The Extended Autocorrelation and Boomerang Tables and Links Between Nonlinearity Properties of Vectorial Boolean Functions

Kaisa Nyberg

kaisa.nyberg@aalto.fi
December 1, 2019

Abstract. Given the links between nonlinearity properties and the related tables such as LAT, DDT, BCT and ACT that have appeared in the literature, the boomerang connectivity table BCT seems to be an outlier as it cannot be derived from the others using Walsh-Hadamard transform. In this paper, a brief unified summary of the existing links for general Boolean vectorial functions is given first and then a link between the autocorrelation and boomerang connectivity tables is established.

Keywords: linear approximation, differential, differential-linear approximation, boomerang, autocorrelation, vectorial Boolean functions

1 Introduction

Since the introduction of differential and linear cryptanalysis, the DDT and LAT tables that capture the probabilities of differentials and correlations of linear approximations have provided useful tools for evaluating the resistance or vulnerability of a block cipher against these attacks. They have also been used in the context of more convoluted attack variants such as the differential-linear and boomerang attacks under assumptions of independence between rounds of the cipher. In particular the boomerang attack requires an independence assumption which is stronger than the usual assumption on independendence of differentials. Almost twenty years after the invention of the boomerang attack, Cid et al. introduced a dedicated tool to evaluate the vulnerability of a cryptographic function against boomerang attacks. Inspired by the boomerang connectivity table, Bar-On et al. presented a similar tool to capture the differential-linear biases and demonstrated it in practice in the context of previously presented differential-linear attacks.

The new tables and the related nonlinearity properties attracted the interest of experts in Boolean functions. A number of new papers on the properties and bounds of boomerang and differential-linear connectivity values for various classes of highly nonlinear Boolean functions and optimal Sboxes has appeared recently. Also some links between the new tables and the known ones have been established. The connections between probabilities of differentials, correlations of linear approximations and biases of differential-linear approximations are fully understood. What is less studied is the boomerang probabilities and their links to the corresponding strength measures of the other attacks. While interesting from the theory point of view such links can be useful also for establishing nonlinearity bounds and evaluating computational complexity.

In this short paper we will give a summary of the tables related to differential, linear, differential-linear attacks for general vectorial Boolean functions. To capture also the boomerang connectivity tables we will introduce a generalization of autocorrelation. This new nonlinearity concept is not only of theoretical interest, since it is closely related to

differential-linear cryptanalysis and can potentially be used to strengthen differential-linear approximations. Further, an extension of boomerang connectivity is introduced and its link to the generalized autocorrelation is established.

We will start by definitions of the known nonlinearity properties and the related tables and also give the references omitted in this introductory section. After establishing the known links in Section 3 we will present the new concept of extended autocorrelation in Section 4.

2 Nonlinearity properties

Let n and m be positive integers. Throughout this paper we consider F to be a function which maps n-bit strings to m-bit strings. We denote the linear space of dimension n over the field $\mathbb{F}_2$ by $\mathbb{F}_2^n$. Then F is a vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. We use " $\oplus$ " to denote the sum operation and " $\cdot$ " to denote the canonical inner product operation between two vectors in $\mathbb{F}_2^n$.

Differential Given $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^m$ a differential of F is defined as

$$F(x) \oplus F(x \oplus a) = b, \text{, for } x \in \mathbb{F}_2^n,$$

where a and b are called differences. The number of $x \in \mathbb{F}_2^n$ that satisfy this relation is denoted by $\mathrm{DDT}_F(a, b)$. The table

$$\mathrm{DDT}_F(a, b),\ a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m,$$

is called the difference distribution table DDT of F.

Linear approximation Given $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$ a linear approximation of F is the following relation

$$u \cdot x = v \cdot F(x),\ \text{for } x \in \mathbb{F}_2^n,$$

where u and v are called masks. The number of $x \in \mathbb{F}_2^n$ that satisfy this relation subtracted by the number of x that do not satisfy it, is denoted by $\mathrm{LAT}_F(u, v)$. The table

$$\mathrm{LAT}_F(u, v),\ u \in \mathbb{F}_2^n,\ v \in \mathbb{F}_2^m,$$

is called the linear approximation table LAT of F.

Boomerang Given $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^m$ a boomerang of F is defined by the following two relations

$$F(x) \oplus F(y) = b \text{ and } F(x \oplus a) \oplus F(y \oplus a) = b,\ \text{for } x, y \in \mathbb{F}_2^n.$$

The number of pairs $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ that satisfy this relation is denoted by $\mathrm{BCT}_F(a, b)$. The table

$$\mathrm{BCT}_F(a, b),\ a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m,$$

is called the boomerang connectivity table BCT of F.

Autocorrelation Given $a \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$ an autocorrelation relation of F is defined as

$$v \cdot (F(x) \oplus F(x \oplus a)) \text{, for } x \in \mathbb{F}_2^n.$$

Then the autocorrelation $\mathrm{ACT}_F(a, v)$ is defined as the number of $x \in \mathbb{F}_2^n$ for which the autocorrelation relation equals 0 subtracted by the number of x for which the relation equals 1. The table

$$\mathrm{ACT}_F(a, v),\ a \in \mathbb{F}_2^n,\ v \in \mathbb{F}_2^m,$$

is called the autocorrelation table ACT of F.

In the description of the nonlinearity properties above we are using the letters a, b, c from the beginning of the alphabet to denote difference vectors. The letters u, v, w towards the end of the alphabet are used to denote masks of linear approximations. We omit the symbol F of the function unless it is not the same for all tables under consideration.

3 Links between nonlinearity tables

All links described in this paper are based on the Walsh-Hadamard transform. Let $f : \mathbb{F}_2^n \to \mathbb{R}$ be a real-valued function of bit strings of length n. The Walsh-Hadamard transform $\widehat{f}$ of f at $y \in \mathbb{F}_2^n$ is defined as

$$\widehat{f}(y) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{y \cdot x}.$$

where the sum is the addition of real numbers. The Walsh-Hadamard transform can be inverted. To compute the inverse Walsh-Hadamard transform one applies the Walsh-Hadamard transform and multiplies the result by the factor 2^{-n}

$$\begin{aligned} \widehat{\widehat{f}}(x) &= 2^{-n} \sum_{y \in \mathbb{F}_2^n} \widehat{f}(y)(-1)^{x \cdot y} \\ &= f(x). \end{aligned}$$

3.1 Link between DDT and LAT

The connection between the differential distribution and linear approximation tables was established by Chabaud and Vaudenay in 1994 [CV94]. Using this link the DDT can be computed from the LAT as follows

$$\mathrm{DDT}(a, b) = 2^{-(n+m)} \sum_u (-1)^{u \cdot a} \sum_v (-1)^{v \cdot b} \mathrm{LAT}(u, v)^2 \tag{1}$$

using the inverse Walsh-Hadamard transform over $\mathbb{F}_2^n \times \mathbb{F}_2^m$. Similarly, the values $\mathrm{LAT}(u, v)^2$ can be computed from the DDT using the Walsh-Hadamard transform.

3.2 Linking ACT to DDT and LAT

The concept of autocorrelation originates from the theory of sequences. In the context of nonlinearity properties of Boolean functions autocorrelation was defined by Zhang and Zheng in late 1990s, see e.g. [ZZ96]. In a subsequent work by Zhang et al. the concept of autocorrelation table of vectorial Boolean functions was introduced [ZZI00].

It seems that autocorrelation was not connected to differential-linear cryptanalysis until 2019 when Bar-On et al. defined the differential-linear connectivity table DLCT, comprising the differential-linear biases of the function [BDKW19], and Canteaut et al. noticed the connection between DLCT and ACT [CKL+19]. Indeed,

$$\mathrm{DLCT}(a, v) = \frac{1}{2}\mathrm{ACT}(a, v),$$

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

Previously, partial links had been established. For example, the following link between differential-linear biases and differential probabilities

$$\sum_v (2\mathrm{DLCT}(a, v))^2 = 2^m \sum_b \mathrm{DDT}(a, b)^2$$

had been mentioned by Nyberg [Nyb15].

By [ZZI00] and Equation (1) we now have

$$\begin{aligned} \mathrm{ACT}(a,v) &= 2^{-n}\sum_u (-1)^{u\cdot a}\,\mathrm{LAT}(u,v)^2 \quad \text{and} \\ \mathrm{ACT}(a,v) &= \sum_b (-1)^{v\cdot b}\,\mathrm{DDT}(a,b). \end{aligned}$$

Accordingly, ACT entries are computed from squared LAT entries by applying the inverse Walsh-Hadamard transform at the input side. Alternatively, ACT entries can be computed from the DDT entries by applying the Walsh-Hadamard transform at the output side as used by Bar-On et al. in [BDKW19].

If $m = n$ and F is bijective, we have $\mathrm{LAT}_{F^{-1}}(v,u) = \mathrm{LAT}_F(u,v)$ and also $\mathrm{DDT}_{F^{-1}}(b,a) = \mathrm{DDT}_F(a,b)$. It follows that the ACT of F^{-1} can be computed from the ACT of F by applying the inverse Walsh-Hadamard transform at the output side of F and the Walsh-Hadamard transform at the input side of F (output side of F^{-1}) as follows

$$\begin{aligned} 2^{-n}\sum_{a,v}(-1)^{u\cdot a\oplus v\cdot b}\,\mathrm{ACT}_F(a,v) &= \sum_a (-1)^{u\cdot a}\,\mathrm{DDT}_F(a,b) \\ &= \sum_a (-1)^{u\cdot a}\,\mathrm{DDT}_{F^{-1}}(b,a) \\ &= \mathrm{ACT}_{F^{-1}}(b,u), \end{aligned}$$

if the transform is applied first on the output side. If the transform is applied first on the input side, then the derivation goes via the squared LAT entries.

Note that there is a typo in [CKL+19] on the left side of Equation (7), which should read $\mathsf{AC}_{F^{-1}}(v,u)$, that is, v in their notation is the input difference to F^{-1} and u is the linear mask of the autocorrelation function of F^{-1}.

3.3 Linking BCT to DDT, LAT, and ACT

Cid et al. gave the definition of BCT table for bijective functions and showed that it can be an efficient tool in estimating the boomerang probability [CHP+18]. Recently, the definition was generalized for arbitrary vectorial Boolean functions by Li et al. to the form given above in Section 2 [LQSL19]. From this definition, we get immediately the following link.

Proposition 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a Boolean function and $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^m$. Then*

$$\sum_b \mathrm{BCT}(a,b) = \sum_b \mathrm{DDT}(a,b)^2.$$

Proof. Using the definition of BCT we get

$$\begin{aligned} \sum_b \mathrm{BCT}(a,b) &= \#\{\,(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid F(x)\oplus F(y) = F(x\oplus a)\oplus F(y\oplus a)\,\} \\ &= \#\{\,(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid F(x)\oplus F(x\oplus a) = F(y)\oplus F(y\oplus a)\,\}. \end{aligned}$$

□

For bijective functions, this link was previously given by Nyberg [Nyb15] and by Mesnager et al. [MTX19].

Using the known links between DDT and ACT, we now have

$$\sum_b \mathrm{BCT}(a,b) = \sum_b \mathrm{DDT}(a,b)^2 = 2^{-m}\sum_v \mathrm{ACT}(a,v)^2.$$

Computing the boomerang connectivity table from the differential distribution or autocorrelation table does not seem possible in general. Next we introduce a generalization of the autocorrelation table. The new table is sufficiently large to capture information of all nonlinearity tables discussed in this paper.

4 Extended autocorrelation table EACT

Let us consider the following Boolean expression

$$v \cdot F(x) \oplus w \cdot F(x \oplus a),$$

where $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a vectorial Boolean function, $a \in \mathbb{F}_2^n$ and $v, w \in \mathbb{F}_2^m$ and denote by $\mathrm{EACT}(a; v, w)$ the number of $x \in \mathbb{F}_2^n$ for which this expression is equal to 0 subtracted by the number of x such that the expression is equal to 1. That is,

$$\mathrm{EACT}_F(a; v, w) = 2\#\{\, x \in \mathbb{F}_2^n \mid v \cdot F(x) \oplus w \cdot F(x \oplus a) = 0 \,\} - 2^n.$$

Let us call the table $\mathrm{EACT}_F(a; v, w)$, $a \in \mathbb{F}_2^n$ and $v, w \in \mathbb{F}_2^m$, extended autocorrelation table EACT of F.

Clearly, $\mathrm{EACT}(a; v, v) = \mathrm{ACT}(a, v)$, for all $a \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$. Hence, given the EACT table, we have the ACT table and can compute the DDT and LAT tables.

4.1 Computing BCT from EACT

Computation of the boomerang connectivity table can be done using the link given by the following proposition.

Proposition 2. *For all vectorial Boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, vectors $a \in \mathbb{F}_2^n$ and $v, w \in \mathbb{F}_2^m$, the following holds:*

$$\mathrm{BCT}(a, b) = 2^{-2m} \sum_{v,w} (-1)^{(u+w)\cdot b} \mathrm{EACT}(a; v, w)^2. \tag{2}$$

Proof.

$$\begin{aligned}
\mathrm{BCT}(a, b) &= 2^{-2m} \sum_{x,y} \sum_{v} (-1)^{v\cdot(F(x)\oplus F(y)\oplus b)} \sum_{w} (-1)^{w\cdot(F(x\oplus a)\oplus F(y\oplus a)\oplus b)} \\
&= 2^{-2m} \sum_{v,w} (-1)^{b\cdot(v\oplus w)} \left(\sum_{x} (-1)^{v\cdot F(x)\oplus w\cdot F(x\oplus a)} \right)^2 \\
&= 2^{-2m} \sum_{v,w} (-1)^{(v\oplus w)\cdot b}\, \mathrm{EACT}(a; v, w)^2.
\end{aligned}$$

□

By changing the summation over w to summation over $\delta = v \oplus w$ we obtain

$$\mathrm{BCT}(a, b) = 2^{-2m} \sum_{v} \sum_{\delta} (-1)^{\delta\cdot b}\, \mathrm{EACT}(a; v, v \oplus \delta)^2.$$

Computing this expression takes one Walsh-Hadamard transform in dimension m for each $v \in \mathbb{F}_2^m$.

4.2 Properties of EACT tables

The extended autocorrelation table is not interesting only due to the fact that the differential distribution, linear approximation and boomerang tables can be computed from it. Entries of EACT tables with large absolute value can be exploited in a differential-linear type attack.

Let us start by the observation that for each fixed $a \in \mathbb{F}_2^n$ the table $\mathrm{EACT}(a; v, w)$ is symmetric, that is $\mathrm{EACT}(a; v, w) = \mathrm{EACT}(a; w, v)$ for all $v, w \in \mathbb{F}_2^m$. It means that if there is an entry $\mathrm{EACT}(a : v, w)$ with $v \neq w$ such that $\mathrm{EACT}(a; v, w) = \pm 2^n$ then $\mathrm{EACT}(a; w, v) = \pm 2^n$ and $\mathrm{EACT}(a; v \oplus w, v \oplus w) = \mathrm{ACT}(a, v \oplus w) = 2^n$. But in general it is possible that $\max_{v,w} |\mathrm{EACT}(a; v, w)| > max_v |\mathrm{ACT}(a, v)|$.

The extended autocorrelation expression relates to an attack which is very similar to the differential-linear attack. In the online phase of the attack, it really does not matter if the masks on $F(x)$ and $F(x \oplus a)$ are different or equal. In the offline phase, the extended expression requires more computation, but on the other hand, offers more freedom in choosing the masks to maximize the differential-linear biases.

To give a small example to motivate the importance of checking also the EACT of a cryptographic function such as Sbox, let us consider the EACT of the following 4×4 Sbox

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

which we denote by S.

We can see that given the input difference $a = 1011$ to S we have $v \cdot S(x) \neq w \cdot S(x \oplus a)$ for all x, if $v = \mathtt{0100}$ and $w = \mathtt{0001}$. Thus $\mathrm{EACT}(a : v, w) = -16$. Then also $\mathrm{EACT}(a : w, v) = -16$ and on the diagonal of EACT we have $\mathrm{EACT}(a : v \oplus w, v \oplus w) = \mathrm{ACT}(a, v \oplus w) = 16$ where $v \oplus w$ is a two-bit mask. Moreover, the highest (absolute) value of $\mathrm{ACT}(a, v')$ for a single-bit mask v' is 8 and is obtained for $v' = \mathtt{1000}$.

Let us assume that single-bit output masks of the differential-linear approximation are preferred. The reason for that can be, for example, the diffusion layer, which makes two active bits from the previous round to activate two Sboxes at the next round. In such a situation, using different masks v and w as given above may be advantageous.

4.3 Extended boomerang connectivity table

It is clear that the link (2) does not work backwards. In order to compute squared EACT entries from boomerang table we need an extended boomerang connectivity table EBCT defined as follows

$$\mathrm{EBCT}_F(a; b, c) = \#\{\, (x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid F(x) \oplus F(y) = b \text{ and } F(x \oplus a) \oplus F(y \oplus a) = c \,\}.$$

It is straightforward to verify that

$$\mathrm{EACT}(a; v, w)^2 = \sum_{b,c} (-1)^{v \cdot b \oplus w \cdot c} \, \mathrm{EBCT}(a; b, c)$$

that is, for all fixed input differences $a \in \mathbb{F}_2^n$, the table with squared EACT entries (denoted as EACT^2)is the Walsh-Hadamard transform of the EBCT table over the pairs (b, c) of output differences in $\mathbb{F}_2^m \times \mathbb{F}_2^m$. Using the inverse Walsh-Hadamard transform, this link works also to the other direction. In summary

$$\mathrm{ACT}^2 \xleftarrow{\text{diagonal}} \mathrm{EACT}^2 \xleftrightarrow{\text{Walsh-Hadamard Transform}} \mathrm{EBCT} \xrightarrow{\text{diagonal}} \mathrm{BCT},$$

where we denoted by ACT^2 the table of squared ACT entries. Similarly as the EACT table offers more options in selecting the output linear approximations for the differential-linear approximation, the EBCT table offers more options for output differences for the boomerang.

5 Conclusion

We have considered the tools for evaluating known non-linearity properties of cryptographic functions such as Sboxes and super Sboxes used in block ciphers. We have also given a unified summary of links between these properties for general vectorial Boolean functions based on the existing literature, some of which considered only bijective functions. Finally, we show that, while not themselves mutually directly linked, the autocorrelation and boomerang connectivity tables are obtained from the diagonals of the extended autocorrelation and boomerang tables that are mutually linked via the Walsh-Hadamard transform.

References

[BDKW19] Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizman. DLCT: A new tool for differential-linear cryptanalysis. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 313–342. Springer, 2019.

[CHP+18] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 683–714. Springer, 2018.

[CKL+19] Anne Canteaut, Lukas Kölsch, Chao Li, Chunlei Li, Kangquan Li, Longjiang Qu, and Friedrich Wiemer. On the differential-linear connectivity table of vectorial boolean functions. *CoRR*, abs/1908.07445, 2019.

[CV94] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In Alfredo De Santis, editor, *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 356–365. Springer, 1994.

[LQSL19] Kangquan Li, Longjiang Qu, Bing Sun, and Chao Li. New results about the boomerang uniformity of permutation polynomials. *IEEE Trans. Information Theory*, 65(11):7542–7553, 2019.

[MTX19] Sihem Mesnager, Chunming Tang, and Maosheng Xiong. On the boomerang uniformity of quadratic permutations. Cryptology ePrint Archive, Report 2019/277, 2019. https://eprint.iacr.org/2019/277.

[Nyb15] Kaisa Nyberg. Reverse-engineering hidden assumptions in differential-linear attacks. https://www.cryptolux.org/mediawiki-esc2015/images/8/82/Nyberg_rev.pdf, 2015. ESC Clervaux.

[ZZ96] Xian-Mo Zhang and Yuliang Zheng. Auto-correlations and new bounds on the nonlinearity of boolean functions. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16,*

1996, Proceeding, volume 1070 of *Lecture Notes in Computer Science*, pages 294–306. Springer, 1996.

[ZZI00] Xian-Mo Zhang, Yuliang Zheng, and Hideki Imai. Relating differential distribution tables to other properties of of substitution boxes. *Des. Codes Cryptogr.*, 19(1):45–63, 2000.