On the Feistel Counterpart of the Boomerang Connectivity Table

Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal, Marine Minier

IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2020, No. 1, pp. 331–362. DOI:10.13154/tosc.v2020.i1.331-362

On the Feistel Counterpart of the Boomerang Connectivity Table

Introduction and Analysis of the FBCT

Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal and Marine Minier

Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France firstname.name@loria.fr

Abstract. At Eurocrypt 2018, Cid et al. introduced the Boomerang Connectivity Table (BCT), a tool to compute the probability of the middle round of a boomerang distinguisher from the description of the cipher's Sbox(es). Their new table and the following works led to a refined understanding of boomerangs, and resulted in a series of improved attacks. Still, these works only addressed the case of Substitution Permutation Networks, and completely left out the case of ciphers following a Feistel construction. In this article, we address this lack by introducing the FBCT, the Feistel counterpart of the BCT. We show that the coefficient at row Δ_i, ∇_o corresponds to the number of times the second order derivative at points (Δ_i, ∇_o) cancels out. We explore the properties of the FBCT and compare it to what is known on the BCT. Taking matters further, we show how to compute the probability of a boomerang switch over multiple rounds with a generic formula.

Keywords: Cryptanalysis · Feistel cipher · Boomerang attack · Boomerang switch

1 Introduction

Boomerang attacks date back to 1999, when David Wagner introduced them at FSE to break COCONUT98 [Wag99]. When presented, this variant of differential attacks [BS91] shook up the conventional thinking that consisted in believing that a cipher with only small probability differentials is secure. Indeed, boomerang attacks make use of two small differentials covering half of the attacked rounds each, and can beat differential cryptanalysis when no high probability differential exists for the whole cipher.

In the basic form of the distinguisher, (represented on the left in Figure 1), the attacker has access to the encryption (E) and decryption (E^{-1}) oracles, and studies particular quartets of messages. First, she chooses M^1 and constructs $M^2 = M^1 \oplus \alpha$; using E, she obtains the corresponding ciphertexts C^1 and C^2 from which she deduces two additional ciphertexts by computing: $C^3 = C^1 \oplus \delta$ and $C^4 = C^2 \oplus \delta$. By calling the decryption oracle she retrieves the corresponding plaintexts M^3 and M^4 and then checks if $M^3 \oplus M^4 = \alpha$. A boomerang distinguisher is obtained if the probability that $M^3 \oplus M^4 = \alpha$ is higher for the cipher than for a random permutation.

In summary, a boomerang distinguisher is based on a couple of plaintext and ciphertext differences (α, δ) for which the following property among quartets of messages has a high probability:

$$E^{-1}(E(M^1) \oplus \delta) \oplus E^{-1}(E(M^1 \oplus \alpha) \oplus \delta) = \alpha.$$

In the original approach, the attacked cipher E is written as the composition of two sub-ciphers E_0 and E_1: $E = E_1 \circ E_0$. If for the sub-cipher E_0 the input difference α leads

Received: 2019-09-01, Revised: 2019-11-23, Accepted: 2020-01-23, Published: 2020-05-07

to the output difference β with probability p (and similarly γ leads to δ with probability q over E_1) the previous event was thought to have a probability of p^2q^2.

Following this breakthrough some variants were proposed including a related-key version [KKH+04, BDK05] and an impossible-differential one (see [CY09]). Improvements were also proposed on top of this, like a version that does not require access to the decryption oracle (named *amplified boomerang attack* [KKS01]) that was further developed into the so-called *rectangle attack* [BDK01].

The validity of boomerang attacks and in particular of the p^2q^2 formula were later questioned by Murphy [Mur11] with an example of distinguisher that seemed valid but was in fact of probability zero. The opposite phenomenon, that is distinguishers that happen with probability higher than what is expected, was also presented by Biryukov and Khovratovich in [BK09], and some particular cases (termed *Ladder Switch*, *Sbox Switch* and *Feistel Switch*) were explained.

All these observations were later formalized in a framework called *sandwich attack* [DKS10] for which the cipher is divided in 3 parts instead of 2, as represented on the right of Figure 1: a middle part E_m (termed *boomerang switch*) is introduced between E_0 and E_1. Dunkelman et al. applied this framework to KASUMI.

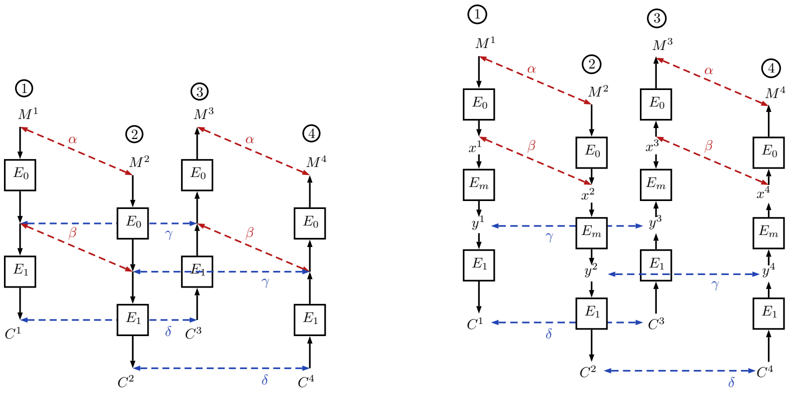

Figure 1: Configuration of the basic boomerang attack (left) and of the sandwich attack (right). Circled numbers correspond to a numbering that helps referencing states in the following discussions.

Cid et al. [CHP+18] recently introduced a tool called the *Boomerang Connectivity Table* that allows to easily evaluate the probability of the middle part E_m in the case where it covers one round and when the studied ciphers follows an SPN construction. Their technique reduces the problem of computing the probability of the boomerang switch over one round function to the one of computing it over one Sbox only.

Equally as an Sbox with a Difference Distribution Table with small coefficients provides resistance against differential attacks, an Sbox with a Boomerang Connectivity Table (BCT) with small coefficients prevents an attacker from building efficient boomerang-style attacks. A study of some important families of Sboxes has been made in [BC18], [BPT19] and [LQSL19], just to cite a few. Another interesting line of work that followed the paper of Cid et al. is the determination of the probability of a boomerang switch E_m that covers more than one round, and that was addressed for SPN ciphers in [WP19, SQH19].

Still, to the best of our knowledge a similar analysis has not been provided yet for Feistel constructions [Fei74], while it cannot be denied that it is an equally important type of block cipher design, instantiated for instance by the widely used 3-DES and by CLEFIA [SSA+07] (ISO/IEC 29192-2).

Our Contributions. In this work, we address this lack and investigate what can be said on a boomerang switch when the studied cipher follows a Feistel construction. In case the Feistel round function contains some affine layers and a single Sbox layer we introduce the FBCT, the Feistel counterpart of the Boomerang Connectivity Table and show that it is related to the second order derivative of the Sbox at play. Our model elucidates the last switch that is not explained by the BCT by showing that the Feistel Switch corresponds to the diagonal of our table.

We study the properties of the FBCT for some categories of cryptographic Sboxes (in particular APN Sboxes and Sboxes based on the inverse mapping) and investigate if the maximum in the FBCT is invariant for Sboxes that are in the same equivalence classes for an equivalence that is affine, extended-affine and CCZ.

In a bottom-up approach, we start from this notion of FBCT (that covers switches of one round) and then introduce the FBDT to deal with a 2-round switch and finally propose the FBET that treats the case of an arbitrary number of rounds. We explain the relation between all these new notions and give examples of their application.

Finally, we illustrate our approach by applying it to the cipher LBlock-s (used in the CAESAR candidate LAC), and provide a 16-round distinguisher which probability is evaluated to be higher than $2^{-56.14}$.

2 Motivation: Disproving the Validity of a Previous Boomerang Distinguisher on LBlock

As a warm up, we study the related-key boomerang distinguisher devised by Liu et al. on LBlock [LGW12] and prove that the middle part contains a contradiction that invalidates the proposed boomerang distinguisher.

2.1 Specification of LBlock

LBlock was proposed at ACNS 2011 [WZ11] by Wenling Wu and Lei Zhang. The cipher is lightweight and works on blocks of 64 bits and requires a key of 80 bits. It follows a Feistel structure and has the particularity to rely on 10 different 4-bit Sboxes. We give a short description of its design below and refer to [WZ11] for more details and in particular for the description of the key schedule.

One LBlock encryption requires to iterate 32 times a round function that follows a 2-branch balanced Feistel structure with a twist, that is the right branch is modified by a rotation of 8 bit positions (see Figure 2). The other half of the internal state is modified by the F function that takes as parameter the 32-bit round key K_i. If the plaintext is denoted $M = X_1||X_0$ (where $||$ denotes the concatenation), we have for all $33 \geq i \geq 2$:

$$X_i = F(X_{i-1}, K_{i-1}) \oplus (X_{i-2} \lll 8).$$

More into details, the function F is defined as:

$$\begin{aligned} F : \{0,1\}^{32} \times \{0,1\}^{32} &\rightarrow \{0,1\}^{32} \\ (X, K_i) &\rightarrow U = P(S(X \oplus K_i)). \end{aligned}$$

S is an Sbox layer that transforms each nibble Y_i into the nibble $Z_i = S_i(Y_i)$:

$$\begin{aligned} S : \{0,1\}^{32} &\rightarrow \{0,1\}^{32} \\ Y_7||Y_6||Y_5||Y_4||Y_3||Y_2||Y_1||Y_0 &\rightarrow Z_7||Z_6||Z_5||Z_4||Z_3||Z_2||Z_1||Z_0, \quad Z_i = S_i(Y_i). \end{aligned}$$

The Sboxes are detailed in Table 5 in Appendix A. P is a permutation given by:

$$\begin{aligned} P : \{0,1\}^{32} &\rightarrow \{0,1\}^{32} \\ Z_7||Z_6||Z_5||Z_4||Z_3||Z_2||Z_1||Z_0 &\rightarrow U = Z_6||Z_4||Z_7||Z_5||Z_2||Z_0||Z_3||Z_1. \end{aligned}$$

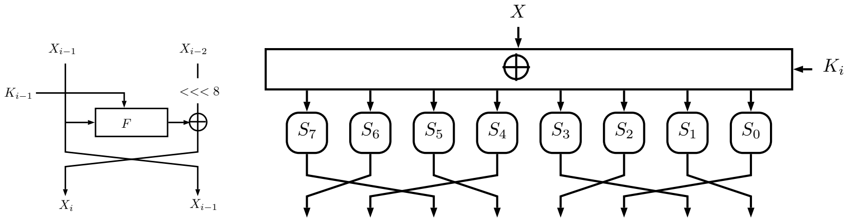

Figure 2: High-level description of one round of LBlock (left) and description of the F function (right).

2.2 Attack of Liu et al.

In 2012, Liu et al. [LGW12] proposed a 16-round related-key boomerang distinguishing attack on LBlock based on two 8-round related-key characteristics of low weight (that is, with very few active Sboxes). This attack is supposed to work in some (very large) weak-key class as it includes a key condition. With their parameters (that we recall in Appendix B), the probability of E_0 is $p = 2^{-14}$, while the probability of E_1 is $q = 2^{-16}$. They next computed the probability of the obtained distinguisher with the approximation p^2q^2, that gives 2^{-60}. Unfortunately, next section details why the two characteristics E_0 and E_1 are in fact incompatible, meaning that the actual probability that the boomerang returns along these differential characteristics is 0.

2.3 Incompatibility in the Distinguisher Proposed by Liu et al.

To help visualize the following discussion, we provide in Figure 3 a representation of the end of E_0 and of the beginning of E_1. In the following, we assume that the required transition happened in the key schedule (that is 0x3 $\to_{S_9}$ 0x8 in round 7).

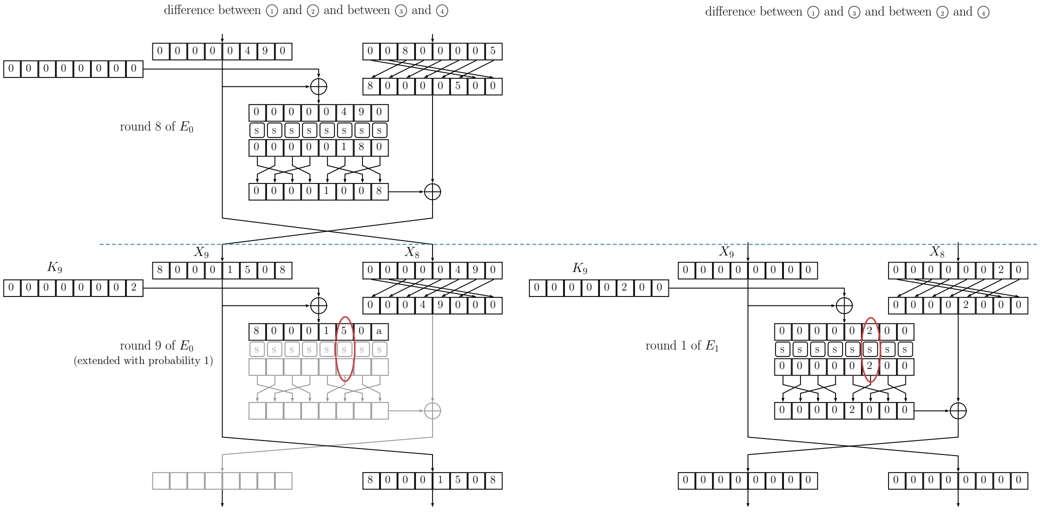

Figure 3: Middle rounds of the boomerang distinguisher proposed in [LGW12].

Suppose that the quartet (M^1, M^2, M^3, M^4) follows the characteristics defining the boomerang specified by Liu et al. When looking at the beginning of the characteristic over E_1 we see that we expect a transition through the second Sbox from a difference of 0x2 to 0x2, while by extending with probability 1 the differential characteristic over E_0 we see that the entering difference for this same Sbox is 0x5 (see Figure 3). If we denote by t^i the nibble that enters the Sbox number 2 of round 9 for M^i, this means that $t^1 \oplus t^3 = t^2 \oplus t^4$ =0x2 and that $S_2(t^1) \oplus S_2(t^3) = S_2(t^2) \oplus S_2(t^4)$ =0x2. Also, we have $t^1 \oplus t^2 = t^3 \oplus t^4$ =0x5.

By referring to S_2, we can list the possible input nibbles that make the transition from an input difference of 0x2 to an output difference of 0x2, and we obtain that $(t^1, t^3) \in$ {(0x1,0x3), (0x3,0x1), (0x8,0xa), (0xa,0x8)}. Since t^2 and t^4 are separated from t^1 and t^3 by a difference of 0x5 we can deduce that their values are in the following set: (t^2, t^4) $\in$ {(0x4,0x6), (0x6,0x4), (0xd,0xf), (0xf,0xd)}.

The contradiction comes from the fact that none of these pairs allows the required transition from 0x2 to 0x2, an observation that can be rewritten as: {(0x1, 0x3), (0x3, 0x1), (0x8, 0xa), (0xa, 0x8)} $\cap$ 0x5 $\oplus$ {(0x1, 0x3), (0x3, 0x1), (0x8, 0xa), (0xa, 0x8)} = $\varnothing$ since we want that the shifted values (t^1, t^3) also allows the desired Sbox transition.

This incompatibility implies that the boomerang over the middle round never returns,[1] and consequently the related-key distinguisher proposed by Liu et al. is invalid as no quartet can follow the required characteristic.

3 FBCT: the Feistel Counterpart of the BCT

The inconsistency found in the previous section (that is reminiscent of the examples given by Murphy in [Mur11]) calls for a tool to automatically study the behavior of the junction between E_0 and E_1.

In fact, this problem has recently been addressed in the case of Substitution-Permutation Networks with the introduction of the *Boomerang Connectivity Table (BCT)* by Cid et al [CHP+18]. However, no similar tool has been devised so far to deal with boomerang attacks on Feistel Networks. We address this shortfall in this section by introducing the[2] FBCT.

3.1 Definition of the FBCT

The (SPN) Boomerang Connectivity Table. The essence of the Boomerang Connectivity Table introduced by Cid et al. is similar to the one of the well-known Difference Distribution Table: instead of looking at the property of a round as a whole (thus at a function of usually 64 or 128 bits), the problem is reduced to one we can easily study given its small size: examining each Sbox of the S-layer independently. While the DDT describes the differential properties of each Sbox from which are deduced the ones of the round, the BCT gives the probability of a boomerang switch over each Sbox from which is deduced the one of the round.

The formal definition of the BCT is recalled below: it is a table that gives at line Δ_i, column ∇_o the number of values for which a boomerang of input Δ_i and output difference ∇_o comes back. It corresponds to the following formula, depicted in Figure 4:

Definition 1 (Boomerang Connectivity Table [CHP+18])**.** Let S be a permutation of $\mathbb{F}_2^n$, and $\Delta_i, \nabla_o \in \mathbb{F}_2^n$. The Boomerang Connectivity Table (BCT) of S is given by a $2^n \times 2^n$ table, in which the entry for the (Δ_i, ∇_o) position is given by:

$$BCT(\Delta_i, \nabla_o) = \#\{x \in \mathbb{F}_2^n | S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_o) = \Delta_i\}.$$

[1] Note that we confirmed this experimentally by verifying that for a sample of 2^{10} keys and 2^{10} messages the boomerang never comes back along the announced differences in one or even two middle rounds.

[2] To stress the similarity between the notions we introduce here and the ones that have been previously introduced in the case of boomerang switches on SPN, we basically use the same acronyms, simply adding the letter "F" in front of them to recall that we are looking at the Feistel case.

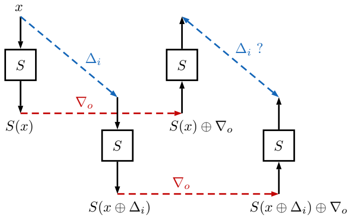

Figure 4: The value of $BCT(\Delta_i, \nabla_o)$ corresponds to the number of Sbox inputs x that make the boomerang over 1 round come back.

The Feistel Boomerang Connectivity Table. The previous definition is only valid for an Sbox that is part of an S-layer in an SPN cipher: the objective of this paper is to address the need of the counterpart for a Feistel cipher.

As a hint of what we introduce below, remember that Feistel ciphers have the practical advantage that decryption is performed by executing the same function as for encryption, simply changing the order of the round keys. This change is at the heart of the Feistel counterpart of the BCT that we introduce now: here, the inverse of the Sbox is never at play.

We start by illustrating our theory on the generic Feistel[3] cipher represented in Figure 5: it is a balanced Feistel with two branches, that we denote L and R. The output of one round is given by $F(L) \oplus R||L$, where the F function is defined by a round key addition, an S-layer and a linear layer L. Note that the details of the linear layers of F play no role in our discussion, and that the only important point is that F contains one S-layer made by the concatenation of t n-bit Sboxes.

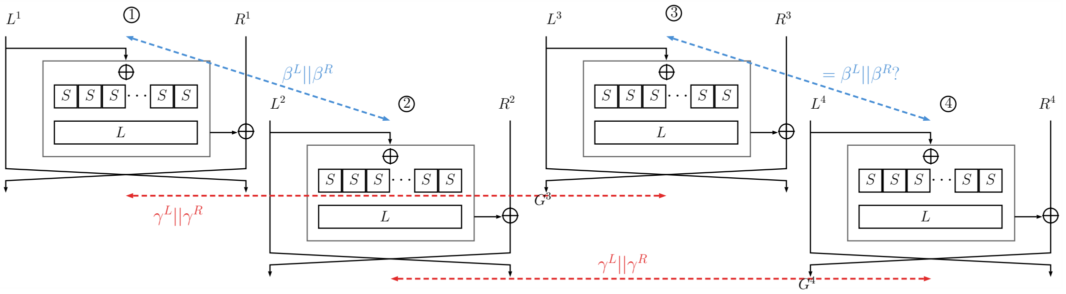

Figure 5: Boomerang switch over a generic Feistel round.

We are interested in the probability of the following 1-round boomerang switch: we have an input difference equal to $\beta^L||\beta^R$ between state ① and ②, an output difference equal to $\gamma^L||\gamma^R$ between state ① and ③, and ② and ④, and we want that the input difference between state ③ and ④ is equal to $\beta^L||\beta^R$.

Left part of the difference. We start by studying the cost of obtaining that the left difference between state ③ and ④ has the desired value of β^L.

Given the fact that the left branch is the one that is not modified through one round of Feistel we can easily conclude that the desired difference comes for free:

$$\begin{aligned} L^3 \oplus L^4 &= (L^3 \oplus L^1) \oplus (L^1 \oplus L^2) \oplus (L^2 \oplus L^4) \\ &= \gamma^R \oplus \beta^L \oplus \gamma^R = \beta^L. \end{aligned}$$

[3] As we are going to show in Appendix C, the same reasoning applies to variants of this construction.

Right part of the difference. We now focus on obtaining a difference of β^R between the right part of state number ③ and ④. By naming G^3 and G^4 the left output after one round in state ③ and ④ (see Figure 5), we obtain the following simplification:

$$\begin{aligned}
R^3 \oplus R^4 &= F(L^1 \oplus \gamma^R) \oplus G^3 \oplus F(L^1 \oplus \gamma^R \oplus \beta^L) \oplus G^4 \\
&= F(L^1 \oplus \gamma^R) \oplus F(L^1) \oplus R^1 \oplus \gamma^L \oplus F(L^1 \oplus \gamma^R \oplus \beta^L) \\
&\quad \oplus F(L^1 \oplus \beta^L) \oplus R^1 \oplus \beta^R \oplus \gamma^L \\
&= F(L^1 \oplus \gamma^R) \oplus F(L^1) \oplus F(L^1 \oplus \gamma^R \oplus \beta^L) \\
&\quad \oplus F(L^1 \oplus \beta^L) \oplus \beta^R.
\end{aligned}$$

For this difference to be equal to β^R we need that

$$F(L^1) \oplus F(L^1 \oplus \gamma^R) \oplus F(L^1 \oplus \beta^L) \oplus F(L^1 \oplus \gamma^R \oplus \beta^L) = 0.$$

We use the fact that the only non-linear function of F is an S-layer made by a concatenation of small Sboxes to rewrite this condition as a set of independent conditions on smaller parts of the states, and obtain t independent equations of the form:

$$S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0.$$

Where Δ_i is the difference at the input of the considered Sbox between state ① and ②, deduced from β^L, and ∇_o is the difference at the input of the considered Sbox between state ① and ③ and ② and ④, deduced from γ^R.

The resulting probability of the boomerang switch over one round is then the product of the probabilities for each Sbox, that are of the form

$$2^{-n} \times \#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0\}.$$

This discussion leads us to the introduction of the following definition:

Definition 2 (FBCT)**.** Let S be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, and $\Delta_i, \nabla_o \in \mathbb{F}_2^n$. The FBCT of S is given by a $2^n \times 2^n$ table T, in which the entry for the (Δ_i, ∇_o) position is given by:

$$\texttt{FBCT}_S(\Delta_i, \nabla_o) = \#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0\}.$$

Since we do not have to consider a bijective Sbox, we define $\texttt{FBCT}_S$ for any Sbox S from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with possibly $n \neq m$. In the following we leave out the S index and simply write FBCT when the Sbox we are referring to is clear from the context.

Once the table is built, the probability that a boomerang comes back over 1 round of a Feistel scheme is simply the product of the corresponding coefficients of the FBCT divided by 2^n. An example of FBCT is provided in Table 1 in the case of the Sbox[4] S_2 of LBlock.

It is easy to see that the formula of the FBCT corresponds to the number of times the order 2 derivative with respect to Δ_i and ∇_o of the vectorial Boolean function S cancels out. We formalize this and study its properties in Section 4.

3.2 Evaluation of the 1-round Boomerang Switch of Liu et al.'s Attack with the FBCT

We focus on the Sbox S_2 of round 9 of the cipher. From E_0, the input difference of Sbox 2 is 0x5, so following previous notation we have $\Delta_i =$ 0x5. When referring to E_1 and taking into account the difference coming from the round key we have $\nabla_o =$ 0x2. The

[4] Note that the FBCT of the 10 Sboxes of LBlock are the same. This is not a direct implication of the fact that the Sboxes are affine equivalent (counter-examples to this can easily be found).

Table 1: `FBCT` of the Sbox S_2 of `LBlock`.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	16	0	0	0	0	0	0	0	0	8	8	0	0	0	0
2	16	0	16	0	0	0	0	0	0	8	0	8	0	0	0	0
3	16	0	0	16	8	8	8	8	0	0	0	0	0	0	0	0
4	16	0	0	8	16	0	0	8	0	0	0	0	0	0	0	0
5	16	0	0	8	0	16	8	0	0	0	0	0	0	0	0	0
6	16	0	0	8	0	8	16	0	0	0	0	0	0	0	0	0
7	16	0	0	8	8	0	0	16	0	0	0	0	0	0	0	0
8	16	0	0	0	0	0	0	0	16	0	0	0	0	0	0	0
9	16	0	8	0	0	0	0	0	0	16	0	8	0	0	0	0
a	16	8	0	0	0	0	0	0	0	0	16	8	0	0	0	0
b	16	8	8	0	0	0	0	0	0	8	8	16	0	0	0	0
c	16	0	0	0	0	0	0	0	0	0	0	0	16	0	0	0
d	16	0	0	0	0	0	0	0	0	0	0	0	0	16	0	0
e	16	0	0	0	0	0	0	0	0	0	0	0	0	0	16	0
f	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16

`FBCT` coefficient we are interested in is then $\texttt{FBCT}_{S_2}(0\text{x}5, 0\text{x}2)$. Referring to Table 1, we see that the corresponding cell has a value equal to 0, meaning that the 1-round boomerang switch is impossible.

Note that this incompatibility is even more general than the one we discussed in Section 2.3, as in Section 2.3 we fixed an additional parameter namely one Sbox output. This vision corresponds to what we introduce in Section 5.1 under the name of Feistel Boomerang Difference Table (`FBDT`).

3.3 Relation Between the `FBCT` and the Feistel Switch

While the Feistel case is not covered by the Boomerang Connectivity Table, a first step in understanding the case of boomerang distinguishers for Feistel constructions has been made by Wagner himself while analyzing Khufu [Wag99]. His observation was later referred under the name of *Feistel Switch*, for instance in the related-key cryptanalysis of the AES-192 and AES-256 by Biryukov and Khovratovich [BK09], in which one can read:

> Surprisingly, a Feistel round with an arbitrary function (e.g., an S-box) can be passed for free in the boomerang attack (this was first observed in the attack on cipher Khufu in [Wag99]). Suppose the internal state (X, Y) is transformed to $(Z = X \oplus f(Y), Y)$ at the end of E_0. Suppose also that the E_0 difference before this transformation is $(\Delta X, \Delta Y)$, and that the E_1 difference after this transformation is $(\Delta Z, \Delta Y)$. [...] Therefore, the decryption phase of the boomerang creates the difference ΔX in X at the end of E_0 "for free".

By analyzing this setting in the way we did in Section 3.1 we can show that an internal state (X, Y) allows the boomerang to come back if Y verifies:

$$f(Y) \oplus f(Y \oplus \Delta Y) \oplus f(Y \oplus \Delta Y) \oplus f(Y \oplus \Delta Y \oplus \Delta Y) = 0,$$

(we have $\gamma^R = \beta^L = \Delta Y$ with our previous notation) which is always true. Moreover if the Feistel round function is made of some linear operations and an S-layer, the previous setting means that for every Sbox we are looking at coefficients that are on the diagonal of the `FBCT`.

4 Properties of the FBCT

This section gives a review of the most important properties of the Feistel boomerang connectivity table. We start by listing the constants of the table and then investigate the properties of the FBCT of two crucial classes of vectorial function, namely APN functions and functions based on the inverse mapping. We also study if the so-called Feistel boomerang uniformity is constant for Sboxes belonging to the same equivalence classes, for various definitions of equivalence. We conclude this section by giving a comparison of the BCT and FBCT properties.

4.1 Basics on vectorial Boolean Functions

Let $S : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ be a vectorial Boolean function. The set of all vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is denoted $\mathcal{B}(n,m)$. The derivative of $S \in \mathcal{B}(n,m)$ at $\Delta_i \in \mathbb{F}_2^n$ is defined as

$$D_{\Delta_i}S(x) = S(x) \oplus S(x \oplus \Delta_i)$$

for all $x \in \mathbb{F}_2^n$.

The first derivative is at the basis of the Difference Distribution Table (DDT) of a given vectorial function S, defined as:

$$\texttt{DDT}_S(\Delta_i, \delta) = \#\{x \in \mathbb{F}_2^n :\ S(x) \oplus S(x \oplus \Delta_i) = \delta\}.$$

The value of $\max_{\Delta_i \neq 0, \delta}\{\texttt{DDT}_S(\Delta_i, \delta)\}$ is called the (differential) uniformity of S.

This definition is extended to higher-order derivatives as follows: let $\Delta_i^1, \Delta_i^2, \dots, \Delta_i^k$ be a basis of a k-dimensional subspace V of $\mathbb{F}_2^n$. The k-th derivative of S with respect to V, denoted by $D_V S$, is defined as $D_V S(x) = D_{\Delta_i^1} D_{\Delta_i^2} \cdots D_{\Delta_i^k} S(x)$, for all $x \in \mathbb{F}_2^n$.

Given this definition, it is direct to see that for an $n \times m$ Sbox seen as an element of $\mathcal{B}(n,m)$, the value of $\texttt{FBCT}(\Delta_i, \nabla_o)$ corresponds to the number of zeroes of the function $D_{\Delta_i} D_{\nabla_o} S$ extended to the cases where Δ_i and ∇_o are not linearly independent.

4.2 Some Direct Properties of any FBCT

We start with a series of simple properties that are easily observable from the definition:

Property 1. The coefficients of the FBCT of $S \in \mathcal{B}(n,m)$ verify the following:

1. Symmetry: for all $0 \leq \Delta_i, \nabla_o \leq 2^n - 1$, $\texttt{FBCT}(\Delta_i, \nabla_o) = \texttt{FBCT}(\nabla_o, \Delta_i)$.
2. Fixed values:
   (a) First line: for all $0 \leq \nabla_o \leq 2^n - 1$, $\texttt{FBCT}(0, \nabla_o) = 2^n$ (ladder switch),
   (b) First column: for all $0 \leq \Delta_i \leq 2^n - 1$, $\texttt{FBCT}(\Delta_i, 0) = 2^n$ (ladder switch),
   (c) Diagonal: for all $0 \leq \Delta_i \leq 2^n - 1$, $\texttt{FBCT}(\Delta_i, \Delta_i) = 2^n$ (Feistel switch).
3. Multiplicity: for all $0 \leq \Delta_i, \nabla_o \leq 2^n - 1$, $\texttt{FBCT}(\Delta_i, \nabla_o) \equiv 0 \bmod 4$.
4. Equalities: for all $0 \leq \Delta_i, \nabla_o \leq 2^n - 1$, $\texttt{FBCT}(\Delta_i, \nabla_o) = \texttt{FBCT}(\Delta_i, \Delta_i \oplus \nabla_o)$.

Proof. All the properties are easily deduced from Definition 2:

(1) and (4) are proven by writing the expressions of the coefficients at play. Note that from symmetry we also have $\texttt{FBCT}(\Delta_i, \Delta_i \oplus \nabla_o) = \texttt{FBCT}(\nabla_o, \Delta_i \oplus \nabla_o)$.

(2)a. and (2)b. correspond to the ladder switch proposed in [BK09] that works the same way for Feistel and SPN ciphers: if either Δ_i or ∇_o is zero, it means that two pairs of messages inside the quartet share the same Sbox input, and the boomerang comes back with probability 1. This is formally shown as follows:

$$\begin{aligned}\texttt{FBCT}(0, \nabla_o) &= \#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \nabla_o) = 0\} \\ &= 2^n,\end{aligned}$$

and similarly $\texttt{FBCT}(\Delta_i, 0) = 2^n$. The Feistel switch recalled in Section 3.3 is also easily proven: if $\Delta_i = \nabla_o$ the FBCT coefficients correspond to the number of $x \in \mathbb{F}_2^n$ that are solutions to $S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \Delta_i) \oplus S(x) = 0$. Since every value of x fulfills this, $\texttt{FBCT}(\Delta_i, \Delta_i) = 2^n$.

(3) The property is verified for the case $\Delta_i = \nabla_o$ (since we can reasonably assume $n > 1$), so we focus on the case where $\Delta_i \neq \nabla_o$. If no x is solution the property is verified, while if there is at least one $x \in \mathbb{F}_2^n$ that is a solution then three more distinct values $x \oplus \Delta_i$, $x \oplus \nabla_o$ and $x \oplus \Delta_i \oplus \nabla_o$ also are, which proves the multiplicity. □

Given that the coefficients in the first line, first column and diagonal of the FBCT are always equal to the maximum that is 2^n, we define the *boomerang uniformity* a bit differently from what has been done for the BCT[5]:

Definition 3 (F-Boomerang Uniformity)**.** The F-Boomerang uniformity corresponds to the highest value in the FBCT without considering the first row, the first column and the diagonal:

$$\beta^F = \max_{\Delta_i \neq 0, \nabla_o \neq 0, \Delta_i \neq \nabla_o.} \texttt{FBCT}(\Delta_i, \nabla_o).$$

From the designer point of view, it is preferable to use an Sbox with a small F-boomerang uniformity. This goal can be reached by opting for an APN function, as we show below.

4.3 On the FBCT of APN Functions

A function $S \in \mathcal{B}(n, n)$ is called almost perfect nonlinear (APN) if for any $\Delta_i, \delta \in \mathbb{F}_2^n$ with $\Delta_i \neq 0$ the equation $S(x) \oplus S(x \oplus \Delta_i) = \delta$ has either 0 or 2 solutions. Alternatively, we know (refer for instance to [Car10], page 417) that S is APN if and only if for any non-zero $\Delta_i, \nabla_o \in \mathbb{F}_2^n$ with $\Delta_i \neq \nabla_o$, $D_{\Delta_i} D_{\nabla_o} S(x) \neq 0$ for all $x \in \mathbb{F}_2^n$. This directly implies the following theorem:

Theorem 1. *Let $S \in \mathcal{B}(n, n)$. S is an APN function if and only if its* FBCT *verifies* $\texttt{FBCT}(\Delta_i, \nabla_o) = 0$ *for all* $1 \leq \Delta_i \neq \nabla_o \leq 2^n - 1$.

A direct implication of this theorem is that any non-APN function has a non-zero coefficient at a position that is not in the first row, first column or diagonal of its FBCT, so in particular a Feistel boomerang uniformity higher or equal to 4.

4.4 On the FBCT of Sboxes based on the Inverse Mapping

Another important and widely used set of Sboxes are the ones based on the inverse mapping, which include (among others) the 8-bit Sboxes of CAMELLIA [AIK+01], Clefia [SSA+07] and SMS4 [Dt08] and the 4-bit Sbox of Twine [SMMK13].

We know that $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ are vector isomorphic over $\mathbb{F}_2$, i.e., with respect to a fixed basis α_i, $1 \leq i \leq n$, of $\mathbb{F}_{2^n}$, any element of $x \in \mathbb{F}_{2^n}$ can be uniquely written as $x = \oplus_{i=1}^n x_i \alpha_i$, where $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$. A mapping $S : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of the form $S(x) = x^{2^n - 2}$ is called an inverse mapping.

[5] Recall that for the BCT the boomerang uniformity of an Sbox is $\beta = \max_{\Delta_i \neq 0, \nabla_o \neq 0} BCT(\Delta_i, \nabla_o)$.

The importance of this family of functions comes from its very good cryptographic properties (that lead to it being selected to build the AES [AES01] Sbox for instance). Indeed, Nyberg [Nyb94] showed that if n is odd, then the inverse function over $\mathbb{F}_{2^n}$ is APN, and if n is even, then each row of its DDT has exactly one 4 and $(2^{n-1}-2)$ occurrences of the number 2 (and in particular that the Sbox is differentially 4-uniform). Given that we already discussed the case of APN functions in Section 4.3, we focus here on the case where n is even.

Property 2. In each row (except the first) of the FBCT of the inverse mapping over an even number of bits, the values 2^n, 4 and 0 occur 2, 2 and 2^n-4 times, respectively.

Proof. Using a *reductio ad absurdum* argument, we start by showing that the only possible values in the FBCT of the inverse mapping over an even number of bits are 0, 4 and 2^n. Since for every FBCT the coefficients in the first line, first column and diagonal are equal to 2^n, we focus on the other positions.

Suppose that for given non-zero Δ_i and ∇_o verifying $\Delta_i \neq \nabla_o$ we have $\texttt{FBCT}(\Delta_i, \nabla_o) > 4$. Given that the coefficients of the FBCT are multiple of 4 this implies that we have at least 8 distinct values $\mathbf{x}, \mathbf{x} \oplus \Delta_i, \mathbf{x} \oplus \nabla_o, \mathbf{x} \oplus \Delta_i \oplus \nabla_o, \mathbf{y}, \mathbf{y} \oplus \Delta_i, \mathbf{y} \oplus \nabla_o, \mathbf{y} \oplus \Delta_i \oplus \nabla_o$ that are solutions of:

$$S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0.$$

This can be rewritten as:

$$S(\mathbf{x}) \oplus S(\mathbf{x} \oplus \Delta_i) = S(\mathbf{x} \oplus \nabla_o) \oplus S(\mathbf{x} \oplus \Delta_i \oplus \nabla_o) = \delta_1, \tag{1}$$
$$S(\mathbf{y}) \oplus S(\mathbf{y} \oplus \Delta_i) = S(\mathbf{y} \oplus \nabla_o) \oplus S(\mathbf{y} \oplus \Delta_i \oplus \nabla_o) = \delta_2. \tag{2}$$

The first line indicates that the equation $S(x) \oplus S(x \oplus \Delta_i) = \delta_1$ has at least 4 distinct solutions, that is $\texttt{DDT}(\Delta_i, \delta_1) \geq 4$. Similarly, the second line shows that $\texttt{DDT}(\Delta_i, \delta_2) \geq 4$. There are two possibilities: if $\delta_1 = \delta_2$ we obtain that $\texttt{DDT}(\Delta_i, \delta_1) \geq 8$ which contradicts that the differential uniformity of the considered Sbox is 4, while if $\delta_1 \neq \delta_2$ we obtain that there are two coefficients in the same line of the DDT with a coefficient higher or equal to 4. In both cases we obtain a contradiction, so we conclude that the only possible values in the FBCT are 0, 4 and 2^n.

To conclude on the number of occurrences of each coefficient we need to prove that there are only 2 coefficients equal to 4 in each line. We consider $\Delta_i, \delta \in \mathbb{F}_2^n$ so that $\texttt{DDT}(\Delta_i, \delta) = 4$. There exist $\mathbf{x}$, $\mathbf{x} \oplus \Delta_i$, $\mathbf{y}$, $\mathbf{y} \oplus \Delta_i \in \mathbb{F}_2^n$ with $\mathbf{x} \neq \mathbf{y}$ and $\mathbf{x} \neq \mathbf{y} \oplus \Delta_i$ such that:

$$\begin{aligned} & S(\mathbf{x}) \oplus S(\mathbf{x} \oplus \Delta_i) = \delta = S(\mathbf{y}) \oplus S(\mathbf{y} \oplus \Delta_i) \\ \textit{i.e.} \quad & S(\mathbf{x}) \oplus S(\mathbf{x} \oplus \Delta_i) \oplus S(\mathbf{x} \oplus \nabla_o) \oplus S(\mathbf{x} \oplus \nabla_o \oplus \Delta_i) = 0, \text{ where } \nabla_o = \mathbf{x} \oplus \mathbf{y}. \end{aligned}$$

As a consequence, $\texttt{FBCT}(\Delta_i, \nabla_o) = \texttt{FBCT}(\Delta_i, \Delta_i \oplus \nabla_o) = 4$ so there are at least two '4' in each line of the FBCT. Suppose there is one more coefficient equal to 4 in this line, that is there exists $\mathbf{c} \in \mathbb{F}_2^n$ with $\mathbf{c} \neq \nabla_o$ and $\mathbf{c} \neq \Delta_i \oplus \nabla_o$ such that $\texttt{FBCT}(\Delta_i, \mathbf{c}) = 4$ and let $\mathbf{z} \in \{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus c) \oplus S(x \oplus \Delta_i \oplus c) = 0\}$. We have:

$$\begin{aligned} & S(\mathbf{z}) \oplus S(\mathbf{z} \oplus \Delta_i) \oplus S(\mathbf{z} \oplus \mathbf{c}) \oplus S(\mathbf{z} \oplus \Delta_i \oplus \mathbf{c}) = 0 \\ \textit{i.e.} \quad & S(\mathbf{z}) \oplus S(\mathbf{z} \oplus \Delta_i) = \delta' = S(\mathbf{w}) \oplus S(\mathbf{w} \oplus \Delta_i), \text{ where } \mathbf{w} = \mathbf{z} \oplus \mathbf{c}. \end{aligned}$$

$\texttt{FBCT}(\Delta_i, \mathbf{c}) = 4$ yields $\mathbf{c} \neq \Delta_i$ and $\mathbf{c} \neq 0$ and thus $\texttt{DDT}(\Delta_i, \delta') = 4 = \texttt{DDT}(\Delta_i, \delta)$. Since each row of the considered Sbox DDT has exactly one entry that equals 4, it follows that $\delta = \delta'$ and that $\mathbf{z}, \mathbf{w} \in \{\mathbf{x}, \mathbf{x} \oplus \Delta_i, \mathbf{y}, \mathbf{y} \oplus \Delta_i\}$, which leads to the contradiction that $\mathbf{c} \in \{\Delta_i, \nabla_o, \Delta_i \oplus \nabla_o\}$.

□

4.5 On the FBCT of Equivalent Sboxes

Various notions of equivalence are frequently used when studying Sboxes, among which linear, affine, extended-affine and CCZ equivalence [CCZ98]. These various concepts play an important role to categorize sets of Sboxes since central cryptographic properties (differential, linear and sometimes algebraic degree) are constant for equivalent Sboxes. In this section we investigate if the F-boomerang uniformity is preserved under these various notions of equivalence.

Linear, Affine and Extended-Affine Equivalence. As their names suggest, the three first flavors we start with are related as follows: linear equivalence is a sub-case of affine equivalence, and affine equivalence is a particular case of extended-affine equivalence.

Definition 4 (Linear, Affine and Extended-Affine Equivalence)**.** Two vectorial Boolean functions $F, G \in \mathcal{B}(n,m)$ are called extended-affine equivalent if there exist two nonsingular matrices $A \in GL(n, \mathbb{F}_2)$, $B \in GL(m, \mathbb{F}_2)$, $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ and an affine function $C : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that for all $x \in \mathbb{F}_2^n$

$$G(x) = B(F(A(x) \oplus a)) \oplus C(x) \oplus b,$$

where $GL(n, \mathbb{F}_2)$ is the set of all nonsingular binary matrices of order n. If $C = 0$, then F and G are affine equivalent, and if in addition a and b are equal to zero then they are linear equivalent.

Theorem 2. *The multi-set composed of all values in the* FBCT *is preserved under extended-affine nonsingular transformation. Namely, we have that* $\texttt{FBCT}_G(u,v) = \texttt{FBCT}_F(u',v')$ *where* $u' = A(u)$ *and* $v' = A(v)$.

Proof. Suppose that $G(x) = B(F(A(x) \oplus a)) \oplus C(x) \oplus b$ for all $x \in \mathbb{F}_2^n$, where $A \in GL(n, \mathbb{F}_2)$, $B \in GL(m, \mathbb{F}_2)$, $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ and $C \in \mathcal{B}(n,m)$ is an affine function. Using the fact that $C(x) \oplus C(x \oplus u) \oplus C(x \oplus v) \oplus C(x \oplus u \oplus v) = 0$, for all $x \in \mathbb{F}_2^n$ and $u, v \in \mathbb{F}_2^n$, we obtain the following relations:

$$\begin{aligned}
\texttt{FBCT}_G(u,v) &= \#\{x \in \mathbb{F}_2^n : \ G(x) \oplus G(x \oplus u) \oplus G(x \oplus v) \oplus G(x \oplus u \oplus v) = 0\} \\
&= \#\{x \in \mathbb{F}_2^n : \ B(F(A(x) \oplus a)) \oplus B(F(A(x \oplus u) \oplus a)) \oplus B(F(A(x \oplus v) \oplus a)) \\
&\qquad \oplus B(F(A(x \oplus u \oplus v) \oplus a)) = 0\} \\
&= \#\{x \in \mathbb{F}_2^n : \ B(F(A(x) \oplus a) \oplus F(A(x \oplus u) \oplus a) \oplus F(A(x \oplus v) \oplus a) \\
&\qquad \oplus F(A(x \oplus u \oplus v) \oplus a)) = 0\} \\
&= \#\{x \in \mathbb{F}_2^n : \ F(A(x) \oplus a) \oplus F(A(x) \oplus u' \oplus a) \oplus F(A(x) \oplus v' \oplus a) \\
&\qquad \oplus F(A(x) \oplus u' \oplus v' \oplus a) = 0\} \\
&= \#\{y \in \mathbb{F}_2^n : \ F(y) \oplus F(y \oplus u') \oplus F(y \oplus v') \oplus F(y \oplus u' \oplus v') = 0\} \\
&= \texttt{FBCT}_F(u',v'),
\end{aligned}$$

where $u' = A(u)$, $v' = A(v)$ and the new variable y corresponds to $A(x) \oplus a$. □

In particular, the F-boomerang uniformity is constant among Sboxes in the same linear, affine or extended-affine equivalence class.

CCZ Equivalence. The last equivalent relation we discuss here is the CCZ equivalence [CCZ98]. Concluding on this case is rather easy: it is known that every permutation is CCZ-equivalent to its inverse, and we show in next subsection that Feistel boomerang uniformity is not necessarily the same for an Sbox and its inverse. Consequently, Sboxes that are CCZ equivalent might not share the same boomerang uniformity.

4.6 FBCT and Inversion

In the case of the BCT, it has been shown that the boomerang uniformity of S and its inverse are the same [BC18]. Before studying the case of the FBCT, let us recall that since we are looking at Feistel constructions the Sboxes at play do not have to be invertible (the most famous example in this category being the DES [DES77]).

For an invertible Sbox, we can find some special cases for which the property is preserved, for instance for APN functions (since the inverse is also APN). Still, in the general case this property does not hold, and one example of this is for instance the 4-bit Sbox SS_0 used in CLEFIA [SSA+07]:

$$\mathrm{SS}_0 = [\text{0xe, 0x6, 0xc, 0xa, 0x8, 0x7, 0x2, 0xf, 0xb, 0x1, 0x4, 0x0, 0x5, 0x9, 0xd, 0x3}].$$

The F-boomerang uniformity of SS_0 is equal to 8, while the one of its inverse is 4.

4.7 Set-based Formulation of the FBCT

In this section, we identify the set[6]

$$\chi_{\texttt{FBCT}}(\Delta_i, \nabla_o) = \{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0\}$$

with the union for all $\delta \in \mathbb{F}_2^n$ of the intersection of $\chi_{DDT}(\Delta_i, \delta)$ and its coset $\chi_{DDT}(\Delta_i, \delta) \oplus \nabla_o$.

First, we recall the definition of $\chi_{DDT}(\Delta_i, \delta)$, a notion that has been introduced in [CLN+17] and used in the context of boomerang attacks in [SQH19] and that corresponds to the set of all $x \in \mathbb{F}_2^n$ that make a given Sbox transition possible:

$$\chi_{DDT}(\Delta_i, \delta) = \{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta_i) = \delta\}.$$

The alternative formulation is given in the following theorem:

Theorem 3. *For any $\Delta_i, \nabla_o \in \mathbb{F}_2^n$ and $S \in \mathcal{B}(n, n)$,*

$$\chi_{\texttt{FBCT}}(\Delta_i, \nabla_o) = \bigcup_{\delta \in \mathbb{F}_2^n} (\chi_{DDT}(\Delta_i, \delta) \cap (\chi_{DDT}(\Delta_i, \delta) \oplus \nabla_o))$$

Proof. For any $\Delta_i, \nabla_o \in \mathbb{F}_2^n$,

$$\begin{aligned}
\chi_{\texttt{FBCT}}(\Delta_i, \nabla_o) &= \{x \in \mathbb{F}_2^n :\ S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0\} \\
&= \{x \in \mathbb{F}_2^n :\ S(x) \oplus S(x \oplus \Delta_i) = S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o)\} \\
&= \bigcup_{\delta \in \mathbb{F}_2^n} \{x \in \mathbb{F}_2^n :\ S(x) \oplus S(x \oplus \Delta_i) = S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = \delta\} \\
&= \bigcup_{\delta \in \mathbb{F}_2^n} \{x \in \mathbb{F}_2^n :\ S(x) \oplus S(x \oplus \Delta_i) = \delta\} \cap \{x \in \mathbb{F}_2^n :\ S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = \delta\} \\
&= \bigcup_{\delta \in \mathbb{F}_2^n} \chi_{DDT}(\Delta_i, \delta) \cap \{\nabla_o \oplus x \in \mathbb{F}_2^n :\ S(x) \oplus S(x \oplus \Delta_i) = \delta\} \\
&= \bigcup_{\delta \in \mathbb{F}_2^n} \chi_{DDT}(\Delta_i, \delta) \cap (\chi_{DDT}(\Delta_i, \delta) \oplus \nabla_o).
\end{aligned}$$

□

Note here that for any fixed Δ_i the equality $\{x, x \oplus \Delta_i\} = \nabla_o \oplus \{x, x \oplus \Delta_i\}$ is satisfied for any x if and only if $\nabla_o = 0$ or $\Delta_i = \nabla_o$.

This reformulation leads to the following rewriting of the FBCT coefficient:

[6] We have $\#\chi_{\texttt{FBCT}}(\Delta_i, \nabla_o) = \texttt{FBCT}(\Delta_i, \nabla_o)$.

Corollary 1.

$$\texttt{FBCT}(\Delta_i, \nabla_o) = \sum_{\delta \in \mathbb{F}_2^n} \#(\chi_{DDT}(\Delta_i, \delta)) \cap (\chi_{DDT}(\Delta_i, \delta) \oplus \nabla_o)$$

Proof. This comes directly from the previous theorem by remarking that once Δ_i is fixed we have $\chi_{DDT}(\Delta_i, \delta) \cap \chi_{DDT}(\Delta_i, \delta') = \varnothing$ for all $\delta \neq \delta'$, which justifies that the unions in Theorem 3 are disjoint and hence that we have a sum. □

Let us again stress the parallel with a similar reformulation of the BCT:

Corollary 2 ([BC18])**.** *Let $S \in \mathcal{B}(n, n)$. We define $\mathcal{Y}_{DDT}$ as the set of all Sbox outputs that make a given transition possible, that is: $\mathcal{Y}_{DDT}(\Delta_i, \delta) = \{S(x) \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta_i) = \delta\}$. The expression of the BCT coefficient becomes:*

$$BCT(\Delta_i, \nabla_o) = \sum_{\delta \in \mathbb{F}_2^n} \#(\mathcal{Y}_{DDT}(\Delta_i, \delta)) \cap (\mathcal{Y}_{DDT}(\Delta_i, \delta) \oplus \nabla_o)$$

4.8 Comparison of the properties of the BCT and of the FBCT

We conclude this section by comparing in Table 2 the main properties explored by Boura and Canteaut [BC18] regarding the BCT with what we proved in the case of the FBCT.

Table 2: Comparison of the properties of the BCT and of the FBCT of n-bit functions.

Property	BCT	FBCT
Boomerang uniformity preserved under affine equivalence	yes	yes
Boomerang uniformity preserved under extended-affine equivalence	no	yes
Boomerang uniformity preserved under CCZ equivalence	no	no
Boomerang uniformity preserved under inversion	yes	no
Value of the boomerang uniformity of an APN function	2	0
Value of the boomerang uniformity of the inverse mapping (n even)	4 or 6	4

Note that another family of Sboxes was studied by Boura and Canteaut, namely the set of quadratic permutations. In the case of the FBCT this instance is rather easy to solve: for any non-zero $\Delta_i, \nabla_o \in \mathbb{F}_2^n$ with $\Delta_i \neq \nabla_o$, $D_{\Delta_i} D_{\nabla_o} S$ is constant. If this constant is not equal to zero we have that $\texttt{FBCT}(\Delta_i, \nabla_o) = 0$, otherwise $\texttt{FBCT}(\Delta_i, \nabla_o) = 2^n$. We can conclude that either the quadratic permutation is APN and then its Feistel boomerang uniformity is equal to 0, or the quadratic permutation is not APN (this is the case of all the quadratic permutations on an even number of variables) and then its Feistel boomerang uniformity is equal to 2^n.

In Appendix D, we provide a (rather intricate) formula linking the FBCT and the recently introduced *Differential-Linear Connectivity Table (DLCT)* [BDKW19]. We expect that other relations can be obtained.

5 Extending our Analysis to Two Rounds

Similarly to what has been done in [WP19, SQH19] for SPN constructions, this section discusses the probability of a boomerang switch E_m that covers two rounds.

5.1 The Feistel counterpart of the BDT

When studying how to extend the BCT theory to boomerang switches on more rounds, Wang and Peyrin [WP19] introduced the BDT (standing for *Boomerang Difference Table*), a variant of the BCT with one supplementary variable fixed, namely the Sbox output difference:

Definition 5 (Boomerang Difference Table [WP19])**.** Let S be an invertible function in $\mathbb{F}_2^n$, and $(\Delta_i, \delta, \nabla_o)$ be elements of $(\mathbb{F}_2^n)^3$. The boomerang difference table (BDT) of S is a three-dimensional table, in which the entry for $(\Delta_i, \delta, \nabla_o)$ is computed by:

$$\begin{aligned} BDT(\Delta_i, \delta, \nabla_o) = \#\{x \in \mathbb{F}_2^n | S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_o) = \Delta_i, \\ S(x) \oplus S(x \oplus \Delta_i) = \delta\}. \end{aligned}$$

As we show next, the counterpart of this table for the Feistel case turns out to be useful to study a switch over two rounds. Following the idea of [WP19], we define it as follows (it can be visualized in Figure 6):

Definition 6 (`FBDT`)**.** Let S be a function from $\mathbb{F}_2^n$ to itself, and $(\Delta_i, \delta, \nabla_o)$ be elements of $(\mathbb{F}_2^n)^3$. The Feistel boomerang difference table (`FBDT`) of S is a three-dimensional table, in which the entry for $(\Delta_i, \delta, \nabla_o)$ is computed by:

$$\begin{aligned} \texttt{FBDT}(\Delta_i, \delta, \nabla_o) = \#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0, \\ S(x) \oplus S(x \oplus \Delta_i) = \delta\}. \end{aligned}$$

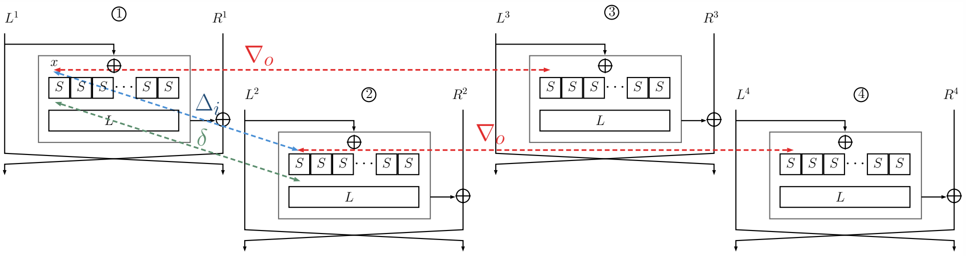

Figure 6: View of the parameters of the `FBDT`: Δ_i is the input difference and δ is the output difference of S when looking at the difference between state ① and ②. ∇_o is the input difference of the same Sbox S when looking at the difference between state ① and ③ (which is the same as the one between state ② and ④).

Given the discussion made in Section 4.7, we can rewrite the `FBDT` as:

$$\texttt{FBDT}(\Delta_i, \delta, \nabla_o) = \#\{(\chi_{DDT}(\Delta_i, \delta)) \cap (\chi_{DDT}(\Delta_i, \delta) \oplus \nabla_o)\}.$$

This is rather straightforward to see that the `FBDT` follows similar relations as the BDT does, namely:

Property 3 (Relations between the DDT, `FBCT` and `FBDT`)**.**

1. $DDT(\Delta_i, \delta) = \texttt{FBDT}(\Delta_i, \delta, 0) = \texttt{FBDT}(\Delta_i, \delta, \Delta_i)$ and in the general case $DDT(\Delta_i, \delta) \geq \texttt{FBDT}(\Delta_i, \delta, \nabla_o)$.
2. $\texttt{FBCT}(\Delta_i, \nabla_o) = \sum_{\delta=0}^{2^n-1} \texttt{FBDT}(\Delta_i, \delta, \nabla_o)$.
3. $\texttt{FBDT}(0, 0, \nabla_o) = 2^n$.

5.2 Probability of a 2-round Boomerang Switch

The theorem we discuss next gives the probability that a boomerang comes back over 2 rounds of a classic Feistel cipher, that is a balanced one with 2 branches. We consider that the input difference between state ① and ② is (Δ_i^L, Δ_i^R), that the output difference between state ② and ④ and ① and ③ is equal to (∇_o^L, ∇_o^R), and we want that the input difference between state ③ and ④ is again (Δ_i^L, Δ_i^R).

Again, we consider a very generic case where the round function is composed of one Sbox layer made of t parallel n-bit Sboxes and of some linear or affine operations, which implies in particular that if the input difference of one round is known together with the output difference of the Sbox layer, then the difference at the input of the next round Sbox layer can be computed. To keep our explanation as generic as possible we introduce the following notations, that can be visualized in Figure 7:

- Δ_i represents the difference at the input of the first round Sbox layer, between state ① and ②. It is fixed to a certain value since it can be deduced from the first round input difference Δ_i^L.
- δ denotes the corresponding output difference of this Sbox layer, but is not specified.
- Δ_i' corresponds to the difference at the input of the second Sbox layer (again with respect to state ① and ②). Its value is deduced from δ and from Δ_i^R.
- In a similar way, the difference at the input of the second round Sbox layer, between state ② and ④ is set to a certain value denoted ∇_o, deduced from ∇_o^R.
- The corresponding output difference is denoted α, but again is not fixed.
- ∇_o' represents the input difference of the first round Sbox layer for these states, and is computed from ∇_o^L and α.

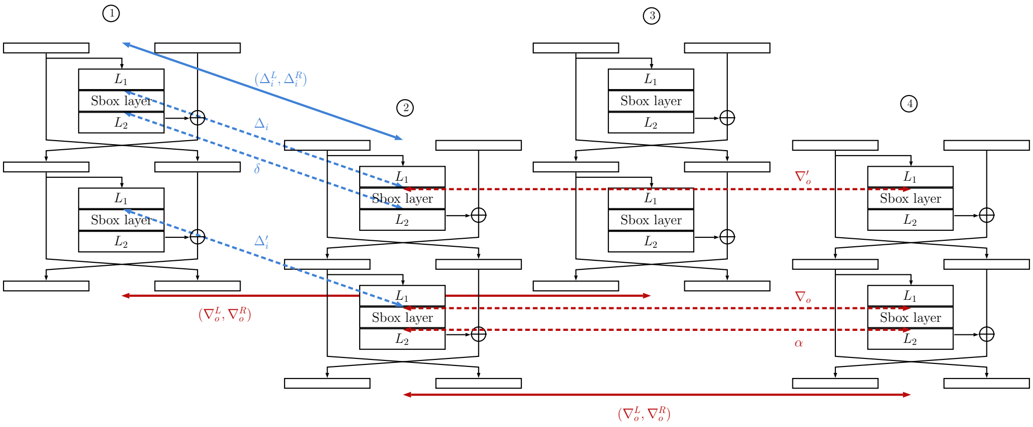

Figure 7: Boomerang Switch over two rounds of a balanced Feistel with two branches. The differences denoted with straight lines are imposed and fixed.

Given this notation we can find a formula for the probability of a 2-round boomerang switch over a Feistel, see Theorem 4. Note that to simplify its writing we extended the definition of the `FBDT` to the case of the Sbox layer (instead of one Sbox only). Naturally, this simply corresponds to the product of the `FBDT` of each Sbox that composes the Sbox layer.

Theorem 4 (Probability of a 2-round Switch)**.** *With the previous notation, the probability that a boomerang comes back over 2 rounds is equal to:*

$$2^{-2tn} \times \sum_{0 \leq \delta, \alpha < 2^n} \mathtt{FBDT}(\Delta_i, \delta, \nabla'_o) \times \mathtt{FBDT}(\nabla_o, \alpha, \Delta'_i). \tag{3}$$

Proof. In order to cover most constructions, in what follows we consider a Feistel cipher as depicted in Figure 7, that is with a round function made of one linear (or affine) layer L_1, followed by one Sbox layer of t n-bit Sboxes and again a linear (or affine) layer L_2.

We start by observing that if the second round Sbox layer output difference between state ② and ④ is equal to a given value α then the same difference is required between state ① and ③ for the boomerang to return.

Denote by α' the second Sbox layer output difference between state ① and ③. Given that the output difference between ① and ③ and ② and ④ is equal to (∇_o^L, ∇_o^R) we deduce that the input difference in the left branch between states ① and ③ and ② and ④ are respectively equal to $\nabla_o^L \oplus L_2(\alpha')$ and $\nabla_o^L \oplus L_2(\alpha)$. The input difference between the left branches of state ① and ② is equal to Δ_i^L so we deduce that the left branch difference between state ③ and ④ is equal to: $\Delta_i^L \oplus \nabla_o^L \oplus L_2(\alpha') \oplus \nabla_o^L \oplus L_2(\alpha) = \Delta_i^L \oplus L_2(\alpha') \oplus L_2(\alpha)$. For the boomerang to return this has to be equal to Δ_i^L, which proves that we must have $\alpha' = \alpha$.

We now demonstrate the formula by first looking at the case where the values of α and δ are fixed. The theorem is deduced by summing over all their possible values.

We focus on the second round of the switch, and more precisely on the difference between state ② and ④. To obtain the required output difference, the Sbox layer must transition from $\nabla_o = L_1(\nabla_o^R)$ to α, an event that is of probability[7]:

$$2^{-nt} \times \mathtt{DDT}(\nabla_o, \alpha).$$

If we denote by X the input value of the second round Sbox layer of state ②, We know that the corresponding value of state ① has to be equal to $X \oplus \Delta'_i$, value that should also allow the transition from ∇_o to α according to the previous discussion. The probability that it is the case is:

$$\frac{\#\chi_{DDT}(\nabla_o, \alpha) \cap (\chi_{DDT}(\nabla_o, \alpha) \oplus \Delta'_i)}{\#\chi_{DDT}(\nabla_o, \alpha)}.$$

Assuming that the previous conditions are fulfilled, the boomerang returns in the first round if the Sbox layer transitions from Δ_i to δ given that the input difference of this Sbox layer between state ② and ④ and ① and ③ is equal to ∇'_o. The probability of this event is $\mathtt{FBDT}(\Delta_i, \delta, \nabla'_o) \times 2^{-nt}$.

Putting things together, we obtain

$$2^{-2tn} \times \sum_{0 \leq \delta, \alpha < 2^n} \mathtt{FBDT}(\Delta_i, \delta, \nabla'_o) \times \mathtt{DDT}(\nabla_o, \alpha) \times \frac{\#\chi_{DDT}(\nabla_o, \alpha) \cap (\chi_{DDT}(\nabla_o, \alpha) \oplus \Delta'_i)}{\#\chi_{DDT}(\nabla_o, \alpha)}$$

Given that $\mathtt{DDT}(\nabla_o, \alpha) = \#\chi_{DDT}(\nabla_o, \alpha)$ and that $\#(\chi_{DDT}(\nabla_o, \alpha) \cap (\chi_{DDT}(\nabla_o, \alpha) \oplus \Delta'_i)) = \mathtt{FBDT}(\nabla_o, \alpha, \Delta'_i)$, we obtain the required expression.

□

Note that our formula is very reminiscent of what is used in the SPN case, as Wang and Peyrin [WP19] proposed to use the product of the BDT and BDT' coefficients to cover the case of a 2-round switch where the same Sbox is active with respect to E_0 and E_1. As a side note, we also remark here that the somewhat more intricate formulation

[7] We again make the shortcut of considering the Sbox layer instead of each individual Sbox.

proposed by Song et al. can be rewritten as the product of the BDT and BDT' in the case of 2 rounds, as in particular the $\mathcal{D}_{BCT}$ coefficient of [SQH19] is in fact equal to the BDT' coefficient.

We show a concrete example of application of this 2-round formula on LBlock in Appendix E.

6 Generic Formula for a Feistel Boomerang Switch over Multiple Rounds

To obtain an accurate estimation of the probability of a boomerang distinguisher, an attacker has to correctly evaluate the size of E_m, that is the number of middle rounds for which there exists a dependency between the characteristic on E_0 and the one on E_1. Once this is done, the formula introduced with the sandwich attack theory [DKS10] can be applied and the value of p^2q^2r (where r is the probability of E_m, p the one of E_0 and q the one of E_1) gives a good estimate (under the usual assumptions).

The problem of evaluating the size of E_m has already been discussed in two papers in the case of SPN ciphers: by Song et al. in [SQH19] and by Wang and Peyrin in [WP19]. The algorithm proposed in [SQH19] (that we recall in Appendix F) is rather natural: additional rounds are added to E_m as long as the probability of the newly added round is higher than the probability that would have been obtained if they were no dependencies. Since this technique directly applies to boomerang distinguishers on Feistel constructions we do not elaborate more on this.

The remaining problem in the case of Feistel ciphers is to compute the probability of a boomerang switch over more than 2 rounds. We address this now, with a setting and notation given in Figure 8 and that is a direct generalization of the one in Figure 7.

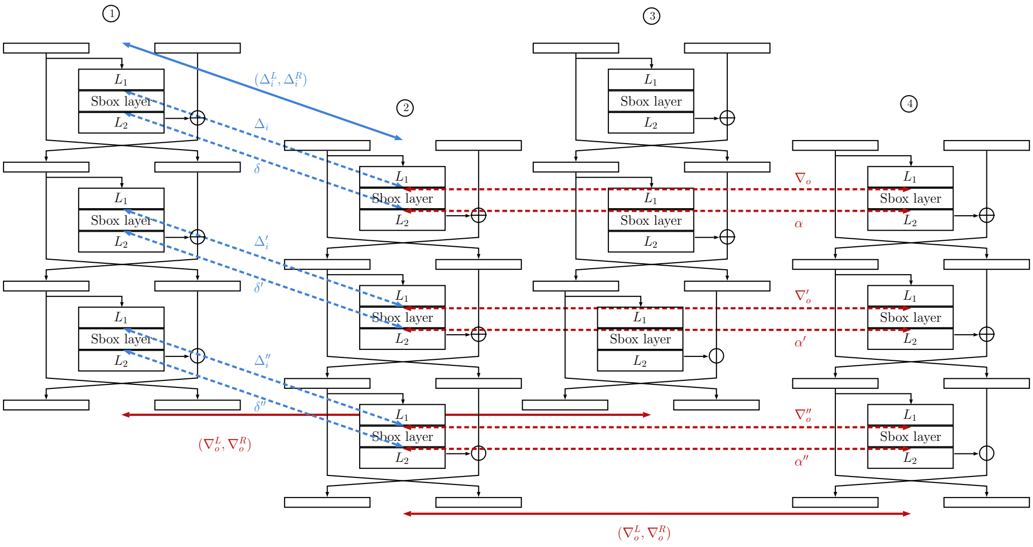

Figure 8: Setting for a boomerang Switch over more than two rounds of a balanced Feistel with two branches. The differences denoted with straight lines are imposed and fixed.

As depicted in the figure, we introduce new variables to represent all the intermediate differences. As we did when discussing the 2-round switch, the idea will be to iterate over all the possible values for these, to compute the probability of the obtained settings and finally to sum together the probabilities.

We introduce a coefficient that corresponds to the situation where an active Sbox in E_0 is in front of an active Sbox in E_1, and for which both Sbox outputs (when looking at state ① and ② and state ② and ④) are fixed. We obtain the following formula:

Definition 7 (FBET)**.** Let S be a function from $\mathbb{F}_2^n$, and $(\Delta_i, \delta, \nabla_o, \alpha)$ be elements of $(\mathbb{F}_2^n)^4$. The Feistel boomerang extended table (FBET) of S is a four-dimensional table, in which the entry for $(\Delta_i, \delta, \nabla_o, \alpha)$ is computed by:

$$\begin{aligned}\texttt{FBET}(\Delta_i, \delta, \nabla_o, \alpha) = \#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0,\\ S(x) \oplus S(x \oplus \Delta_i) = \delta,\\ S(x \oplus \Delta_i) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = \alpha\}.\end{aligned}$$

The probability of a switch is then estimated to be[8] the sum over all the possible intermediate differences of the product of the FBET coefficient (divided by 2^n) of each Sbox. For instance, the probability of the 3-round boomerang switch depicted in Figure 7 can be approximated by:

$$2^{-3tn} \sum_{0 \leq \delta, \alpha, \delta', \alpha', \delta'', \alpha'' < 2^n} \texttt{FBET}(\Delta_i, \delta, \nabla_o, \alpha) \times \texttt{FBET}(\Delta'_i, \delta', \nabla'_o, \alpha') \times \texttt{FBET}(\Delta''_i, \delta'', \nabla''_o, \alpha'')$$

where again by abuse of notation the FBET coefficient is the one of the full S-layer, but should be replaced by the ones of the individual Sboxes. Note that Δ_i and ∇''_o are determined by (Δ_i^L, Δ_i^R) and (∇_o^L, ∇_o^R), the input and output differences of the switch. Also, the values of Δ'_i, Δ''_i, ∇_o and ∇'_o are deduced from the other parameters on which we iterate (for instance $\Delta'_i = L_1(L_2(\delta) \oplus \Delta_i^R)$).

As we show in the following property, the obtained formula can be simplified when we sum coefficients over all the possible values of some variables. Further simplifications are obtained with Property 3.

Property 4 (Relations between the FBET and the previous tables)**.**

$$\sum_{0 \leq \delta < 2^n} \texttt{FBET}(\Delta_i, \delta, \nabla_o, \alpha) = \texttt{FBDT}(\nabla_o, \alpha, \Delta_i).$$

$$\sum_{0 \leq \alpha < 2^n} \texttt{FBET}(\Delta_i, \delta, \nabla_o, \alpha) = \texttt{FBDT}(\Delta_i, \delta, \nabla_o).$$

$$\texttt{FBET}(0, 0, \nabla_o, \alpha) = \texttt{FBET}(\nabla_o, \alpha, 0, 0) = \texttt{DDT}(\nabla_o, \alpha).$$

It is rather easy to show that the FBET view covers the previous formula for the 2-round switch (given in Theorem 4): we use the notation of Figure 7 and additionally denote by δ' the output difference between state ① and ② of the second-round S-layer, and by α' the output difference between state ② and ④ of the first-round S-layer. The sum we have to compute is:

$$2^{-2tn} \sum_{0 \leq \delta, \alpha', \delta', \alpha < 2^n} \texttt{FBET}(\Delta_i, \delta, \nabla'_o, \alpha') \times \texttt{FBET}(\Delta'_i, \delta', \nabla_o, \alpha).$$

[8] Note that this approximation considers that the same characteristic is followed between state ① and ② and between state ③ and ④. For 3 rounds and more it is not apparent that this is always the only possible case.

Since α' and δ' have no impact on the other values we can rewrite the previous sum as:

$$\begin{aligned}
& 2^{-2tn} \sum_{0\leq\delta,\alpha',\alpha<2^n} (\texttt{FBET}(\Delta_i,\delta,\nabla'_o,\alpha') \times \sum_{0\leq\delta'<2^n} \texttt{FBET}(\Delta'_i,\delta',\nabla_o,\alpha)) \\
= \; & 2^{-2tn} \sum_{0\leq\delta,\alpha',\alpha<2^n} (\texttt{FBET}(\Delta_i,\delta,\nabla'_o,\alpha') \times \texttt{FBDT}(\nabla_o,\alpha,\Delta'_i)) \\
= \; & 2^{-2tn} \sum_{0\leq\delta,\alpha<2^n} (\texttt{FBDT}(\nabla_o,\alpha,\Delta'_i) \times \sum_{0\leq\alpha'<2^n} \texttt{FBET}(\Delta_i,\delta,\nabla'_o,\alpha')) \\
= \; & 2^{-2tn} \sum_{0\leq\delta,\alpha<2^n} (\texttt{FBDT}(\nabla_o,\alpha,\Delta'_i) \times \texttt{FBDT}(\Delta_i,\delta,\nabla'_o)).
\end{aligned}$$

In a similar way, if we focus on one round only, we have to compute

$$2^{-tn} \sum_{0\leq\delta,\alpha<2^n} \texttt{FBET}(\Delta_i,\delta,\nabla_o,\alpha).$$

Since both δ and α have no impact on the other variables it can be rewritten as:

$$2^{-tn} \sum_{0\leq\delta<2^n} \texttt{FBDT}(\Delta_i,\delta,\nabla_o) = 2^{-tn}\texttt{FBCT}(\Delta_i,\nabla_o).$$

So the FBET coefficient allows to recover our previous formulas.

Note that when looking at a switch covering many rounds the application of this formula may require too much time if many Sboxes are involved, so it might be preferable to evaluate the probability of E_m experimentally.

Short Discussion on the SPN Case. While we focused on the Feistel case, it seems that a similar technique can be used to get the probability of a multiple-round boomerang switch on an SPN cipher. In particular, the counterpart of the FBET would be:

$$\begin{aligned}
BET(\Delta_i,\delta,\nabla_o,\alpha) = \#\{x\in\mathbb{F}_2^n | S^{-1}(S(x)\oplus\nabla_o)\oplus S^{-1}(S(x\oplus\Delta_i)\oplus\nabla_o) &= \Delta_i, \\
S(x)\oplus S(x\oplus\Delta_i) &= \delta, \\
x\oplus S^{-1}(S(x)\oplus\nabla_o) &= \alpha\}.
\end{aligned}$$

and we have the following direct properties:

Property 5 (Relation between the BET and the previous tables)**.**

$$\begin{aligned}
\sum_{0\leq\alpha<2^n} BET(\Delta_i,\delta,\nabla_o,\alpha) &= BDT(\Delta_i,\delta,\nabla_o), \\
\sum_{0\leq\delta<2^n} BET(\Delta_i,\delta,\nabla_o,\alpha) &= BDT'(\nabla_o,\alpha,\Delta_i) = \mathcal{D}_{BCT}(\Delta_i,\nabla_o,\alpha) \\
\sum_{0\leq\alpha,\delta<2^n} BET(\Delta_i,\delta,\nabla_o,\alpha) &= BCT(\Delta_i,\nabla_o)
\end{aligned}$$

Our bet is that it provides a generic formula covering the previous particular cases discussed in [SQH19] and [WP19].

7 Application to LBlock-s

We propose here to study the case of LBlock-s, the Feistel cipher used in LAC, in order to illustrate the way our formula can be used to estimate the probability of a boomerang distinguisher.

LAC was a first-round candidate to the CAESAR competition submitted by Lei Zhang et al. [ZWW+14]. It is a lightweight authenticated encryption scheme that relies on a modified version of LBlock called LBlock-s. In this version, the 10 different 4-bit Sboxes are replaced with one unique Sbox, which corresponds to the one called S_0 in LBlock. The block cipher also includes a modified key schedule algorithm that we do not detail here since it plays no role in the following discussion. The LAC algorithm uses both full 32-round LBlock-s as well as a round-reduced LBlock-s iterating 16 rounds.

In this section, we evaluate with the p^2q^2r formula the probability of a 16-round boomerang distinguisher on LBlock-s when the size of E_m varies from 2 to 8 rounds. We found out that when E_m covers 8 rounds the expected probability of the resulting distinguisher is $2^{-56.14}$.

This value is higher than the probability of the distinguisher that was proposed by Leurent in [Leu15]. In this paper, the author showed the existence of collections of differential characteristics with probability as high as $2^{-61.52}$. Still, our distinguisher cannot be used for forgery contrary to what is done in [Leu15].

7.1 Finding the Best 7-round Differential Characteristics for E_0 and E_1

As a starting point, we look at the setting where E_m covers 2 rounds and search the best characteristics over 7 rounds for E_0 and E_1. To find these, we use the two-step strategy described in [GLMS18]:

- In the first step, we abstract all the nibble differences by Boolean variables (if a nibble is active then its associated Boolean value is 1, else it is 0) and we look for the truncated differentials with the minimum number of active Sboxes. We implement this step using a high-level modeling language called MiniZinc [NSB+07]. MiniZinc models are translated into a simple subset of MiniZinc called FlatZinc, using a compiler provided by MiniZinc. Most existing constraint programming solvers (including SAT solvers and MILP solvers) have developed FlatZinc interfaces (there are currently fifteen solvers with FlatZinc interfaces). Using the PICAT SAT solver we found 8 possible optimal truncated differential characteristics that are valid for both E_0 and E_1.
- In the second step, we look for the best differential characteristics (in terms of probability) that follow the previous truncated differential paths. To do so, we use the constraint programming language Choco [PFL16]. For each possible truncated differential characteristics on 7 rounds we obtain 2766 solutions with an optimal probability equal to 2^{-16}. We tried several combinations and picked the one that gave the best probability for the 2-round E_m. We present it in Table 3.

7.2 Choosing a Switch E_m

To obtain an accurate evaluation of the boomerang distinguisher, we evaluate the size and probability of E_m with the algorithm recalled in Appendix F. When E_m covers few rounds we were able to apply our formulas to compute its probability but we then switched to experiments to avoid intricate expressions with many parameters. As detailed in Table 4, we were able to apply the algorithm for an E_m covering up to 8 rounds, thus obtaining an estimation of the probability of the distinguisher of $2^{-56.14}$. Our observation is that E_m

Table 3: The two differential characteristics on 7 rounds of E_0 and of E_1 in hexadecimal notations.

	Differential characteristic used in E_0		Differential characteristic used in E_1
Input	20400000 00001460	Output r9	00004020 41000006
Output r1	00006000 20400000	Output r10	00000600 00004020
Output r2	40000000 00006000	Output r11	00400000 00000600
Output r3	00000000 40000000	Output r12	00000000 00400000
Output r4	00000040 00000000	Output r13	40000000 00000000
Output r5	00000004 00000040	Output r14	00400000 40000000
Output r6	00004400 00000004	Output r15	00060040 00400000
Output r7	00004440 00004400	Output r16	42000004 00060040

covers more than 8 rounds, but we were limited by computational power to get its exact size.

Table 4: Theoretical and practical values of r for various sizes of E_m and corresponding probability of the 16-round distinguisher when applying the p^2q^2r formula. We detail the theoretical computation for 3 rounds in Appendix G.

E_m	α	δ	theoretical r	practical r	p^2q^2r
0 rounds	-	-	-	-	2^{-88}
2 rounds	$(0x00004440, 0x00004400)$	$(0x00004020, 0x41000006)$	$2^{-3.09}$	$2^{-3.09}$	$2^{-67.09}$
3 rounds	$(0x00004440, 0x00004400)$	$(0x00000600, 0x00004020)$	$2^{-6.80}$	$2^{-6.80}$	$2^{-62.8}$
4 rounds	$(0x00004400, 0x00000004)$	$(0x00000600, 0x00004020)$	n/a	$2^{-14.10}$	$2^{-62.1}$
6 rounds	$(0x00000004, 0x00000040)$	$(0x00400000, 0x00000600)$	n/a	$2^{-19.04}$	$2^{-59.04}$
8 rounds	$(0x00000040, 0x00000000)$	$(0x00000000, 0x00400000)$	n/a	$2^{-24.14}$	$2^{-56.14}$

7.3 Deriving a Boomerang Distinguisher

The previous discussion indicates that the 16-round boomerang distinguisher we are looking at has a probability higher than $2^{-56.14}$. It can be used as follows:

The attacker randomly chooses M_i^1 $(0 \leq i < m)$ and compute $M_i^2 = M_i^1 \oplus \alpha$ with $\alpha = (20400000, 00001460)$. She encrypts these plaintexts over 16 rounds of LBlock-s to obtain the ciphertexts C_i^1 and C_i^2 from which she deduces $C_i^3 = C_i^1 \oplus \delta$ and $C_i^4 = C_i^2 \oplus \delta$ with $\delta = (0x42000004, 0x00060040)$ and asks for their corresponding plaintexts M_i^3 and M_i^4. Finally she checks if the boomerang comes back by testing if $M_i^3 \oplus M_i^4 = \alpha$.

Given our estimate, $m = 2^{56.14}$ quartets are sufficient to expect one boomerang to return (using $2^{58.14}$ ciphering/deciphering operations).

8 Conclusion

Starting from an observation similar to the one made by Murphy in 2011, we develop a new theory that explains the behavior of boomerang switches for Feistel ciphers. We introduce the adequate notion of FBCT and give its main properties and relations with other well-known cryptographic tables. Taking things further, we provide a rather simple expression of the probability of a boomerang switch over two rounds, and a (more intricate) general expression of the one over multiple rounds.

Acknowledgments

This work has been partly funded by the French Direction Générale des Entreprises (DGE) under grant FUI 23 PACLIDO and by the ANR under grant Decrypt ANR-18-CE39-0007.

References

[AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology (NIST), FIPS PUB 197, U.S. Department of Commerce, November 2001.

[AIK$^+$01] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-bit block cipher suitable for multiple platforms - Design and analysis. In Douglas R. Stinson and Stafford E. Tavares, editors, *SAC 2000*, volume 2012 of *LNCS*, pages 39–56. Springer, Heidelberg, August 2001.

[BC18] Christina Boura and Anne Canteaut. On the boomerang uniformity of cryptographic sboxes. *IACR Trans. Symm. Cryptol.*, 2018(3):290–310, 2018.

[BDK01] Eli Biham, Orr Dunkelman, and Nathan Keller. The rectangle attack - rectangling the Serpent. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 340–357. Springer, Heidelberg, May 2001.

[BDK05] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 507–525. Springer, Heidelberg, May 2005.

[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, *EUROCRYPT 2019, Part I*, volume 11476 of *LNCS*, pages 313–342. Springer, Heidelberg, May 2019.

[BK09] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 1–18. Springer, Heidelberg, December 2009.

[BPT19] Christina Boura, Léo Perrin, and Shizhu Tian. Boomerang uniformity of popular s-box constructions. In *Proceedings of The Eleventh International Workshop on Coding and Cryptograph (WCC)*, 2019.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 2–21. Springer, Heidelberg, August 1991.

[Car10] Claude Carlet. Vectorial boolean functions for cryptography. *Boolean models and methods in mathematics, computer science, and engineering*, 134:398–469, 2010.

[CCZ98] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[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, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 683–714. Springer, Heidelberg, April / May 2018.

[CLN$^+$17] Anne Canteaut, Eran Lambooij, Samuel Neves, Shahram Rasoolzadeh, Yu Sasaki, and Marc Stevens. Refined probability of differential characteristics including dependency between multiple rounds. *IACR Trans. Symm. Cryptol.*, 2017(2):203–227, 2017.

[CM13] Jiageng Chen and Atsuko Miyaji. Differential Cryptanalysis and Boomerang Cryptanalysis of LBlock. In Alfredo Cuzzocrea, Christian Kittl, Dimitris E. Simos, Edgar R. Weippl, and Lida Xu, editors, *Security Engineering and Intelligence Informatics - CD-ARES 2013 Workshops: MoCrySEn and SeCIHD*, volume 8128 of *LNCS*, pages 1–15. Springer, 2013.

[CY09] Jiali Choy and Huihui Yap. Impossible boomerang attack for block cipher structures. In Tsuyoshi Takagi and Masahiro Mambo, editors, *IWSEC 09*, volume 5824 of *LNCS*, pages 22–37. Springer, Heidelberg, October 2009.

[DES77] Data encryption standard. National Bureau of Standards, NBS FIPS PUB 46, U.S. Department of Commerce, January 1977.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 393–410. Springer, Heidelberg, August 2010.

[Dt08] Whitfield Diffie and George Ledin (translators). SMS4 encryption algorithm for wireless networks. Cryptology ePrint Archive, Report 2008/329, 2008. http://eprint.iacr.org/2008/329.

[Fei74] Horst Feistel. Block cipher cryptographic system, March 19 1974. US Patent 3,798,359.

[GLMS18] David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon. Revisiting AES related-key differential attacks with constraint programming. *Inf. Process. Lett.*, 139:24–29, 2018.

[KKH$^+$04] Jongsung Kim, Guil Kim, Seokhie Hong, Sangjin Lee, and Dowon Hong. The related-key rectangle attack - application to SHACAL-1. In Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, editors, *ACISP 04*, volume 3108 of *LNCS*, pages 123–136. Springer, Heidelberg, July 2004.

[KKS01] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 75–93. Springer, Heidelberg, April 2001.

[Leu15] Gaëtan Leurent. Differential forgery attack against LAC. In *Selected Areas in Cryptography - SAC 2015*, volume 9566 of *Lecture Notes in Computer Science*, pages 217–224. Springer, 2015.

[LGW12] Shusheng Liu, Zheng Gong, and Libin Wang. Improved related-key differential attacks on reduced-round LBlock. In Tat Wing Chim and Tsz Hon Yuen, editors, *ICICS 12*, volume 7618 of *LNCS*, pages 58–69. Springer, Heidelberg, October 2012.

[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.

[Mur11] Sean Murphy. The return of the cryptographic boomerang. *IEEE Trans. Information Theory*, 57(4):2517–2521, 2011.

[NSB$^+$07] Nicholas Nethercote, Peter J. Stuckey, Ralph Becket, Sebastian Brand, Gregory J. Duck, and Guido Tack. Minizinc: Towards a standard CP modelling language. In *Principles and Practice of Constraint Programming - CP 2007*, volume 4741 of *LNCS*, pages 529–543. Springer, 2007.

[Nyb94] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 55–64. Springer, Heidelberg, May 1994.

[PFL16] Charles Prud'homme, Jean-Guillaume Fages, and Xavier Lorca. *Choco Documentation.* TASC, INRIA Rennes, LINA CNRS UMR 6241, COSLING S.A.S., 2016.

[SMMK13] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE : A lightweight block cipher for multiple platforms. In Lars R. Knudsen and Huapeng Wu, editors, *SAC 2012*, volume 7707 of *LNCS*, pages 339–354. Springer, Heidelberg, August 2013.

[SQH19] Ling Song, Xianrui Qin, and Lei Hu. Boomerang connectivity table revisited. *IACR Trans. Symm. Cryptol.*, 2019(1):118–141, 2019.

[SSA$^+$07] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher CLEFIA (extended abstract). In Alex Biryukov, editor, *FSE 2007*, volume 4593 of *LNCS*, pages 181–195. Springer, Heidelberg, March 2007.

[Wag99] David Wagner. The boomerang attack. In Lars R. Knudsen, editor, *FSE'99*, volume 1636 of *LNCS*, pages 156–170. Springer, Heidelberg, March 1999.

[WP19] Haoyang Wang and Thomas Peyrin. Boomerang switch in multiple rounds. *IACR Trans. Symm. Cryptol.*, 2019(1):142–169, 2019.

[WZ11] Wenling Wu and Lei Zhang. LBlock: A lightweight block cipher. In Javier Lopez and Gene Tsudik, editors, *ACNS 11*, volume 6715 of *LNCS*, pages 327–344. Springer, Heidelberg, June 2011.

[ZMI90] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 461–480. Springer, Heidelberg, August 1990.

[ZWW$^+$14] Lei Zhang, Wenling Wu, Yanfeng Wang, Shengbao Wu, and Jian Zhang. LAC: a lightweight authenticated encryption cipher, March 2014. Submission to CAESAR. Available from http://competitions.cr.yp.to/round1/lacv1.pdf.

A Specification of the Sboxes of LBlock

Table 5: The 10 Sboxes used in LBlock.

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
S_0	0xe	0x9	0xf	0x0	0xd	0x4	0xa	0xb	0x1	0x2	0x8	0x3	0x7	0x6	0xc	0x5
S_1	0x4	0xb	0xe	0x9	0xf	0xd	0x0	0xa	0x7	0xc	0x5	0x6	0x2	0x8	0x1	0x3
S_2	0x1	0xe	0x7	0xc	0xf	0xd	0x0	0x6	0xb	0x5	0x9	0x3	0x2	0x4	0x8	0xa
S_3	0x7	0x6	0x8	0xb	0x0	0xf	0x3	0xe	0x9	0xa	0xc	0xd	0x5	0x2	0x4	0x1
S_4	0xe	0x5	0xf	0x0	0x7	0x2	0xc	0xd	0x1	0x8	0x4	0x9	0xb	0xa	0x6	0x3
S_5	0x2	0xd	0xb	0xc	0xf	0xe	0x0	0x9	0x7	0xa	0x6	0x3	0x1	0x8	0x4	0x5
S_6	0xb	0x9	0x4	0xe	0x0	0xf	0xa	0xd	0x6	0xc	0x5	0x7	0x3	0x8	0x1	0x2
S_7	0xd	0xa	0xf	0x0	0xe	0x4	0x9	0xb	0x2	0x1	0x8	0x3	0x7	0x5	0xc	0x6
S_8	0x8	0x7	0xe	0x5	0xf	0xd	0x0	0x6	0xb	0xc	0x9	0xa	0x2	0x4	0x1	0x3
S_9	0xb	0x5	0xf	0x0	0x7	0x2	0x9	0xd	0x4	0x8	0x1	0xc	0xe	0xa	0x3	0x6

B Parameters of Liu et al.'s Related-Key Boomerang Distinguisher on LBlock

For E_0, there are seven active Sbox transitions all of probability 2^{-2}, and no active Sboxes in the key schedule, resulting in $p = 2^{-14}$. E_1 is defined by the same 8-round characteristic positioned from round 9 to 16 with the change that for the master key difference to reach the required difference at the output of E_1 (in round 9), one Sbox is activated in the key schedule (transition probability of 2^{-2}), meaning that $q = 2^{-16}$.

More into details and as depicted in Figure 9, the parameters of E_0 and E_1 are:

$$\Delta_i^L = 0x00000000,\ \Delta_i^R = 0x00000020,\ \Delta_o^L = 0x80001508,\ \Delta_o^R = 0x00000490.$$

Regarding the differences in the keys, we have:

$$\Delta_K^0 = 0x00000200000000000000,\ \Delta_K^1 = 0x0000c000000000000000.$$

The key derivation gives the following subkeys from $\Delta_K^0 = 0x00000200000000000000$:

$$\begin{array}{ll}
\Delta K_1 = 00000200 & \Delta K_5 = 00000000 \\
\Delta K_2 = 00000000 & \Delta K_6 = 00000000 \\
\Delta K_3 = 00000000 & \Delta K_7 = 00800000 \\
\Delta K_4 = 00010000 & \Delta K_8 = 00000000
\end{array}$$

While from $\Delta_K^1 = 0x0000c000000000000000$ we get:

$$\begin{array}{llll}
\Delta K_1 : 0000c000 & \Delta K_5 : 00000000 & \Delta K_9 : 00000200 & \Delta K_{13} : 00000000 \\
\Delta K_2 : 00000000 & \Delta K_6 : 00000001 & \Delta K_{10} : 00000000 & \Delta K_{14} : 00000000 \\
\Delta K_3 : 00000000 & \Delta K_7 : 80000000 & \Delta K_{11} : 00000000 & \Delta K_{15} : 00800000 \\
\Delta K_4 : 00600000 & \Delta K_8 : 00000000 & \Delta K_{12} : 00010000 & \Delta K_{16} : 00000000
\end{array}$$

The active Sbox in the key schedule of E_1 appears in the round key 7 and uses the transition $S_9(0x3) = 0x8$ with probability 2^{-2}.

C Some Variants of Feistel Constructions for which the FBCT Apply

We show here that the FBCT tool covers more constructions than the classical Feistel cipher, by providing three examples: the type I and II variants introduced by Zheng,

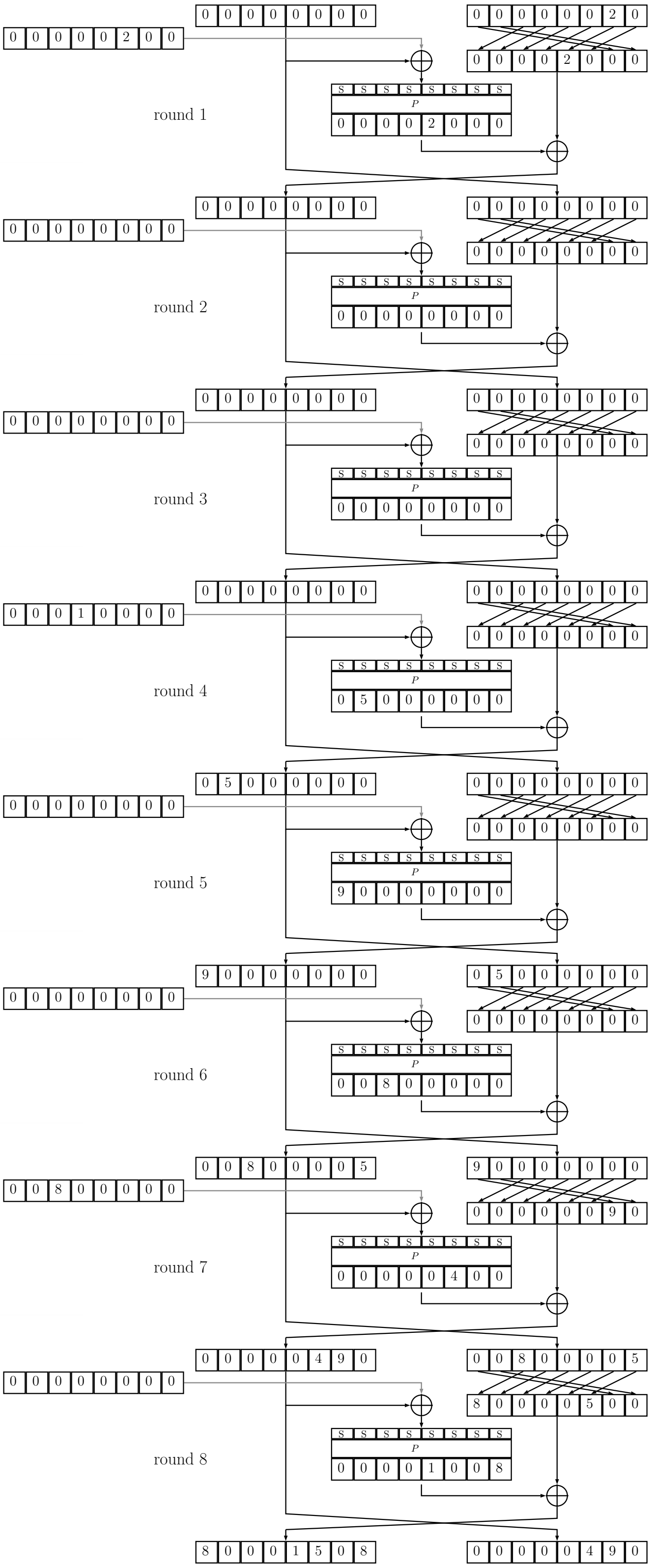

Figure 9: The 8-round related key characteristic used in Liu et al.'s attack, used for both E_0 and E_1 with $\Delta K_1 = \Delta K_9, \Delta K_2 = \Delta K_{10}, \cdots, \Delta K_8 = \Delta K_{16}$.

Matsumoto and Imai in [ZMI90] and the source-heavy (also called contracting) construction as implemented in SMS4 [Dt08]. A representation of the round structure of these types is given in Figure 10 in the case of 4-branch networks.

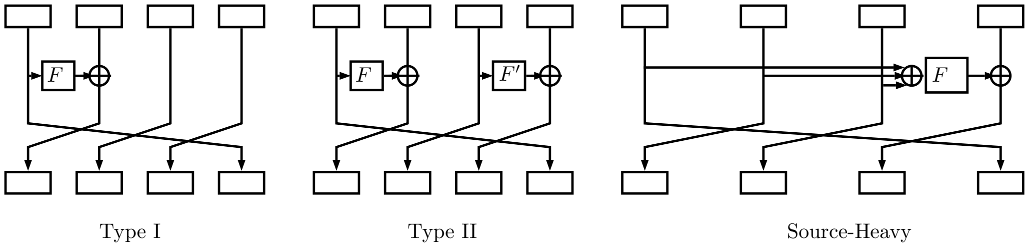

Figure 10: One round of the Feistel construction of type I, type II and source-heavy for variants with 4 branches.

The only assumption we make is that the F and F' functions used in theses constructions are composed of some linear or affine operations (like for instance matrix multiplication, permutations, Xor of constants or of round keys) and of one S-layer. We show below that the relations that need to be fulfilled in these cases can also be expressed as a product of `FBCT` coefficients.

Type I: Referring to Figure 10, one round of type I can be seen as one round of classic Feistel with some (2 in the picture) additional branches that are independent and not affected by a F function. Thus, the reasoning made in Section 3.1 can be extended to the case of type I construction and the probability that the boomerang switch over one round happens as required is the product of the `FBCT` coefficients corresponding to the Sboxes contained in F.

Type II: In a similar way, one round of type II can be seen as the concatenation of several (2 in the picture) classical Feistels that are independent one from the others. The reasoning made in Section 3.1 applies to this case and the probability of the boomerang switch is made by the product of the `FBCT` coefficients of the Sboxes of the F functions at play.

Source-Heavy: This case can also easily be treated with the `FBCT`. It can be shown that the one-round boomerang switch represented in Figure 11 comes back if the following condition is fulfilled:

$$F(x_1^1 \oplus x_2^1 \oplus x_3^1) \oplus F(x_1^1 \oplus x_2^1 \oplus x_3^1 \oplus (A \oplus B \oplus C)) \oplus$$
$$F(x_1^1 \oplus x_2^1 \oplus x_3^1 \oplus (a \oplus b \oplus d)) \oplus F(x_1^1 \oplus x_2^1 \oplus x_3^1 \oplus (A \oplus B \oplus C) \oplus (a \oplus b \oplus d)) = 0$$

Which can be rewritten as a product of the `FBCT` coefficients of the Sbox of F, with the two parameters depending on A, B, and C for one, and a, b and d for the other.

Note that the discussion above has to be nuanced as the application of the `FBCT` to other cases (as for instance type III construction) might not be straightforward.

D A Relation Between the DLCT and the `FBCT`

As before, we consider n, m two positive integers and $S \in \mathcal{B}(n,m)$. The set of all non-zero elements of $\mathbb{F}_2^n$ is denoted by $\mathbb{F}_2^{n*}$. For x and $\lambda \in \mathbb{F}_2^n$ we denote by $\lambda \cdot x$ the canonical inner product.

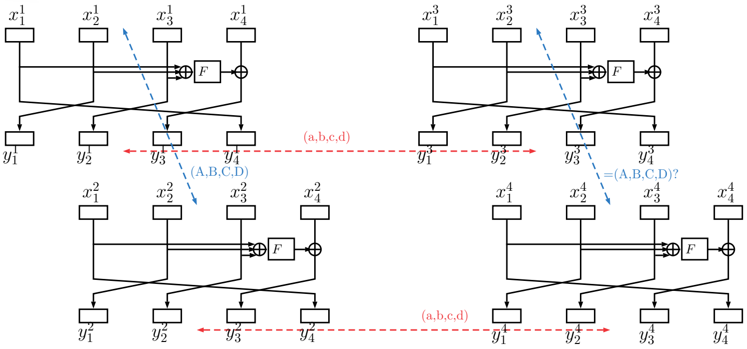
x_1^1 x_2^1 x_3^1 x_4^1
F
y_1^1 y_2^1 y_3^1 y_4^1
(a,b,c,d)
(A,B,C,D)
x_1^3 x_2^3 x_3^3 x_4^3
F
y_1^3 y_2^3 y_3^3 y_4^3
=(A,B,C,D)?
x_1^2 x_2^2 x_3^2 x_4^2
F
y_1^2 y_2^2 y_3^2 y_4^2
(a,b,c,d)
x_1^4 x_2^4 x_3^4 x_4^4
F
y_1^4 y_2^4 y_3^4 y_4^4

Figure 11: Boomerang switch over one round of the source-heavy construction.

The Differential-Linear Connectivity Table (DLCT) was introduced by Achiya Bar-On et al. in [BDKW19] and is defined as follows:

Definition 8 ([BDKW19])**.** For a vectorial Boolean function $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the differential-linear connectivity table (DLCT) of S is an $2^n \times 2^m$ table whose rows correspond to input differences to S and whose columns correspond to bit masks of outputs of S. The DLCT entry (Δ, λ), where $\Delta \in \mathbb{F}_2^n$ is a difference and $\lambda \in \mathbb{F}_2^m$ is a mask, is

$$DLCT_S(\Delta, \lambda) = \#\{x \in \mathbb{F}_2^n : \ \lambda \cdot S(x) = \lambda \cdot S(x \oplus \Delta)\} - 2^{n-1}.$$

Recall that the autocorrelation of an n-variable Boolean function f at point $\Delta \in \mathbb{F}_2^n$, denoted $C_f(\Delta)$, is defined as:

$$C_f(\Delta) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus \Delta)}.$$

It can be easily proven that $DLCT_S(\Delta, \lambda) = \frac{1}{2} \mathrm{C}_{\lambda \cdot S}(\Delta)$.

In the following, we consider a vectorial Boolean function S and derive a relation between its FBCT and the autocorrelation of its component functions. Using this relation, we provide a relation between the FBCT and the DLCT of S.

Theorem 5. *Let $S \in \mathcal{B}(n, m)$. Then for any non-zero $\Delta \in \mathbb{F}_2^{n*}$*

$$\sum_{\lambda \in \mathbb{F}_2^{m*}} C_{\lambda \cdot S}^2(\Delta) = 2^m \sum_{\nabla \in \mathbb{F}_2^{n*}:\ \nabla \neq \Delta} \mathtt{FBCT}_S(\Delta, \nabla) + 2^n(2^{m+1} - 2^n).$$

Proof. For any non-zero $\Delta \in \mathbb{F}_2^{n*}$, we have

$$\begin{aligned}
\sum_{\lambda \in \mathbb{F}_2^{m*}} C_{\lambda \cdot S}^2(\Delta) &= \sum_{\lambda \in \mathbb{F}_2^{m*}} \Big(\sum_{x \in \mathbb{F}_2^n} (-1)^{\lambda \cdot S(x) \oplus \lambda \cdot S(x \oplus \Delta)}\Big)\Big(\sum_{y \in \mathbb{F}_2^n} (-1)^{\lambda \cdot S(y) \oplus \lambda \cdot S(y \oplus \Delta)}\Big) \\
&= \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^n} \sum_{\lambda \in \mathbb{F}_2^{m*}} (-1)^{\lambda \cdot (S(x) \oplus S(x \oplus \Delta) \oplus S(y) \oplus S(y \oplus \Delta))} \\
&= \sum_{x \in \mathbb{F}_2^n} \sum_{\nabla \in \mathbb{F}_2^n} \Big(\sum_{\lambda \in \mathbb{F}_2^m} (-1)^{\lambda \cdot (S(x) \oplus S(x \oplus \Delta) \oplus S(x \oplus \nabla) \oplus S(x \oplus \Delta \oplus \nabla))} - 1\Big) \\
&= 2^m \sum_{\nabla \in \mathbb{F}_2^n} \#\{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus \Delta) \oplus S(x \oplus \nabla) \oplus S(x \oplus \Delta \oplus \nabla) = 0\} - 2^{2n} \\
&= 2^m \sum_{\nabla \in \mathbb{F}_2^{n*}:\ \nabla \neq \Delta} \mathtt{FBCT}_S(\Delta, \nabla) + 2^n(2^{m+1} - 2^n).
\end{aligned}$$

□

From this theorem and the relation between the DLCT and the autocorrelation of the component functions of S, we directly deduce the following corollary:

Corollary 3. *Let $S \in \mathcal{B}(n,m)$. Then for any non-zero $\Delta \in \mathbb{F}_2^{n*}$*

$$\sum_{\lambda \in \mathbb{F}_2^{m*}} DLCT_S^2(\Delta,\lambda) = 2^{m-2} \sum_{\nabla \in \mathbb{F}_2^{n*}:\ \nabla \neq \Delta} \texttt{FBCT}_S(\Delta,\nabla) + 2^n(2^{m-1} - 2^{n-2}).$$

E Example of a 2-round Switch on LBlock

This section shows how to apply Equation (3) to a concrete cipher, namely LBlock. We consider a 2-round boomerang switch that is deduced from the proposed boomerang distinguisher of the paper by Chen and Miyaji [CM13].

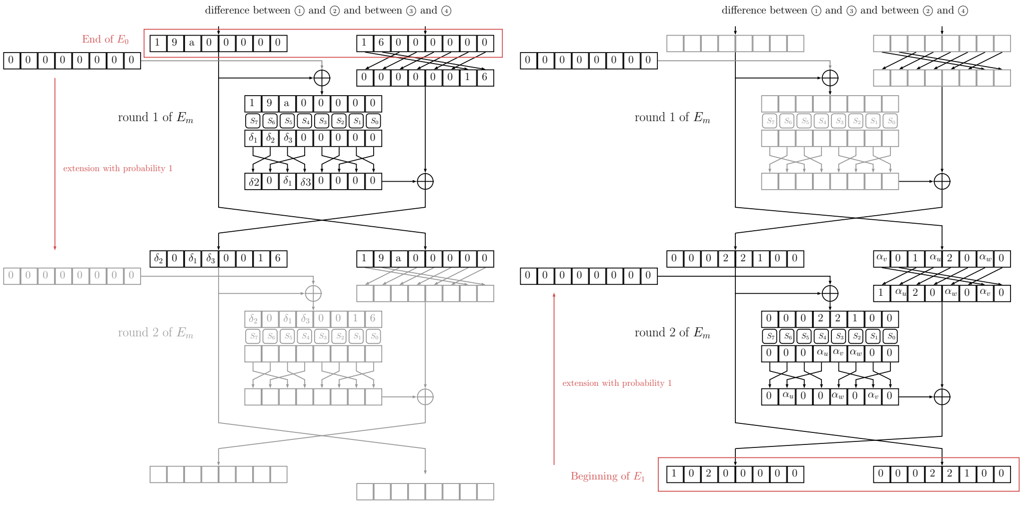
difference between ① and ② and between ③ and ④
End of E_0
round 1 of E_m
extension with probability 1
round 2 of E_m
difference between ① and ③ and between ② and ④
round 1 of E_m
round 2 of E_m
extension with probability 1
Beginning of E_1

Figure 12: Concrete 2-round boomerang switch on LBlock, derived from [CM13].

The switch and the notation used below are represented in Figure 12. By careful identification of the differences at play, Equation (3) gives:

$$\begin{aligned} P = 2^{-2\times 8\times 4} \times \sum_{0\leq \delta,\alpha<2^n} & \texttt{FBDT}_{S_7}(0\text{x}1,\delta_1,\alpha_v) \times \texttt{FBDT}_{S_7}(0,0,\delta_2) \times \\ & \texttt{FBDT}_{S_6}(0\text{x}9,\delta_2,0) \times \texttt{FBDT}_{S_6}(0,0,0) \times \\ & \texttt{FBDT}_{S_5}(0\text{x}a,\delta_3,0\text{x}1) \times \texttt{FBDT}_{S_5}(0,0,\delta_1) \times \\ & \texttt{FBDT}_{S_4}(0,0,\alpha_u) \times \texttt{FBDT}_{S_4}(0\text{x}2,\alpha_u,\delta_3) \times \\ & \texttt{FBDT}_{S_3}(0,0,0\text{x}2) \times \texttt{FBDT}_{S_3}(0\text{x}2,\alpha_v,0) \times \\ & \texttt{FBDT}_{S_2}(0,0,0) \times \texttt{FBDT}_{S_2}(0\text{x}1,\alpha_w,0) \times \\ & \texttt{FBDT}_{S_1}(0,0,\alpha_w) \times \texttt{FBDT}_{S_1}(0,0,0\text{x}1) \times \\ & \texttt{FBDT}_{S_0}(0,0,0) \times \texttt{FBDT}_{S_0}(0,0,0\text{x}6) \end{aligned}$$

Using the properties of the FBDT, this can be simplified into:

$$P = 2^{-6\times 4} \times \sum_{0\leq\delta,\alpha<2^n} \mathtt{FBDT}_{S_7}(0\text{x}1,\delta_1,\alpha_v) \times DDT_{S_6}(0\text{x}9,\delta_2) \times \mathtt{FBDT}_{S_5}(0\text{x}a,\delta_3,0\text{x}1)$$
$$\times \mathtt{FBDT}_{S_4}(0\text{x}2,\alpha_u,\delta_3) \times DDT_{S_3}(0\text{x}2,\alpha_v) \times DDT_{S_2}(0\text{x}1,\alpha_w)$$

Referring to the DDT and FBDT we found that it is equal to $2^{-24} \times 2^{19} = 2^{-5}$, which closely matches what we found experimentally (we obtained a probability of $2^{-4.998}$ when doing 2^{20} tests corresponding to 2^{10} keys with 2^{10} messages each).

F Algorithm for Evaluating the Number of Rounds of the Boomerang Switch ([SQH19])

For completeness, we recall here the algorithm that was proposed by Song et al. [SQH19] to compute the size of E_m.

1. Extend both E_0 and E_1 with probability 1.
2. Initialize E_m with the last round of E_0 and the first round of E_1.
3. Prepend one round to E_m
   (a) Check whether the lower crossing differences for the newly added round are distributed uniformly. If they are, peel off the first round of E_m and go to step 4.
   (b) Go to step 3.
4. Append one more round to E_m
   (a) Check whether the upper crossing differences for the newly added round are distributed uniformly. If they are, peel off the last round of E_m and go to step 5.
   (b) Go to step 4.
5. Compute the probability of E_m.

G Example of Instantiation of the Generic Formula

As an example of the application of the switch formulas proposed in the paper, we detail here how to compute the probability of the 3-round switch on LBlock-s with the parameters provided in Table 4 and depicted in Figure 13:

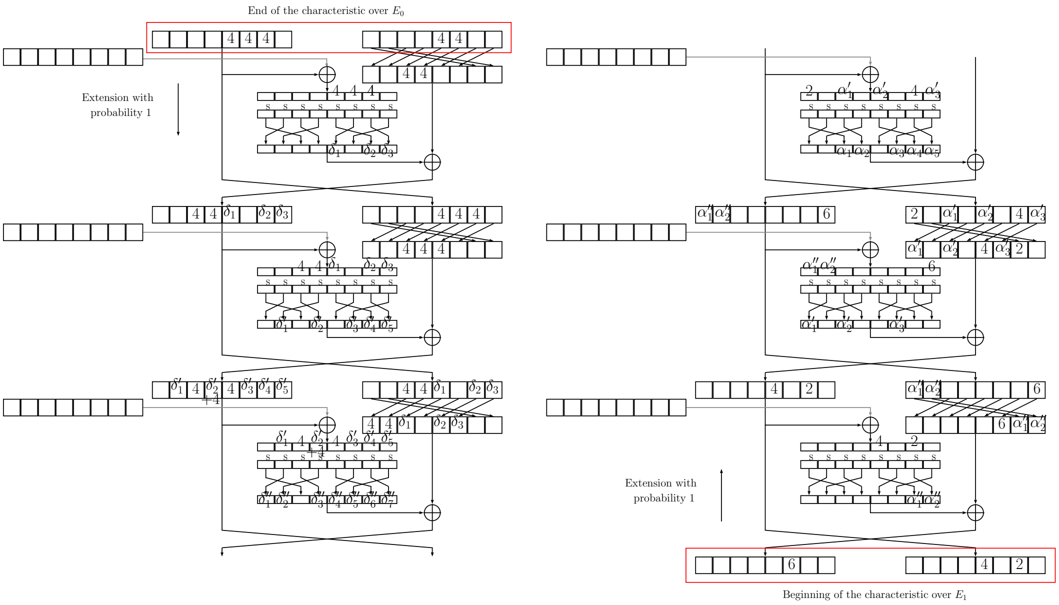
End of the characteristic over E_0
Extension with probability 1
Extension with probability 1
Beginning of the characteristic over E_1

Figure 13: Setting for the switch over three rounds of LBlock-s.

According to our theory, an approximation of the 3-round switch is given by the sum over all the possible intermediate differences (the δ and α in the figure) of the product of the FBET coefficients of each Sbox, each divided by 2^n. Since $\texttt{FBET}(0,0,0,0) = 2^n$ and $\texttt{FBET}(0,0,\nabla_o,\alpha) = \texttt{FBET}(\nabla_o,\alpha,0,0) = \texttt{DDT}(\nabla_o,\alpha)$, we expect only 5 FBET coefficients corresponding to the Sboxes that are active on both sides, and 15 DDT coefficients corresponding to Sboxes that are only active in one side.

An additional simplification comes from the following fact: the active Sboxes in the first round of the right part of the figure and the ones in the last round of the left part of the figure have an output that is free of constraints, so they don't have an impact on the probability we are computing (this comes from the fact that $\frac{1}{2^n}\sum_\alpha \texttt{DDT}(\gamma,\alpha) = 1$).

Putting things together, we obtain the following expression, where the sum is over all the involved variables:

$$\begin{aligned} r \;=\; & 2^{-4\times 12}\sum \texttt{FBET}(4,\delta_2,\alpha_2',\alpha_4)\cdot\texttt{DDT}(4,\delta_1)\cdot\texttt{FBET}(4,\delta_3,4,\alpha_5) \\ & \cdot\texttt{DDT}(4,\delta_2')\cdot\texttt{DDT}(4,\delta_1')\cdot\texttt{DDT}(\delta_1,\delta_4')\cdot\texttt{DDT}(\delta_2,\delta_5')\cdot\texttt{FBET}(\delta_3,\delta_3',6,\alpha_3') \\ & \cdot\texttt{DDT}(\alpha_1'',\alpha_2')\cdot\texttt{DDT}(\alpha_2'',\alpha_1') \\ & \cdot\texttt{FBET}(4,\delta_6'',4,\alpha_1'')\cdot\texttt{FBET}(\delta_4',\delta_7'',2,\alpha_2''). \end{aligned}$$

We can further simplify this expression by using the relations between the tables discussed in the paper. It gives:

$$\begin{aligned} r \;=\; & 2^{-4\times 8}\sum \texttt{FBCT}(4,\alpha_2')\cdot\texttt{DDT}(4,\delta_1)\cdot\texttt{DDT}(4,\delta_3) \\ & \cdot\texttt{DDT}(\delta_1,\delta_4')\cdot\texttt{FBCT}(\delta_3,6)\cdot\texttt{DDT}(\alpha_1'',\alpha_2') \\ & \cdot\texttt{DDT}(4,\alpha_1'')\cdot\texttt{FBCT}(2,\delta_4') \end{aligned}$$

We computed this sum and we obtained $r = \frac{38338560}{(2^4)^8} = 2^{-6.807}$, which confirms the experiment reported in Table 4.