Further Study c-Differential-Linear Connectivity Table of Vectorial Boolean Functions toward Promising Applications in Coding Theory

Said Eddahmani and Sihem Mesnager *

Posted Date: 17 January 2024

doi: 10.20944/preprints202401.1310.v1

Keywords: Differential uniformity; Vectorial Function; S-Box; Linear Codes; Minimal Codes

Article

Further Study *c*-Differential-Linear Connectivity Table of Vectorial Boolean Functions toward Promising Applications in Coding Theory

Said Eddahmani [1] **and Sihem Mesnager** [1,2,*]

[1] Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, Laboratory Geometry, Analysis and Applications, LAGA, University Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France; said.eddahmani@etud.univ-paris8.fr

[2] Telecom Paris, Polytechnic institute, 91120 Palaiseau, France; smesnager@univ-paris8.fr

* Correspondence: said.eddahmani@etud.univ-paris8.fr

Abstract: Vectorial Boolean functions and codes are closely related, and each corresponding domain gives been to each other. On the one hand, various requirements of binary linear codes are needed for their theatrical interests but, more importantly, for their practical applicants (such as few-weight codes or minimal codes for secret sharing, locally recoverable codes for storage, etc.). On the other hand, various criteria and tables have been introduced to analyse the security of S-boxes that are related to vectorial Boolean functions, such as the Differential Distribution Table (DDT), the Boomerang Connectivity Table (BCT), and the Differential-Linear Connectivity Table (DLCT). In previous years, two new tables have been proposed for which the literature was pretty abundant: the *c*-DDT to extend the DDT and the *c*-BCT to extend the BCT. In the same vein, we propose extended concepts to study further the security of vectorial Boolean functions, especially the *c*-Walsh transform, the *c*-autocorrelation, and the *c*-differential-linear uniformity, and its accompanying table, the *c*-Differential-Linear Connectivity Table (*c*-DLCT). We study these properties of the novel functions at their optimal level concerning these concepts and describe the *c*-DLCT of the crucial inverse vectorial (Boolean) function case. Finally, the derived functions could lead to new families of binary minimal codes, as the recent achievements on minimal codes from low differential uniformity. We draw new avenues for future research toward linear code designs.

Keywords: differential uniformity; vectorial function; S-box; linear codes; minimal codes

MSC: 94B15; 94B05; 94A55; 11B83; 94A60; 14G50; 11T71

1. Introduction

Vectorial Boolean functions are intensively used to produce S-boxes in block ciphers such as DES [15], Rinjdael or AES [14], Blowfish [40], GOST [18], and Serpent [6]. Various criteria have been proposed to test the resistance of S-boxes and the corresponding vectorial Boolean functions to known cryptanalytical attacks, such as the differential attack [5], the linear attack [27] and some of their variants.

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a (n, m)-vectorial Boolean function. The derivative of F in direction of $a \in \mathbb{F}_{2^n}$ is the function $D_a(F)(x) = F(x) + F(x + a)$. The derivative is used to analyse the resistance of a vectorial boolean function to the differential attack [5], and serves to build the Differential Distribution Table (DDT). The derivative is also used in the Boomerang Connectivity Table (BCT) [13], and in the Differential-Linear Connectivity Table (DLCT) [2,26]. The entry at $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ of the DDT is defined by

$$\mathtt{DDT}_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : F(x) + F(x + a) = b\}.$$

To measure the resistance of a vectorial Boolean function, Nyberg [36] introduced the differential uniformity as

$$\delta_F = \max\{\mathtt{DDT}_F(a, b) \mid (a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}, \text{ and } a \neq 0\}.$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

The most resistant vectorial Boolean functions have small differential uniformities. The reader can consult the [12] for a complete background on vectorial Boolean functions with a deep analysis of their cryptographic aspects.

At FSE 2002, Borisov et al. [8] proposed a variant of the differential attack to study ciphers' resistance based on using modular multiplication as a primitive operation. This motivated Ellingsen et al. [16] to introduce the concept of c-differentials to study the resistance of a vectorial Boolean function to multiplicative variants of the differential attack. For a vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, and $c \in \mathbb{F}_{2^m}$, the c-derivative F with respect to $a \in \mathbb{F}_{2^n}$ is the (n, m)-vectorial Boolean function ${}_cD_aF$ defined by ${}_cD_aF(x) = F(x + a) + cF(x)$ for all $x \in \mathbb{F}_{2^n}$. The c-derivative is used to study the resistance of ciphers based on popular vectorial Boolean functions such as the inverse function [42], the Gold function [43], and various other functions [3,45,48–50]. As for the DDT, a c-differential table was proposed in [16] where the entry at $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is defined by

$$ {}_c\mathtt{DDT}_F(a, b) = \#\{x \in \mathbb{F}_{2^n} \mid F(x + a) + cF(x) = b\}.$$

Also, a c-differential uniformity was proposed in [16] by

$$ {}_c\delta_F = \max\{{}_c\mathtt{DDT}_F(a, b) \mid (a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}, \text{ and } a \neq 0 \text{ if } c = 1\}.$$

The construction of functions, particularly permutations, with low c-differential uniformity is an interesting problem, and recent work has focused heavily on this direction. Likewise, regarding the original notion of differential uniformity leading to optimal functions, Perfect Nonlinear (PN) and Almost Perfect Nonlinear (APN) over finite fields in odd and even characteristics, respectively, optimal functions having the lowest possible values of a c-differential uniformity have also been introduced. One can refer to [17,19,22,25,48,51,52] and the references therein. Some of those functions with low c-differential uniformity have been investigated. There are relatively few known (non-trivial, nonlinear) optimal classes of PcN and APcN functions over finite fields with an even characteristic (see, e.g., [20,23,38,45,46] and the references therein).

Another popular cryptanalysis attack on S-boxes derived from Boolean functions is the boomerang attack, proposed by Wagner [47] in 1999. In connection with the boomerang attack, Cid et al. [13] proposed the Boomerang Connectivity Table (BCT) for a vectorial Boolean function where the entry at $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is defined by

$$\mathtt{BCT}_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : F^{-1}(F(x) + b) + F^{-1}(F(x + a) + b) = a\}.$$

Based on the BCT, Boura and Canteaut [9] introduced the boomerang uniformity of a vectorial Boolean function to measure its resistance against boomerang attack. The boomerang uniformity of F is defined by

$$\beta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m}^*} \mathtt{BCT}_F(a, b).$$

To extend the BCT and the boomerang uniformity of a vectorial Boolean function, Stănică [41] introduced the concept of the c-Boomerang Connectivity Table (c-BCT). For $c \in \mathbb{F}_{2^m}^*$, the c-BCT is defined at the entry $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ by

$$ {}_c\mathtt{BCT}_F(a, b) = \#\{x \in \mathbb{F}_{2^n} : F^{-1}(cF(x) + b) + F^{-1}\left(c^{-1}F(x + a) + b\right) = a\}.$$

The corresponding c-boomerang uniformity is defined by

$$ {}_c\beta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m}^*} {}_c\mathtt{BCT}_F(a, b).$$

More generalizations of the differential and boomerang uniformities can be found in [30].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

In 2019, Bar-On et al. [2] (see also [26]) introduced the Differential-Linear Connectivity Table (DLCT) of a vectorial Boolean function where the entry at $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is defined by

$$\mathtt{DLCT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n} \mid b \cdot (F(x+a)+F(x)) = 0\} - 2^{n-1},$$

where $x \cdot y$ is the inner product of x and y on $\mathbb{F}_{2^m}$. To measure the resistance of an S-box connected to a vectorial Boolean function, the differential-linear uniformity of F can be used, as defined by Li et al. in [24],

$$\gamma_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m}^*} |\mathtt{DLCT}_F(a,b)|.$$

Various links exist between the DLCT and the Autocorrelation Table (ACT) of a vectorial Boolean function F. The ACT is defined at $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ by

$$\mathtt{ACT}_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{b \cdot (F(x)+F(x+a))}.$$

The corresponding absolute indicator is defined as

$$\Delta_F = \max_{\substack{u \in \mathbb{F}_{2^n}, u \neq 0, \\ b \in \mathbb{F}_{2^m}^*}} |\mathtt{ACT}_F(a,b)|.$$

In [10], Canteaut et al. showed that the DLCT and the ACT of a vectorial Boolean function satisfy $\gamma_F = \frac{1}{2}\Delta_F$ and $\mathtt{DLCT}_F(a,b) = \frac{1}{2}\mathtt{ACT}_F(a,b)$ for all $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$.

One can observe that the derivative $D_a(F)(x) = F(x) + F(x+a)$ of a Boolean function F is used in various tables, such as the DDT, the BCT, and the DLCT. Motivated by the crucial role of the derivative in the former tables and the attacks related to them, we propose three new concepts towards the c-derivative ${}_cD_a(F)(x) = F(x+a) + cF(x)$:

- The c-Walsh transform of a vectorial Boolean function F. For $c \in \mathbb{F}_{2^m}^*$, it is defined for $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$ by
$$ {}_cW_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{a \cdot x + b \cdot cF(x)}.$$
- The c-autocorrelation of a vectorial Boolean function. Let $c \in \mathbb{F}_{2^m}$, $c \neq 0$. The c-autocorrelation of F at $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is the integer
$$ {}_c\mathrm{AC}_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{b \cdot (F(x+a)+cF(x))}.$$
The absolute indicator is
$$ {}_c\Delta_F = \max_{\substack{u \in \mathbb{F}_{2^n}, u \neq 0 \text{ if } c=1, \\ b \in \mathbb{F}_{2^m}^*}} |{}_c\mathrm{AC}_F(a,b)|,$$
and the autocorrelation spectrum is
$$ {}_c\Lambda_F = \{{}_c\mathrm{AC}_F(a,b), a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m}^*\}.$$
- The c-Differential-Linear Connectivity Table (c-DLCT) where we use the c-derivative. Let $c \in \mathbb{F}_{2^m}^*$. The c-DLCT of F is a $2^n \times 2^m$ table where the entry at $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is defined by
$$ {}_c\mathtt{DLCT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n} \mid b \cdot (F(x+a)+cF(x)) = 0\} - 2^{n-1}.$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

We also define the c-differential-linear uniformity of F as

$$ {}_c\gamma_F = \max_{\substack{u\in\mathbb{F}_{2^n}, u\neq 0 \text{ if } c=1,\\ b\in\mathbb{F}_{2^m}^*}} |{}_c\mathrm{DLCT}_F(a,b)|, $$

and, also we define the c-DLCT spectrum of F by

$$ {}_c\Gamma_F = \{{}_c\mathrm{DLCT}_F(a,b), a\in\mathbb{F}_{2^n}, b\in\mathbb{F}_{2^m}\}. $$

We show that there are numerous relationships between the three new concepts. Typically, we show that ${}_c\mathtt{DLCT}_F(a,b) = \frac{1}{2}{}_c\mathtt{AC}_F(a,b)$ for all $(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^m}$, and ${}_c\gamma_F = \frac{1}{2}{}_c\Delta_F$.

Moreover, we focus on the inverse function defined on $\mathbb{F}_{2^n}$ by $F(x) = \frac{1}{x}$ if $x\neq 0$, and $F(0) = 0$. We study its c-DLCT and give an explicit value for the entries, including when $c = 1$.

We mention that there is an interesting connection between c differential uniformity and combinatorial designs, which has been highlighted in [1] by showing that the graph of a perfect c-nonlinear function (an optimal function concerning the c differential uniformity) is a set of differences in a quasigroup. Difference sets give rise to symmetric designs, which are known to build optimal self-complementary codes. Some types of designs also have application implications, such as secret sharing and visual cryptography.

Finally, we emphasise that one of our practical applications in brother research lines is to use the derived (optimal) functions (see, e.g., [12]) to derive minimal binary linear codes (see, e.g., [21]) that are needed for their theatrical interests but, more importantly, for their practical applicants such as few-weight codes or minimal codes for secret sharing and secure two-party computation.

The rest of this paper is organized as follows. Section 2 presents some known results that will be used in this paper. In Section 3, we define the c-Walsh and the c-autocorrelation of a vectorial Boolean function and study some of their properties. In Section 4, we present the concept of the c-DLCT and study its properties. We investigate the c-DLCT of the inverse function in Section 5. Finally, Section 6 concludes the paper and draws new avenues for future research toward linear code designs along the same lines as designing (minimal) codes from Almost Perfect Nonlinear (APN) and recent achievements ([31]) on minimal codes from low differential uniformity.

2. Preliminaries

In this section, we present some results and definitions that will be used in the next sections, including the c-derivative and the c-differential uniformity of a vectorial Boolean function.

For $b\in\mathbb{F}_{2^n}$, we define the orthogonal space $b^\perp$ of b as follows.

Definition 1. *For $b\in\mathbb{F}_{2^n}$, the orthogonal space $b^\perp$ of b is defined by*

$$ b^\perp = \{x\in\mathbb{F}_{2^n} \mid b\cdot x = 0\}, $$

where $b\cdot x$ is the inner product of b and x on $\mathbb{F}_{2^n}$.

The following result gives an explicit value for $\#b^\perp$.

Proposition 1. *For $b\in\mathbb{F}_{2^n}$, the orthogonal space $b^\perp$ of b satisfies*

$$ \#b^\perp = \begin{cases} 2^n & \text{if } b = 0,\\ 2^{n-1} & \text{if } b\neq 0. \end{cases} $$

Proof. It is obvious that $\#0^\perp = 2^n$. Suppose that $b\neq 0$. Then, the binary expansion of b is in the form.

$$ b = (b_{n-1}, b_{n-2}, \ldots, b_j, \ldots, b_0). $$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

Suppose that $b_j = 1$ for some j with $0 \leq j \leq n-1$. Let $x \in \mathbb{F}_{2^n}$ such that $x \notin b^\perp$, that is $b \cdot x = 1$, with the binary expansion

$$x = (x_{n-1}, x_{n-2}, \ldots, x_j, \ldots, x_0).$$

Let $y \in \mathbb{F}_{2^n}$ with the binary expansion

$$y = (y_{n-1}, y_{n-2}, \ldots, x_j + 1 \pmod 2, \ldots, x_0).$$

Then

$$b \cdot y = b \cdot x + b_j \equiv 1 + 1 \equiv 0 \pmod 2.$$

Hence $y \in b^\perp$. It follows that for $b \neq 0$, each element x of $\mathbb{F}_{2^n}$ satisfying $b \cdot x = 1$ is in correspondence with one element y of $\mathbb{F}_{2^n}$ satisfying $b \cdot y = 0$. As a consequence, we have $\#b^\perp = 2^{n-1}$. □ □

For $n \geq 1$, let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. The trace of an element $x \in \mathbb{F}_{2^n}$ is given by

$$\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{n-1}},$$

and satisfies $\mathrm{Tr}(x) \in \{0, 1\}$. The trace function satisfies $\mathrm{Tr}(x^2) = \mathrm{Tr}(x)$ for all $x \in \mathbb{F}_{2^n}$.

The following lemma is well-known and is useful for our work.

Lemma 1. *Let n and k be positive integers and $e = \gcd(k, n)$. Then*

$$\gcd\left(2^k + 1, 2^n - 1\right) = \begin{cases} 1 & \text{if } \frac{n}{e} \text{ is odd,} \\ 2^e + 1 & \text{if } \frac{n}{e} \text{ is even.} \end{cases}$$

Some specific equations on $\mathbb{F}_{2^n}$ may be involved. The following result deals with the quadratic equation.

Lemma 2. *(Proposition 1 of [39]) Let $a, b, c \in \mathbb{F}_{2^n}$. The equation $ax^2 + bx + c = 0$ has*

(i) One root if and only if $b = 0$.
(ii) Two roots if and only if $b \neq 0$ and $Tr\left(\frac{ac}{b^2}\right) = 0$.
(iii) No root if and only if $b \neq 0$ and $Tr\left(\frac{ac}{b^2}\right) = 1$.

The following lemma concerns another equation on $\mathbb{F}_{2^n}$.

Lemma 3. *Let k and n be positive integers such that $k < n$. Let $d = \gcd(k, n)$, $m = \frac{n}{d} > 1$, and $\beta_{m-1} = \mathrm{Tr}_d^n(B)$. Then, the trinomial $f(X) = X^{2^k} + X + B$ has no root if $\beta_{m-1} \neq 0$, and has 2^d roots $x + \delta\tau$ in $\mathbb{F}_{2^n}$ if $\beta_{m-1} = 0$ where $\delta \in \mathbb{F}_{2^d}$, $\tau \in \mathbb{F}_{2^n}$ is any element satisfying $\tau^{2^k - 1} = 1$, and*

$$x = \frac{1}{\mathrm{Tr}_d^n(c)} \sum_{i=0}^{m-1} \left(\sum_{j=0}^{i} c^{2^{kj}} \right) B^{2^{ki}},$$

with any $c \in \mathbb{F}_{2^n}^*$ satisfying $\mathrm{Tr}_d^n(c) \in \mathbb{F}_{2^d}^*$.

In [16], Ellingsen et al. proposed the concept of c-differentials. The following definitions are valid for binary finite fields.

Definition 2. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a (n, m)-vectorial Boolean function and $c \in \mathbb{F}_{2^m}$. The c-derivative F with respect to $a \in \mathbb{F}_{2^n}$ is the (n, m)-vectorial function ${}_cD_aF$ satisfying ${}_tp_x$*

$${}_cD_aF(x) = F(x + a) + cF(x)$$

for all $x \in \mathbb{F}_{2^n}$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

Definition 3. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a (n,m)-vectorial Boolean function, and $c \in \mathbb{F}_{2^m}$. The c-differential table of F is an $2^n \times 2^m$ table whose components are defined for $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$ by*

$$_c\Delta_F(a,b) = \#\{x \in \mathbb{F}_{2^n} \mid F(x+a) + cF(x) = b\}.$$

Definition 4. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a (n,m)-vectorial Boolean function, and $c \in \mathbb{F}_{2^m}$. The c-differential uniformity of F is*

$$_c\Delta_F = \begin{cases} \max\limits_{a\in\mathbb{F}_{2^n}, b\in\mathbb{F}_{2^m}} {}_c\Delta_F(a,b) & \text{if } c \neq 1, \\ \max\limits_{a\in\mathbb{F}_{2^n}\setminus\{0\}, b\in\mathbb{F}_{2^m}} {}_c\Delta_F(a,b) & \text{if } c = 1. \end{cases}$$

3. The c-Walsh and c-Autocorrelation of a Vectorial Boolean function

The Walsh transform of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined at $u \in \mathbb{F}_{2^n}$ by

$$W_f(u) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{u\cdot x + f(x)},$$

where $u \cdot x$ is the inner product of u and x. The Walsh transform serves to compute the linearity of f as

$$\mathrm{L}(f) = \max_{u\in\mathbb{F}_{2^n}} |W_f(u)|.$$

For a vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, the Walsh transform of F is defined for $u \in \mathbb{F}_{2^n}$ and $v \in \mathbb{F}_{2^m}$ by

$$W_F(u,v) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{u\cdot x + v\cdot F(x)},$$

and is used to compute the linearity of F by

$$\mathrm{L}(F) = \max_{u\in\mathbb{F}_{2^n}, v\in\mathbb{F}_{2^n}\setminus\{0\}} |W_F(u,v)|.$$

We extend the Walsh transform of a vectorial Boolean function to the c-Walsh transform as follows.

Definition 5. *Let F be an (n,m)-vectorial Boolean function, and $c \in \mathbb{F}_{2^m}^*$. The c-Walsh transform of F is defined for $u \in \mathbb{F}_{2^n}$ and $v \in \mathbb{F}_{2^m}$ by*

$$_cW_F(u,v) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{u\cdot x + v\cdot cF(x)}.$$

The autocorrelation function is used to study various properties of the Boolean functions (see [11]).

Definition 6. *Let f be Boolean function defined on $\mathbb{F}_{2^n}$. The autocorrelation of f at $u \in \mathbb{F}_{2^n}$ is the integer*

$$AC_f(u) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(x+u)},$$

and its absolute indicator is $\Delta_f = \max_{u\in\mathbb{F}_{2^n}, u\neq 0} \left|AC_f(u)\right|$.

We notice that $u = 0$ is excluded in the definition of the absolute indicator since $\mathrm{AC}_f(0) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+f(x)} = 2^n$. The generalization of the autocorrelation to vectorial Boolean functions can be then defined as follows.

Definition 7. *Let F be an (n,m)-vectorial Boolean function defined on $\mathbb{F}_{2^n}$. The autocorrelation of F at $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is the integer*

$$AC_F(u,v) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{v\cdot(F(x)+F(x+u))}.$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

The absolute indicator is

$$\Delta_F = \max_{\substack{u\in\mathbb{F}_{2^n},u\neq 0,\\ v\in\mathbb{F}_{2^m},v\neq 0}} |AC_F(u,v)|,$$

and the autocorrelation spectrum is

$$\Lambda_F = \{AC_F(u,v), u \in \mathbb{F}_{2^n}, u \neq 0, v \in \mathbb{F}_{2^m}, v \neq 0\}.$$

The trivial values are not considered in the definition of the absolute indicator since $\mathrm{AC}_F(0,v) = \mathrm{AC}_F(u,0) = 2^n$.

Inspired by Definition 6, we introduce the notion of c-autocorrelation of a Boolean function.

Definition 8. *Let f be Boolean function defined on $\mathbb{F}_{2^n}$, and $c \in \mathbb{F}_{2^m}$, $c \neq 0$. The c-autocorrelation of f at $u \in \mathbb{F}_{2^n}$ is the integer*

$$_cAC_f(u) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x+u)+cf(x)},$$

and the c-absolute indicator is $_c\Delta_f = \max_{u\in\mathbb{F}_{2^n}} \left|AC_f(u)\right|$.

Similarly, to generalize Definition 7, we define the c-autocorrelation of a vectorial Boolean function.

Definition 9. *Let F be an (n,m)-vectorial Boolean function defined on $\mathbb{F}_{2^n}$, and $c \in \mathbb{F}_{2^m}$, $c \neq 0$. The c-autocorrelation of F at $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is the integer*

$$_cAC_F(u,v) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{v\cdot(F(x+u)+cF(x))}.$$

The absolute indicator is

$$_c\Delta_F = \max_{\substack{u\in\mathbb{F}_{2^n},u\neq 0 \text{ if } c=1,\\ v\in\mathbb{F}_{2^m},v\neq 0}} |_cAC_F(u,v)|,$$

and the autocorrelation spectrum is

$$_c\Lambda_F = \{_cAC_F(u,v), u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^m},\}.$$

To ease the study of the c-autocorrelation of a vectorial Boolean function F, we presnent its c-autocorrelation table defined at $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ by

$$_c\mathrm{ACT}_F(u,v) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{v\cdot(F(x+u)+cF(x))}.$$

The following result links the c-autocorrelation of a vectorial Boolean function and its c-Walsh transform.

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

$$W_F(u,v)_cW_F(u,v) = \sum_{z\in\mathbb{F}_{2^n}} (-1)^{u\cdot z}{}_cAC_F(z,v).$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

Proof. We have

$$\begin{aligned} W_F(u,v)_c W_F(u,v) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{u\cdot x+v\cdot F(x)} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{u\cdot y+v\cdot cF(y)} \\ &= \sum_{x,y\in\mathbb{F}_{2^n}} (-1)^{u\cdot(x+y)+v\cdot(F(x)+cF(y)} \\ &= \sum_{y,z\in\mathbb{F}_{2^n}} (-1)^{u\cdot z+v\cdot(F(y+z)+cF(y))} \\ &= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{u\cdot z} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{v\cdot(F(y+z)+cF(y))} \\ &= \sum_{z\in\mathbb{F}_{2^n}} (-1)^{u\cdot z} {}_c\mathrm{AC}_F(z,v). \end{aligned}$$

This finishes the proof. □ □

4. The c-Differential-Linear Connectivity Table of a Vectorial Boolean Function

In this section, we present a new concept, called the c-Differential-Linear Connectivity Table (c-DLCT), which generalizes the standard DLCT, independently defined in 2018 by Kim et al. [26] and Bar-On et al. [2]

We start by defining the standard Differential-Linear Connectivity Table (DLCT).

Definition 10. *Let F be an (n,m)-vectorial Boolean function. The DLCT of F is an $2^n \times 2^m$ table where the entry at $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is*

$$\mathtt{DLCT}_F(u,v) = \#\{x \in \mathbb{F}_{2^n} \mid v\cdot(F(x+u)+F(x)) = 0\} - 2^{n-1}.$$

The DLCT is a tool that could analyse the relationships between differential and linear parts of a block cipher. One can observe that if $x \in \mathbb{F}_{2^n}$ is such that $v\cdot(F(x+u)+F(x)) = 0$, then $v\cdot(F((x+u)+u)+F(x+u)) = 0$. Consequently, $\mathrm{DLCT}_F(u,v)$ is always even. Moreover, if $u = 0$, or if $v = 0$, then $\mathrm{DLCT}_F(u,v) = 2^{n-1}$. This induces the following definition for differential-linear connectivity uniformity.

Definition 11. *Let F be an (n,m)-vectorial Boolean function. The differential-linear connectivity uniformity of F is*

$$\gamma_F = \max_{u\in\mathbb{F}_{2^n}^*, v\in\mathbb{F}_{2^m}^*} |DLCT_F(u,v)|.$$

The DLCT of a vectorial Boolean function is related to the autocorrelation function by the following relation.

$$\begin{aligned} \mathtt{AC}_F(u,v) &= \#\{x \in \mathbb{F}_{2^n} \mid v\cdot(F(x)+F(x+u)) = 0)\} \\ &\quad - \#\{x \in \mathbb{F}_{2^n} \mid v\cdot(F(x)+F(x+u)) = 1\} \\ &= 2\#\{x \in \mathbb{F}_{2^n} \mid v\cdot(F(x)+F(x+u)) = 0\} - 2^n \\ &= 2\mathtt{DLCT}_F(u,v). \end{aligned}$$

The DLCT is a tool to study the relationships between the linear and the differential properties of a block cipher. For $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$, it counts the number of elements $x \in \mathbb{F}_{2^n}$ such that $v\cdot(F(x+u)+F(x)) = 0$. Let $a \in \mathbb{F}_{2^m}$, $a \neq 0$, and $b \in \mathbb{F}_{2^m}$, $b \neq 0$, be two fixed non-zero elements. It is possible to study the relationships between the linear and the differential properties of a block cipher by studying the number of solutions of the equation $v\cdot(aF(x+u)+bF(x)) = 0$, or equivalently $v\cdot(F(x+u)+cF(x)) = 0$ where $c = \frac{a}{b}$. This leads us to define a function's c-Differential-Linear Connectivity Table (c-DLCT).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

Definition 12. *Let F be an (n,m)-vectorial Boolean function, and $c \in \mathbb{F}_{2^m}$, $c \neq 0$. The c-DLCT of F is an $2^n \times 2^m$ table where the entry at $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is*

$$_cDLCT_F(u,v) = \#\{x \in \mathbb{F}_{2^n} \mid v \cdot (F(x+u) + cF(x)) = 0\} - 2^{n-1}.$$

Moreover, the c-differential-linear connectivity uniformity of F is

$$_c\gamma_F = \max_{\substack{u \in \mathbb{F}_{2^n}, u \neq 0 \text{ if } c=1, \\ v \in \mathbb{F}_{2^m}, v \neq 0}} |_cDLCT_F(u,v)|,$$

and the c-DLCT spectrum of F is defined for $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ by

$$_c\Gamma_F = \{_cDLCT_F(u,v), u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^m}\}.$$

From Definition 9 and Definition 12, we obtain the following connection between the $_c$ACT and the $_c$DLCT of a vectorial Boolean function.

Proposition 3. *Let F be (n,m)-vectorial Boolean function. Then for all $u \in \mathbb{F}_{2^n}$ and $v \in \mathbb{F}_{2^m}$,*

$$_c\mathtt{DLCT}_F(u,v) = \frac{1}{2}{}_c\mathtt{AC}_F(u,v), \text{ and } {}_c\gamma_F = \frac{1}{2}{}_c\Delta_F.$$

Proof. We have

$$\begin{aligned} _c\mathtt{AC}_F(u,v) &= \#\{x \in \mathbb{F}_{2^n} \mid v \cdot (F(x+u) + cF(x)) = 0)\} \\ &\quad - \#\{x \in \mathbb{F}_{2^n} \mid v \cdot (F(x+u) + cF(x)) = 1\} \\ &= 2\#\{x \in \mathbb{F}_{2^n} \mid v \cdot (F(x+u) + cF(x)) = 0\} - 2^n \\ &= 2{}_c\mathtt{DLCT}_F(u,v). \end{aligned}$$

which gives $_c\mathtt{DLCT}_F(u,v) = \frac{1}{2}{}_c\mathtt{AC}_F(u,v)$. On the other hand, we have

$${}_c\Delta_F = \max_{\substack{u \in \mathbb{F}_{2^n}, u \neq 0 \text{ if } c=1, \\ v \in \mathbb{F}_{2^m}, v \neq 0}} |{}_c\mathtt{AC}_F(u,v)| = 2 \max_{\substack{u \in \mathbb{F}_{2^n}, u \neq 0 \text{ if } c=1, \\ v \in \mathbb{F}_{2^m}, v \neq 0}} {}_c\mathtt{DLCT}_F(u,v) = 2{}_c\gamma_F,$$

and $_c\gamma_F = \frac{1}{2}{}_c\Delta_F$. This finishes the proof. □ □

As a consequence of the former proposition, the following result connects the c-DLCT and the c-derivative of a vectorial Boolean function via the Walsh transform.

Proposition 4. *Let F be an (n,m)-vectorial Boolean function, and $c \in \mathbb{F}_{2^m}$, $c \neq 0$. Then for any $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$,*

$$_c\mathtt{DLCT}_F(u,v) = \frac{1}{2}W_{(_cD_uF)}(0,v).$$

Proof. Combining Definition 2 and the definition of the Walsh transform, we get

$$W_{(_cD_uF)}(0,v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{v \cdot (F(x+u) + cF(x))} = {}_c\mathtt{AC}_F(u,v).$$

Then, using Proposition 3, we get

$$W_{_cD_uF}(0,v) = {}_c\mathtt{AC}_F(u,v) = 2{}_c\mathtt{DLCT}_F(u,v),$$

and $_c\mathtt{DLCT}_F(u,v) = \frac{1}{2}W_{(_cD_uF)}(0,v)$. □ □

The following result shows a connection between the c-DLCT and the c-derivative of a vectorial Boolean function via the Walsh transform.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

Proposition 5. *Let F be an (n,m)-vectorial Boolean function, and $c \in \mathbb{F}_{2^m}$, $c \neq 0$. Then for any $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$,*

$$W_F(u,v)_c W_F(u,v) = 2 \sum_{\omega \in \mathbb{F}_{2^n}} (-1)^{u\cdot\omega}{}_c\mathtt{DLCT}_F(\omega,v).$$

Proof. Combining Proposition 2 and Proposition 5, we get

$$\begin{aligned} W_F(u,v)_c W_F(u,v) &= \sum_{z \in \mathbb{F}_{2^n}} (-1)^{u\cdot z}{}_c\mathrm{AC}_F(z,v) \\ &= 2 \sum_{\omega \in \mathbb{F}_{2^n}} (-1)^{u\cdot\omega}{}_c\mathtt{DLCT}_F(\omega,v), \end{aligned}$$

as claimed. □ □

The following result gives a link between ${}_c\mathtt{DLCT}_F$ and ${}_c\Delta_F(a,b)$.

Proposition 6. *Let F be an (n,m)-vectorial Boolean function, and $c \in \mathbb{F}_{2^m}$, $c \neq 0$. Then for any $(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$,*

$${}_c\mathtt{DLCT}_F(u,v) = \frac{1}{2} \sum_{\omega \in \mathbb{F}_{2^n}} (-1)^{\omega\cdot v}{}_c\Delta_F(u,\omega).$$

Proof. By Proposition 3, we have

$$\begin{aligned} 2{}_c\mathtt{DLCT}_F(u,v) &= {}_c\mathtt{AC}_F(u,v) \\ &= \#\{x \in \mathbb{F}_{2^n} \mid v\cdot(F(x+u)+cF(x)) = 0)\} \\ &\quad - \#\{x \in \mathbb{F}_{2^n} \mid v\cdot(F(x+u)+cF(x)) = 1\} \\ &= \sum_{\omega \in \mathbb{F}_{2^n}, \omega\cdot v = 0} \#\{x \in \mathbb{F}_{2^n} \mid F(x+u)+cF(x) = \omega\} \\ &\quad - \sum_{\omega \in \mathbb{F}_{2^n}, \omega\cdot v = 1} \#\{x \in \mathbb{F}_{2^n} \mid F(x+u)+cF(x) = \omega\} \\ &= \sum_{\omega \in \mathbb{F}_{2^n}} (-1)^{\omega\cdot v} \#\{x \in \mathbb{F}_{2^n} \mid F(x+u)+cF(x) = \omega\} \\ &= \sum_{\omega \in \mathbb{F}_{2^n}} (-1)^{\omega\cdot v}{}_c\Delta_F(u,\omega). \end{aligned}$$

This leads to

$${}_c\mathtt{DLCT}_F(u,v) = \frac{1}{2} \sum_{\omega \in \mathbb{F}_{2^n}} (-1)^{\omega\cdot v}{}_c\Delta_F(u,\omega),$$

which finishes the proof. □ □

5. The c-DLCT of the Inverse Function

In this section, we give the explicit values of the entries of the c-DLCT, including the case $c = 1$, and give some numerical results on $\mathbb{F}_{2^n}$ with $3 \leq n \leq 8$.

5.1. The 1-DLCT of the inverse function

For $c = 1$, the 1-DLCT satisfies the following result.

Theorem 1. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the inverse function defined by $F(0) = 0$, and $F(x) = x^{2^{n-2}}$ for $x \neq 0$. For $a, b \in \mathbb{F}_{2^n}$, define the set*

$$E_0(a,b) = \left\{ z \in b^{\perp} \mid z \neq 0, Tr\left(\frac{1}{az}\right) = 0 \right\},$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

where $b^{\perp}$ is the orthogonal space of b. Then

$$ {}_1DLCT_F(a,b) = \begin{cases} 2^{n-1} & \text{if } a = 0, \text{ or } b = 0, \\ 2\#E_0(a,b) + 2 - 2^{n-1} & \text{if } \frac{1}{a} \in b^{\perp}, \\ 2\#E_0(a,b) - 2^{n-1} & \text{if } \frac{1}{a} \notin b^{\perp}. \end{cases} $$

Proof. We use the definition

$$ {}_1\mathrm{DLCT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n} \mid b \cdot (F(x+a) + F(x)) = 0\} - 2^{n-1}. $$

We consider the following cases.
Case 1. Suppose that $b = 0$. Then, for all $x \in \mathbb{F}_{2^n}$, $b \cdot (F(x+a) + F(x)) = 0$. Hence

$$ {}_1\mathrm{DLCT}_F(a,0) = 2^n - 2^{n-1} = 2^{n-1}. $$

Case 2. Suppose that $b \neq 0$ and $a = 0$. Then, for all $x \in \mathbb{F}_{2^n}$, $b \cdot (F(x+a) + F(x)) = b \cdot 0 = 0$. This leads to

$$ {}_1\mathrm{DLCT}_F(0,b) = 2^n - 2^{n-1} = 2^{n-1}. $$

Case 3. Suppose that $b \neq 0$ and $a \neq 0$. Consider the equation

$$ b \cdot (F(x+a) + F(x)) = 0. \tag{1} $$

Case 3.1. If $x = 0$, then

$$ b \cdot (F(x+a) + F(x)) = b \cdot F(a) = b \cdot \frac{1}{a}. $$

Hence $x = 0$ is a solution of the equation (1) if and only if $\frac{1}{a} \in b^{\perp}$.
Case 3.2. If $x = a$, then

$$ b \cdot (F(x+a) + F(x)) = b \cdot F(a) = b \cdot \frac{1}{a}. $$

Hence $x = a$ is a solution of the equation (1) if and only if $\frac{1}{a} \in b^{\perp}$.
Case 3.3. Suppose that $x \neq 0$ and $x \neq a$. We have

$$ F(a+x) + F(x) = \frac{1}{a+x} + \frac{1}{x} = \frac{a}{x^2 + ax}. $$

If $b \cdot (F(a+x) + F(x)) = 0$, then $F(a+x) + F(x) = z$ for some $z \in b^{\perp}$, that is $\frac{a}{x^2+ax} = z$, or equivalently

$$ zx^2 + azx + a = 0. \tag{2} $$

Case 3.3.1. If $z = 0$, then the equation 2 reduces to $a = 0$ which is not possible.
Case 3.3.2. Suppose that $z \neq 0$. If $\mathrm{Tr}\left(\frac{1}{az}\right) = 1$, then, by Lemma 2, the equation (2) has no solution, and if $\mathrm{Tr}\left(\frac{1}{az}\right) = 0$, it has two solutions.
Define the set

$$ E_0(a,b) = \left\{ z \in b^{\perp} \mid z \neq 0, \mathrm{Tr}\left(\frac{1}{az}\right) = 0 \right\}. $$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

The ${}_1$DLCT in Case 3 is then

$${}_1\mathrm{DLCT}_F(a,b) = \begin{cases} 2\#E_0(a,b) + 2 - 2^{n-1} & \text{if } \frac{1}{a} \in b^\perp, \\ 2\#E_0(a,b) - 2^{n-1} & \text{if } \frac{1}{a} \notin b^\perp, \end{cases}$$

which finishes the proof. □ □

5.2. The c-DLCT of the inverse function for $c \neq 1$.

Theorem 2. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the inverse function defined by $F(0) = 0$, and $F(x) = \frac{1}{x}$ for $x \neq 0$. Let $c \in \mathbb{F}_{2^n}$ with $c \neq 0$ and $c \neq 1$. For $a, b \in \mathbb{F}_{2^n}$, define the set*

$$E_0(a,b,c) = \left\{ z \in b^\perp \mid z \neq 0, z \neq \frac{1+c}{a}, Tr\left(\frac{acz}{(1+c+az)^2}\right) = 0 \right\},$$

where $b^\perp$ is the orthogonal space of b. Then

$${}_c DLCT_F(a,b) = \begin{cases} 2^{n-1} & \text{if } b = 0, \\ 0 & \text{if } a = 0, b \neq 0, \\ 2\#E_0(a,b,c) + 2 - 2^{n-1} & \text{if } \frac{1}{a} \in b^\perp, \frac{c}{a} \notin b^\perp, \\ 2\#E_0(a,b,c) + 2 - 2^{n-1} & \text{if } \frac{1}{a} \notin b^\perp, \frac{c}{a} \in b^\perp, \\ 2\#E_0(a,b,c) + 4 - 2^{n-1} & \text{if } \frac{1}{a} \in b^\perp, \frac{c}{a} \in b^\perp, \\ 2\#E_0(a,b,c) + 2 - 2^{n-1} & \text{if } \frac{1}{a} \notin b^\perp, \frac{c}{a} \notin b^\perp. \end{cases}$$

Proof. Suppose that $c \neq 0$ and $c \neq 1$. We use the definition

$${}_c\mathrm{DLCT}_F(a,b) = \#\{x \in \mathbb{F}_{2^n} \mid b \cdot (F(x+a) + cF(x)) = 0\} - 2^{n-1}.$$

We consider the following cases.
Case 1. Suppose that $b = 0$. Then, for all $x \in \mathbb{F}_{2^n}$, $b \cdot (F(x+a) + cF(x)) = 0$. Hence

$${}_c\mathrm{DLCT}_F(a,0) = 2^n - 2^{n-1} = 2^{n-1}.$$

Case 2. Suppose that $b \neq 0$ and $a = 0$. If $b \cdot (F(x+a) + cF(x)) = 0$, then $b \cdot (1+c)F(x) = 0$, and $(1+c)F(x) \in b^\perp$. Observe that $x = 0$ is a possible solution. If $x \neq 0$, then there exists $z \in b^\perp \backslash \{0\}$ such that $(1+c)F(x) = z$, that is $\frac{1+c}{x} = z$, and $x = \frac{1+c}{z}$. This leads to

$${}_c\mathrm{DLCT}_F(0,b) = \#b^\perp - 2^{n-1} = 0.$$

Case 3. Suppose that $a \neq 0$ and $b \neq 0$. Consider the equation

$$b \cdot (F(x+a) + cF(x)) = 0. \tag{3}$$

Case 3.1. If $x = 0$, then

$$b \cdot (F(x+a) + cF(x)) = b \cdot F(a) = b \cdot \frac{1}{a}.$$

Hence $x = 0$ is a solution of the equation (3) if and only if $\frac{1}{a} \in b^\perp$.
Case 3.2. If $x = a$, then

$$b \cdot (F(x+a) + cF(x)) = b \cdot cF(a) = b \cdot \frac{c}{a}.$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

Hence $x = a$ is a solution of the equation (3) if and only if $\frac{c}{a} \in b^\perp$.
Case 3.3. Suppose that $x \neq 0$ and $x \neq a$. We have

$$F(a+x) + cF(x) = \frac{1}{a+x} + \frac{c}{x} = \frac{(1+c)x + ac}{x^2 + ax}.$$

If $b \cdot (F(a+x) + cF(x)) = 0$, then $F(a+x) + cF(x) = z$ for some $z \in b^\perp$, that is $\frac{(1+c)x+ac}{x^2+ax} = z$, or equivalently

$$zx^2 + (1 + c + az)x + ac = 0. \tag{4}$$

Case 3.3.1. If $z = 0$, then the equation 4 reduces to $(1+c)x + ac = 0$ wich has one solution $x = \frac{ac}{1+c}$.
Case 3.3.2. If $z_0 = \frac{1+c}{a} \in b^\perp$, then for z_0, the equation 4 reduces to $z_0x^2 + ac = 0$ which, by Lemma 2, has one solution.
Case 3.3.3. Suppose that $z \neq 0$ and $z \neq \frac{1+c}{a}$. If $\mathrm{Tr}\left(\frac{acz}{(1+c+az)^2}\right) = 1$, then, by Lemma 2, the equation (4) has no solution, and if $\mathrm{Tr}\left(\frac{acz}{(1+c+az)^2}\right) = 0$, it has two solutions.
To summarize all the cases, we define the set

$$E_0(a,b,c) = \left\{ z \in b^\perp \mid z \neq 0, z \neq \frac{1+c}{a}, \mathrm{Tr}\left(\frac{acz}{(1+c+az)^2}\right) = 0 \right\}.$$

The ${}_c$DLCT in Case 3 is then

$${}_c\mathrm{DLCT}_F(a,b) = \begin{cases} 2\#E_0(a,b,c) + 2 - 2^{n-1} & \text{if } \frac{1}{a} \in b^\perp, \frac{c}{a} \notin b^\perp, \\ 2\#E_0(a,b,c) + 2 - 2^{n-1} & \text{if } \frac{1}{a} \notin b^\perp, \frac{c}{a} \in b^\perp, \\ 2\#E_0(a,b,c) + 4 - 2^{n-1} & \text{if } \frac{1}{a} \in b^\perp, \frac{c}{a} \in b^\perp, \\ 2\#E_0(a,b,c) + 2 - 2^{n-1} & \text{if } \frac{1}{a} \notin b^\perp, \frac{c}{a} \notin b^\perp, \end{cases}$$

which finishes the proof. □ □

5.3. Numerical results for the c-DLCT of the inverse function

We have computed the c-DLCT of the inverse function over $\mathbb{F}_{2^n}$ for $3 \leq n \leq 7$, and all $c \in \mathbb{F}_{2^n}^*$, while for $n = 8$, we only compute it for $c = 1, 2, \ldots, 10$. The inversion and multiplication in $\mathbb{F}_{2^n}$ are processed modulo the polynomials presented in Table 1.

Table 1. The polynomials of $\mathbb{F}_{2^n}$ for $3 \leq n \leq 8$.

$\mathbb{F}_{2^n}$	Polynomial
$\mathbb{F}_{2^3}$	$x^3 + x + 1$
$\mathbb{F}_{2^4}$	$x^4 + x + 1$
$\mathbb{F}_{2^5}$	$x^5 + x^3 + 1$
$\mathbb{F}_{2^6}$	$x^6 + x^3 + 1$
$\mathbb{F}_{2^7}$	$x^7 + x^3 + 1$
$\mathbb{F}_{2^8}$	$x^8 + x^4 + x^3 + x^2 + 1$

In Table 2, we present the values of ${}_c\mathrm{DLCT}_F(u,v)$ of the inverse function over $\mathbb{F}_{2^4}$ with $c = 0x9$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 January 2024 doi:10.20944/preprints202401.1310.v1

Table 2. The values of ${}_c\mathrm{DLCT}_F(u,v)$ of the c-DLCT of the inverse function over $\mathbb{F}_{2^4}$ for $c = 0x9$.

$u\backslash v$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	8	0	2	2	0	-4	2	-2	2	-4	0	2	2	0	0	-2
2	8	2	0	-2	2	2	2	-2	0	2	-4	2	-4	0	0	0
3	8	0	2	0	-2	-4	0	0	-2	0	2	2	2	2	2	-4
4	8	-2	2	-2	0	2	-4	0	2	0	2	2	2	-4	0	0
5	8	2	0	2	0	0	-2	2	-4	0	2	2	-2	0	2	-4
6	8	0	-2	0	-2	2	2	-4	0	2	-4	0	0	2	2	2
7	8	2	-4	-4	2	-2	0	2	2	0	2	-2	0	0	2	0
8	8	-2	0	0	2	2	2	0	-2	2	2	-4	0	2	-4	0
9	8	2	-4	0	2	0	2	2	0	2	0	-4	2	0	-2	-2
a	8	2	0	2	-4	2	-2	-4	2	0	0	-2	0	2	0	2
b	8	-4	0	2	0	2	2	2	0	-2	0	0	-2	2	-4	2
c	8	0	-2	-4	0	0	0	2	0	-2	2	2	2	-4	2	2
d	8	0	2	2	-4	0	-4	0	2	2	0	0	2	-2	-2	2
e	8	-4	2	2	2	-2	0	0	2	-4	-2	0	0	2	0	2
f	8	2	2	0	2	0	0	2	-4	2	-2	0	-4	-2	2	0

For the inverse function over $\mathbb{F}_{2^n}$, we present in Table 3 the c-DLCT spectrum ${}_c\Gamma_F$, and c-differential-linear uniformity ${}_c\gamma_F$ for $3 \leq n \leq 8$ and for small values of c. All the other c-DLCT spectrums reduce to one of the listed ones in the table.

Table 3. The c-DLCT spectrum and the c-differential-linear connectivity uniformity of the inverse function over $\mathbb{F}_{2^n}$ for $3 \leq n \leq 8$ and small c.

$\mathbb{F}_{2^n}$	c	${}_c\Gamma_F$	${}_c\gamma_F$
$\mathbb{F}_{2^3}$	1	$\{-4,0,4\}$	4
$\mathbb{F}_{2^3}$	2	$\{-2,0,2,4\}$	2
$\mathbb{F}_{2^4}$	1	$\{-4,0,4,8\}$	4
$\mathbb{F}_{2^4}$	2	$\{-4,-2,0,2,8\}$	4
$\mathbb{F}_{2^4}$	6	$\{-2,0,2,4,8\}$	4
$\mathbb{F}_{2^5}$	1	$\{-4,0,4,16\}$	4
$\mathbb{F}_{2^5}$	2	$\{-6,-4,-2,0,2,4,6,16\}$	6
$\mathbb{F}_{2^5}$	3	$\{-6,-4,-2,0,2,4,16\}$	6
$\mathbb{F}_{2^5}$	7	$\{-4,-2,0,2,4,16\}$	4
$\mathbb{F}_{2^6}$	1	$\{-8,-4,0,4,8,32\}$	8
$\mathbb{F}_{2^6}$	2	$\{-8,-6,-4,-2,0,2,4,6,8,32\}$	8
$\mathbb{F}_{2^6}$	6	$\{-8,-6,-4,-2,0,2,4,6,32\}$	8
$\mathbb{F}_{2^6}$	8	$\{-6,-4,-2,0,2,6,8,32\}$	8
$\mathbb{F}_{2^7}$	1	$\{-12,-8,-4,0,4,8,64\}$	12
$\mathbb{F}_{2^7}$	2	$\{-12,-10,-8,-6,-4,-2,0,2,4,6,8,10,64\}$	12
$\mathbb{F}_{2^8}$	1	$\{-16,-12,-8,-4,0,4,8,12,16,128\}$	16
$\mathbb{F}_{2^8}$	2	$\{-16,-14,-12,-10,-8,-6,-4,-2,0,2,4,6,8,10,12,14,16,128\}$	16
$\mathbb{F}_{2^8}$	6	$\{-16,-14,-12,-10,-8,-6,-4,-2,0,2,4,6,8,10,12,14,128\}$	16
$\mathbb{F}_{2^8}$	10	$\{-14,-12,-10,-8,-6,-4,-2,0,2,4,6,8,10,12,14,16,128\}$	16

 doi:10.20944/preprints202401.1310.v1

6. Conclusion

In this paper, we introduced and studied new cryptographic tools and parameters to help us quantify the security of S-boxes (mathematically, vectorial Boolean functions) involving block cyphers as main components: the c-Walsh transform, the c-autocorrelation, and the c-differential-linear uniformity. We also introduced a new table called the c-Differential-Linear Connectivity Table (c-DLCT) to analyse attacks related to the differential and the linear attacks. We considered various S-box family properties associated with the above-mentioned notion and presented the values of the c-DLCT of the particular crucial case of the inverse function. Finally, recall that codes over finite fields have been studied extensively because of their linear structures and practical implementations. It is the basis of the research on various kinds of codes. One well-known construction method of linear codes is derived from special functions (essentially from cryptographic functions which play a crucial role in symmetric cryptography) over finite fields (see the book [12]). Cryptographic multi-output Boolean functions and codes have essential data communication and storage applications. These two areas are closely related and have had a fascinating interplay (see, e.g. the book's chapter [29] and the reference therein). Cryptographic functions and linear codes are closely related and have had a fascinating interplay. Cryptographic functions (e.g., highly nonlinear functions, Perfect-Nonlinear (PN), Almost Perfect Nonlinear (APN), Bent, Almost Bent (AB), Plateaued) have essential applications in coding theory. For instance, perfect nonlinear (APN or PN) functions have been employed to construct optimal linear codes (see, e.g., [28,32–35] and the references therein). Very recently, Mesnager, Shi and Zhu ([31]) proposed several constructions of minimal (cyclic) codes from low differential uniform functions. Given these works, the derived functions from this paper would help design new families of binary minimal codes. We will keep an in-depth study of them in future work and cordially invite interested readers to investigate them.

References

1. Anbar, N., Kalayci, T., Meidl, W., Riera, C., Stănică, P.: PcN functions, complete mappings and quasi-group difference sets, https://arxiv.org/abs/2212.12943, (2022)
2. Bar-On, A., Dunkelman, O., Keller, N., Weizman, A.: DLCT: A new tool for differential-linear cryptanalysis. Y. Ishai, V. Rijmen (Eds): EUROCRYPT 2019, LNCS 11476, pp. 313-342, (2019)
3. Bartoli, D., Calderini, M., Riera, C., Stănică, P.: Low c-differential uniformity for functions modified on subfields. Cryptography and Communications, 14(6), pp. 1211–1227 (2022) https://arxiv.org/abs/2112.02987
4. Picek, S., Batina, L., Jakobović, D., Ege, B. Golub, M.: S-box, SET, Match: A Toolbox for S-box Analysis. 8th IFIP International Workshop on Information Security Theory and Practice (WISTP), Jun 2014, Heraklion, Crete, Greece. pp. 140–149, 10.1007/978-3-662-43826-8-10.HAL-01400936.
5. Biham, E., and Shamir, A.: Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, vol.4, no.1, pp. 3–72, (1991)
6. Biham, E., Anderson, R.J., Knudsen, L.R.: Serpent: A new block cipher proposal. In Serge Vaudenay, editor, Fast Software Encryption, 5th International Workshop, FSE'98, Paris, France, March 23-25, 1998, Proceedings, volume 1372 of Lecture Notes in Computer Science, pages 222–238. Springer (1998)
7. Bluher, A.W.: On $x^{q+1} + x + b$. Finite Fields and Their Applications, 10(3): pp. 285–305 (2004)
8. Borisov, N., Chew, M., Johnson, R., Wagner, D.: Multiplicative differentials. In: Daemen, J., Rijmen, V. (eds) Fast Software Encryption. FSE 2002, LNCS, vol. 2365, pp. 17–33. Springer, Berlin, Heidelberg (2002)
9. Boura, C., Canteaut, A.: On the Boomerang Uniformity of Cryptographic Sboxes. IACR Transactions on Symmetric Cryptology, Ruhr Universität Bochum, 2018, 2018 (3), pp. 290–310 (2018)
10. Canteaut, A., Kölsch, L., Li, C., Li, C., Li, K., Qu, L., Wiemer, F.: On the differential-linear connectivity table of vectorial boolean functions, arXiv:1908.07445 (2019) http://arxiv.org/abs/1908.07445
11. Canteaut, A., Kölsch, L., Li. C., Li. C., Li K., Qu, L., Wiemer, F.: Autocorrelations of vectorial Boolean functions, Cryptology ePrint Archive, Paper 2021/947, (2021), https://eprint.iacr.org/2021/947
12. Carlet, C.: Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge, U.K. (2021)

13. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang Connectivity Table: A New Cryptanalysis Tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, Advances in Cryptology - EUROCRYPT 2018 -Proceedings, Part II, volume 10821 of Lecture Notes in Computer Science, 683–714. Springer (2018)
14. Daemen, J., and Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Springer, (2002)
15. Data Encryption Standard, National Bureau of Standards, NBS FIPS PUB 46, U.S. Department Of Commerce, January (1977)
16. Ellingsen, P., Felke, P., Riera, C., Stănică, P., Tkachenko, A.: C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity, IEEE Trans. Inf. Theory, 2020, https://doi.org/10.1109/TIT.2020.2971988
17. Garg, K., Hasan, S.U., Stănică, P. : Several classes of permutation polynomials and their differential uniformity properties, https://arxiv.org/abs/2212.01931 (2022)
18. GOST 28147-89: Cryptographic Protection for Data Processing Systems, Cryptographic Transformation Algorithm. Government Standard of the U.S.S.R., Inv. No. 3583, UDC 681.325.6:006.354., 1998 (in Russian)
19. Hasan, S.U., Pal, M., Riera, C., Stănică, P. : On the c-differential uniformity of certain maps over finite fields, Des. Codes Cryptogr. 89, 221-239, (2021)
20. Hasan, S.U., Pal, M., Stănică, P. : On the c-differential uniformity and boomerang uniformity of two classes of permutation polynomials, IEEE Trans. Inf. Theory 68, 679-691 (2022)
21. Huffman, W.C., Pless, V. : *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Published in the United States of America by Cambridge University Press, New York, (2003).
22. Jeong, J., Koo, N., Kwon, S.: Investigations of c-differential uniformity of permutations with Carlitz rank 3, Finite Fields Appl. 86, 102145 (2023)
23. Jeong, J., Koo, N., Kwon, S.: On non-monomial APcN permutations over finite fields of even characteristic, https://arxiv.org/abs/2205.11418 (2022)
24. Li, K., Li, C., Li, C., Qu, L.: On the differential linear connectivity table of vectorial boolean functions, arXiv:1907.05986 http://arxiv.org/abs/1907.05986 (2019)
25. Li, C., Riera, C., Stănică, P.: Low c-differentially uniform functions via an extension of Dillon's switching method, https://arxiv.org/abs/2204.08760 (2022)
26. Kim, H., Kim, S., Hong, D., Sung, J., Hong, S.: Improved Differential-Linear Cryptanalysis Using DLCT, Journal of The Korea Institute of Information Security & Cryptology VOL.28, NO.6, Dec. 2018 (2018)
27. Matsui, M. (1994) Linear Cryptanalysis Method for DES Cipher. In: Helleseth T. (eds) Advances in Cryptology - EUROCRYPT'93. EUROCRYPT 1993. Lecture Notes in Computer Science, vol 765. pp. 386-397, Springer, Berlin, Heidelberg (1994)
28. Mesnager, S.: Linear codes with few weights from weakly regular bent functions based on a generic construction, Cryptogr. Commun., vol. 9, no. 1, pp. 71-84, (2017)
29. Mesnager, S.: Linear codes from functions. Chapter 20 in A Concise Encyclopedia of Coding Theory CRC Press/Taylor and Francis Group (Publisher) London, New York, 2021 (94 pages), In W-C. Huffman, J-L. Kim, Patrick Solé (eds)
30. Mesnager, S., Mandal, B., Msahli, M.: Survey on recent trends towards generalized differential and boomerang uniformities. Cryptography and Communications. https://doi.org/10.1007/s12095-021-00551-6 (2021)
31. Mesnager, S., Shi, M., Zhu, H.: Cyclic codes from low differentially uniform functions. CoRR abs/2210.12092 (2022)
32. Mesnager, S., Özbudak, F., and Sßnak, A. "Linear codes from weakly regular plateaued functions and their secret sharing schemes," *Des. Codes Cryptogr.*, vol. 87, no 3, pp. 463-480, (2019)
33. Mesnager, S., Qi, Y., Ru, H., and Tang, C. "Minimal linear codes from characteristic functions," *IEEE Trans. Inf. Theory*, vol. 66, no. 9, pp. 5404-5413, (2020)
34. Mesnager, S., and Sßnak, A. "Several classes of minimal linear codes with few weights from weakly regular plateaued functions," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 2296-2310, 2020.
35. S. Mesnager, A. Sßnak and O. Yayla, "Minimal linear codes with few weights and their Secret Sharing," *International Journal of Information Security Science*, Springer, vol.8, no.3, pp.44-52, (2019)
36. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth T. (eds) Advances in Cryptology - EUROCRYPT'93. Lecture Notes in Computer Science, vol 765. pp. 55-64, Springer, Berlin, Heidelberg (1994)

37. National Institute of Standards and Technology. Federal Information Processing Standards Publication 197: Announcing the Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
38. Pal, M. Some new classes of (almost) perfect c-nonlinear permutations https://arxiv.org/abs/2208.01004 (2022)
39. Pommerening, Kl.: Quadratic equations in finite fields of characteristic 2, February (2012) http://www.staff.uni-mainz.de/pommeren/MathMisc/QuGlChar2.pdf
40. Schneier, B.: Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish). In Ross Anderson, editor, Fast Software Encryption, volume 809 of Lecture Notes in Computer Science, pages 191-204. Springer Berlin Heidelberg (1994)
41. Stănică, P.: Investigations on c-boomerang uniformity and perfect nonlinearity, (2021) https://arxiv.org/abs/2004.11859
42. Stănică, P., Geary, A.: The c-differential behavior of the inverse function under the EA-equivalence, Cryptogr. Commun. 13, pp. 295–306 (2021)
43. Stănică, P.: Low c-differential uniformity for the Gold function modified on a subfield, Proc. International Conf. on Security and Privacy, Springer (ICSP 2020), LNEE 744, Springer 2021, pp. 131–137 (2021)
44. Tang, D., Carlet, C., and Zhou, Z. : Binary linear codes from vectorial Boolean functions and their weight distribution. Discret. Math., vol. 340, no. 12, pp. 3055-3072, (2017)
45. Tu, Z., Li, N., Wu, Y., Zeng, X., Tang, X., Jiang, Y.: On the Differential Spectrum and the APcN Property of a Class of Power Functions Over Finite Fields, IEEE Trans. Inf. Theory 69:1 582-597, (2023)
46. Tu, Z., Zeng, X., Jiang, Y., Tang, X. : A class of APcN power functions over finite fields of even characteristic, (https://arxiv.org/abs/2107.06464v1) (2021)
47. Wagner, D.: The Boomerang Attack. In Lars R. Knudsen, editor, Fast Software Encryption, volume 1636 of Lecture Notes in Computer Science, pages 156–170. Springer (1999)
48. Wang, X., Zheng, D., Hu, L.: Several classes of PcN power functions over finite fields. Discrete Applied Mathematics 322, pp. 171-182 (2022)
49. Wang, Z., Mesnager, S., Li, N., Zeng, X.: On the c-differential uniformity of a class of Niho-type power functions. arXiv:2003.13019 (2020) https://arxiv.org/abs/2003.13019
50. Yan, H., Zhang, K.: On the c-differential spectrum of power functions over finite fields. Des. Codes Cryptogr. 90, 2385-2405 (2022)
51. Wu, Y., Li, N., Zeng, X.: New PcN and APcN functions over finite fields, Des. Codes Cryptogr. 89 -46, 2637-2651 (2021)
52. Zha, Z., Hu, L. : Some classes of power functions with low c-differential uniformity over finite fields, 50 Des. Codes Cryptogr. 89 1193-1210 (2021)