Boomerang Uniformity of Popular S-box Constructions

Christina Boura, Léo Perrin, Shizhu Tian

Boomerang Uniformity of Popular S-box Constructions

Christina Boura[1,2], Léo Perrin[1], and Shizhu Tian[1,3,4]

[1] Inria, Paris, France.
leo.perrin@inria.fr, shizhu.tian@inria.fr
[2] Université de Versailles, Versailles, France
christina.boura@uvsq.fr
[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[4] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

Abstract. In order to study the resistance of a block cipher against boomerang attacks, a tool called the Boomerang Connectivity Table (BCT) for S-boxes was recently introduced. Very little is known today about the properties of this table especially for bijective S-boxes defined for n variables with $n \equiv 0 \mod 4$. In this work we study the boomerang uniformity of some popular constructions used for building large S-boxes, e.g. for 8 variables, from smaller ones. We show that the BCTs of all the studied constructions have abnormally high values in some positions. This remark permits us in some cases to link the boomerang properties of an S-box with other well-known cryptanalytic techniques on such constructions while in other cases it leads to the discovery of new ones. A surprising outcome concerns notably the Feistel and MISTY networks. While these two structures are very similar, their boomerang uniformity can be very different.
Keywords: BCT, S-box, Feistel, MISTY, Lai-Massey.

1 Introduction

To evaluate the security level of a block cipher, cryptanalysts have designed multiple techniques that aim at searching for undesirable patterns. One such technique is the so-called *differential cryptanalysis* [2] which looks for pairs (a, b) of input and output differences such that $E_k(x \oplus a) \oplus E_k(x) = b$, where E_k is (a round-reduced version of) the studied block cipher.

Block ciphers—but also other symmetric primitives such as hash functions for example—are often built using the so-called *S-boxes* as the source of their non-linearity. These are small functions mapping n bits to m, specified by their lookup tables. Typical values of n and m would be $n = m = 8$ and $n = m = 4$. In order to study the resilience of a block cipher against differential attacks, we first study the differential properties of its S-boxes. To this end, a key tool is the *Difference Distribution Table* (DDT). It is a table defined for any function $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ which is of size $2^n \times 2^m$ and such that

$$\delta_S(a, b) = \#\left\{x \in \mathbb{F}_2^n, S(x \oplus a) \oplus S(x) = b\right\}$$

for all $a \neq 0$. The maximal coefficient in the DDT of a function is called its *differential uniformity* and is denoted by δ_S. If the S-boxes of a block cipher have a low differential uniformity, we can expect—and, depending on the properties of its diffusion layer, prove—that it does not have any high probability differential pattern.

Since its inception, many variants of the differential cryptanalysis have been designed. In particular, the *boomerang attack* [15] considers both the encryption and the decryption functions at the same time by looking for pairs (a, b) such that

$$\begin{cases} E_k(x) & = y \\ E_k(x \oplus a) & = y' \end{cases} \text{ and } \begin{cases} E_k^{-1}(y \oplus b) & = z \\ E_k^{-1}(y' \oplus b) & = z \oplus a \end{cases},$$

where E_k is the block cipher under consideration. In order to estimate the probability of such an event in an S-box-based block cipher, we need to use the DDT of its S-box. However, in order to properly take into account the coupling between the different encryptions, we also need to look at another table called the *Boomerang Connectivity Table* (BCT) introduced in [7]. For a permutation $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$, it is a $2^n \times 2^n$ table of integers $\beta_S(a, b)$ defined as

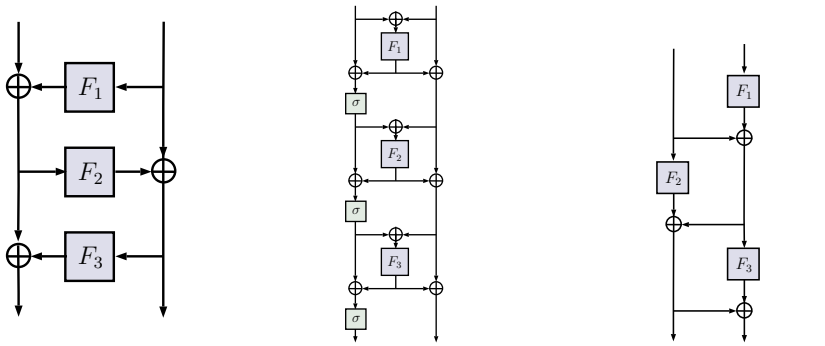
$$\beta_S(a, b) = \#\left\{x \in \mathbb{F}_2^n, S^{-1}\big(S(x) \oplus b\big) \oplus S^{-1}\big(S(x \oplus a) \oplus b\big) = a\right\} .$$

The BCT coefficients are always equal to 2^n (the maximum) when $a = 0$ or $b = 0$. Thus, we define the *boomerang uniformity* of S, denoted β_S, to be the maximum value of $\beta_S(a, b)$ for $a \neq 0$ and $b \neq 0$. As with the differential uniformity, the lower the boomerang uniformity the better. Note, that the boomerang uniformity could also be defined, by a slight modification, for non-bijective functions. However, for such functions the cryptographic interpretation of the property is not clear. As we are interested in this article in S-boxes used in practice, we only concentrate in the bijective case.

Unlike the DDT, little is known about the BCT of even the most common cryptographic components. It is easy for example to prove (see e.g. [7]) that for any function S, $\beta_S \geq \delta_S$ and that for permutations S providing an optimal resistance to differential cryptanalysis, called *Almost Perfect Nonlinear (APN)* permutations, $\beta_S = \delta_S = 2$. Then, Boura and Canteaut studied in [5] the boomerang properties of the inverse mapping and of differentially 4-uniform quadratic power permutations of $\mathbb{F}_{2^n}$. They showed that both families have an optimal boomerang uniformity when $n \equiv 2 \mod 4$, where optimal means that the boomerang uniformity equals the differential uniformity and is 4 in both cases. However, besides these first results, determining the boomerang uniformity of other cryptographically relevant families of permutations or constructions remains an open problem.

In order to ease the implementation of their ciphers on constrained platforms, cryptographers often use specific block-cipher-like structures for their S-boxes. This technique permits the construction of large S-boxes from smaller, much cheaper ones. In this paper, we investigate the BCT of several such lightweight S-box structures, notably the 3-round Feistel, Lai-Massey and (unbalanced) MISTY structures. These three classical constructions are depicted in Figures 1a, 1b

and 1c respectively. We then look at two 1-round structures: the 1-round SPN and the specific structure used in the FLY block cipher [12].



(a) 3-round Feistel. **(b)** 3-round Lai-Massey. **(c)** 3-round MISTY.

Fig. 1: The structures investigated in this paper.

For each of those structures, we derive a lower bound on the boomerang uniformity of S-boxes built using it. Table 1 presents the differential and boomerang uniformity of several S-boxes from the literature. It also contains the lower bounds derived in this paper.

Rounds	S-box Struct.	Cipher	Ref.	δ_S	β_S	Lower bound
3	Feistel	Scream	[6, 11]	8	**256**	256
	MISTY-like	Fantomas	[10]	16	**160**	64 $(*)$
	Lai-Massey	Fox	[14]	16	**256**	256
1	SPN	Midori	[1]	64	**256**	256
	Lai-Massey-like	FLY	[12]	16	**256**	256 $(*)$

Table 1: The boomerang and differential uniformity of various 8-bit S-boxes. $(*)$ The bound depends on the inner components of these constructions.

Before going any further, we recall some basic properties of the BCT which were established in [5, 7].

Proposition 1. *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation. Then S has the same boomerang uniformity as S^{-1} and $B \circ S \circ A$, where A and B are affine permutations, and $\beta_S \geq \delta_S$. Furthermore, denote by S_b the permutation $x \mapsto S^{-1}(S(x) \oplus b)$. Then,*

$$\beta_S(a, b) = \#\left\{x \in \mathbb{F}_2^n, S_b(x) \oplus S_b(x \oplus a) = a\right\} . \tag{1}$$

2 3-round Feistel and Lai-Massey Networks

We study in this section the properties of the BCT of 3-round Feistel and Lai-Massey constructions and show that the boomerang uniformity of both is the worst one possible. The two proofs are similar and for this reason we provide here only the proof for the Lai-Massey one. In both cases, the results we derive are an inherent property of the structures used: even if the subcomponents are chosen so as to have excellent properties, the boomerang uniformity will be the worst possible.

2.1 The Feistel case

A popular way to construct large S-boxes from smaller ones is by using the Feistel construction. This scheme was used for constructing the 8-bit S-boxes of multiple ciphers including ZUC [9], and Scream [11]. All use 3 rounds. This number of rounds is the smallest allowing the overall structure to have good properties. In particular, if only 2 are used, a part of the output depends linearly on a part of the input.

A 3-round Feistel network has the worst possible boomerang uniformity, no matter the choice of the inner functions. Proposition 2 (whose proof will be given in the full version) formalizes this statement.

Proposition 2. *Let $S : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^n \times \mathbb{F}_2^m$ be a 3-round Feistel network and let F_1, F_2 and F_3 be its inner functions as depicted in Fig. 1a, with $F_1, F_3 : \mathbb{F}_2^m \to \mathbb{F}_2^n$ and $F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then, for any $b \in \mathbb{F}_2^n \times \mathbb{F}_2^m$,*

$$\beta_S(b, b) = \beta_S = 2^{n+m}.$$

The property corresponding to Proposition 2 was known before. In fact, this property was recently used by Biryukov et al. for performing guess and determine attacks against Feistel networks [3]. We deduce that the knowledge of the BCT can help the cryptanalyst in contexts different from boomerang attacks. We discuss such applications later in Section 5.

2.2 The Lai-Massey case

We consider a variant of the structure depicted in Fig. 1b where the last application of the linear orthomorphism σ is removed for two reasons. First, the S-box of the cipher Fox is built in this way. Second, this version yields a simpler proof but, since σ is linear and since the boomerang uniformity is constant in an affine-equivalence class, the result still holds if the last σ is present.

Proposition 3. *Let $S : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$ be a 3-round Lai-Massey structure. Let $F_1, F_2, F_3 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be its inner functions and let σ be a linear permutation. For any nonzero $a \in \mathbb{F}_2^n$, consider $a_1 = (a, a)$ and $b = (\sigma(a), \sigma(a)) \in (\mathbb{F}_2^n)^2$. Then,*

$$\beta_S(a_1, b) = \beta_S = 2^{2n}.$$

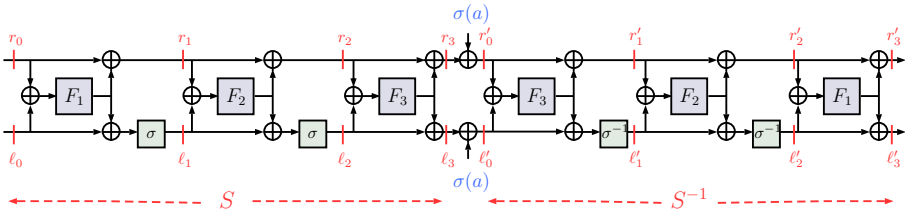


Fig. 2: The function $S_b(x) = S^{-1}(S(x, y) + b)$, where S is a 3-round Lai-Massey construction where the last application of σ is omitted.

Proof. Let $b \in (\mathbb{F}_2^n)^2$ be of the form $b = (\sigma(a), \sigma(a)) \in (\mathbb{F}_2^n)^2$ where a is nonzero. Furthermore, let S_b be as defined in Eq. (1) (see Fig. 2). Our aim is to prove that

$$S_b(x, y) + S_b((x, y) + (a, a)) = (a, a), \text{ for all } (x, y) \in (\mathbb{F}_2^n)^2. \tag{2}$$

The remainder of the proof consists in checking Eq. (2) by developing the expression of S_b.

Begin with the input $(\ell_0, r_0) = (x, y) \in \mathbb{F}_2^{2n}$ and denote

$$\begin{aligned}
A_1(x, y) &= A_1 = x + y, \quad A_2(x, y) = A_2 = \sigma(x) + y + F_1(A_1) + \sigma(F_1(A_1)),\\
A_3(x, y) &= A_3 = \sigma(\sigma(x + F_1(A_1)) + F_2(A_2)) + y + F_1(A_1) + F_2(A_2),\\
T(x, y) &= T = F_2(A_2) + F_2(A_2 + \sigma(a) + a),\\
B_1(x, y) &= B_1 = A_1 + \sigma^{-1}(a) + \sigma(a) + T + \sigma^{-1}(T).
\end{aligned}$$

The output (ℓ_i, r_i) of the i-th round, $i = 1, 2, 3$ of S, is detailed below:

$$\begin{aligned}
(\ell_1, r_1) &= (\sigma(x + F_1(A_1)), y + F_1(A_1)),\\
(\ell_2, r_2) &= (\sigma(\sigma(x + F_1(A_1)) + F_2(A_2)), y + F_1(A_1) + F_2(A_2)),\\
(\ell_3, r_3) &= (\sigma(\sigma(x + F_1(A_1)) + F_2(A_2)) + F_3(A_3), y + F_1(A_1) + F_2(A_2) + F_3(A_3)).
\end{aligned}$$

Denote by $(\ell'_0, r'_0) = (\ell_3, r_3) + (\sigma(a), \sigma(a))$ the input of S^{-1}. Similarly, we have

$$\begin{aligned}
(\ell'_1, r'_1) &= (a + \sigma(x + F_1(A_1)) + F_2(A_2), \sigma(a) + y + F_1(A_1) + F_2(A_2)),\\
(\ell'_2, r'_2) &= \left(\sigma^{-1}(a) + x + F_1(A_1) + \sigma^{-1}(T), \sigma(a) + y + F_1(A_1) + T\right),\\
(\ell'_3, r'_3) &= ((\sigma^{-1}(a) + x + F_1(A_1) + F_1(B_1) + \sigma^{-1}(T),\\
&\qquad \sigma(a) + y + F_1(A_1) + F_1(B_1) + T).
\end{aligned}$$

As $A_1(x + a, y + a) = A_1(x, y)$ and $A_2(x + a, y + a) = A_2(x, y) + \sigma(a) + a$, it holds that $T(x + a, y + a) = T(x, y)$ and $B_1(x + a, y + a) = B_1(x, y)$. Therefore, Eq. (2) holds and we deduce the proposition. □

3 BCTs of 3-round MISTY Networks

The MISTY network mimicks a structure used in the MISTY cipher [13]. While it might ressemble a Feistel network it requires all three inner functions to

be bijective in order for the whole function to be a permutation. As we will show, the MISTY structure also differs from the Feistel one via its BCT: the boomerang uniformity of a 3-round MISTY structure *depends* on the specifics of the subfunctions used.

Though the results are similar in both cases, the case where the branches are of the same size (balanced) and of different sizes (unbalanced) require different analyses which we provide in Sections 3.1 and 3.2 respectively.

3.1 3-round Balanced MISTY Networks

Proposition 4. *Let $S : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$ be a 3-round balanced MISTY network and let F_1, F_2 and F_3 be its inner functions as depicted in Fig. 1c, with $F_1, F_2, F_3 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ bijective. Then,*

$$\beta_S \geq 2^n \beta_{F_2}.$$

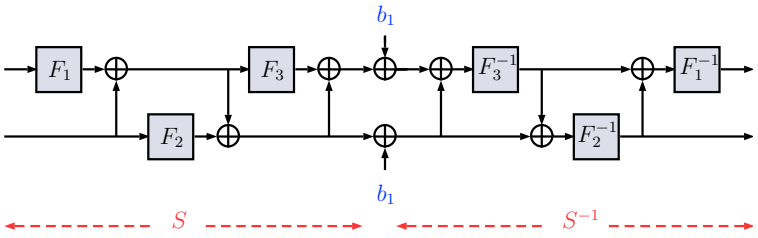


Fig. 3: The function $S_b(x) = S^{-1}(S(x) + b)$, for $x \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ and $b = (b_1, b_1)$ where S is a 3-round balanced MISTY structure.

Proof. The boomerang uniformity of F_2 is β_{F_2} meaning that there exists $(a_1, b_1) \in (\mathbb{F}_2^n)^2$ such that $\beta_{F_2}(a_1, b_1) = \beta_{F_2}$. If $a = (a_1, 0), b = (b_1, b_1)$ then we deduce from Proposition 1 that

$$\beta_S(a, b) = \#\left\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid S_b(x, y) + S_b(x + a_1, y) = (a_1, 0)\right\} ,$$

where S_b is as depicted in Fig. 3. Since $b = (b_1, b_1)$, it can be simplified into

$$S_b(x, y) \;=\; \big(F_2^{-1}(F_2(x) + b_1),\; F_1^{-1}(F_2^{-1}(F_2(x) + b_1) + F_1(y) + x)\big)$$

so we deduce

$$\begin{aligned} S_b(x, y) + S_b(x + a_1, y) = \Big(& F_2^{-1}(F_2(x) + b_1) + F_2^{-1}(F_2(x + a_1) + b_1), \\ & F_1^{-1}\big(F_2^{-1}(F_2(x) + b_1) + F_1(y) + x\big) + \\ & F_1^{-1}\big(F_2^{-1}(F_2(x + a_1) + b_1) + F_1(y) + x + a_1\big)\Big) . \end{aligned} \tag{3}$$

We now show that $\beta_S(a, b) = 2^n |A|$, where

$$A \;=\; \left\{x \in \mathbb{F}_2^n \mid F_2^{-1}(F_2(x) + b_1) + F_2^{-1}(F_2(x + a_1) + b_1) = a_1\right\} .$$

For any $x \in A$, the right hand side of $S_b(x,y) + S_b(x+a_1,y)$ can be simplified:

$$\begin{aligned} & F_1^{-1}\big(F_2^{-1}(F_2(x)+b_1)+F_1(y)+x\big) \\ & \quad + F_1^{-1}\big(F_2^{-1}(F_2(x+a_1)+b_1)+F_1(y)+x+a_1\big) \\ = \;& F_1^{-1}\big(F_2^{-1}(F_2(x)+b_1)+F_1(y)+x\big) + F_1^{-1}\big(F_2^{-1}(F_2(x)+b_1)+F_1(y)+x\big) \\ = \;& 0\ . \end{aligned}$$

As $|A| = \beta_{F_2}(a_1,b_1) = \beta_{F_2}$, we conclude that the boomerang uniformity of a 3-round balanced MISTY network is lower bounded by $2^n\beta_{F_2}$.

Remark 1. We give here the minimal bounds for a 3-round MISTY network, for some popular choices of n. All functions F_1, F_2 and F_3 are supposed bijective.

n = 4 As proved in [5], the minimal boomerang uniformity for a permutation of $\mathbb{F}_2^4$ is 6. Therefore, by choosing F_2, with $\beta_{F_2} = 6$, we get that $\beta_S \geq 96$. As we will argue in Section 5 this is a high value for an 8-bit S-box.

n = 3 APN permutations exist for $n = 3$. Using one as F_2, we obtain $\beta_S \geq 16$.

Proposition 5. *Let $S : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$ be a 3-round MISTY network with inner functions F_1, F_2 and F_3. If F_1 or F_3 is an affine permutation, then $\beta_S = 2^{2n}$.*

The proof of this proposition will be given in the full version of this paper.

3.2 3-round Unbalanced MISTY Networks

In practice, all known MISTY constructions are unbalanced. More specifically, they use branches of $n-1$ and $n+1$ bits. This is the case for the original MISTY1 cipher [13], where some inner components follow a 3-round construction with one 7-bit and one 9-bit branch. It is also the case of the 8-bit S-box of Fantomas [10], where a 3-bit and a 5-bit branch are used. One reason for this is that an unbalanced 3-round MISTY structure can potentially achieve a better differential uniformity than a balanced one. For example, Canteaut et al. showed in [6] that for $n = 4$, a $2n$-bit permutation S following a balanced MISTY structure has $\delta_S \geq 16$, while by taking a 3-bit and a 5-bit branch it is possible to find a permutation S with $\delta_S = 8$. Another reason is that taking branches of an odd length of bits permits to use APN permutations for the inner components—as was indeed done in MISTY1.

We studied the boomerang uniformity of 3-round unbalanced MISTY networks. Our arguments differ slightly depending on whether the widest branch is on the left or on the right. Let m be the size of the smallest branch and n the size of the biggest one. If S_1 is the construction with F_2 applying to the smallest branch and S_2 is the other one then we get that

$$\beta_{S_1} \geq 2^n\beta_{F_2} \quad \text{and} \quad \beta_{S_2} \geq 2^m\beta_{F_2|_{\mathbb{F}_2^m}}\ .$$

Both proofs will appear in an extended version of this abstract.

4 Non-iterative constructions

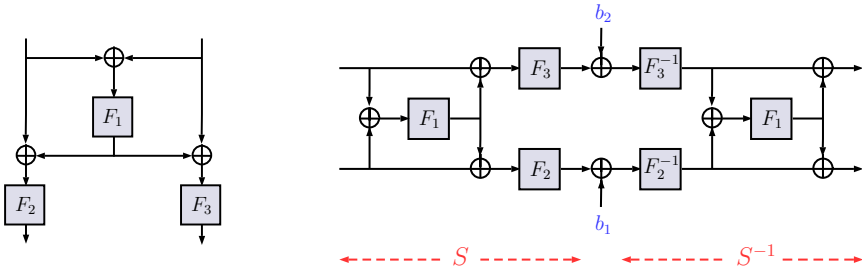
Until now, we have only considered 3-round constructions. However, S-box designers sometimes choose non-iterative structures. In this section, we look at 1-round SPN (as used e.g. in Midori [1]) and at the *ad hoc* Lai-Massey like structure used by the *Littlun* S-Box of the block cipher FLY [12]. It is composed of a single Lai-Massey round followed by an S-box layer (see Fig. 4a). While Littlun is such that $F_1 = F_2 = F_3$, we do not make this assumption.

The following straightforward proposition deals with the properties of a 1-round SPN.

Proposition 6. *Let F_1, F_2 be n-bit permutations and let $S : (\mathbb{F}_2^n)^2 \to (\mathbb{F}_2^n)^2$ be such that $S(x_1, x_2) = (F_1(x_1), F_2(x_2))$. Then we have*

$$\beta_S\left((a_1, a_2), (b_1, b_2)\right) \;=\; \beta_{F_1}(a_1, b_1) \times \beta_{F_2}(a_2, b_2)\ ,$$

so that in particular $\beta_S = \beta_S\left((a, 0), (0, b)\right) = 2^{2n}$. □



(a) Littlun S-box.

(b) The function $S_b(x) = S^{-1}(S(x, y) + b)$, where S is the Littlun S-box.

Fig. 4: Analysis of the Littlun structure

Let us now consider the Littlun construction. If F_1 is an affine permutation, then the corresponding Littlun-like S-box is a 1-round SPN structure which has thus the worst possible boomerang uniformity. If not, the following proposition relates its boomerang uniformity to that of its subcomponents.

Proposition 7. *Let S be a generalised-Littlun structure with n-bit permutations F_1, F_2 and F_3 (see Fig. 4a). Then $\beta_S \geq 2^n \max\{\beta_{F_2}, \beta_{F_3}\}$.*

Proof. We define the two following functions H and G over $(\mathbb{F}_2^n)^2$:

$$H(x, y) = (x + F_1(x + y), y + F_1(x + y)) \quad \text{and} \quad G(x, y) = (F_2(x), F_3(y))\ .$$

Both H and G are permutations of $(\mathbb{F}_2^n)^2$, H is an involution, and $S(x, y) = (G \circ H)(x, y)$. we claim that $\beta_S(a, b) \geq \beta_G(a, b)$, for $a = (a_1, a_1)$, $a_1 \neq 0$ and

$b = (b_1, b_2)$. Indeed,

$$\begin{aligned}
\beta_S(a,b) &= \#\left\{X \in (\mathbb{F}_2^n)^2 \mid H(G^{-1}(G(H(X)+a)+b)) + H(G^{-1}(G(H(X)+b))) = a\right\} \\
&= \#\left\{Y \in (\mathbb{F}_2^n)^2 \mid H(G^{-1}(G(Y+a)+b)) + H(G^{-1}(G(Y)+b)) = a\right\} \\
&= \#\left\{Y \in (\mathbb{F}_2^n)^2 \mid H(G^{-1}(G(Y)+b) + G^{-1}(G(Y)+b)) \right. \\
&\qquad \left. + G^{-1}(G(Y+a)+b)) + H(G^{-1}(G(Y)+b)) = a\right\} \\
&\geq \#\left\{Y \in (\mathbb{F}_2^n)^2 \mid G^{-1}(G(Y)+b) + G^{-1}(G(Y+a)+b) = a\right\} = \beta_G(a,b)\ .
\end{aligned}$$

By applying Proposition 6 to $\beta_G(a,b)$ with $a = (a_1, a_1), b = (b_1, b_2)$, we obtain that $\beta_S(a,b) = 2^n \beta_{F_2}(a_1, b_1)$ when $b_2 = 0$ and $\beta_S(a,b) = 2^n \beta_{F_2}(a_1, b_2)$ when $b_1 = 0$. We deduce that $\beta_S \geq 2^n \max(\beta_{F_2}, \beta_{F_3})$. □

5 Conclusion

Our results on the BCT and on the boomerang uniformity of permutations with various structures have several consequences. First, by the fact that $\beta_S = 2$ if and only if S is APN, we can immediately see that 3-round Feistel, Lai-Massey and MISTY structures can never be APN.

As mentioned in Section 2.1, the consequences in terms of cryptanalysis can also extend further than boomerang attacks. The guess and determine of Biryukov et al. [3] uses a property equivalent to the fact that the boomerang uniformity of a 3-round Feistel network is always maximal. We can therefore expect the same attack to work against Lai-Massey structures. Interestingly, our results show that it is possible to construct a 3-round MISTY structure immune against the existence of such probability 1 patterns, meaning that they seem to offer some inherent resilience against these attacks. Not only are our results regarding Feistel and Lai-Massey structures very similar, the arguments we used to derive them are also very close—independently of the choice of the linear mapping σ. While the similarity between these two structures makes intuitive sense, we find it interesting to see it displayed in such a clear manner.

We have encountered several cases: for 3-round Lai-Massey, 3-round Feistel and 1-round SPN, the boomerang uniformity is maximal regardless of the subcomponents used. In the 3-round MISTY case, the boomerang uniformity is bounded by the *differential* uniformity of its subfunction and, in the Littlun case, it is bounded by the *boomerang* uniformity of its subfunction.

Finally, another application of our results lies in S-box reverse-engineering [4]. In this context, the aim is to recover the hidden structure of an S-box using only its lookup table. If an S-box has non-trivial differential and linear properties but a boomerang uniformity equal to 2^n then we can suspect that it is a 3-round Lai-Massey or Feistel structure. Since the boomerang uniformity is preserved under the composition with an affine permutation, this test would work even if the S-box structure is obfuscated by such permutations—as is the case for instance in the S-box of ZUC [9].

We generated 1000 different permutations for various block sizes n and obtained averages of A_n with

$$A_4 = 11.9,\ A_6 = 16.5,\ A_8 = 20.3,\ A_{10} = 24.0\ .$$

This shows that a maximal boomerang uniformity is an extremely rare event indicative of a very strong structure. In fact, the non-maximal but still very high boomerang uniformity of the 3-round MISTY and Littlun structures can also be leveraged to identify such potentially hidden structures.

References

1. S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni. Midori: A block cipher for low energy. In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 411–436. Springer, Heidelberg, Nov. / Dec. 2015.
2. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, Jan. 1991.
3. A. Biryukov, G. Leurent, and L. Perrin. Cryptanalysis of Feistel networks with secret round functions. In Dunkelman and Keliher [8], pages 102–121.
4. A. Biryukov and L. Perrin. On reverse-engineering S-boxes with hidden design criteria or structure. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 116–140. Springer, Heidelberg, Aug. 2015.
5. C. Boura and A. Canteaut. On the boomerang uniformity of cryptographic sboxes. *IACR Trans. Symm. Cryptol.*, 2018(3):290–310, 2018.
6. A. Canteaut, S. Duval, and G. Leurent. Construction of lightweight S-boxes using Feistel and MISTY structures. In Dunkelman and Keliher [8], pages 373–393.
7. C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song. Boomerang connectivity table: A new cryptanalysis tool. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 683–714. Springer, Heidelberg, Apr. / May 2018.
8. O. Dunkelman and L. Keliher, editors. *SAC 2015*, volume 9566 of *LNCS*. Springer, Heidelberg, Aug. 2016.
9. ETSI/Sage. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 4 : Design and Evaluation Report. Technical report, ETSI/Sage, September 2011. Available at http://www.gsma.com/aboutus/wp-content/uploads/2014/12/EEA3_EIA3_Design_Evaluation_v2_0.pdf.
10. V. Grosso, G. Leurent, F.-X. Standaert, and K. Varici. LS-designs: Bitslice encryption for efficient masked software implementations. In C. Cid and C. Rechberger, editors, *FSE 2014*, volume 8540 of *LNCS*, pages 18–37. Springer, Heidelberg, Mar. 2015.
11. V. Grosso, G. Leurent, F.-X. Standaert, K. Varici, F. D. Anthony Journault, L. Gaspar, and S. Kerckhof. SCREAM & iSCREAM Side-Channel Resistant Authenticated Encryption with Masking. Candidate for the CAESAR Competition. See also http://perso.uclouvain.be/fstandae/SCREAM/, 2014.
12. P. Karpman and B. Grégoire. The LITTLUN S-box and the FLY block cipher. In *Lightweight Cryptography Workshop 2016, October 17-18 (informal proceedings)*. National Institute of Standards and Technology, 2016.
13. M. Matsui. New block encryption algorithm MISTY. In E. Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 54–68. Springer, Heidelberg, Jan. 1997.
14. S. Vaudenay and P. Junod. Device and method for encrypting and decrypting a block of data. United States Patent (20040247117), see also "Fox, a New Family of Block Ciphers" http://crypto.junod.info/sac04a.pdf, 2004.
15. D. Wagner. The boomerang attack. In L. R. Knudsen, editor, *FSE'99*, volume 1636 of *LNCS*, pages 156–170. Springer, Heidelberg, Mar. 1999.