Observations on the DLCT and Absolute Indicators

Anne Canteaut[1], Lukas Kölsch[2] and Friedrich Wiemer[3]

[1] INRIA, Paris, France
anne.canteaut@inria.fr
[2] University of Rostock, Germany
lukas.koelsch@uni-rostock.de
[3] Horst Görtz Institute for IT Security,
Ruhr University Bochum, Germany
friedrich.wiemer@rub.de

Abstract. Recently Bar-On et al. proposed the Differential-Linear Connectivity Table (DLCT) for a tighter analysis of probabilities for differential-linear distinguishers. We extend the analysis of the DLCT, and gain new insights about this notion.

The DLCT entries correspond to the autocorrelation spectrum of the component functions and thus the DLCT is nothing else as the Autocorrelation Table (ACT). We note that the ACT spectrum is invariant under some equivalence relations. Interestingly the ACT spectrum is not invariant under inversion (and thus not under CCZ equivalence), implying that it might be beneficial to look at the decryption for a differential-linear cryptanalysis.

Furthermore, while for Boolean functions a lower bound for the maximal absolute autocorrelation, the absolute indicator, is not known, the case for vectorial Boolean functions is different. Here, we prove that for any vectorial Boolean function, its absolute indicator is lower bounded by $2^{n/2}$. Eventually, for APN functions we show a connection of the absolute indicator to the linearity of balanced Boolean functions, and exhibit APN permutations with absolute indicator bounded by $2^{(n+1)/2}$.

Keywords: DLCT · ACT · Autocorrelation · Absolute Indicator · Differential-Linear Attack

1 Introduction

Differential-Linear cryptanalysis was developed by Langford and Hellman [LH94]. The main idea is to split the cipher under scrutiny into two parts, $E = E^{\top} \circ E^{\perp}$. Langford and Hellman then exploited deterministic differentials over $E^{\perp}$ in combination with a linear approximation of $E^{\top}$ with a high correlation.

Recently, Bar-On et al. [Bar+19] proposed the so-called DLCT as a new tool for differential-linear style cryptanalysis. The DLCT enables us to exactly analyse the probabilities for the connection of the differential and linear parts in a differential-linear attack. However, only few properties of the DLCT were discussed.

We provide some insights on this new notion. In particular, we show that the DLCT of F corresponds to its Autocorrelation Table (ACT), see Section 3. There exists also a correspondence between the ACT of F and its Difference Distribution Table (DDT), resp. its Walsh transform, revealing the well-known relation between the DDT and the corresponding Walsh transform already observed by Blondeau and Nyberg [BN13] and Chabaud and Vaudenay [CV95]. We further note that (somewhat trivially) the ACT spectrum of a function is invariant under affine transformations. However in contrast to the DDT or LAT spectra, we observe that the ACT spectrum is *not invariant* under inversion, and thus also not under CCZ equivalence. This implies that for differential-linear cryptanalysis it might be better to look at the decryption function than the encryption – which is in sharp contrast to differential or linear cryptanalysis.

Apart from this we analyse the absolute indicator (the maximal absolute autocorrelation value) of a vectorial Boolean function in Section 4. In contrast to the case of Boolean functions, where no lower bound on the absolute indicator is known, we prove here that for vectorial Boolean functions in n variables the absolute indicator is lower bounded by $2^{\frac{n}{2}}$. Furthermore, we specify this analysis for Almost Perfect Nonlinear (APN) functions. In particular, we first show that the absolute indicator of an APN function corresponds to the linearity of a balanced Boolean function. This observation allows a nice explanation of the relation between the absolute indicator of the inverse mapping over $\mathbb{F}_{2^n}$ when n is odd, and its linearity as shown in [Cha+07].

Second, for n odd, we bound the absolute indicator of a class of permutations in n variables, namely for inverses of quadratic APN permutations (that is inverses of crooked functions), by $2^{\frac{n+1}{2}}$.

2 Preliminaries

We denote the finite field with two elements as $\mathbb{F}_2 = \{0, 1\}$ and the n-dimensional vector space over $\mathbb{F}_2$ as $\mathbb{F}_2^n$, where $\cdot$ denotes the canonical inner product. The support of a function is denoted by $\operatorname{supp}(F)$, that is the set of elements where $F \neq 0$. A *Boolean function* maps an n-bit vector from $\mathbb{F}_2^n$ to one bit in $\mathbb{F}_2$ and is called *vectorial Boolean function* when mapping to m-bits. Every vectorial Boolean function F consists of m *coordinates* that are the Boolean functions $F_{e_i}(x) = e_i \cdot F(x)$ or 2^m *components* $F_b(x) = b \cdot F(x)$ for any $b \in \mathbb{F}_2^m$. In the following $f : \mathbb{F}_2^n \to \mathbb{F}_2$ denotes a Boolean function and $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ a vectorial Boolean function.

Properties of (vectorial) Boolean functions. The *derivative of f in direction a* is defined as

$$\Delta_a(f)(x) \coloneqq f(x) + f(x+a),$$

and analogously for F. The i-th order derivative is $\Delta_{a_1,\dots,a_i}(f) = \Delta_{a_i}\big(\Delta_{a_1,\dots,a_{i-1}}(f)\big)$. The so-called DDT is related to the sizes of the preimages of the derivatives:

$$\mathrm{DDT}_F[a,b] = \delta_F(a,b) \coloneqq \left|\Delta_a(F)^{-1}(b)\right| .$$

Differentially 2-uniform functions, that are functions with a maximum entry of two in their DDT, are called APN.

Note that the b-th component of the derivative equals the derivative of the b-th component: $b \cdot \Delta_a(F)(x) = \Delta_a(F_b)(x)$.

The *Walsh coefficient of f* is defined as

$$\mathcal{W}_f(a) \coloneqq \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + f(x)},$$

while for F it is defined as

$$\mathcal{W}_F(a,b) \coloneqq \mathcal{W}_{F_b}(a) = \mathcal{W}_{b \cdot F}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)}.$$

As for the DDT, the so-called Linear Approximation Table (LAT) of F contains the Walsh coefficients of F: $\mathrm{LAT}_F[a,b] \coloneqq \mathcal{W}_F(a,b)$. The maximum absolute entry of the LAT, ignoring the 0-th row, is called the linearity of F, written $\mathcal{L}(F)$, and functions that reach the lowest possible linearity of $2^{\frac{n+1}{2}}$ are Almost Bent (AB).

Finally the *linear space* of f is defined as

$$\mathsf{LS}(f) \coloneqq \{a \in \mathbb{F}_2^n \mid \Delta_a(f) \text{ is constant zero or one}\},$$

and

$$\mathsf{LS}(F) \coloneqq \{(a,b) \in \mathbb{F}_2^n \mid b \cdot \Delta_a(F) = \Delta_a(F_b) \text{ is constant zero or one}\}.$$

An element from the linear space is also called a *linear structure*.

3 On the DLCT and ACT

Let us define the DLCT as follows.

Definition 1 (Differential-Linear Connectivity Table)**.** Given a permutation $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the corresponding *Differential-Linear Connectivity Table (DLCT)* consists of the following elements:

$$\mathrm{DLCT}_F[a,b] \coloneqq \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot (F(x)+F(x+a))} \tag{1}$$

We leave out the subscript, if it is clear from the context.

While Bar-On et al. [BO+19] defined the entry at position (a,b) as

$$\mathrm{DLCT}_F[a,b] = |\{x \mid b \cdot (F(x) + F(x+a)) = 0\}| - 2^{n-1},$$

it is easy to see that both definitions only differ in a factor of 2 for each entry:

$$\begin{aligned} &2 \cdot \left(|\{x \in \mathbb{F}_2^n \mid b \cdot (F(x) + F(x+a)) = 0\}| - 2^{n-1}\right) = |M_0| + |M_0| - 2^n \\ &= |M_0| + (2^n - |M_1|) - 2^n = |M_0| - |M_1| = \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot (F(x)+F(x+a))}, \end{aligned}$$

where we define $M_i = \{x \in \mathbb{F}_2^n \mid b \cdot (F(x) + F(x+a)) = i\}$ for the sake of readability.

Our first observation on the DLCT is that it basically contains the autocorrelation spectra of the component functions of F. Recall that the *autocorrelation of* f is defined as, see e. g. Carlet [Car10, p. 277],

$$\mathcal{A}_f(a) \coloneqq \mathcal{W}_{\Delta_a(f)}(0).$$

Similar to Walsh coefficients, this notion can naturally be generalized to vectorial Boolean functions as

$$\mathcal{A}_F(a,b) \coloneqq \mathcal{A}_{F_b}(a) = \mathcal{W}_{\Delta_a(F_b)}(0),$$

and we name the $\mathcal{A}_F(a,b)$ the *autocorrelation coefficients* of F. In other words, the autocorrelation coefficients of a vectorial Boolean function consist of the autocorrelation of its component functions. To easily see the correspondence, we only have to conclude that

$$\mathcal{W}_{\Delta_a(F_b)}(0) = \sum_x (-1)^{b \cdot (F(x)+F(x+a))}.$$

Zhang et al. [Zha+00, Section 3] introduced the term Autocorrelation Table (ACT) for a vectorial Boolean function which, analogously to the Walsh coefficient and LAT again, contains the autocorrelation spectra of F's component functions. This implies for the DLCT that

$$\mathrm{DLCT}_F[a,b] = \mathcal{A}_F(a,b) = \mathrm{ACT}_F[a,b].$$

For the remainder of this paper we thus stick to the established notion of the autocorrelation.

Zhang and Zheng [ZZ96] termed the *absolute indicator* $\mathcal{M}(f)$ as the maximum absolute value of the autocorrelation (of a Boolean function f). Analogously for a vectorial Boolean function, we define

Definition 2 (Absolute indicator)**.** Given a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. The *absolute indicator* of F is

$$\mathcal{M}(F) \coloneqq \max_{b \in \mathbb{F}_2^n \setminus \{0\}} \mathcal{M}(F_b) = \max_{a,b \in \mathbb{F}_2^n \setminus \{0\}} |\mathcal{A}_F(a,b)| \,,$$

that is the maximum absolute indicator of F's non-trivial component functions.

We call the multiset $\{\mathcal{A}_F(a,b) \mid a,b \in \mathbb{F}_2^n\}$ the *autocorrelation* or ACT *spectrum* of F. Zhang et al. [Zha+00, Section 3] further showed that

$$\mathrm{ACT} = \mathrm{DDT} \cdot H$$

where H is the Walsh matrix of order n. In other words, the ACT is the Walsh transformed DDT of F:

$$\begin{aligned}(\mathrm{DDT}_F \cdot H)[a,b] &= \sum_{c \in \mathbb{F}_2^n} |\{x \in \mathbb{F}_2^n \mid F(x) + F(x+a) = c\}| \cdot H[c,b] \\ &= \sum_{c \in \mathbb{F}_2^n} |\{x \in \mathbb{F}_2^n \mid F(x) + F(x+a) = c\}| \cdot (-1)^{c \cdot b} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot (F(x) + F(x+a))} \\ &= \mathcal{A}_F[a,b] \,.\end{aligned}$$

Because of the correspondence between the ACT and the DLCT, this corresponds to [Bar+19, Prop. 1].

Let us now recall some properties of and links between the above discussed notations.

3.1 Links between the ACT, DDT, and Walsh transformation

Sum of the ACT entries, within a row or a column. It is well-known that the entries $\mathcal{A}_F(a,b)$, $b \neq 0$ in each nonzero row in the ACT of F sum to zero if and only if F is a permutation (see e. g. [Ber+06, Prop. 2]). The same property holds when the entries $\mathcal{A}_F(a,b)$, $a \neq 0$ in each nonzero column in the ACT are considered (see e. g. [Ber+06, Eq. (9)]).

Link between differential and linear cryptanalysis. The following proposition shows that the restriction of the autocorrelation function $a \mapsto \mathcal{A}_F(a,b)$ can be seen as the discrete Fourier transform of the squared Walsh transform of F_b: $u \mapsto \mathcal{W}_F^2(u,b)$. As previously mentioned, $b \mapsto \mathcal{A}_F(a,b)$ similarly corresponds to the Fourier transform of the row of index a in the DDT: $v \mapsto \delta_F(a,v)$. It is worth noticing that this correspondence points out the well-known relationship between the Walsh transform of F and its DDT exhibited by Blondeau and Nyberg [BN13] and Chabaud and Vaudenay [CV95].

Proposition 1. *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Then, for all $a,b \in \mathbb{F}_2^n$, we have*

$$\begin{aligned}\mathcal{A}_F(a,b) &= 2^{-n} \sum_{u \in \mathbb{F}_2^n} (-1)^{a \cdot u} \mathcal{W}_F^2(u,b) &(2)\\ &= \sum_{v \in \mathbb{F}_2^n} (-1)^{b \cdot u} \delta_F(a,v) \,. &(3)\end{aligned}$$

Conversely, the inverse Fourier transform leads to

$$\mathcal{W}_F^2(a,b) = \sum_{u \in \mathbb{F}_2^n} (-1)^{a \cdot u} \mathcal{A}_F(u,b) \quad (4)$$

$$\delta_F(a,b) = 2^{-n} \sum_{v \in \mathbb{F}_2^n} (-1)^{b \cdot v} \mathcal{A}_F(a,v) \,, \quad (5)$$

for all $a, b \in \mathbb{F}_2^n$.

Proof. We first prove Relation (2) which involves the squared Walsh transform. For all $a, b \in \mathbb{F}_2^n$, we have

$$\begin{aligned}\sum_{u \in \mathbb{F}_2^n} (-1)^{a \cdot u} \mathcal{W}_F^2(u, b) &= \sum_{u \in \mathbb{F}_2^n} (-1)^{a \cdot u} \sum_{x \in \mathbb{F}_2^n} (-1)^{F_b(x)+u \cdot x} \sum_{y \in \mathbb{F}_2^n} (-1)^{F_b(y)+u \cdot y} \\ &= \sum_{x,y \in \mathbb{F}_2^n} (-1)^{F_b(x)+F_b(y)} \left(\sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot (a+x+y)} \right) \\ &= 2^n \sum_{x \in \mathbb{F}_2^n} (-1)^{F_b(x)+F_b(x+a)} = 2^n \mathcal{A}_F(a, b)\end{aligned}$$

where the last equality comes from the fact that

$$\sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot (a+x+y)} = \begin{cases} 2^n & \text{for } a + x + y = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Obviously, Eq. (4) can be directly derived from Eq. (2) by applying the inverse Fourier transform. We now prove the relation involving the DDT, namely Eq. (5). For all $a, b \in \mathbb{F}_2^n$, we have

$$\begin{aligned}\sum_{v \in \mathbb{F}_2^n} (-1)^{b \cdot v} \mathcal{A}_F(a, v) &= \sum_{v \in \mathbb{F}_2^n} (-1)^{b \cdot v} \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot \Delta_a(F)(x)} \\ &= \sum_{x \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^n} (-1)^{v \cdot (b+\Delta_a(F)(x)))} \\ &= \sum_{x \in \Delta_a(F)^{-1}(b)} 2^n = 2^n \delta_F(a, b) \ .\end{aligned}$$

Eq. (3) then follows directly by applying the inverse Fourier transform. □

As a corollary, Parseval's equality leads to an expression of the sum of all squared entries in each row, and in each column of the autocorrelation table.

Corollary 1. *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Then, for all $a, b \in \mathbb{F}_2^n$, we have*

$$\sum_{a \in \mathbb{F}_2^n} \mathcal{A}_F^2(a, b) = 2^{-n} \sum_{u \in \mathbb{F}_2^n} \mathcal{W}_F^4(u, b) \quad \text{and} \quad \sum_{b \in \mathbb{F}_2^n} \mathcal{A}_F^2(a, b) = 2^n \sum_{v \in \mathbb{F}_2^n} \delta_F^2(a, v) \ .$$

In the following, we show that the ACT spectrum is affine invariant, the extended ACT spectrum is extended affine invariant and the ACT spectrum is not invariant under CCZ equivalence.

3.2 Invariance under Equivalence Relations

Having an equivalence relation on the set of all n-bit functions, allows us to partition these functions into equivalence classes. Properties which are invariant under this equivalence notion can then be tested on only one representative of each class – resulting in a massive decrease of complexity, if we want to characterise the whole set of functions under this property. Three well-known equivalences are the following:

Definition 3 (Equivalence relations for vectorial Boolean functions)**.** Given two functions F and $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$. We say these functions are

1. *affine equivalent* ($F \overset{\text{A}}{\sim} G$) if there exist two affine permutations A and B such that $G = B \circ F \circ A$,
2. *extended affine equivalent* ($F \overset{\text{EA}}{\sim} G$) if there exist two affine permutations A and B, and an affine function C such that $G = B \circ F \circ A + C$,
3. *CCZ equivalent* ($F \overset{\text{CCZ}}{\sim} G$) if their graphs are affine equivalent.

Here, the graph of a function is defined as $\{(x, F(x)) \mid x \in \mathbb{F}_2^n\}$.

A nice property of the ACT is that its spectrum is invariant under affine equivalence, and further its extended ACT spectrum, that is the multiset $\{|\mathcal{A}_F(a,b)| \mid a, b \in \mathbb{F}_2^n\}$, is invariant under extended affine equivalence.

Proposition 2 (Affine and Extended Affine Invariance)**.** *Given two permutations F, and G on $\mathbb{F}_2^n$. Let further $A = L_a + \alpha$, $B = L_b + \beta$ be two affine permutations and $C = L_c + \gamma$ be an affine function. Then*

$$G = B \circ F \circ A \quad \Rightarrow \quad \mathcal{A}_G(a,b) = \mathcal{A}_F(L_a(a), L_b^*(b))$$

and

$$G = B \circ F \circ A + C \quad \Rightarrow \quad |\mathcal{A}_G(a,b)| = |\mathcal{A}_F(L_a(a), L_b^*(b))| \,,$$

where L^* denotes the adjoint of the linear mapping L.

Proof. From the affine equivalence of F and G, we have $G(x) = L_b(F(L_a(x) + \alpha)) + \beta$. Each entry $\text{ACT}_F[a,b]$ corresponds to the number of solutions x for the equation

$$b \cdot (F(x) + F(x+a)) = 0.$$

Thus for each entry of G's ACT at position a, b, we count the number of solutions for

$$b \cdot [L_b(F(L_a(x) + \alpha)) + \beta + L_b(F(L_a(x+a) + \alpha)) + \beta] = 0.$$

Substituting $x' = L_a(x) + \alpha$, this simplifies to

$$\begin{aligned} & b \cdot L_b(F(x') + F(x' + L_a(a))) = 0 \\ \Leftrightarrow \quad & L_b^*(b) \cdot (F(x') + F(x' + L_a(a))) = 0 \end{aligned}$$

thus the number of solutions for this equation is nothing else as the ACT entry of F at position $(L_a(a), L_b^*(b))$.

For the second point, we now only have to show how $G = F + C$ behaves. By definition of the autocorrelation we have

$$\begin{aligned} \mathcal{A}_G(a,b) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot (G(x) + G(x+a))} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot (F(x) + L_c(x) + \gamma + F(x+a) + L_c(x+a) + \gamma)} \end{aligned}$$

where $C(x) = L_c(x) + \gamma$

$$\begin{aligned} &= \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot (F(x) + F(x+a) + L_c(a))} \\ &= (-1)^{b \cdot (L_c(a))} \mathcal{A}_F(a,b), \end{aligned}$$

and thus the affine map C only influences the sign of the autocorrelation value. □

The (extended) affine invariance of the (extended) ACT spectra follows directly from this proposition.

Corollary 2. *Given two permutations F, and G on $\mathbb{F}_2^n$.*

- *If $F \overset{A}{\sim} G$, the ACT spectrum of F equals that of G.*
- *If $F \overset{EA}{\sim} G$, the extended ACT spectrum of F equals that of G.*

To examine the behaviour under CCZ equivalence, let us first recall that the ACT is related to linear structures in the following way, see also [MT14; Zha+00].

Lemma 1 (Linear Structures)**.** *Given $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, then*

$$\mathcal{A}_F(a, b) = \pm 2^n$$

if and only if (a, b) forms a linear structure for F.

Proof. This follows from the fact that, for a linear structure, by definition,

$$b \cdot (F(x) + F(x + a))$$

is constant zero or one. The sign of the entry thus determines, if the linear structure is constant one (negative) or zero (positive). □

One consequence of this is the next corollary.

Corollary 3 (Inversion)**.** *Given a permutation $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, then the ACT spectrum of F is in general not equal to the ACT spectrum of F^{-1}.*

Proof. Counterexamples are the S-boxes from Safer [Mas94], SC2000 [Shi+02], and fides [Bil+13], where the S-box has linear structures in one direction but non in the other direction, and the Gold permutations as analysed in Section 4.4. □

An interesting implication of this is that it might be advantageous when doing a differential-linear cryptanalysis, to look at both directions, encryption and decryption, of a cipher.

Another direct consequence of Corollary 3 is the following result.

Corollary 4. *Given two CCZ-equivalent permutations $F \overset{CCZ}{\sim} G$ on $\mathbb{F}_2^n$. Their ACT spectrum is in general not invariant.*

Proof. A function and its inverse are always CCZ equivalent. Thus Corollary 3 gives a counterexample. □

Zhang et al. further showed how the ACT of F and its inverse F^{-1} are related, see [Zha+00, Corollary 1]. In particular they showed that

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

which in our notation is

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

4 Lower bound on the absolute indicator

Finding the smallest possible absolute indicator for a *Boolean function* is an open question investigated by many authors. Zhang and Zheng conjectured [ZZ96, Conjecture 1] that the absolute indicator of a balanced Boolean function of n variables was at least $2^{\frac{n+1}{2}}$. But this was later disproved first for odd values of $n \geqslant 9$ by modifying the Patterson-Wiedemann construction, namely for $n \in \{9, 11\}$ in [Kav+07], for $n = 15$ in [Kav16; MS02] and for $n = 21$ in [Gan+06]. For the case n even, Tang and Maitra [TM18] 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 Kavut et al. [Kav+19]. However, we now show that such small values for the absolute indicator cannot be achieved for *vectorial Boolean functions*.

4.1 General Case

Parseval's equality leads to the following upper bound on the sum of all *squared* autocorrelation coefficients in each row. This result can be found in [Nyb95] (see also [Ber+06, Theorem 2]), but we recall the proof for the sake of completeness.

Proposition 3. *Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. Then, for all $a \in \mathbb{F}_2^n$, we have*

$$\sum_{b \in \mathbb{F}_2^n, b \neq 0} \mathcal{A}_F^2(a, b) \geqslant 2^{2n} \, .$$

Moreover, equality holds for all nonzero $a \in \mathbb{F}_2^n$ if and only if F is APN.

Proof. From Corollary 1, we have that, for all $a \in \mathbb{F}_2^n$,

$$\sum_{b \in \mathbb{F}_2^n} \mathcal{A}_F^2(a, b) = 2^n \sum_{v \in \mathbb{F}_2^n} \delta_F^2(a, v)$$

Cauchy-Schwarz inequality implies that

$$\left(\sum_{v \in \mathbb{F}_2^n} \delta_F(a, v) \right)^2 \leqslant \left(\sum_{v \in \mathbb{F}_2^n} \delta_F^2(a, v) \right) \times |\{v \in \mathbb{F}_2^n \mid \delta_F(a, v) \neq 0\}| \, ,$$

with equality if and only if all nonzero elements in $\{\delta_F(a, v) \mid v \in \mathbb{F}_2^n\}$ are equal. Using that

$$|\{v \in \mathbb{F}_2^n \mid \delta_F(a, v) \neq 0\}| \leqslant 2^{n-1}$$

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

$$\sum_{v \in \mathbb{F}_2^n} \delta_F^2(a, v) \geqslant 2^{2n} \times 2^{-(n-1)} = 2^{n+1}$$

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

$$\sum_{b \in \mathbb{F}_2^n} \mathcal{A}_F^2(a, b) \geqslant 2^{2n+1}$$

with equality for all nonzero a if and only if F is APN. Then the result follows from the fact that

$$\sum_{b \in \mathbb{F}_2^n} \mathcal{A}_F^2(a, b) = 2^{2n} + \sum_{b \in \mathbb{F}_2^n, b \neq 0} \mathcal{A}_F^2(a, b) \, .$$

□

From the lower bound on the sum of all squared coefficients within a row of the ACT, we deduce the following lower bound on the absolute indicator.

Proposition 4 (Lowest possible absolute indicator)**.** *Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. Then,*

$$\mathcal{M}(F) \geqslant \frac{2^n}{\sqrt{2^n - 1}} > 2^{n/2} .$$

Proof. From the facts that

$$\sum_{b \in \mathbb{F}_2^n, b \neq 0} \mathcal{A}_F^2(a, b) \geqslant 2^{2n}$$

and

$$\sum_{b \in \mathbb{F}_2^n, b \neq 0} \mathcal{A}_F^2(a, b) \leqslant \mathcal{M}(F)^2 (2^n - 1)$$

the result directly follows. □

We can get a more precise lower bound on the absolute indicator by using the fact that all autocorrelation coefficients are divisible by 8. We even have a stronger property for functions having a lower algebraic degree as shown in the following proposition.

Proposition 5 (Divisibility)**.** *Let $n > 2$ and $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation with algebraic degree at most d. Then, for any a, $b \in \mathbb{F}_2^n$, $\mathcal{A}_F(a, b)$ is divisible by $2^{\lceil \frac{n}{d-1} \rceil + 1}$.*

Most notably, the autocorrelation coefficients of a permutation are divisible by 8.

Proof. From the definition of the autocorrelation, we know that

$$\mathcal{A}_F(a, b) = \mathcal{W}_{\Delta_a(F_b)}(0).$$

For the sake of readability, we define $h_{a,b} = \Delta_a(F_b)$. We can derive two properties of this Boolean function $h_{a,b}$. First, as F has degree at most d, $\deg(h_{a,b}) \leqslant d - 1$. Second, $h_{a,b}(x) = h_{a,b}(x + a)$.

We now focus on the divisibility of $\mathcal{W}_{h_{a,b}}(0)$. First, assume for simplicity that $a = e_n$, we discuss the general case afterwards. Then we can write $h_{e_n,b}$ as $h_{e_n,b}(x) = g(x_1, \ldots, x_{n-1})$ with $g : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$, because $h_{e_n,b}(x + e_n) = h_{e_n,b}(x)$. The Walsh coefficient of $h_{e_n,b}$ at point 0 can then be computed as

$$\mathcal{W}_{h_{e_n,b}}(0) = \sum_{x \in \mathbb{F}_2^{n-1}, x_n \in \mathbb{F}_2} (-1)^{f(x, x_n)} = 2 \cdot \sum_{x \in \mathbb{F}_2^{n-1}} (-1)^{g(x)} = 2 \cdot \mathcal{W}_g(0)$$

Now $\deg g \leqslant d - 1$. It is well-known that the Walsh coefficients of a Boolean function f are divisible by $2^{\lceil \frac{n}{\deg f} \rceil}$ (see [McE72] or [Car10, Section 3.1]). We then deduce that $\mathcal{W}_g(0)$ is divisible by $2^{\lceil \frac{n-1}{d-1} \rceil}$, implying that $\mathcal{W}_{h_{e_n,b}}(0)$ is divisible by $2^{\lceil \frac{n-1}{d-1} \rceil + 1}$. Most notably, if F is bijective, $d \leqslant n - 1$. We then have that

$$\left\lceil \frac{n-1}{d-1} \right\rceil + 1 \geqslant 3,$$

implying that $\mathcal{W}_{h_{e_n,b}}(0)$ is divisible by 8.

In the case that $a \neq e_n$, we can find a linear transformation L, s. t. $L(e_n) = a$, with which we have the affine equivalent function $G = F \circ L \sim F$. Now for G the same argument as above holds and thus $\mathcal{A}_G(a, b)$ is divisible by $2^{\lceil \frac{n}{d-1} \rceil + 1}$. Due to the affine invariance of G's and F's ACT spectra the same holds for $\mathcal{A}_F(a, b)$ in this case. □

The absolute indicator is known for very few permutations only, except in the case of permutations of degree less than or equal to 2, where the result is trivial. To our best knowledge, one of the only functions whose absolute indicator is known is the inverse mapping $F(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$ [Cha+07]: $\mathcal{M}(F) = 2^{\frac{n}{2}+1}$ when n is even. When n is odd, $\mathcal{M}(F) = \mathcal{L}(F)$ when $\mathcal{L}(F) \equiv 0 \bmod 8$, and $\mathcal{M}(F) = \mathcal{L}(F) \pm 4$ otherwise (see Section 4.3 for an alternative proof).

We now study the absolute indicator of some types of vectorial Boolean functions.

4.2 Case of power permutations

For power permutations on $\mathbb{F}_{2^n}$ we can show that the autocorrelation spectrum is invariant for all component functions, analogously to the same well known fact for the Walsh spectrum. In this case, the trace function is used as the inner product, i. e. $a \cdot b = \mathrm{tr}_n(ab)$ with

$$\begin{aligned} \mathrm{tr}_n &: \mathbb{F}_{2^n} \to \mathbb{F}_2 \\ \mathrm{tr}_n(x) &\coloneqq \sum_{i=0}^{n-1} x^{2^i} \end{aligned}$$

where we leave out the subscript, if it is clear from the context. Thus we have the following corollary.

Corollary 5. *Let F be a power permutation on $\mathbb{F}_{2^n}$, i. e. $F = x^k$ with $\gcd(k, 2^n - 1) = 1$. Then, for all non-zero a and b in $\mathbb{F}_{2^n}$,*

$$\mathcal{A}_F(a, b) = \mathcal{A}_F(1, a^k b) = \mathcal{A}_F(ab^{\frac{1}{k}}, 1) \; .$$

Most notably, all non-zero component functions F_b of F have the same (Boolean) absolute indicator: $\mathcal{M}(F) = \mathcal{M}(F_b)$ for all $b \in \mathbb{F}_{2^n}^*$ and $\mathcal{M}(F_b) > 2^{n/2}$.

Proof. The fact that $\mathcal{A}_F(a, b) = \mathcal{A}_F(1, a^k b)$ has been proved for instance in [Ber+06, Prop. 4]. The second equality comes from the fact that

$$b \cdot \left(x^k + (x+a)^k\right) = 1 \cdot \left(\left(b^{\frac{1}{k}} x\right)^k + \left(b^{\frac{1}{k}} x + ab^{\frac{1}{k}}\right)^d\right),$$

where $b^{\frac{1}{k}}$ only exists if $\gcd(k, 2^n - 1) = 1$. It follows that it is enough to compute only one column of the ACT, as the remaining ones are just permutations of each other. In other words, all Boolean functions F_b, $b \neq 0$, have the same absolute indicator. □

4.3 Case of APN functions

In the specific case of APN functions, we can also exhibit a stronger condition than Proposition 4 on the lowest possible absolute indicator.

Proposition 6 (Lowest possible indicator for APN functions)**.** *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 M, then there exists a balanced Boolean function of n variables with linearity M.*

Proof. If F is APN, then $\delta_F(a, b) \in \{0, 2\}$ for all a, b, $a \neq 0$. It follows that, for each nonzero a, we can define a Boolean function g_a of n variables such that

$$g_a(b) = \begin{cases} 0 & \text{if } \delta_F(a, b) = 0 \\ 1 & \text{if } \delta_F(a, b) = 2 \; . \end{cases}$$

Equivalently,

$$\delta_F(a,b) = 1 - (-1)^{g_a(b)} \ .$$

Obviously, all g_a are balanced. Moreover, we deduce from Eq. (3) that, for all nonzero a, b,

$$\begin{aligned}\mathcal{A}_F(a,b) &= \sum_{v\in\mathbb{F}_2^n} (-1)^{b\cdot v}\delta_F(a,v)\\ &= \sum_{v\in\mathbb{F}_2^n} (-1)^{b\cdot v}\Big(1-(-1)^{g_a(v)}\Big)\\ &= -\sum_{v\in\mathbb{F}_2^n} (-1)^{b\cdot v + g_a(v)} = -\mathcal{W}_{g_a}(b)\end{aligned}$$

where $\mathcal{W}_{g_a}(b)$ denotes the value of the Walsh transform of g_a at point b. This implies that

$$\max_{b\neq 0} |\mathcal{A}_F(a,b)| = \mathcal{L}(g_a) \ .$$

The result then directly follows. □

To our best knowledge, the smallest known linearity for a balanced Boolean function is obtained by Dobbertin's recursive construction [Dob95]. 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.

It is worth noticing that the proof of the previous proposition shows that the knowledge of g directly determines the ACT. This explains why the absolute indicator of the inverse mapping over $\mathbb{F}_{2^n}$, n odd, is derived from its linearity as proved in [Cha+07, Theorem 1] and detailed in the following example.

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

$$g_a(b) = \begin{cases} 1 + \mathrm{tr}(a^{-1}b^{-1}) & \text{if } b \notin \{0, a^{-1}\}\\ 0 & \text{if } b = 0\\ 1 & \text{if } b = a^{-1}\end{cases} \ .$$

This comes from the fact that the equation

$$(x+a)^{-1} + x^{-1} = b$$

for $b \neq a^{-1}$ can be rewritten as

$$x + (x+a) = b(x+a)x$$

or equivalently when $b \neq 0$, by setting $y = a^{-1}x$,

$$y^2 + y = a^{-1}b^{-1} \ .$$

It follows that this equation has two solutions if and only if $\mathrm{tr}(a^{-1}b^{-1}) = 0$. From the proof of the previous proposition, we deduce

$$\begin{aligned}\mathcal{A}_F(a,b) &= -\mathcal{W}_{g_a}(b)\\ &= \mathcal{W}_{F_{a^{-1}}}(b) + 2\Big(1 - (-1)^{\mathrm{tr}(a^{-1}b)}\Big) \ ,\end{aligned}$$

where the additional term corresponds to the value of the sum defining the Walsh transform $\mathcal{W}_{F_{a^{-1}}}(b)$ at points 0 and a^{-1}.

It can be observed that Propositions 3 and 6 are actually more general and apply as soon as the DDT of F contains one row composed of 0s and 2s only.

Proposition 7. *Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. Then, for any fixed $a \in \mathbb{F}_2^n \setminus \{0\}$, the following properties are equivalent:*

(i) $\displaystyle\sum_{b \in \mathbb{F}_2^n \setminus \{0\}} \mathcal{A}_F^2(a,b) = 2^{2n}$

(ii) For all $b \in \mathbb{F}_2^n$, $\delta_F(a,b) \in \{0,2\}$.

Moreover, if these properties hold, then there exists a balanced Boolean function $g : \mathbb{F}_2^n \to \mathbb{F}_2$ such that

$$\mathcal{L}(g) = \max_{b \in \mathbb{F}_2^n \setminus \{0\}} |\mathcal{A}_F(a,b)| \ .$$

Let us now take a closer look at the absolute indicator of some specific APN permutations.

4.4 Case of APN permutations

As previously observed, the ACT and the absolute indicator are not invariant under inversion. Then, while the absolute indicator of a quadratic permutation is trivially equal to 2^n, computing the absolute indicator of the inverse of a quadratic permutation is not obvious at all. Indeed, the absolute indicator depends on the considered function, as we will see next.

Inverses of quadratic APN permutations, n odd. For instance, 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* [BF98], which means that the image sets of their derivatives $\Delta_a(F)$, $a \neq 0$, is the complement of a hyperplane $\langle \pi(a) \rangle^\perp$. Moreover, it is known (see e. g. [CC03, 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 ACT of F^{-1} corresponds to the Walsh transform of π.

Proposition 8. *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*

$$\mathrm{Im}\,(\Delta_a(F)) = \mathbb{F}_2^n \setminus \langle \pi(a) \rangle^\perp, \textit{when } a \neq 0 \ ,$$

and $\pi(0) = 0$. Then, for any nonzero a and b in $\mathbb{F}_2^n$, we have

$$\mathcal{A}_{F^{-1}}(a,b) = -\mathcal{W}_\pi(b,a) \ .$$

It follows that

$$\mathcal{M}\big(F^{-1}\big) \geqslant 2^{\frac{n+1}{2}}$$

with equality if and only if π is an AB permutation.

Proof. Let a and b be two nonzero elements in $\mathbb{F}_2^n$. Then, from Relation (3), we deduce

$$\begin{aligned}\mathcal{A}_{F^{-1}}(a,b) &= \sum_{u \in \mathbb{F}_2^n} (-1)^{b \cdot u} \delta_{F^{-1}}(a,u) \\ &= \sum_{u \in \mathbb{F}_2^n} (-1)^{b \cdot u} \delta_F(u,a) \ .\end{aligned}$$

By definition of π, we have that, for any nonzero u,

$$\delta_F(u,v) = \begin{cases} 2 & \text{if } v \cdot \pi(u) = 1 \\ 0 & \text{if } v \cdot \pi(u) = 0 \end{cases} .$$

It then follows that

$$\delta_F(u,v) = 1 - (-1)^{\pi(u)\cdot v}$$

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

$$\mathcal{A}_{F^{-1}}(a,b) = \sum_{u \in \mathbb{F}_2^n} (-1)^{b\cdot u}\Big(1 - (-1)^{\pi(u)\cdot a}\Big) = -\mathcal{W}_\pi(b,a) .$$

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

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 Gold exponents, i. e. $F(x) = x^{2^i+1}$. 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 6. *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 a and b in $\mathbb{F}_2^n$, we have*

$$\mathcal{A}_{F^{-1}}(a,b) = -\mathcal{W}_\pi(b,a) \textit{ where } \pi(x) = x^{2^n-2^i-2} .$$

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

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

$$(x+a)^{2^i+1} + x^{2^i+1} = b$$

is equal to the number of solutions of

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

which is nonzero if and only if $\mathrm{tr}(ba^{-(2^i+1)}) = 1$. It follows that

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

The autocorrelation spectrum of F^{-1} then follows from Proposition 8. Moreover, this function π cannot be AB since AB functions have algebraic degree at most $\frac{n+1}{2}$ [Car+98, Theorem 1], while π has degree $(n-2)$. It follows that π cannot be AB when $n > 5$. Therefore, the absolute indicator of the inverse of F^{-1}, i. e. the linearity of π, is strictly higher than $2^{\frac{n+1}{2}}$. □

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.

Cubic APN permutations. In the case of APN permutations of degree 3, we have a more precise result.

Proposition 9 (Cubic APN permutations)**.** *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be APN with degree 3. Then we have that for non-zero a and λ*

$$|\mathcal{A}_F(a,\lambda)| \in \left\{0, 2^{\frac{n+d(a,\lambda)}{2}}\right\},$$

where $d(a,\lambda) = \dim \mathsf{LS}(\Delta_a(F_\lambda)) = \dim\{b \mid \Delta_{a,b}(F_\lambda) = c\}$ and $c \in \mathbb{F}_2$ is constant. Moreover, $\mathcal{A}_F(a,\lambda) = 0$ if and only if $\Delta_a(F_\lambda)$ is balanced, which equivalently means that it has a all-one derivative.

From this proposition, if n is odd, we obviously have that $\mathcal{M}(F) \geqslant 2^{\frac{n+1}{2}}$ with equality if and only if, for any nonzero $a, \lambda \in \mathbb{F}_2^n$, either $\mathsf{LS}(\Delta_a(F_\lambda)) = \{0, a\}$ or there exists b such that $\Delta_b(\Delta_a(F_\lambda)) = 1$. Moreover, if F is APN and $\mathcal{M}(F) = 2^{\frac{n+1}{2}}$, it follows from Proposition 3 that the number of nonzero λ such that $\mathsf{LS}(\Delta_a(F_\lambda)) = \{0, a\}$ is exactly 2^{n-1}.

Additionally, an upper bound on the absolute indicator can be established for two cubic APN permutations, namely the first Kasami power function and the Welch function. We denote the Kasami power functions K_i and the Welch power function W by

$$\begin{aligned} K_i &: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \\ K_i &: x \mapsto x^{(2^{3i}+1)/(2^i+1)} \\ &= x^{4^i - 2^i + 1} \end{aligned} \qquad \text{and} \qquad \begin{aligned} W &: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \\ W &: x \mapsto x^{2^{(n-1)/2}+3} \end{aligned}.$$

Proposition 10 ([Car08], Lemma 1)**.** *The absolute indicator for W on $\mathbb{F}_{2^n}$ is bounded from above by*

$$\mathcal{M}(W) \leqslant 2^{\frac{n+5}{2}}$$

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 11. *The absolute indicator of K_i on $\mathbb{F}_{2^n}$ is bounded from above by*

$$\mathcal{M}(K_i) \leqslant (4^i - 2^{i+1}) \times 2^{\frac{n}{2}}.$$

In particular,

$$\mathcal{M}(K_2) \leqslant 2^{\frac{n+5}{2}}.$$

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 $\mathrm{tr}(y^2) = \mathrm{tr}(y)$. The result then follows from the Weil bound. Combining the bound with Proposition 9 yields the bound on K_2. □

In the two cases of W and K_2, we deduce that the absolute indicator belongs to $\{2^{\frac{n+1}{2}}, 2^{\frac{n+3}{2}}, 2^{\frac{n+5}{2}}\}$. We actually conjecture the following.

Conjecture 1. *Let $n \geqslant 9$ be odd. Then $\mathcal{M}(K_2) \geqslant 2^{\frac{n+3}{2}}$ and $\mathcal{M}(W) \geqslant 2^{\frac{n+3}{2}}$.*

Conjecture 2. *If n odd and $n \not\equiv 0 \bmod 3$, then $\mathcal{M}(K_i) = 2^{\frac{n+1}{2}}$.*

Some other results on the autocorrelations of the Boolean functions $\mathrm{tr}(x^k)$ are known in the literature, which can be trivially extended to the vectorial functions x^k if $\gcd(k, n) = 1$, see [GK04, Theorem 5], [Car08] and [SW09, Lemmas 2 and 3]. In the case $n = 6r$ and $k = 2^{2r} + 2^r + 1$, the power monomial x^k is not a permutation, but results for all component functions of x^k were derived in [Can+08]. We summarize the results in the following proposition.

Proposition 12. *Let $F(x) = x^k$ be a function on $\mathbb{F}_{2^n}$.*

1. *If n is odd and $k = 2^r + 3$ with $r = \frac{n+1}{2}$ then $\mathcal{M}(F) \in \{2^{\frac{n+1}{2}}, 2^{\frac{n+3}{2}}\}$.*
2. *If n is odd and k is the i-th Kasami exponent, where $3i \equiv \pm 1 \pmod n$, then $\mathcal{M}(F) = 2^{\frac{n+1}{2}}$.*
3. *If $n = 2m$ and $k = 2^{m+1} + 3$ then $\mathcal{M}(F) \leqslant 2^{\frac{3m}{2}+1}$.*
4. *If $n = 2m$, m odd and $k = 2^m + 2^{\frac{m+1}{2}} + 1$ then $\mathcal{M}(F) \leqslant 2^{\frac{3m}{2}+1}$.*
5. *If $n = 6r$ and $k = 2^{2r} + 2^r + 1$ then $\mathcal{M}(F) = 2^{5r}$.*

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 13 ([Dil99])**.** *Let n odd, not divisible by 3 and $3i \equiv \pm 1 \pmod n$. Set $f = \mathrm{tr}(x^k)$ where $k = 4^i - 2^i + 1$ is the i-th Kasami exponent. Then*

$$\mathrm{supp}(\mathcal{W}_f) = \left\{ a \;\middle|\; \mathrm{tr}(a^{2^k+1}) = 1 \right\} .$$

Proposition 14. *Let n odd, not divisible by 3 and $3i \equiv \pm 1 \pmod n$. Then*

$$\mathcal{A}_{K_i}(a, b) = -\sum_{u \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(ab^{1/k}u + u^{2^k+1})},$$

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

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 $\mathcal{W}_F(1, b)$. Indeed, for $b \neq 0$,

$$\begin{aligned} \mathcal{W}_{K_i}(u, b) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(bx^k + ux)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(x^k + ub^{-1/k}x)} = \mathcal{W}_{K_i}(1, ub^{-1/k}) \in \left\{0, \pm 2^{\frac{n+1}{2}}\right\} , \end{aligned}$$

where the last fact follows because the Kasami function is AB. Then, by Eq. (2) and Proposition 13, for any nonzero a and b,

$$\begin{aligned} \mathcal{A}_{K_i}(a, b) &= 2^{-n} \sum_{u \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(au)} \mathcal{W}^2_{K_i}(u, b) = 2^{-n} \sum_{u \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(au)} \mathcal{W}^2_{K_i}(1, ub^{-1/k}) \\ &= 2^{-n} \sum_{ub^{-1/k} \in \mathrm{supp}(\mathcal{W}_{\mathrm{tr}(x^k)})} (-1)^{\mathrm{tr}(au)} 2^{n+1} = 2 \sum_{u \in B} (-1)^{\mathrm{tr}(au)} , \end{aligned} \tag{6}$$

where $B = \left\{u \in \mathbb{F}_{2^n} \,\middle|\, \mathrm{tr}((ub^{-1/k})^{2^k+1}) = 1\right\}$. We have

$$\begin{aligned} 0 &= \sum_{u \notin B} (-1)^{\mathrm{tr}(au)} + \sum_{u \in B} (-1)^{\mathrm{tr}(au)} \\ &= \sum_{u \notin B} (-1)^{\mathrm{tr}(au+(ub^{-1/k})^{2^k+1})} - \sum_{u \in B} (-1)^{\mathrm{tr}(au+(ub^{-1/k})^{2^k+1})} , \end{aligned}$$

so

$$\sum_{u \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(au+(ub^{-1/k})^{2^k+1})} = 2 \sum_{u \in B} (-1)^{\mathrm{tr}(au+(ub^{-1/k})^{2^k+1})} = -2 \sum_{u \in B} (-1)^{\mathrm{tr}(au)} .$$

Plugging this into Eq. (6), we obtain

$$\mathcal{A}_{K_i}(a,b) = - \sum_{u \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(au+(ub^{-1/k})^{2^k+1})} = - \sum_{u \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(ab^{1/k}u+u^{2^k+1})} .$$

It can be easily checked that the equation also holds for $b = 0$. Observe that $\gcd(k, n) = 1$, so the Gold function is AB and

$$\mathcal{M}(K_i) = 2^{\frac{n+1}{2}} .$$

□

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, $(4^{(n-i)} - 2^{n-i} + 1)2^{2i} \equiv 4^i - 2^i + 1 \pmod{2^n - 1}$.

Note. Li et al. [Li+19] independently made similar observations on the DLCT.

References

[BF98] T. D. Bending and Dmitry Fon-Der-Flaass. “Crooked Functions, Bent Functions, and Distance Regular Graphs.” In: *Electr. J. Comb.* 5 (1998).

[BN13] Céline Blondeau and Kaisa Nyberg. “New Links between Differential and Linear Cryptanalysis.” In: *EUROCRYPT 2013*. Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. LNCS. Springer, Heidelberg, May 2013, pp. 388–404. DOI: 10.1007/978-3-642-38348-9_24.

[BO+19] Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizmann. *DLCT: A New Tool for Differential-Linear Cryptanalysis*. To appear at Eurocrypt 2019; Preprint available as Cryptology ePrint Archive, Report 2019/256. https://ia.cr/2019/256. 2019.

[Ber+06] Thierry P. Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy. “On Almost Perfect Nonlinear Functions Over $\mathbf{F}_2^n$.” In: *IEEE Trans. Information Theory* 52.9 (2006), pp. 4160–4170.

[Bil+13] Begül Bilgin, Andrey Bogdanov, Miroslav Knežević, Florian Mendel, and Qingju Wang. “Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware.” In: *CHES 2013*. Ed. by Guido Bertoni and Jean-Sébastien Coron. Vol. 8086. LNCS. Springer, Heidelberg, Aug. 2013, pp. 142–158. DOI: 10.1007/978-3-642-40349-1_9.

[CC03] Anne Canteaut and Pascale Charpin. “Decomposing bent functions.” In: *IEEE Trans. Information Theory* 49.8 (2003), pp. 2004–2019.

[CV95] Florent Chabaud and Serge Vaudenay. “Links Between Differential and Linear Cryptanalysis.” In: *EUROCRYPT'94*. Ed. by Alfredo De Santis. Vol. 950. LNCS. Springer, Heidelberg, May 1995, pp. 356–365. DOI: 10.1007/BFb0053450.

[Can+08] Anne Canteaut, Pascale Charpin, and Gohar M. Kyureghyan. “A new class of monomial bent functions.” In: *Finite Fields and Their Applications* 14.1 (2008), pp. 221–241. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2007.02.004.

[Car+98] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. “Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems.” In: *Des. Codes Cryptography* 15.2 (1998), pp. 125–156. DOI: 10.1023/A:1008344232130.

[Car08] Claude Carlet. “Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications.” In: *IEEE Transactions on Information Theory* 54.3 (Mar. 2008), pp. 1262–1272. ISSN: 0018-9448. DOI: 10.1109/TIT.2007.915704.

[Car10] Claude Carlet. “Boolean Functions for Cryptography and Error-Correcting Codes.” In: *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Ed. by Yves Crama and Peter L. Hammer. Cambridge University Press, 2010, pp. 257–397. DOI: 10.1017/CBO9780511780448.011.

[Cha+07] Pascale Charpin, Tor Helleseth, and Victor A. Zinoviev. “Propagation characteristics of $x \mapsto x^{-1}$ and Kloosterman sums.” In: *Finite Fields and Their Applications* 13.2 (2007), pp. 366–381. DOI: 10.1016/j.ffa.2005.08.007.

[Dil99] John F. Dillon. “Multiplicative Difference Sets via Additive Characters.” In: *Des. Codes Cryptography* 17.1 (Sept. 1999), pp. 225–235. ISSN: 1573-7586. DOI: 10.1023/A:1026435428030.

[Dob95] Hans Dobbertin. “Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity.” In: *FSE'94*. Ed. by Bart Preneel. Vol. 1008. LNCS. Springer, Heidelberg, Dec. 1995, pp. 61–74. DOI: 10.1007/3-540-60590-8_5.

[GK04] Guang Gong and Khoongming Khoo. “Additive Autocorrelation of Resilient Boolean Functions.” In: *Selected Areas in Cryptography*. Ed. by Mitsuru Matsui and Robert J. Zuccherato. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 275–290. ISBN: 978-3-540-24654-1.

[Gan+06] Sugata Gangopadhyay, Pradipkumar H. Keskar, and Subhamoy Maitra. “Patterson-Wiedemann construction revisited.” In: *Discrete Mathematics* 306.14 (2006), pp. 1540–1556. DOI: 10.1016/j.disc.2005.06.033.

[Kav+07] Selçuk Kavut, Subhamoy Maitra, and Melek D. Yücel. “Search for Boolean Functions With Excellent Profiles in the Rotation Symmetric Class.” In: *IEEE Trans. Information Theory* 53.5 (2007), pp. 1743–1751. DOI: 10.1109/TIT.2007.894696.

[Kav+19] Selçuk Kavut, Subhamoy Maitra, and Deng Tang. “Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile.” In: *Des. Codes Cryptogrography* 87.2–3 (2019), pp. 261–276. DOI: 10.1007/s10623-018-0522-1.

[Kav16] Selçuk Kavut. “Correction to the paper: Patterson-Wiedemann construction revisited.” In: *Discrete Applied Mathematics* 202 (2016), pp. 185–187. ISSN: 0166-218X. DOI: 10.1016/j.dam.2015.07.044.

[LH94] Susan K. Langford and Martin E. Hellman. “Differential-Linear Cryptanalysis.” In: *CRYPTO'94*. Ed. by Yvo Desmedt. Vol. 839. LNCS. Springer, Heidelberg, Aug. 1994, pp. 17–25. DOI: 10.1007/3-540-48658-5_3.

[Li+19] Kangquan Li, Chunlei Li, Chao Li, and Longjiang Qu. *On the Differential Linear Connectivity Table of Vectorial Boolean Functions.* 2019. arXiv: 1907.05986 [cs.IT].

[MS02] Subhamoy Maitra and Palash Sarkar. "Modifications of Patterson-Wiedemann functions for cryptographic applications." In: *IEEE Trans. Information Theory* 48.1 (2002), pp. 278–284. DOI: 10.1109/18.971756.

[MT14] Rusydi H. Makarim and Cihangir Tezcan. "Relating Undisturbed Bits to Other Properties of Substitution Boxes." In: *LightSec'14.* Vol. 8898. LNCS. Springer Berlin Heidelberg, 2014, pp. 109–125. DOI: 10.1007/978-3-319-16363-5_7.

[Mas94] James L. Massey. "SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm." In: *FSE'93.* Ed. by Ross J. Anderson. Vol. 809. LNCS. Springer, Heidelberg, Dec. 1994, pp. 1–17. DOI: 10.1007/3-540-58108-1_1.

[McE72] Robert J. McEliece. "Weight congruences for p-ary cyclic codes." In: *Discrete Mathematics* 3.1–3 (1972), pp. 177–192. DOI: 10.1016/0012-365X(72)90032-5.

[Nyb95] Kaisa Nyberg. "S-boxes and Round Functions with Controllable Linearity and Differential Uniformity." In: *FSE'94.* Ed. by Bart Preneel. Vol. 1008. LNCS. Springer, Heidelberg, Dec. 1995, pp. 111–130. DOI: 10.1007/3-540-60590-8_9.

[SW09] Guanghong Sun and Chuankun Wu. "The lower bounds on the second order nonlinearity of three classes of Boolean functions with high nonlinearity." In: *Information Sciences* 179.3 (2009), pp. 267–278. ISSN: 0020-0255. DOI: 10.1016/j.ins.2008.10.002.

[Shi+02] Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun Yajima, Naoya Torii, and Hidema Tanaka. "The Block Cipher SC2000." In: *FSE 2001.* Ed. by Mitsuru Matsui. Vol. 2355. LNCS. Springer, Heidelberg, Apr. 2002, pp. 312–327. DOI: 10.1007/3-540-45473-X_26.

[TM18] Deng Tang and Subhamoy Maitra. "Construction of n-Variable ($n \equiv 2 \bmod 4$) Balanced Boolean Functions With Maximum Absolute Value in Autocorrelation Spectra $< 2^{n/2}$." In: *IEEE Trans. Information Theory* 64.1 (2018), pp. 393–402. DOI: 10.1109/TIT.2017.2769092.

[ZZ96] Xian-Mo Zhang and Yuliang Zheng. "GAC — the Criterion for Global Avalanche Characteristics of Cryptographic Functions." In: (1996). Ed. by Hermann Maurer, Cristian Calude, and Arto Salomaa, pp. 320–337. DOI: 10.1007/978-3-642-80350-5_30.

[Zha+00] Xian-Mo Zhang, Yuliang Zheng, and Hideki Imai. "Relating Differential Distribution Tables to Other Properties of of Substitution Boxes." In: *Des. Codes Cryptography* 19.1 (2000), pp. 45–63. ISSN: 1573-7586. DOI: 10.1023/A:1008359713877.

[Bar+19] Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizman. "DLCT: A New Tool for Differential-Linear Cryptanalysis." In: *EUROCRYPT 2019, Part I.* Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11476. LNCS. Springer, Heidelberg, May 2019, pp. 313–342. DOI: 10.1007/978-3-030-17653-2_11.