. The migration from a Boolean-function invariant to a correlation-robustness guarantee is not a change in vocabulary for the same fact: it is valid only in the regime  $\ell \leq \kappa/2$  and statistical security, and it must hand off to a computational assumption or an idealized model everywhere else. Locating that hand-off is, in our view, the right way to read both the positive characterization of Section 4 and the impossibility of Section 7.

#### 8.4. Open Problems

1. Determine the minimal absolute indicator  $\Delta_f$  achievable by balanced functions on  $n = 2k + 1$  variables with explicit (e.g., algebraic) structure and whether it can reach  $O(2^{n/2})$ , matching the near-bent lower bound of Theorem 4.
2. Characterize the achievable region of pairs  $(\kappa, \ell)$  for which an explicit deterministic hash is statistically  $\varepsilon$ -CR with small  $\varepsilon$ ; Theorem 5 gives the boundary  $\ell \leq \kappa/2$ , and the positive side (construction meeting it) is open.
3. For the scalar setting, decide whether *any* family combining balancedness with a small absolute indicator can be evaluated in  $O(\kappa)$  bit operations without a block-cipher assumption.
4. Extend the analysis to the circular CR property [4] required for actively secure extension [5], where the offset may depend on  $H(x)$ .

### 9. Conclusions

Near-bent functions are the natural odd-dimension analog of bent functions and the obvious candidate for an algebraic, standard-model correlation-robust hash. We have shown that the candidacy fails for two independent reasons. The Maiorana–McFarland doubling family has its autocorrelation concentrated on a single family of directions and is provably no better than  $\varepsilon \geq \frac{1}{4}(2^k - 1)^{-1/2}$  and exactly  $\varepsilon = \frac{1}{4}$  for every balanced member when  $k \leq 2$  because the term that preserves near-bentness also injects a linear structure. More fundamentally, every near-bent function has an absolute indicator of at least  $2^n / \sqrt{2^n - 1}$ , so high nonlinearity buys no correlation robustness at all; the governing invariant is the absolute indicator, a propagation property that nonlinearity does not control. Independently, a support-counting argument shows that statistical multi-output correlation robustness is impossible for any deterministic hash with output length exceeding half the input length, ruling out the IKNP regime in the standard model regardless of the function. The constructive content of these negative results is a sharpened target: minimize the absolute indicator among balanced functions and confine statistical multi-output guarantees to outputs of length at most  $\kappa/2$ .

**Funding:** This research received no external funding.

**Data Availability Statement:** The exhaustive enumeration supporting Theorem 3 is a finite computation; the verification script and its output are available from the author on request.

**Conflicts of Interest:** The author declares no conflicts of interest.

### Abbreviations

The following abbreviations are used in this manuscript:

|      |                             |
|------|-----------------------------|
| CR   | Correlation-robust          |
| OT   | Oblivious Transfer          |
| MPC  | Multi-Party Computation     |
| ROM  | Random Oracle Model         |
| IKNP | Ishai–Kilian–Nissim–Petrack |

|     |                            |
|-----|----------------------------|
| MM  | Maiorana–McFarland         |
| WHT | Walsh–Hadamard Transform   |
| LPN | Learning Parity with Noise |
| SAC | Strict Avalanche Criterion |

## References

1. Kilian, J. Founding Cryptography on Oblivious Transfer. In *STOC '88: Proceedings of the 20th Annual ACM Symposium on Theory of Computing*; ACM: New York, NY, USA, 1988; pp. 20–31.
2. Goldreich, O.; Micali, S.; Wigderson, A. How to Play Any Mental Game or A Completeness Theorem for Protocols with Honest Majority. In *STOC '87: Proceedings of the 19th Annual ACM Symposium on Theory of Computing*; ACM: New York, NY, USA, 1987; pp. 218–229.
3. Ishai, Y.; Kilian, J.; Nissim, K.; Petrank, E. Extending Oblivious Transfers Efficiently. In *Proceedings of the Advances in Cryptology CRYPTO 2003*; Boneh, D., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2729, pp. 145–161.
4. Asharov, G.; Lindell, Y.; Schneider, T.; Zohner, M. More Efficient Oblivious Transfer and Extensions for Faster Secure Computation. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*; Association for Computing Machinery: New York, NY, USA, 2013; pp. 535–548.
5. Keller, M.; Orsini, E.; Scholl, P. Actively Secure OT Extension with Optimal Overhead. In *Proceedings of the Advances in Cryptology CRYPTO 2015*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9215, pp. 724–741.
6. Kolesnikov, V.; Kumaresan, R. Improved OT Extension for Transferring Short Secrets. In *Proceedings of the Advances in Cryptology CRYPTO 2013*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8043, pp. 54–70.
7. Guo, C.; Katz, J.; Wang, X.; Yu, Y. Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers. In *Proceedings of the 2020 IEEE Symposium on Security and Privacy*; IEEE: New York, NY, USA, 2020; pp. 825–841.
8. Chen, Y.L.; Tessaro, S. Better Security–Efficiency Trade-Offs in Permutation-Based Two-Party Computation. In *Proceedings of the Advances in Cryptology ASIACRYPT 2021*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2021; Volume 13091, pp. 275–304.
9. Boyle, E.; Couteau, G.; Gilboa, N.; Ishai, Y.; Kohl, L.; Scholl, P. Efficient Pseudorandom Correlation Generators: Silent OT Extension and More. In *Proceedings of the Advances in Cryptology CRYPTO 2019*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11694, pp. 489–518.
10. Peikert, C.; Vaikuntanathan, V.; Waters, B. A Framework for Efficient and Composable Oblivious Transfer. In *Proceedings of the Advances in Cryptology CRYPTO 2008*; Wagner, D.A., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5157, pp. 554–571. [CrossRef]
11. Carlet, C.; Mesnager, S. A Note on Semi-Bent Boolean Functions. Cryptology ePrint Archive. 2010/486. 2010. Available online: <https://eprint.iacr.org/2010/486> (accessed on 15 April 2026).
12. McFarland, R.L. A Family of Difference Sets in Non-Cyclic Groups. *J. Comb. Theory Ser. A* **1973**, *15*, 1–10. [CrossRef]
13. Rabin, M.O. *How to Exchange Secrets with Oblivious Transfer*; Technical Report TR-81; Aiken Computation Lab, Harvard University: Cambridge, MA, USA, 1981.
14. Even, S.; Goldreich, O.; Lempel, A. A Randomized Protocol for Signing Contracts. *Commun. ACM* **1985**, *28*, 637–647. [CrossRef]
15. Beaver, D. Correlated Pseudorandomness and the Complexity of Private Computations. In *STOC '96: Proceedings of the 28th Annual ACM Symposium on Theory of Computing*; ACM: New York, NY, USA, 1996; pp. 479–488.
16. Rothaus, O.S. On “Bent” Functions. *J. Comb. Theory Ser. A* **1976**, *20*, 300–305. [CrossRef]
17. Dillon, J.F. Elementary Hadamard Difference Sets. Ph.D. Thesis, University of Maryland, College Park, MD, USA, 1974.
18. Tokareva, N. Generalizations of Bent Functions: A Survey. Cryptology ePrint Archive. 2011/111. 2011. Available online: <https://eprint.iacr.org/2011/111> (accessed on 11 April 2026).
19. Carlet, C. Boolean Functions for Cryptography and Error Correcting Codes. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*; Crama, Y., Hammer, P.L., Eds.; Cambridge University Press: Cambridge, UK, 2010; pp. 257–397.
20. Carlet, C. Four Decades of Research on Bent Functions. *Des. Codes Cryptogr.* **2016**, *78*, 5–50.
21. Zhang, X.M.; Zheng, Y. GAC The Criterion for Global Avalanche Characteristics of Cryptographic Functions. *J. Univers. Comput. Sci.* **1995**, *1*, 320–337. [CrossRef]

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.