

Autocorrelations of Vectorial Boolean Functions

Anne Canteaut, Lukas Kölsch, Chao Li, Chunlei Li, Kangquan Li, Longjiang Qu, Friedrich Wiemer

▶ **To cite this version:**

Anne Canteaut, Lukas Kölsch, Chao Li, Chunlei Li, Kangquan Li, et al.. Autocorrelations of Vectorial Boolean Functions. LATINCRYPT 2021 - 7th International Conference on Cryptology and Information Security in Latin America, Oct 2021, Bogota, Colombia. pp.233-253, 10.1007/978-3-030-88238-9_12 . hal-03520200

HAL Id: hal-03520200
https://inria.hal.science/hal-03520200

Submitted on 10 Jan 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Autocorrelations of vectorial Boolean functions

Anne Canteaut[1], Lukas Kölsch[2], Chao Li[3], Chunlei Li[4⋆], Kangquan Li[3], Longjiang Qu[3⋆⋆], and Friedrich Wiemer[5]

[1] Inria, Paris, France, anne.canteaut@inria.fr
[2] University of Rostock, Rostock, Germany, lukas.koelsch@uni-rostock.de
[3] College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, China, and
Hunan Engineering Research Center of Commercial Cryptography Theory and Technology Innovation, Changsha, China
lichao_nudt@sina.com, likangquan11@nudt.edu.cn, ljqu_happy@hotmail.com
[4] Department of Informatics, University of Bergen, Bergen N-5020, Norway, chunlei.li@uib.no
[5] Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany, and cryptosolutions, Essen, Germany, friedrich.wiemer@mailbox.org

Abstract Recently, Bar-On et al. introduced at Eurocrypt'19 a new tool, called the differential-linear connectivity table (DLCT), which allows for taking into account the dependency between the two subciphers E_0 and E_1 involved in differential-linear attacks.
This paper presents a theoretical characterization of the DLCT, which corresponds to an autocorrelation table (ACT) of a vectorial Boolean function. We further provide some new theoretical results on ACTs of vectorial Boolean functions.

Keywords: Vectorial Boolean Functions · Differential-Linear Connectivity Table · Autocorrelation Table · Absolute Indicator

1 Introduction

Let n, m be two arbitrary positive integers. We denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements and by $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$. Vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, also called (n, m)-functions, play a crucial role in block ciphers. Many attacks have been proposed against block ciphers, and have led to diverse criteria, such as low differential uniformity, high nonlinearity, high algebraic degree, etc., that the implemented cryptographic functions must satisfy. At Eurocrypt'18, Cid et al. [17] introduced a new concept on S-boxes:

⋆ The research of Chunlei Li is supported by the Research Council of Norway (No. 247742/O70) and the National Natural Science Foundation of China under Grant (No. 61771021).
⋆⋆ The research of Longjiang Qu is supported by National Key R&D Program of China (No.2017YFB0802000), and the National Natural Science Foundation of China (NSFC) under Grant 61722213, 11531002, 61572026.

the boomerang connectivity table (BCT) that analyzes the dependency between the upper part and lower part of a block cipher in a boomerang attack. The work of [17] quickly attracted attention in the study of BCT property of cryptographic functions [6,27,32,39] and stimulated research progress in other cryptanalysis methods. Very recently, in Eurocrypt'19, Bar-On et al. [1] introduced a new tool called the differential-linear connectivity table (DLCT) that similarly analyzes the dependency between the two subciphers in differential-linear attacks, thereby improving the efficiency of the attacks introduced in [25]. The authors of [1] also presented the relation between the DLCT and the differential distribution table (DDT) of S-boxes.

This paper aims to provide a theoretical characterization of the main properties of the DLCT, explicitly of the set formed by all its entries and of the highest magnitude in this set, for generic vectorial Boolean functions. To this end, we first observe that the DLCT coincides (up to a factor 2) with the autocorrelation table (ACT) of vectorial Boolean functions, which is extended from Boolean functions. Based on the study of the autocorrelation of vectorial Boolean functions, we give some characterizations of the DLCT by means of the Walsh transform and the DDT, and provide a lower bound on the absolute indicator (i.e., equivalently, on the highest absolute value in the DLCT excluding the first row and first column) of any (n, m)-function; then we exhibit an interesting divisibility property of the autocorrelation of (n, m)-functions F, which implies that the entries of DLCT of any (n, n)-permutations are divisible by 4. Next, we investigate the invariance property of the autocorrelation (and the DLCT) of vectorial Boolean functions under affine, extended-affine (EA) and Carlet-Charpin-Zinoviev (CCZ) equivalence, and show that the autocorrelation spectrum is affine-invariant and its maximum in magnitude is EA-invariant but not CCZ-invariant. Based on the classification of optimal 4-bit S-boxes by Leander and Poschmann [26], we explicitly calculate their autocorrelation spectra (see Table 2). Moreover, for certain functions like APN, plateaued and AB functions, we present the relation of their autocorrelation (and DLCT) with other cryptographic criteria. We show that the autocorrelation of APN and AB/plateaued functions can be converted to the Walsh transform of two classes of balanced Boolean functions. Finally, we investigate the autocorrelation spectra of some special polynomials with optimal or low differential uniformity, including monomials, cubic functions, quadratic functions and inverses of quadratic permutations.

The rest of this paper is organized as follows. Section 2 recalls basic definitions, particularly the generalized notion of autocorrelation, the new notion of DLCT, and the connection between them. Most notably, we show that the highest magnitude in the DLCT coincides (up to a factor 2) with the absolute indicator of the function. Section 3 is devoted to the characterization of the autocorrelation: we first characterize the autocorrelation by means of the Walsh transform and of the DDT of the function. We then exhibit generic lower bounds on the absolute indicator of any vectorial Boolean function and study the divisibility of the autocorrelation coefficients. Besides, we study the invariance of the absolute indicator and of the autocorrelation spectrum under the affine, EA and CCZ

equivalences. We also present all possible autocorrelation spectra of optimal 4-bit S-boxes. At the end of this section, we study some properties of the autocorrelation of APN, plateaued and AB functions. In Section 4, we consider the autocorrelation of some special polynomials. Finally, Section 5 draws some conclusions of our work.

2 Preliminaries

In this section, we first recall some basics on (vectorial) Boolean functions and known results that will be useful for our subsequent discussions. Since the vector space $\mathbb{F}_2^n$ can be deemed as the finite field $\mathbb{F}_{2^n}$ for a fixed choice of basis, we will use the notation $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ interchangeably when there is no ambiguity. We will also use the inner product $a \cdot b$ and $\mathrm{Tr}_{2^n}(ab)$ in the context of vector spaces and finite fields interchangeably. For any set E, we denote the nonzero elements of E by E^* (or $E \setminus \{0\}$) and the cardinality of E by $\#E$.

2.1 Walsh transform, Bent functions, AB functions and Plateaued functions

An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. For any n-variable Boolean function f, $W_f(\omega) \coloneqq \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+\omega\cdot x}$ is its *Walsh transform*, where "$\cdot$" is an inner product on $\mathbb{F}_2^n$. The Walsh transform of f can be seen as the *discrete Fourier transform* of the function $(-1)^{f(x)}$ and yields the well known Parseval's relation [13]: $\sum_{\omega\in\mathbb{F}_2^n} W_f^2(\omega) = 2^{2n}$. The *linearity* of f is defined by $\mathtt{L}(f) \coloneqq \max_{\omega\in\mathbb{F}_2^n} |W_f(\omega)|$, where $|r|$ denotes the absolute value of any real value r, and the *nonlinearity* of f is defined by $\mathtt{NL}(f) \coloneqq 2^{n-1} - \frac{1}{2}\mathtt{L}(f)$. According to the Parseval's relation, it is easily seen that the nonlinearity of an n-variable Boolean function is upper bounded by $2^{n-1} - 2^{n/2-1}$. Boolean functions achieving the maximum nonlinearity are called *bent* functions and exist only for even n; their Walsh transforms take only two values $\pm 2^{n/2}$ [37].

For an (n, m)-function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, its *component* corresponding to a nonzero $v \in \mathbb{F}_2^m$ is the Boolean function given by $F_v(x) \coloneqq v \cdot F(x)$. For any $u \in \mathbb{F}_2^n$ and nonzero $v \in \mathbb{F}_2^m$, the Walsh transform of F is defined by those of its components F_v, i.e., $W_F(u, v) \coloneqq \sum_{x\in\mathbb{F}_2^n}(-1)^{u\cdot x+v\cdot F(x)}$. The linear approximation table (LAT) of an (n, m)-function F is the $2^n \times 2^m$ table, in which the entry at position (u, v) is: $\mathtt{LAT}_F(u, v) = W_F(u, v)$, where $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$. The maximum absolute entry of the LAT, ignoring the 0-th column, is the linearity of F denoted as $\mathtt{L}(F)$, i.e., $\mathtt{L}(F) \coloneqq \max_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m\setminus\{0\}} |W_F(u, v)|$. Similarly, the nonlinearity of F is defined by the nonlinearities of the components, namely, $\mathtt{NL}(F) \coloneqq 2^{n-1} - \frac{1}{2}\mathtt{L}(F)$.

An (n, m)-function F is called *vectorial bent*, or shortly *bent* if all its components $F_v(x) = v \cdot F(x)$ for each nonzero $v \in \mathbb{F}_2^m$ are bent. It is well known (n, m)-bent functions exist only if n is even and $m \leq \frac{n}{2}$. Interested readers can refer to [31,42] for more results on bent functions. For (n, m)-functions F with

$m \geq n-1$, the Sidelnikov-Chabaud-Vaudenay bound

$$\mathtt{NL}(F) \leq 2^{n-1} - \frac{1}{2}\left(\frac{3\cdot 2^n - 2(2^n-1)(2^{n-1}-1)}{2^m-1} - 2\right)^{1/2}$$

gives a better upper bound for nonlinearity than the universal bound [15]. When $n = m$ and n is odd, the inequality becomes $\mathtt{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$, and it is achieved by the *almost bent* (AB) functions. It is well known that an (n,n)-function F is AB if and only if its Walsh transform takes only three values $0, \pm 2^{\frac{n+1}{2}}$ [15].

A Boolean function is called *plateaued* if its Walsh transform takes at most three values: 0 and $\pm\mu$, where μ, a positive integer, is called the *amplitude* of the plateaued function. It is clear that bent functions are plateaued. Because of Parseval's relation, the amplitude μ of any plateaued function must be of the form 2^r for certain integer $r \geq n/2$. An (n,m)-function is called *plateaued* if all its components are plateaued, with possibly different amplitudes. In particular, an (n,m)-function F is called *plateaued with single amplitude* if all its components are plateaued with the same amplitude. It is clear that AB functions form a subclass of plateaued functions with the single amplitude $2^{\frac{n+1}{2}}$.

2.2 Differential uniformity and APN functions

For an (n,m)-function F and any $u \in \mathbb{F}_2^n \backslash \{0\}$, the function $D_uF(x) \coloneqq F(x) + F(x+u)$ is called the *derivative of F in direction u*. The *differential distribution table* (DDT) of F is the $2^n \times 2^m$ table, in which the entry at position (u,v) is $\mathtt{DDT}_F(u,v) = \#\{x \in \mathbb{F}_2^n \mid D_uF(x) = v\}$, where $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$. The *differential uniformity* [33] of F is defined as $\max_{u\in\mathbb{F}_2^n\backslash\{0\}, v\in\mathbb{F}_2^m} \mathtt{DDT}_F(u,v)$. Since $D_uF(x) = D_uF(x+u)$ for any x, u in $\mathbb{F}_2^n$, the entries of DDT are always even and the minimum of differential uniformity of F is 2. The functions with differential uniformity 2 are called *almost perfect nonlinear* (APN) functions.

2.3 The DLCT and the autocorrelation table

Differential-linear cryptanalysis tries to exploit a strong differential over one part of an iterated block cipher in combination with a strong linear hull over the other part. They are then combined into a relation of the form $v \cdot (F(x) + F(x+u))$ and the differential-linear bias is defined as

$$\varepsilon(u,v) = 2^{-n}\#\{x \in \mathbb{F}_2^n \mid v \cdot (F(x) + F(x+u)) = 0\} - \frac{1}{2}\ ,$$

where F is an (n,m)-function. Until recently we had to assume the differential and linear parts of the relation to be independent, while several real world examples observed inaccuracies for the resulting bias. The recent work by Bar-On et al. [1] introduced the concept of the differential-linear connectivity table (DLCT) of (n,m)-functions F, to better handle this combination, when dependencies between the two parts of the differential-linear relation occur.

Definition 1 ([1]). *Let F be an (n,m)-function. The DLCT of F is the $2^n \times 2^m$ table whose rows correspond to input differences to F and whose columns correspond to output masks of F, defined as follows: for $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, the DLCT entry at (u,v) is defined by*

$$\mathtt{DLCT}_F(u,v) = \#\{x \in \mathbb{F}_2^n \mid v \cdot F(x) = v \cdot F(x+u)\} - 2^{n-1}.$$

The DLCT is then used to analyse the transition between the differential and linear parts, similar to the sandwich extension for boomerang attacks and the recently introduced boomerang connectivity table (BCT).

Since for any $u \in \mathbb{F}_2^n \backslash \{0\}$, $D_uF(x) = D_uF(x+u)$, $\mathtt{DLCT}_F(u,v)$ must be even. Furthermore, for a given $u \in \mathbb{F}_2^n \backslash \{0\}$, if $D_uF(x)$ is a 2ℓ-to-1 mapping for a positive integer ℓ, then $\mathtt{DLCT}_F(u,v)$ is a multiple of 2ℓ. Moreover, it is trivial that for any $(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$, $|\mathtt{DLCT}_F(u,v)| \leq 2^{n-1}$, and $\mathtt{DLCT}_F(u,v) = 2^{n-1}$ when either $u = 0$ or $v = 0$. Therefore, we only need to focus on the cases for $u \in \mathbb{F}_2^n \backslash \{0\}$ and $v \in \mathbb{F}_2^m \backslash \{0\}$.

Our first observation on the DLCT is that it coincides with the *autocorrelation table* (ACT) of F [44, Section 3]. Below we recall the definition of the autocorrelation of Boolean functions, see e.g. [13, P. 277], and extend it to vectorial Boolean functions.

Definition 2 ([43]). *Given a Boolean function f on $\mathbb{F}_2^n$, the* autocorrelation *of the function f at u is defined as $\mathsf{AC}_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+u)}$. Furthermore, the* absolute indicator *of f is defined as $\Delta_f = \max_{u \in \mathbb{F}_2^n \backslash \{0\}} |\mathsf{AC}_f(u)|$.*

Similarly to Walsh coefficients, this notion can naturally be generalized to vectorial Boolean functions as follows.

Definition 3. *Let F be an (n,m)-function. For any $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, the* autocorrelation *of F at (u,v) is defined as $\mathsf{AC}_F(u,v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x)+F(x+u))}$, the* autocorrelation spectrum *is $\Lambda_F = \{\mathsf{AC}_F(u,v) \mid u \in \mathbb{F}_2^n \setminus \{0\}, v \in \mathbb{F}_2^m \setminus \{0\}\}$. Moreover, $\Delta_F \coloneqq \max_{u \in \mathbb{F}_2^n \backslash \{0\}, v \in \mathbb{F}_2^m \backslash \{0\}} |\mathsf{AC}_F(u,v)|$ is the F's* absolute indicator.

In [44], the term Autocorrelation Table (ACT) for a vectorial Boolean function was introduced. Similarly to the LAT, it contains the autocorrelation spectra of the components of F: $\mathsf{ACT}_F(u,v) = \mathsf{AC}_F(u,v)$. It is also worth noticing that $\mathsf{AC}_F(u,v) = W_{D_uF}(0,v)$.

From Definitions 1 and 3, we immediately have the following connection between the DLCT and the autocorrelation of vectorial Boolean functions.

Proposition 1. *Let F be an (n,m)-function. Then for any $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, the autocorrelation of F at (u,v) is twice the value of the DLCT of F at the same position (u,v), i.e., $\mathtt{DLCT}_F(u,v) = \frac{1}{2}\mathsf{AC}_F(u,v)$. Moreover*

$$\max_{u \in \mathbb{F}_2^n \backslash \{0\}, v \in \mathbb{F}_2^m \backslash \{0\}} |\mathtt{DLCT}_F(u,v)| = \frac{1}{2}\Delta_F \ .$$

For the remainder of this paper we thus stick to the established notion of the autocorrelation table instead of DLCT, and we will study the absolute indicator of the function since it determines the highest magnitude in the DLCT.

Remark 1. Let us recall some relevant results on the autocorrelation table. The entries $\mathsf{AC}_F(u,v), v \neq 0$ in each nonzero row in the ACT of an (n,n)-function F sum to zero if and only if F is a permutation (see e.g. [3, Proposition 2]). The same property holds when the entries $\mathsf{AC}_F(u,v)$, $u \neq 0$ in each nonzero column in the ACT are considered (see e.g. [3, Eq. (9)]).

3 Properties of the autocorrelation table

In this section, we give some characterizations and properties of the ACT of vectorial Boolean functions introduced in Subsection 2.3.

3.1 Links between the autocorrelation and the Walsh transform

In this subsection, we express the autocorrelation by the Walsh transform of the function. The following proposition shows that the restriction of the autocorrelation function $u \mapsto \mathsf{AC}_F(u,v)$ can be seen as the discrete Fourier transform of the squared Walsh transform of F_v: $\omega \mapsto W_F(\omega,v)^2$.

Proposition 2. *Let F be an (n,m)-function. Then for any $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$,*

$$W_F(u,v)^2 = \sum_{\omega \in \mathbb{F}_2^n} (-1)^{\omega \cdot u} \mathsf{AC}_F(\omega,v).$$

Conversely, the inverse Fourier transform leads to

$$\mathsf{AC}_F(\omega,v) = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot \omega} W_F(u,v)^2 \tag{1}$$

Moreover, we have

$$\sum_{u \in \mathbb{F}_2^n} \mathsf{AC}_F(u,v) = W_F(0,v)^2 \tag{2}$$

and

$$\sum_{u \in \mathbb{F}_2^n} \mathsf{AC}_F(u,v)^2 = \frac{1}{2^n} \sum_{\omega \in \mathbb{F}_2^n} W_F(\omega,v)^4. \tag{3}$$

Proof. According to the definition, for any $u \in \mathbb{F}_2^n$,

$$\begin{aligned}
W_F(u,v)^2 &= \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot F(x)} \sum_{y \in \mathbb{F}_2^n} (-1)^{u \cdot y + v \cdot F(y)} \\
&= \sum_{x,y \in \mathbb{F}_2^n} (-1)^{u \cdot (x+y) + v \cdot (F(x)+F(y))} \\
&= \sum_{x,\omega \in \mathbb{F}_2^n} (-1)^{u \cdot \omega + v \cdot (F(x)+F(x+\omega))} \\
&= \sum_{\omega \in \mathbb{F}_2^n} (-1)^{u \cdot \omega} \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x)+F(x+\omega))} \\
&= \sum_{\omega \in \mathbb{F}_2^n} (-1)^{u \cdot \omega} \mathsf{AC}_F(\omega,v).
\end{aligned}$$

The inverse Fourier Transform then leads to Eq. (1). Then Eq. (2) is obtained from Eq. (1) by summing over u. Furthermore, Parseval's equality leads to Eq. (3).

Remark 2. It should be noted that the relations Eq. (1) and Eq. (3) were already obtained in [21] and [43] for Boolean functions. Here we generalize the results to vectorial Boolean functions.

3.2 Links between the autocorrelation and the DDT

[44, Section 3] showed that, for an (n, n)-function, the row of index a in the autocorrelation table $b \mapsto \mathsf{AC}_F(a, b)$ corresponds to the Fourier transform of the row of index a in the DDT: $v \mapsto \mathtt{DDT}_F(a, v)$. This relation coincides with the one provided in [1, Proposition 1]. We here express it in the case of (n, m)-functions. It is worth noticing that this correspondence points out the well known relation between the Walsh transform of F and its DDT exhibited by [15,5].

Proposition 3. *Let F be an (n, m)-function. Then, for any $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, we have*

$$\mathsf{AC}_F(u, v) = \sum_{\omega \in \mathbb{F}_2^m} (-1)^{v \cdot \omega} \mathtt{DDT}_F(u, \omega) \tag{4}$$

$$\mathtt{DDT}_F(u, v) = 2^{-m} \sum_{\omega \in \mathbb{F}_2^m} (-1)^{v \cdot \omega} \mathsf{AC}_F(u, \omega). \tag{5}$$

Most notably,

$$\sum_{v \in \mathbb{F}_2^m} \mathsf{AC}_F(u, v) = 2^m \mathtt{DDT}_F(u, 0) \tag{6}$$

implying

$$\sum_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m} \mathsf{AC}_F(u, v) = 2^{m+n}, \tag{7}$$

and

$$\sum_{v \in \mathbb{F}_2^m} \mathsf{AC}_F(u, v)^2 = 2^m \sum_{\omega \in \mathbb{F}_2^m} \mathtt{DDT}_F(u, \omega)^2. \tag{8}$$

Proof. The first equation holds since $\mathsf{AC}_F(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x) + F(x+u))} = \sum_{\omega \in \mathbb{F}_2^m} (-1)^{v \cdot \omega} \mathtt{DDT}_F(u, \omega)$. The inverse Fourier transform then leads to Eq. (5). For $v = 0$, we then get Eqs. (6) and (7). Finally, Parseval's relation implies Eq. (8).

Note that Nyberg [35,36] and Mesnanger et al. [32] linked the boomerang connectivity table (BCT) to the DDT, which results in the following link to the ACT (see e.g., [36, Proposition 1]): $\sum_{v \in \mathbb{F}_2^m} \mathsf{AC}_F(u, v)^2 = 2^m \sum_{\omega \in \mathbb{F}_2^m} \mathtt{BCT}_F(u, \omega)$.

3.3 Bounds on the absolute indicator

Similar to other cryptographic criteria, it is interesting and important to know how "good" the absolute indicator of a vectorial Boolean function could be. It is clear that the absolute indicator of any (n,m)-function is upper bounded by 2^n. But finding its smallest possible value is an open question investigated by many authors. From the definition, the autocorrelation spectrum of F equals $\{0\}$ if and only if F is a bent function, which implies that n is even and $m \leq \frac{n}{2}$. However, finding lower bounds in other cases is much more difficult. For instance, Zhang and Zheng conjectured [43, Conjecture 1] that the absolute indicator of a balanced Boolean function of n variables is at least $2^{\frac{n+1}{2}}$. But this was later disproved first for odd values of $n \geq 9$ by modifying the Patterson-Wiedemann construction, namely for $n \in \{9, 11\}$ in [24], for $n = 15$ in [28,22] and for $n = 21$ in [20]. For the case n even, [41] gave a construction for balanced Boolean functions with absolute indicator strictly less than $2^{n/2}$ when $n \equiv 2 \bmod 4$. Very recently, similar examples for $n \equiv 0 \bmod 4$ were exhibited by [23]. However, we now show that such small values for the absolute indicator cannot be achieved for (n,n)-*vectorial functions*.

Proposition 3 leads to the following lower bound on the sum of all squared autocorrelation coefficients in each row. This result can be found in [34] (see also [3, Theorem 2]) in the case of (n,n)-functions. We here detail the proof in the case of (n,m)-functions for the sake of completeness.

Proposition 4. *Let F be an (n,m)-function. Then, for all $u \in \mathbb{F}_2^n$, we have $\sum_{v \in \mathbb{F}_2^m} \mathsf{AC}_F(u,v)^2 \geq 2^{n+m+1}$. Moreover, equality holds for all nonzero $u \in \mathbb{F}_2^n$ if and only if F is APN.*

Proof. From Eq. (8), we have that, for all $u \in \mathbb{F}_2^n$,

$$\sum_{v \in \mathbb{F}_2^m} \mathsf{AC}_F(u,v)^2 = 2^m \sum_{\omega \in \mathbb{F}_2^m} \mathtt{DDT}_F(u,\omega)^2$$

Cauchy-Schwarz inequality implies that

$$\left(\sum_{\omega \in \mathbb{F}_2^m} \mathtt{DDT}_F(u,\omega) \right)^2 \leq \left(\sum_{\omega \in \mathbb{F}_2^m} \mathtt{DDT}_F(u,\omega)^2 \right) \times \#\{\omega \in \mathbb{F}_2^m | \mathtt{DDT}_F(u,\omega) \neq 0\} \ ,$$

with equality if and only if all nonzero elements in $\{\mathtt{DDT}_F(u,\omega) | \omega \in \mathbb{F}_2^m\}$ are equal. Using that

$$\#\{\omega \in \mathbb{F}_2^m | \mathtt{DDT}_F(u,\omega) \neq 0\} \leq 2^{n-1}$$

with equality for all nonzero u if and only if F is APN, we deduce that

$$\sum_{\omega \in \mathbb{F}_2^m} \mathtt{DDT}_F(u,\omega)^2 \geq 2^{n+1}$$

with equality for all nonzero u if and only if F is APN. Equivalently, we deduce that

$$\sum_{v\in\mathbb{F}_2^m} \mathsf{AC}_F(u,v)^2 \geq 2^{n+m+1}$$

with equality for all nonzero u if and only if F is APN.

From the previous proposition, we deduce that $\sum_{v\in\mathbb{F}_2^m\setminus\{0\}} \mathsf{AC}_F(u,v)^2 \geq 2^{n+m+1}-2^{2n}$. Since $\sum_{v\in\mathbb{F}_2^m\setminus\{0\}} \mathsf{AC}_F(u,v)^2 \leq \Delta_F^2(2^m-1)$, we get for the absolute indicator $\Delta_F \geq \sqrt{\frac{2^{m+n+1}-2^{2n}}{2^m-1}}$. Thus we have the following result.

Theorem 1. *Let F be an (n,m)-function, where $m \geq n$. Then*

$$\Delta_F \geq \sqrt{\frac{2^{m+n+1}-2^{2n}}{2^m-1}}. \tag{9}$$

Most notably, if $m = n$, $\Delta_F > 2^{n/2}$.

Note that the condition $m \geq n$ in Theorem 1 is to ensure the term under the square root is strictly greater than 0.

3.4 Divisibility of the autocorrelation

In this subsection, we investigate the divisibility property of the autocorrelation coefficients of vectorial Boolean functions.

Proposition 5. *Let $n > 2$ and $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a vectorial Boolean function with algebraic degree at most d. Then, for any $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, $\mathsf{AC}_F(u,v)$ is divisible by $2^{\lceil \frac{n-1}{d-1} \rceil+1}$. In particular, when $m = n$ and F is a permutation, $\mathsf{AC}_F(u,v)$ is divisible by 8.*

Proof. By definition, for any $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$,

$$\mathsf{AC}_F(u,v) = W_{D_uF_v}(0).$$

Note that for given $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$, the Boolean function

$$h_{u,v}(x) = D_uF_v(x) = v \cdot (F(x) + F(x+u)),$$

satisfies two properties: $\deg(h_{u,v}) \leq d-1$ since F has degree at most d and $h_{u,v}(x) = h_{u,v}(x+u)$.

We now focus on the divisibility of $W_{h_{u,v}}(0)$. First, assume for simplicity that $u = e_n = (0,\cdots,0,1)$, we discuss the general case afterwards. Since $h_{e_n,v}(x+e_n) = h_{e_n,v}(x)$, the value of $h_{e_n,v}(x)$ is actually determined by the first $(n-1)$ coordinates of x. Hence $h_{e_n,v}(x)$ can be expressed as $h_{e_n,v}(x) = h(x') : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ and the Walsh transform of $h_{e_n,v}$ at point 0 satisfies

$$W_{h_{e_n,v}}(0) = \sum_{x'\in\mathbb{F}_2^{n-1}, x_n\in\mathbb{F}_2} (-1)^{h_{e_n,v}(x',x_n)} = 2 \cdot \sum_{x'\in\mathbb{F}_2^{n-1}} (-1)^{h(x')} = 2 \cdot W_h(0).$$

It is well known that the values taken by the Walsh transform of a Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ with degree d are divisible by $2^{\lceil \frac{n}{d-1} \rceil}$ (see [30] or [13, Section 3.1]). We then deduce that $W_h(0)$ is divisible by $2^{\lceil \frac{n-1}{d-1} \rceil}$, implying that $W_{h_{e_n,v}}(0)$ is divisible by $2^{\lceil \frac{n-1}{d-1} \rceil + 1}$. Most notably, if $m = n$ and F is bijective, then $d < n$. We then have that

$$\left\lceil \frac{n-1}{d-1} \right\rceil \geq 2,$$

implying that $\mathsf{AC}_F(u,v)$ is divisible by 8.

In the case that $u \neq e_n$, we can find a linear transformation L such that $L(e_n) = u$, with which we have the affine equivalent function $G = F \circ L$. We will show in a moment, see the next section, that for affine equivalent functions, their autocorrelation spectra are invariant (Theorem 2). Thus, the same holds for $\mathsf{AC}_G(u,v)$ in this case.

In particular, for (n,m)-functions of algebraic degree 3, we have the following result.

Proposition 6. *Suppose an (n,m)-function F has algebraic degree 3. Then for nonzero u and v, we have*

$$|\mathsf{AC}_F(u,v)| \in \left\{0, 2^{\frac{n+\delta(u,v)}{2}}\right\},$$

where $\delta(u,v) = \dim\{w \in \mathbb{F}_2^n \mid D_u D_w f_v = c\}$ and $c \in \mathbb{F}_2$ is constant.

The proof can be found in Appendix B. Proposition 6 implies that any entry in the autocorrelation table of a cubic function is divisible by $2^{\frac{n+\psi}{2}}$, where ψ is the smallest integer among $\delta(u,v)$ when u, v run through $\mathbb{F}_2^n \setminus \{0\}$ and $\mathbb{F}_2^m \setminus \{0\}$, respectively. It is clear that $\psi \geq 1$. Furthermore, when $\psi \geq 2$, Proposition 6 improves the result in Proposition 5.

3.5 Invariance under Equivalence Relations

Let n, m be two positive integers. There are several equivalence relations of functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ and they play vital roles in classifying functions with good properties, like AB and APN functions [9]. In this subsection, we first recall three equivalence relations, i.e., affine, EA and CCZ [14]. Then we study the autocorrelation and related concepts with respect to these equivalence relations.

Definition 4. *[8] Let n, m be two positive integers. Two functions F and F' from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called*

1. *affine equivalent (resp. linear equivalent) if $F' = A_1 \circ F \circ A_2$, where the mappings A_1 and A_2 are affine (resp. linear) permutations of $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$, respectively;*
2. *extended affine equivalent (EA equivalent) if $F' = A_1 \circ F \circ A_2 + A$, where the mappings $A : \mathbb{F}_2^n \to \mathbb{F}_2^m, A_1 : \mathbb{F}_2^m \to \mathbb{F}_2^m, A_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are affine and where A_1 and A_2 are permutations;*

3. *Carlet-Charpin-Zinoviev equivalent (CCZ equivalent) if for some affine permutation $\mathcal{L}$ over $\mathbb{F}_2^n \times \mathbb{F}_2^m$, the image by $\mathcal{L}$ of the graph of F is the graph of F', that is $\mathcal{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) | x \in \mathbb{F}_2^n\}$ and $G_{F'} = \{(x, F'(x)) | x \in \mathbb{F}_2^n\}$.*

It is known that affine equivalence is a particular case of EA-equivalence, which is again a particular case of CCZ-equivalence. In addition, every permutation is CCZ-equivalent to its compositional inverse. Two important properties of cryptographic functions, the differential uniformity and the nonlinearity, are invariant under CCZ-equivalence. However, as we will show in this subsection, the autocorrelation spectrum is invariant under affine equivalence, and further its extended autocorrelation spectrum, i.e., the multiset $\{|\mathsf{AC}_F(u, v)| : u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m\}$, is invariant under extended affine equivalence. However, they are generally not invariant under compositional inverse, thereby are not invariant under CCZ-equivalence.

Theorem 2. *Assume two (n, m)-functions F and F' are EA-equivalent. Then the extended autocorrelation spectrum of F equals that of F'. In particular, if they are affine equivalent, then the autocorrelation spectrum of F equals that of F'.*

The proof is detailed in Appendix C.

To examine the behavior under CCZ equivalence, we focus on the autocorrelation of a permutation and the autocorrelation of its compositional inverse. When $n = m$ and F permutes $\mathbb{F}_2^n$, Zhang et al. showed in [44, Corollary 1] that

$$\mathtt{ACT}_{F^{-1}} = H^{-1} \cdot \mathtt{ACT}_F \cdot H,$$

where H is the Walsh-Hadamard matrix of order 2^n. In our notation this is

$$\mathsf{AC}_{F^{-1}}(u, v) = \frac{1}{2^n} \sum_{a,b \in \mathbb{F}_2^n} (-1)^{u \cdot b + v \cdot a} \mathsf{AC}_F(a, b). \tag{10}$$

The relation in Eq. (10) indicates that the autocorrelation spectrum of an (n, n)-permutation F is in general not equal to that of F^{-1}.

This observation is indeed confirmed by many examples, in which an (n, n)-permutation F has linear structures but its inverse has not. Recall from [44] that a linear structure for an (n, m)-function F is a tuple $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ such that $x \mapsto v \cdot (F(x) + F(x + u))$ is constant, zero or one, and $\mathsf{AC}_F(u, v) = \pm 2^n$ if and only (u, v) forms a linear structure. For instance, the S-boxes from SAFER [29], SC2000 [38], and FIDES [4] have linear structures in one direction but not in the other direction. This is also the case of the infinite family formed by the Gold permutations as analyzed in Section 4.2.

Below, we also provide an example that demonstrates that the autocorrelation spectrum is not invariant under EA-equivalence.

Example 1. Let $F(x) = \frac{1}{x} \in \mathbb{F}_{2^7}[x]$ and $F'(x) = \frac{1}{x} + x$. Then F and F' are EA-equivalent. However, F's autocorrelation spectrum is $\Lambda_F = \{-24, -16, -8, 0, 8, 16\}$ where as $\Lambda_{F'} = \{-24, -16, -8, 0, 8, 16, 24\}$.

In [26], the authors classified all optimal permutations over $\mathbb{F}_2^4$ having the best differential uniformity and nonlinearity (both 4) up to affine equivalence and found that there are only 16 different optimal S-boxes, see Table 1 in Appendix A. Based on the classification of optimal S-boxes, we exhaust all possibilities of the autocorrelation spectra of optimal S-boxes in Table 2, where the superscript of each autocorrelation value indicates the number of its occurrences in the spectrum.

3.6 Autocorrelation of Plateaued, AB and APN functions

APN and AB functions provide optimal resistance against differential attacks and linear attacks, respectively. Many researchers have studied some other properties of APN and AB functions (see for example [8]). This subsection will investigate the autocorrelation of these optimal functions. We start with a general result for plateaued functions, which generalizes a result from [21], where the authors studied the autocorrelation of a plateaued Boolean function f in terms of its dual function.

Proposition 7. *Let F be an (n,m)-plateaued function. For $v \in \mathbb{F}_2^m \backslash \{0\}$, we denote the amplitude of the component F_v by 2^{r_v} and define a dual Boolean function of f_v as*

$$\widetilde{f}_v(b) = \begin{cases} 1, & \text{if } W_{f_v}(b) \neq 0, \\ 0, & \text{if } W_{f_v}(b) = 0. \end{cases} \tag{11}$$

Then

$$\mathsf{AC}_F(u,v) = -2^{2r_v-n-1} W_{\widetilde{f}_v}(u).$$

Furthermore, when F is an AB function from $\mathbb{F}_2^n$ to itself, namely, $r_v = \frac{n+1}{2}$ for any $v \in \mathbb{F}_2^n \backslash \{0\}$,

$$\mathsf{AC}_F(u,v) = -W_{\widetilde{f}_v}(u).$$

Proof. According to Eq. (1), we have

$$\begin{aligned} \mathsf{AC}_F(u,v) &= \frac{1}{2^n} \sum_{\omega \in \mathbb{F}_2^n} (-1)^{u\cdot\omega} W_F(\omega,v)^2 = 2^{2r_v-n} \sum_{\omega \in \mathbb{F}_2^n} (-1)^{u\cdot\omega} \widetilde{f}_v(\omega) \\ &= 2^{2r_v-n} \sum_{\omega \in \mathbb{F}_2^n} \left(\frac{1}{2} \left(1 - (-1)^{\widetilde{f}_v(\omega)} \right) \right) (-1)^{u\cdot\omega} = -2^{2r_v-n-1} \sum_{\omega \in \mathbb{F}_2^n} (-1)^{\widetilde{f}_v(\omega)+u\cdot\omega} \\ &= -2^{2r_v-n-1} W_{\widetilde{f}_v}(u). \end{aligned}$$

Particularly, when F is an AB function, i.e., $r_v = \frac{n+1}{2}$ for any $v \in \mathbb{F}_2^m \backslash \{0\}$, it is clear that $\mathsf{AC}_F(u,v) = -W_{\widetilde{f}_v}(u)$.

Similar to the AB functions, the autocorrelation of APN functions can also be expressed in terms of the Walsh transforms of some balanced Boolean functions.

Proposition 8. *Let F be an APN function from $\mathbb{F}_2^n$ to itself. For any nonzero $u \in \mathbb{F}_2^n$, we define the Boolean function*

$$\gamma_u(x) = \begin{cases} 1, & \text{if } x \in \mathsf{Im}(D_uF), \\ 0, & \text{if } x \in \mathbb{F}_2^n \setminus \mathsf{Im}(D_uF). \end{cases} \tag{12}$$

Then the autocorrelation of F can be expressed by the Walsh transform of γ_u as

$$\mathsf{AC}_F(u, v) = -W_{\gamma_u}(v).$$

Proof. Since the APN function F has a 2-to-1 derivative function $D_uF(x)$ at any nonzero u, we know that $\mathsf{Im}(D_uF)$ has cardinality 2^{n-1}. Then,

$$\begin{aligned} \mathsf{AC}_F(u, v) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x+u)+F(x))} = 2 \sum_{y \in \mathsf{Im}(D_uF)} (-1)^{v \cdot y} \\ &= \sum_{y \in \mathsf{Im}(D_uF)} (-1)^{v \cdot y} - \sum_{y \in \mathbb{F}_2^n \setminus \mathsf{Im}(D_uF)} (-1)^{v \cdot y} = -\sum_{y \in \mathbb{F}_2^n} (-1)^{\gamma_u(y)+v \cdot y} = -W_{\gamma_u}(v). \end{aligned}$$

From Proposition 8, we see that the autocorrelation of any APN function corresponds to the Walsh transform of the Boolean function γ_u in Eq. (12), which is balanced. We then immediately deduce the following corollary.

Corollary 1. *Let n be a positive integer. If there exists an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ with absolute indicator Δ, then there exists a balanced Boolean function of n variables with linearity Δ.*

To our best knowledge, the smallest known linearity for a balanced function is obtained by Dobbertin's recursive construction [19]. For instance, for $n = 9$, the smallest possible linearity for a balanced Boolean function is known to belong to the set $\{24, 28, 32\}$, which implies that exhibiting an APN function over $\mathbb{F}_2^9$ with absolute indicator 24 would determine the smallest linearity for such a function.

One of the functions whose absolute indicator is known is the inverse mapping $F(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$.

Proposition 9 (Charpin et al. [16]). *The autocorrelation spectrum of the inverse function $F(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$ is given by*

$$\Lambda_F = \left\{ K(v) - 1 + 2 \times (-1)^{\mathrm{Tr}_{2^n}(v)} \middle| v \in \mathbb{F}_{2^n}^* \right\},$$

where $K(a) = \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{Tr}_{2^n}\left(\frac{1}{x} + ax\right)}$ is the Kloosterman sum over $\mathbb{F}_{2^n}$. Furthermore, the absolute indicator of the inverse function is given by:

i) when n is even, $\Delta_F = 2^{\frac{n}{2}+1}$;
ii) when n is odd, $\Delta_F = \mathtt{L}(F)$ if $\mathtt{L}(F) \equiv 0 \pmod 8$, and $\Delta_F = \mathtt{L}(F) \pm 4$ otherwise.

When n is odd, the inverse mapping is APN. Then, from Proposition 8, its autocorrelation table is directly determined by the corresponding Boolean function γ. This explains why the absolute indicator of the inverse mapping when n is odd, is derived from its linearity as detailed in the following example.

Example 2 (ACT of the inverse mapping, n odd). For any $u \in \mathbb{F}_{2^n}^*$, the Boolean function γ_u, which characterizes the support of Row u in the DDT of the inverse mapping $F : x \mapsto x^{-1}$, coincides with $(1 + F_{u^{-1}})$ except on two points:

$$\gamma_u(x) = \begin{cases} 1 + \mathrm{Tr}_{2^n}(u^{-1}x^{-1}) & \text{if } x \notin \{0, u^{-1}\} \\ 0 & \text{if } x = 0 \\ 1 & \text{if } x = u^{-1} \end{cases} .$$

This comes from the fact that the equation $(x+u)^{-1} + x^{-1} = v$ for $v \neq u^{-1}$ can be rewritten as $x + (x+u) = v(x+u)x$ or equivalently when $v \neq 0$, by setting $y = u^{-1}x$, $y^2 + y = u^{-1}v^{-1}$. It follows that this equation has two solutions if and only if $\mathrm{Tr}_{2^n}(u^{-1}v^{-1}) = 0$. From the proof of the previous proposition, we deduce

$$\mathsf{AC}_F(u, v) = -W_{\gamma_u}(v) = W_{F_{u^{-1}}}(v) + 2\left(1 - (-1)^{\mathrm{Tr}_{2^n}(u^{-1}v)}\right) ,$$

where the additional term corresponds to the value of the sum defining the Walsh transform $W_{F_{u^{-1}}}(v)$ at points 0 and u^{-1}.

4 Autocorrelation spectra and absolute indicator of special polynomials

This section mainly considers some polynomials of special forms. Explicitly, we investigate the autocorrelation spectra and the absolute indicator of the Gold permutations and their inverses, and of the Bracken-Leander functions. Our study is divided into two subsections.

4.1 Monomials

In the subsection, we consider the autocorrelation of some special monomials of cryptographic interest, mainly APN permutations and one class of permutations with differential uniformity 4, over the finite field $\mathbb{F}_{2^n}$. Firstly, we present a general observation on the autocorrelation of monomials, which is similar with other cryptographic criteria.

Proposition 10. *Let* $F(x) = x^d \in \mathbb{F}_{2^n}[x]$. *Then* $\Lambda_F = \{\mathsf{AC}_F(1, v) \mid v \in \mathbb{F}_{2^n}^*\}$. *Moreover, if* $\gcd(d, 2^n - 1) = 1$, *then* $\Lambda_F = \{\mathsf{AC}_F(u, 1) \mid u \in \mathbb{F}_{2^n}^*\}$.

Proposition 10 implies that it suffices to focus on the autocorrelation of the single component function $\mathrm{Tr}_{2^n}\left(x^d\right)$ in the study of the autocorrelation table of the monomial x^d with $\gcd(d, 2^n - 1) = 1$.

We next discuss the autocorrelation of some cubic monomials. From Proposition 6, if $n = m$ is odd, we obviously have that $\Delta_F \geq 2^{\frac{n+1}{2}}$. Furthermore, the equality is achieved when $\dim(\{w \in \mathbb{F}_2^n \mid D_u D_w F_v = c\}) = 1$ for all nonzero u and v. Additionally, an upper bound on the absolute indicator can be established for two cubic APN permutations, namely the Kasami power function and the Welch function. We denote the Kasami power functions K_i and the Welch power function W by

$$K_i : \begin{array}{rcl} \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ x & \mapsto & x^{2^{2i}-2^i+1} \end{array} \qquad \text{and} \qquad W : \begin{array}{rcl} \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ x & \mapsto & x^{2^{(n-1)/2}+3} \end{array}.$$

Proposition 11 (Carlet [12], Lemma 1). *The absolute indicator for W on $\mathbb{F}_{2^n}$ is upper bounded by $\Delta_W \leq 2^{\frac{n+5}{2}}$.*

As long as the (regular) degree of the derivatives is small compared to the field size, the Weil bound gives a nontrivial upper bound for the absolute indicator of a vectorial Boolean function. This is particularly interesting for the Kasami functions as the Kasami exponents do not depend on the field size (contrary to for example the Welch exponent).

Proposition 12. *The absolute indicator of K_i on $\mathbb{F}_{2^n}$ is upper bounded by $\Delta_{K_i} \leq (4^i - 2^{i+1}) \times 2^{\frac{n}{2}}$. In particular, $\Delta_{K_2} \leq 2^{\frac{n+5}{2}}$.*

Proof. Note that the two exponents with the highest degree of any derivative of K_i are $4^i - 2^i$ and $4^i - 2^{i+1} + 1$. The first exponent is even, so it can be reduced using the relation $\mathrm{Tr}_{2^n}(y^2) = \mathrm{Tr}_{2^n}(y)$. The result then follows from the Weil bound. Combining the bound with Proposition 6 yields the bound on K_2.

Some other results on the autocorrelations of cubic Boolean functions $\mathrm{Tr}_{2^n}(x^d)$ are known in the literature, which can be trivially extended to the vectorial functions x^d if $\gcd(d, n) = 1$, see [21, Theorem 5], [12] and [40, Lemmas 2 and 3]. In the case $n = 6r$ and $d = 2^{2r} + 2^r + 1$, the power monomial x^d is not a permutation, but results for all component functions of x^d were derived in [11]. We summarize these results about the absolute indicator in the following proposition.

Proposition 13. *Let $F(x) = x^d$ be a function on $\mathbb{F}_{2^n}$.*

1. *If n is odd and $d = 2^r + 3$ with $r = \frac{n+1}{2}$, then $\Delta_F \in \{2^{\frac{n+1}{2}}, 2^{\frac{n+3}{2}}\}$.*
2. *If n is odd and d is the i-th Kasami exponent, where $3i \equiv \pm 1 \pmod{n}$, then $\Delta_F = 2^{\frac{n+1}{2}}$.*
3. *If $n = 2m$ and $d = 2^{m+1} + 3$, then $\Delta_F \leq 2^{\frac{3m}{2}+1}$.*
4. *If $n = 2m$, m odd and $d = 2^m + 2^{\frac{m+1}{2}} + 1$, then $\Delta_F \leq 2^{\frac{3m}{2}+1}$.*
5. *If $n = 6r$ and $d = 2^{2r} + 2^r + 1$, then $\Delta_F = 2^{5r}$.*

We now provide a different proof of the second case in the previous proposition that additionally relates the autocorrelation table of K_i with the Walsh spectrum of a Gold function.

Proposition 14 (Dillon [18]). *Let n be odd, not divisible by 3 and $3i \equiv \pm 1 \pmod{n}$. Set $f = \mathrm{Tr}_{2^n}(x^d)$ where $d = 4^i - 2^i + 1$ is the i-th Kasami exponent. Then* $\mathrm{Supp}(W_f) = \left\{x \mid \mathrm{Tr}_{2^n}\left(x^{2^i+1}\right) = 1\right\}$.

Proposition 15. *Let n be odd, not divisible by 3 and $3i \equiv \pm 1 \pmod{n}$. Then*

$$\mathsf{AC}_{K_i}(u,v) = -\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n}(uv^{1/d}x + x^{2^i+1})},$$

where $d = 4^i - 2^i + 1$ is the i-th Kasami exponent and $1/d$ denotes the inverse of d in $\mathbb{Z}_{2^n-1}$. In particular, $\Delta_{K_i} = 2^{\frac{n+1}{2}}$.

Refer to Appendix D for the proof. Note that the cases $3i \equiv 1 \pmod{n}$ and $3i \equiv -1 \pmod{n}$ are essentially only one case because the i-th and $(n-i)$-th Kasami exponents belong to the same cyclotomic coset. Indeed, $(4^{n-i} - 2^{n-i} + 1)2^{2i} \equiv 4^i - 2^i + 1 \pmod{2^n - 1}$.

From the known result in the literature, it appears that (n,n)-functions with a low absolute indicator are rare objects, which is also confirmed by experimental results for small integer n.

The Bracken-Leander function [7] is a cubic permutation with differential uniformity 4. In the following, we determine the autocorrelation spectrum and the absolute indicator of the Bracken-Leander function.

Theorem 3. *Let $F(x) = x^{q^2+q+1} \in \mathbb{F}_{q^4}[x]$, where $q = 2^k$. Then for any nonzero u, v, $\mathsf{AC}_F(u,v) \in \left\{-q^3, 0, q^3\right\}$ and $\Delta_F = q^3$.*

The proof is listed in Appendix E.

4.2 Quadratic functions and their inverses

In this subsection, we first consider the general quadratic functions and determine the autocorrelation spectra of the Gold functions and of their inverses. The possible values in the autocorrelation table of a quadratic function are easy to be computed since the differential function of a quadratic function is linearized.

Proposition 16. *Let $F(x) = \sum_{0 \le i < j \le n-1} a_{ij} x^{2^i+2^j} \in \mathbb{F}_{2^n}[x]$. Then the autocorrelation table of F takes values from $\{0, \pm 2^n\}$ and $\Delta_F = 2^n$.*

More precisely, we can determine the autocorrelation spectrum of the Gold functions completely.

Corollary 2. *Let $F(x) = x^{2^i+1} \in \mathbb{F}_{2^n}[x]$. Assume $k = \gcd(i,n)$ and $n' = n/k$. Then*

$$\Lambda_F = \begin{cases} \{0, 2^n\} & \text{if } n' \text{ is even,} \\ \{-2^n, 0\} & \text{if } n' \text{ is odd and } k = 1, \\ \{-2^n, 0, 2^n\} & \text{otherwise.} \end{cases}$$

See Appendix F for the proof.

As previously observed, the autocorrelation spectrum and the absolute indicator are not invariant under compositional inversion. Then, in the following, we consider the absolute indicator of the inverse of a quadratic permutation, which is not obvious at all. Indeed, the absolute indicator depends on the considered function, as we will see later.

Example 3. For $n = 9$, the inverses of the two APN Gold permutations x^3 and x^5, namely x^{341} and x^{409}, do not have the same absolute indicator: the absolute indicator of x^{341} is 56 while the absolute indicator of x^{409} is 72.

Nevertheless, the specificity of quadratic APN permutations for n odd is that they are *crooked* [2], which means that the image set of every derivative $D_uF, u \neq 0$, is the complement of a hyperplane $\langle \pi(u) \rangle^\perp$. Moreover, it is known (see e.g. [10, Proof of Lemma 5]) that all these hyperplanes are distinct, which implies that π is a permutation of $\mathbb{F}_2^n$ when we add to the definition that $\pi(0) = 0$. Then, the following proposition shows that, for any quadratic APN permutation F, the autocorrelation of F^{-1} corresponds to the Walsh transform of π.

Proposition 17. *Let n be an odd integer and F be a quadratic APN permutation over $\mathbb{F}_2^n$. Let further π be the permutation of $\mathbb{F}_2^n$ defined by*

$$\mathsf{Im}(D_uF) = \mathbb{F}_2^n \backslash \langle \pi(u) \rangle^\perp, \quad \textit{when} \quad u \neq 0,$$

and $\pi(0) = 0$. Then for any nonzero u, v in $\mathbb{F}_2^n$, we have $\mathsf{AC}_{F^{-1}}(u, v) = -W_\pi(v, u)$. It follows that $\Delta_{F^{-1}} \geq 2^{\frac{n+1}{2}}$ with equality if and only if π is an AB permutation.

The proof is given in Appendix G.

It is worth noticing that the previous proposition is valid, not only for quadratic APN permutations, but for all crooked permutations, which are a particular case of AB functions. However, the existence of crooked permutations of degree strictly higher than 2 is an open question.

As a corollary of the previous proposition, we get some more precise information on the autocorrelation spectrum of the quadratic power permutations corresponding to the inverses of the Gold functions. Recall that x^{2^i+1} and $x^{2^{n-i}+1}$ are affine equivalent since the two exponents belong to the same cyclotomic coset modulo $(2^n - 1)$. This implies that their inverses share the same autocorrelation spectrum.

Corollary 3. *Let $n > 5$ be an odd integer and $0 < i < n$ with $\gcd(i, n) = 1$. Let F be the APN power permutation over $\mathbb{F}_{2^n}$ defined by $F(x) = x^{2^i+1}$. Then, for any nonzero u and v in $\mathbb{F}_{2^n}$, we have*

$$\mathsf{AC}_{F^{-1}}(u, v) = -W_\pi(v, u), \quad \textit{where} \quad \pi(x) = x^{2^n - 2^i - 2}.$$

Most notably, the absolute indicator of F^{-1} is strictly higher than $2^{\frac{n+1}{2}}$.

Again, see Appendix H for the proof.

In the specific case $n = 5$, it can easily be checked that the inverses of all Gold APN permutations $F(x) = x^{2^i+1}$ have absolute indicator 8.

5 Conclusion

This paper intensively investigates the differential-linear connectivity table (DLCT) of vectorial Boolean functions by clarifing its connection to the autocorrelation table of vectorial Boolean functions. The main contributions of this paper are the following. Firstly, we provide bounds on the absolute indicator of (n, m)-functions when $m \geq n$ and we exhibit the divisibility property of the autocorrelation of any vectorial Boolean function. Moreover, we investigate the invariance of the autocorrelation table under affine, EA and CCZ equivalence and exhaustively compute the autocorrelation spectra of optimal 4-bit S-boxes. Secondly, we analyze some properties of the autocorrelation of cryptographically desirable functions, including APN, plateaued and AB functions and express the autocorrelation of APN and AB functions with the Walsh transform of certain Boolean functions. Finally, we investigate the autocorrelation spectra of some special polynomials, including monomials with low differential uniformity, cubic monomials, quadratic functions and inverses of quadratic permutations.

Open problems

1. Determine a (tight) lower bound on the absolute indicator of vectorial Boolean functions. Are there constructions exhibiting (near) optimal vectorial Boolean functions with respect to that bound?
2. For an odd integer n, are there (n, n)-power functions F with $\Delta_F = 2^{(n+1)/2}$ other than the Kasami APN functions?
3. From Corollary 1 it follows that an APN function with very low absolute indicator is of interest. Is there an APN function in 9 variables with absolute indicator $\Delta = 24$?
4. In addition, the absolute indicators of the Kasami and Welch functions have not been determined completely. Determine the absolute indicators of the Kasami and Welch functions completely.

References

1. Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizman. DLCT: A new tool for differential-linear cryptanalysis. pages 313–342, 2019.
2. Thomas D. Bending and Dmitry Fon-Der-Flaass. Crooked functions, bent functions, and distance regular graphs. *The Electronic Journal of Combinatorics*, 5, 1998.
3. Thierry P. Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbb{F}_2^n$. *IEEE Transactions on Information Theory*, 52(9):4160–4170, 2006.
4. Begül Bilgin, Andrey Bogdanov, Miroslav Knežević, Florian Mendel, and Qingju Wang. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. pages 142–158, 2013.
5. Céline Blondeau and Kaisa Nyberg. New links between differential and linear cryptanalysis. pages 388–404, 2013.
6. Christina Boura and Anne Canteaut. On the boomerang uniformity of cryptographic sboxes. 2018(3):290–310, 2018.

7. Carl Bracken and Gregor Leander. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. *Finite Fields and Their Applications*, 16(4):231–242, 2010.
8. Lilya Budaghyan. *Construction and Analysis of Cryptographic Functions*. New York, NY, USA: Springer-Verlag, 2014.
9. Lilya Budaghyan, Claude Carlet, and Alexander Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.
10. Anne Canteaut and Pascale Charpin. Decomposing bent functions. *IEEE Transactions on Information Theory*, 49(8):2004–2019, 2003.
11. Anne Canteaut, Pascale Charpin, and Gohar M. Kyureghyan. A new class of monomial bent functions. *Finite Fields and Their Applications*, 14(1):221–241, 2008.
12. Claude Carlet. Recursive lower bounds on the nonlinearity profile of boolean functions and their applications. *IEEE Transactions on Information Theory*, 54(3):1262–1272, 2008.
13. Claude Carlet. Boolean functions for cryptography and error-correcting codes. In Yves Crama and Peter L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 257–397. Cambridge University Press, 2010.
14. Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.
15. Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. pages 356–365, 1995.
16. Pascale Charpin, Tor Helleseth, and Victor Zinoviev. Propagation characteristics of $x^{-1} \mapsto x$ and Kloosterman sums. *Finite Fields and Their Applications*, 13(2):366–381, 2007.
17. Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. pages 683–714, 2018.
18. John F. Dillon. Multiplicative difference sets via additive characters. *Designs, Codes and Cryptography*, 17(1-3):225–235, 1999.
19. Hans Dobbertin. Construction of Bent functions and balanced Boolean functions with high nonlinearity. pages 61–74, 1995.
20. Sugata Gangopadhyay, Pradipkumar H. Keskar, and Subhamoy Maitra. Patterson-Wiedemann construction revisited. *Discrete Mathematics*, 306(14):1540–1556, 2006.
21. Guang Gong and Khoongming Khoo. Additive autocorrelation of resilient Boolean functions. pages 275–290, 2004.
22. Selçuk Kavut. Correction to the paper: Patterson-Wiedemann construction revisited. *Discrete Applied Mathematics*, 202:185–187, 2016.
23. Selçuk Kavut, Subhamoy Maitra, and Deng Tang. Construction and search of balanced boolean functions on even number of variables towards excellent autocorrelation profile. *Designs, Codes and Cryptography*, 87(2–3):261–276, 2019.
24. Selçuk Kavut, Subhamoy Maitra, and Melek D. Yücel. Search for boolean functions with excellent profiles in the rotation symmetric class. *IEEE Transactions on Information Theory*, 53(5):1743–1751, 2007.
25. Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. pages 17–25, 1994.
26. Gregor Leander and Axel Poschmann. On the classification of 4 bit S-boxes. In *Arithmetic of Finite Fields*, pages 159–176. Springer Berlin Heidelberg, 2007.

27. Kangquan Li, Longjiang Qu, Bing Sun, and Chao Li. New results about the boomerang uniformity of permutation polynomials. *IEEE Transactions on Information Theory*, 65(11):7542–7553, 2019.
28. Subhamoy Maitra and Palash Sarkar. Modifications of Patterson-Wiedemann functions for cryptographic applications. *IEEE Transactions on Information Theory*, 48(1):278–284, 2002.
29. James L. Massey. SAFER K-64: A byte-oriented block-ciphering algorithm. pages 1–17, 1994.
30. Robert J. McEliece. Weight congruences for p-ary cyclic codes. *Discrete Mathematics*, 3(1-3):177–192, 1972.
31. Sihem Mesnager. *Bent Functions: Fundamentals and Results*. Springer International Publishing, 2016.
32. Sihem Mesnager, Chunming Tang, and Maosheng Xiong. On the boomerang uniformity of quadratic permutations. Cryptology ePrint Archive, Report 2019/277 `https://eprint.iacr.org/2019/277`, 2019.
33. Kaisa Nyberg. Differentially uniform mappings for cryptography. pages 55–64, 1994.
34. Kaisa Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. pages 111–130, 1995.
35. Kaisa Nyberg. Reverse-engineering hidden assumptions in differential-linear attacks. `https://www.cryptolux.org/mediawiki-esc2015/images/8/82/Nyberg_rev.pdf`, 2015.
36. Kaisa Nyberg. The extended autocorrelation and boomerang tables and links between nonlinearity properties of vectorial boolean functions. Cryptology ePrint Archive, Report 2019/1381 `https://eprint.iacr.org/2019/1381`, 2019.
37. O.S Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, 1976.
38. Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun Yajima, Naoya Torii, and Hidema Tanaka. The block cipher SC2000. pages 312–327, 2002.
39. Ling Song, Xianrui Qin, and Lei Hu. Boomerang connectivity table revisited. 2019(1):118–141, 2019.
40. Guanghong Sun and Chuankun Wu. The lower bound on the second-order nonlinearity of a class of boolean functions with high nonlinearity. *Applicable Algebra in Engineering, Communication and Computing*, 22(1):37–45, 2009.
41. Deng Tang and Subhamoy Maitra. Construction of n-variable ($n \equiv 2 \bmod 4$) balanced boolean functions with maximum absolute value in autocorrelation spectra $< 2^{n/2}$. *IEEE Transactions on Information Theory*, 64(1):393–402, 2018.
42. Natalia Tokareva. *Bent Functions: Results and Applications to Cryptography*. Academic Press, 2015.
43. Xian-Mo Zhang and Yuliang Zheng. GAC — the criterion for global avalanche characteristics of cryptographic functions. In *J.UCS The Journal of Universal Computer Science*, pages 320–337. Springer Berlin Heidelberg, 1996.
44. Xian-Mo Zhang, Yuliang Zheng, and Hideki Imai. Relating differential distribution tables to other properties of of substitution boxes. *Designs, Codes and Cryptography*, 19(1):45–63, 2000.

A Tables for optimal 4 bit Sboxes

Table 1: Representatives for all 16 classes of optimal 4 bit Sboxes

F_0	$0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 12, 9, 3, 14, 10, 5$
F_1	$0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 14, 3, 5, 9, 10, 12$
F_2	$0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 14, 3, 10, 12, 5, 9$
F_3	$0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 5, 3, 10, 14, 11, 9$
F_4	$0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 9, 11, 10, 14, 5, 3$
F_5	$0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 3, 5$
F_6	$0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 5, 3$
F_7	$0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 14, 11, 10, 9, 3, 5$
F_8	$0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 9, 5, 10, 11, 3, 12$
F_9	$0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 3, 5, 9, 10, 12$
F_{10}	$0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 5, 10, 9, 3, 12$
F_{11}	$0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 10, 5, 9, 12, 3$
F_{12}	$0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 10, 9, 3, 12, 5$
F_{13}	$0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 9, 5, 11, 10, 3$
F_{14}	$0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 11, 3, 9, 5, 10$
F_{15}	$0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 11, 9, 3, 10, 5$

Table 2: Autocorrelation spectrum of F_i for $0 \leq i \leq 15$

F_i	Autocorrelation spectrum
$i \in \{3, 4, 5, 6, 7, 11, 12, 13\}$	$\{-8^{60}, 0^{135}, 8^{30}\}$
$i \in \{0, 1, 2, 8\}$	$\{-16^6, -8^{48}, 0^{144}, 8^{24}, 16^3\}$
$i \in \{9, 10, 14, 15\}$	$\{-16^2, -8^{56}, 0^{138}, 8^{28}, 16^1\}$

B Proof of Proposition 6

Proof. Since F has algebraic degree 3, the derivative of order two $D_u D_w F_v(x) = A_{u,v}(w) \cdot x + C_{u,v}(w)$ is affine over $\mathbb{F}_{2^n}$, where $A_{u,v}(w)$ and $C_{u,v}(w)$ belong to $\mathbb{F}_2$. Moreover, the function $w \mapsto C_{u,v}(w)$ is linear over the linear subspace $L(u,v) = \{w \in \mathbb{F}_2^n : A_{u,v}(w) = 0\} = \{w \in \mathbb{F}_2^n : D_u D_w F_v(x) = C_{u,v}(w)\}$. From the definition of autocorrelation, we have

$$\begin{aligned}
\mathsf{AC}_F(u,v)^2 &= \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{v \cdot (F(x+u)+F(x))} \right)^2 \\
&= \sum_{x,y \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x+u)+F(x)+F(y+u)+F(y))} \\
&= \sum_{x,w \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x+u)+F(x)+F(x+w+u)+F(x+w))} \\
&= \sum_{x,w \in \mathbb{F}_2^n} (-1)^{D_u D_w F_v(x)} \\
&= \sum_{w \in \mathbb{F}_2^n} (-1)^{C_{u,v}(w)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{A_{u,v}(w) \cdot x}.
\end{aligned}$$

Hence,

$$\mathsf{AC}_F(u,v)^2 = \begin{cases} 0, & \text{if } A_{u,v}(w) \neq 0, \\ 2^{n+\delta(u,v)} & \text{if } A_{u,v}(w) = 0 \text{ and } C_{u,v}(w) = c \text{ in } L(u,v). \end{cases}$$

The desired conclusion directly follows.

C Proof of Theorem 2

Proof. Since F and F' are EA equivalent, there exist affine mappings $A : \mathbb{F}_2^n \to \mathbb{F}_2^m, A_1 : \mathbb{F}_2^m \to \mathbb{F}_2^m, A_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where A_1, A_2 are permutations, such that $F' = A_1 \circ F \circ A_2 + A$. Assume that the linear parts of A, A_1, A_2 are L, L_1, L_2

respectively. Then for any $u \in \mathbb{F}_2^n \backslash \{0\}$ and $v \in \mathbb{F}_2^m \backslash \{0\}$,

$$\begin{aligned}
\mathsf{AC}_{F'}(u,v) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot\left(F'(x)+F'(x+u)\right)} \\
&= \sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot(A_1\circ F\circ A_2(x)+A(x)+A_1\circ F\circ A_2(x+u)+A(x+u))} \\
&= (-1)^{v\cdot L(u)} \sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot(A_1\circ F\circ A_2(x)+A_1\circ F\circ A_2(x+u))} \\
&= (-1)^{v\cdot L(u)} \sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot L_1(F\circ A_2(x)+F\circ A_2(x+u))} \\
&= (-1)^{v\cdot L(u)} \sum_{x\in\mathbb{F}_2^n} (-1)^{L_1^{\mathrm{T}}(v)\cdot(F\circ A_2(x)+F\circ A_2(x+u))} \\
&= (-1)^{v\cdot L(u)} \sum_{y\in\mathbb{F}_2^n} (-1)^{L_1^{\mathrm{T}}(v)\cdot(F(y)+F(y+L_2(u)))} \\
&= (-1)^{v\cdot L(u)} \mathsf{AC}_F(L_2(u), L_1^{\mathrm{T}}(v)),
\end{aligned}$$

where L_1^{T} denotes the transpose of L_1. Moreover, when F and F' from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are affine equivalent, namely, $A = 0$, we have

$$\mathsf{AC}_{F'}(u,v) = \mathsf{AC}_F(L_2(u), L_1^{\mathrm{T}}(v)).$$

D Proof of Proposition 15

Proof. It is well known that, if F is a power permutation over a finite field, its Walsh spectrum is uniquely defined by the entries $W_F(1,b)$. Indeed, for $v \neq 0$,

$$W_{K_i}(u,v) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n}(ux+vx^d)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n}(uv^{-1/d}x+x^d)} = W_{K_i}(uv^{-1/d},1).$$

Define a Boolean function

$$\widetilde{f}_v(x) = \begin{cases} 1, & \text{if } W_{K_i}(x,v) \neq 0 \\ 0, & \text{if } W_{K_i}(x,v) = 0. \end{cases}$$

By Proposition 14, the function $\widetilde{f}_v$ becomes

$$\widetilde{f}_v(x) = \mathrm{Tr}_{2^n}((v^{-1/d}x)^{2^i+1}).$$

It follows from Proposition 7 that, for any u and v,

$$\mathsf{AC}_{K_i}(u,v) = -W_{\widetilde{f}_v}(u) = -\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n}(ux+(v^{-1/d}x)^{2^i+1})} = -\sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n}(uv^{1/d}x+x^{2^i+1})}.$$

Observe that $\gcd(i,n) = 1$, so the Gold function x^{2^i+1} is AB and $\mathsf{AC}_{K_i} = 2^{\frac{n+1}{2}}$.

E Proof of Theorem 3

Proof. For any $v \in \mathbb{F}_{q^4}^*$,

$$\begin{aligned}
\mathsf{AC}_F(1,v) &= \sum_{x\in\mathbb{F}_{q^4}} (-1)^{\mathrm{Tr}_{q^4}(v(F(x)+F(x+1)))} \\
&= \sum_{x\in\mathbb{F}_{q^4}} (-1)^{\mathrm{Tr}_{q^4}\left(v\left(x^{q^2+q}+x^{q^2+1}+x^{q+1}+x^{q^2}+x^q+x+1\right)\right)} \\
&= (-1)^{\mathrm{Tr}_{q^4}(v)} \sum_{x\in\mathbb{F}_{q^4}} (-1)^{\mathrm{Tr}_{q^4}\left(vx^{q^2+1}+\left(v^{q^3}+v\right)x^{q+1}+\left(v^{q^3}+v^{q^2}+v\right)x\right)}
\end{aligned}$$

Moreover,

$$\begin{aligned}
\mathsf{AC}_F(1,v)^2 &= \sum_{x,y\in\mathbb{F}_{q^4}} (-1)^{\mathrm{Tr}_{q^4}\left(vx^{q^2+1}+\left(v^{q^3}+v\right)x^{q+1}+\left(v^{q^3}+v^{q^2}+v\right)x+vy^{q^2+1}+\left(v^{q^3}+v\right)y^{q+1}+\left(v^{q^3}+v^{q^2}+v\right)y\right)} \\
&= \sum_{x,y\in\mathbb{F}_{q^4}} (-1)^{\mathrm{Tr}_{q^4}\left(v(x+y)^{q^2+1}+\left(v^{q^3}+v\right)(x+y)^{q+1}+\left(v^{q^3}+v^{q^2}+v\right)(x+y)+vy^{q^2+1}+\left(v^{q^3}+v\right)y^{q+1}+\left(v^{q^3}+v^{q^2}+v\right)y\right)} \\
&= \sum_{x,y\in\mathbb{F}_{q^4}} (-1)^{\mathrm{Tr}_{q^4}\left(v\left(x^{q^2+1}+xy^{q^2}+x^{q^2}y\right)+\left(v^{q^3}+v\right)\left(x^{q+1}+xy^q+x^qy\right)+\left(v^{q^3}+v^{q^2}+v\right)x\right)} \\
&= \sum_{x\in\mathbb{F}_{q^4}} (-1)^{\mathrm{Tr}_{q^4}\left(vx^{q^2+1}+\left(v^{q^3}+v\right)x^{q+1}+\left(v^{q^3}+v^{q^2}+v\right)x\right)} \sum_{y\in\mathbb{F}_{q^4}} (-1)^{\mathrm{Tr}_{q^4}(L_v(x)y)},
\end{aligned}$$

where $L_v(x) = \left(v^{q^3}+v^{q^2}\right)x^{q^3} + \left(v^{q^2}+v\right)x^{q^2} + \left(v^{q^3}+v\right)x^q$. Let $\ker(L_v) := \left\{x \in \mathbb{F}_{q^4} | L_v(x) = 0\right\}$. Then

$$\mathsf{AC}_F(1,v)^2 = q^4 \times \sum_{x\in\ker(L_v)} (-1)^{\phi_v(x)},$$

where $\phi_v(x) = \mathrm{Tr}_{q^4}\left(vx^{q^2+1} + \left(v^{q^3}+v\right)x^{q+1} + \left(v^{q^3}+v^{q^2}+v\right)x\right)$.

(1) When $v \in \mathbb{F}_q^*$, $L_v(x) = 0$ and thus $\ker(L_v) = \mathbb{F}_{q^4}$. Moreover, $\phi_v(x) = \mathrm{Tr}_{q^4}\left(vx^{q^2+1} + vx\right) = \mathrm{Tr}_{q^4}(vx)$. Therefore,

$$\mathsf{AC}_F(1,v)^2 = q^4 \times \sum_{x\in\mathbb{F}_{q^4}} (-1)^{\mathrm{Tr}_{q^4}(vx)} = 0.$$

(2) When $v \in \mathbb{F}_{q^4}\backslash\mathbb{F}_q$, ϕ_v is linear on $\ker(L_v)$, which can be proved by direct computations. Thus $\mathsf{AC}_F(1,v)^2 \neq 0$ only when ϕ_v is the all-zero mapping on $\ker(L_v)$. In addition, there must exist some v such that $\mathsf{AC}_F(1,v) \neq 0$ since F is

not bent. Moreover, the Dickson matrix of L_v is

$$D = \begin{pmatrix} 0 & v^{q^3}+v & v^{q^2}+v & v^{q^3}+v^{q^2} \\ v^{q^3}+v & 0 & v^q+v & v^{q^3}+v^q \\ v^{q^2}+v & v^q+v & 0 & v^{q^2}+v^q \\ v^{q^3}+v^{q^2} & v^{q^3}+v^q & v^{q^2}+v^q & 0 \end{pmatrix}.$$

It is easy to compute that the rank of D is 2 and thus $\#\ker(L_v) = q^2$. Therefore, there exists some v with

$$\mathsf{AC}_F(1,v)^2 = q^4 \sum_{x\in\ker(L_v)} (-1)^{\phi_v(x)} = q^4 \#\ker(L_v) = q^6.$$

This completes the proof.

F Proof of Corollary 2

Proof. It is easy to get

$$\mathsf{AC}_F(1,v) = (-1)^{\mathrm{Tr}_{2^n}(v)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n}(L(v)x)},$$

where $L(v) = v^{2^{-i}} + v$. Thus $\ker(L) = \mathbb{F}_{2^{\gcd(i,n)}} = \mathbb{F}_{2^k}$. Furthermore, for any $v \in \mathbb{F}_{2^k}$, $\mathrm{Tr}_{2^n}(v) = n' \mathrm{Tr}_{2^k}(v)$. Therefore,

$$\mathsf{AC}_F(1,v) = \begin{cases} 0 & \text{if } v \in \mathbb{F}_2^n \backslash \mathbb{F}_2^k, \\ 2^n \times (-1)^{n' \mathrm{Tr}_{2^k}(v)} & \text{if } v \in \mathbb{F}_2^k. \end{cases}$$

It follows that

$$\Lambda_F = \begin{cases} \{0, 2^n\} & \text{if } n' \text{ is even}, \\ \{-2^n, 0\} & \text{if } n' \text{ is odd and } k = 1, \\ \{-2^n, 0, 2^n\} & \text{otherwise.} \end{cases}$$

G Proof of Proposition 17

Proof. Let u, v be two nonzero elements of $\mathbb{F}_2^n$. Then, from Eq. (4), we deduce

$$\begin{aligned} \mathsf{AC}_{F^{-1}}(u,v) &= \sum_{\omega\in\mathbb{F}_2^m} (-1)^{v\cdot\omega} \mathtt{DDT}_{F^{-1}}(u,\omega) \\ &= \sum_{\omega\in\mathbb{F}_2^m} (-1)^{v\cdot\omega} \mathtt{DDT}_F(\omega,u). \end{aligned}$$

By the definition of π, we have that, for any nonzero a,

$$\mathtt{DDT}_F(a,b) = \begin{cases} 2, & \text{if } \ b\cdot\pi(a) = 1, \\ 0, & \text{if } \ b\cdot\pi(a) = 0. \end{cases}$$

It then follows that

$$\mathtt{DDT}_F(a,b) = 1 - (-1)^{\pi(a)\cdot b},$$

where this equality holds for all $(a,b) \neq (0,0)$ by using that $\pi(0) = 0$. Therefore, we have, for any nonzero u and v,

$$\mathsf{AC}_{F^{-1}}(u,v) = -\sum_{\omega \in \mathbb{F}_2^m} (-1)^{v\cdot\omega} \left(1 - (-1)^{\pi(\omega)\cdot u}\right) = -W_\pi(v,u).$$

As a consequence, $\Delta_{F^{-1}}$ is equal to half of the linearity of π, which is at least $2^{\frac{n+1}{2}}$ with equality for AB functions.

H Proof of Corollary 3

Proof. The result comes from the form of the function π which defines the DDT of x^{2^i+1}. Indeed, for any nonzero $u \in \mathbb{F}_{2^n}$ the number $\mathtt{DDT}_F(u,v)$ of solutions of

$$(x+u)^{2^i+1} + x^{2^i+1} = v$$

is equal to the number of solutions of

$$x^{2^i} + x = 1 + vu^{-(2^i+1)},$$

which is nonzero if and only if $\mathrm{Tr}_{2^n}\left(vu^{-(2^i+1)}\right) = 1$. It follows that

$$\pi(x) = x^{2^n-2^i-2}.$$

Then the autocorrelation of F^{-1} then follows from Proposition 17. Moreover, this function π cannot be AB since AB functions have algebraic degree at most $\frac{n+1}{2}$ [14, Theorem 1], while π has degree $(n-2)$. It follows that π cannot be AB when $n > 5$. Therefore, the absolute indeed of F^{-1} is strictly higher than $2^{\frac{n+1}{2}}$.