On Perfect Linear Approximations and Differentials over Two-Round SPNs

Christof Beierle[1], Patrick Felke[2], Gregor Leander[1], Patrick Neumann[1], and Lukas Stennes[1]

[1] Ruhr University Bochum, Bochum, Germany
firstname.lastname@rub.de
[2] University of Applied Sciences Emden/Leer
patrick.felke@hs-emden-leer.de

Abstract. Recent constructions of (tweakable) block ciphers with an embedded cryptographic backdoor relied on the existence of probability-one differentials or perfect (non-)linear approximations over a reduced-round version of the primitive. In this work, we study how the existence of probability-one differentials or perfect linear approximations over two rounds of a substitution-permutation network can be avoided by design. More precisely, we develop criteria on the s-box and the linear layer that guarantee the absence of probability-one differentials for all keys. We further present an algorithm that allows to efficiently exclude the existence of keys for which there exists a perfect linear approximation.

Keywords: differential cryptanalysis · linear cryptanalysis · decomposition · boomerang connectivity table · weak keys

1 Introduction

The vast majority of data is protected by symmetric cryptography due to its performance advantage, typically in a hybrid setting with public-key components surrounding the actual encryption. Almost all designs in symmetric cryptography can be subsumed as performance driven. Indeed, beyond security, the main criteria and innovation incentive for symmetric cryptography is efficiency. Consequently, as a community we have made impressive improvements when it comes to designing performant ciphers. We managed to design primitives that allow the encryption of data significantly faster than AES on modern CPUs, even on platforms where AES is directly supported in hardware. For other criteria, e.g., chip-size, latency, code size, side-channel protection, or multiplicative depth, the improvement is even bigger.

With respect to understanding the security of symmetric cryptographic primitives, not much progress has been made in recent years. Even if we look at the resilience against dedicated attack vectors, we still rely on unproven assumptions. One fundamental example is that we often assume independence of the

inputs to all parts of a cipher. This is obviously not true as the output of one part serves as the direct input for the next part. Another classical example is that we study weaknesses, e.g., differential and linear properties or (non-linear) invariants, by studying all parts of a cipher separately, while we actually only want to exclude that the weaknesses in question apply to the cipher as a whole.

Resistance Against Linear and Differential Attacks. To be more specific, to argue about the resistance of a given cipher with respect to the most important attack vectors, differential [8] and linear cryptanalysis [21], we basically have to give arguments that, for almost all keys, no exploitable differential resp., linear approximation exists, i.e., to bound the probability resp., bias for an overwhelming fraction of all keys. However, in almost all cases we only manage to bound the average probability for a differential or linear characteristic assuming independent round keys.

The case of linear approximations with absolute correlation one and differentials with probability one that work *for all keys* of a key-alternating cipher are trivial to avoid. Indeed, they imply one round linear approximations and differentials with the same property. That is a round function with non-maximal linearity or differential uniformity is enough to rule out those cases.

While for one round of almost any modern design the problem is trivial, already two rounds (as depicted in Fig. 1) have not been thoroughly considered in the past. Given a keyed (or tweaked) two-round construction, not even the question whether there exists a key for which the construction allows a probability-one differential resp., affine approximation has been answered in general.

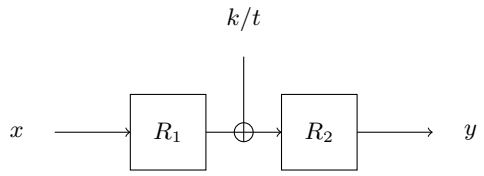

Fig. 1. Two rounds of a key-alternating block cipher.

For one key, while no good arguments for the non-existence of such maximally biased linear and differential properties where given, such properties indeed occurred in designs, either unintentionally or on purpose. For the former cases, the cipher SKINNY [3] is a good example as it actually has perfect two-round linear approximations as has been shown by carefully tracing the bits through the circuit of the s-box recently in [18]. For the latter, the cipher Boomslang [2] is a recent example. Here, a non-linear two-round iterative characteristic has been planted as a backdoor. A closer look at this construction actually reveals that this is based on a two-round linear approximation that has absolute correlation one for the backdoor tweak. As we will see below, further examples exist.

However, intriguingly, such examples only appear for linear approximations, while no (non-trivial) example of a keyed two-round construction is known that exhibits a key for which there is a probability-one differential. One example is the Malicious framework [23] that builds upon a probability-one differential through a partial non-linear layer. Since the probability-one differential appears already over a single round, it belongs to the class of trivial examples.

Our Contribution. In this work we manage to derive conditions under which no key exists such that a differential with probability one occurs in two-round substitution-permutation networks (SPNs). This is captured in Theorem 2 and turns out to be surprisingly technical. However, it is possible to derive several special cases, for mild and natural conditions on the s-box and the linear-layer, that we state in Corollary 7, Corollary 8, and Corollary 9. Besides our results on the non-existence, we further construct several non-trivial examples of two-round SPNs with probability-one differentials, e.g., Example 1.

Interestingly, the boomerang connectivity table (BCT), introduced in [10] appears in our conditions. With this, the most straightforward way of ensuring that no probability-one differential exists for two rounds is to use any linear layer with a non-trivial branch number and any s-box with a non-trivial boomerang uniformity. Our conditions are applicable to virtually any modern SPN design and we give various examples in Table 1.

For the case of a linear approximation, we are able to give efficient algorithms that allow an efficient computation of all keys and the corresponding input and output masks of a linear approximation with absolute correlation one. Using this, we show that Boomslang actually exhibits several other weak tweaks that lead to probability-one linear approximations. Another interesting example is CRAFT [4], where our approach allows an automated way of reproducing results given previously in [20,17].

Table 1 summarizes our results of both the differential and linear parts. From a technical viewpoint, we deploy recent results on decomposing an s-box layer [19] and in particular conditions for the uniqueness of such a decomposition.

Related Work. There is a large variety of work related to one or another aspect of arguing resistance against differential and linear attacks, starting with the seminal wide-trail strategy [12,11] focusing on linear and differential characteristics. The decorrelation theory [24] is a mean to ensure security against linear and differential attacks (or in general statistical attacks using only a few numbers of plaintext/ciphertext pairs at a time) on average. It does not cover the existence of weak keys or tweaks.

The key-dependent behavior was treated for a large class of two-round SPNs for the case of characteristics in [13] where it was observed that the right pairs can often be seen as the intersection of linear spaces translated by the round key. More recently, the key-dependent behavior of differentials has been approximated using the notion of quasidifferential trails in [7].

Regarding the algorithmic detection of highly-biased linear approximations or highly-probable differentials, we like to mention [16] that deploys links to

Table 1. Overview of our results. ✓indicates that we can exclude the existence of non-trivial perfect linear approximations resp., differentials whereas ✗ means that there are non-trivial perfect linear approximations. ⊥ indicates that our computations aborted and - indicates that the cipher is not AES-like and therefore was not tested for four rounds. r is the number of rounds.

Cipher	Linear			Differential for $r = 2$			
	$r = 2$	$r = 3$	$r = 4$	Cor. 7	Cor. 8	Cor. 9	Thm. 2 & Cor. 10
Boomslang	✗	✓	✗	✓			✓
CRAFT	✗	✓	✓				✓
MANTIS	✗	✓	✗	✓			✓
Midori64	✗	✓	✗	✓			✓
SKINNY-64	✗	✓	✓				✓
SKINNY-128	✗	⊥	⊥				✓
AES	✓	✓	⊥	✓	✓		✓
GIFT-64	✓	✓	✓			✓	✓
GIFT-128	✓	✓	✓			✓	✓
LED	✓	✓	✓	✓			✓
PRESENT	✓	✓	✓			✓	✓
PRINCE	✓	✓	✓		✓		✓
Streebog	✓	✓	⊥	✓	✓		✓
Ascon	✓	✓	-	✓	✓		✓
iSCREAM	✓	⊥	-	✓			✓
Keccak-100	✓	✓	-		✓		✓
Kuznechik	✓	⊥	-	✓	✓		✓
PRIDE	✓	✓	-				✓
RECTANGLE	✓	✓	-			✓	✓

coding theory or, very recently, [14] from EUROCRYPT 2023 that allow to detect such approximations and differentials in a black-box manner. Thus, from our perspective, the limitation here is that those results do not allow to tackle keyed primitives without iterating over all (round) keys.

For Feistel ciphers, one concrete example that allows to make statements about weak keys is the KN cipher [22]. This construction allows to bound the differential uniformity for any key for two (Feistel) rounds.

Outline In Section 2, we start by fixing notations and recalling the basic properties needed. We then first describe the results for the case of linear approximations in Section 3, focusing more on algorithmic solutions. The differential case, with the general statement given in Theorem 2, that leads to various more accessible conditions given in Corollaries 7 to 9, is explained in Section 4. As is shown in Table 1, for many SPNs those arguments are sufficient to exclude the existence of probability-one differentials. We conclude the paper in Section 5 with some open questions and possible improvements of our work.

2 Preliminaries

We recall some basic properties needed throughout the paper and we fix our notation. We work with bits, which we understand as elements in the field with two elements $\mathbb{F}_2$, and with bit strings, which we understand as vectors in $\mathbb{F}_2^n$, the n-dimensional vector space over $\mathbb{F}_2$. The addition of vectors in $\mathbb{F}_2^n$ is simply denoted by $+$ and corresponds to an xor of bit strings. The canonical inner product of vectors $x, y \in \mathbb{F}_2^n$ is denoted by

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

and used in particular for defining an *affine approximation* for a function $E\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ by the equation

$$\langle \alpha, x \rangle + \langle \beta, E(x) \rangle = c \tag{1}$$

for $\alpha \in \mathbb{F}_2^n$, $\beta \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. If $c = 0$ we call the approximation *linear*. The *correlation* of a linear approximation is given by

$$\mathrm{cor}_E(\alpha, \beta) \coloneqq \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle \alpha, x \rangle + \langle \beta, E(x) \rangle}.$$

If Eq. (1) holds with absolute correlation equal to one, i.e., there exists a constant c such that it is fulfilled for all x, we say it is a *perfect linear approximation* which we also denote simply by the tuple (α, β, c) or just (α, β) in case we do not care about the constant. We call a perfect linear approximation *non-trivial* if $(\alpha, \beta) \neq (0, 0)$. The *linearity* of E is defined as $\max_{\alpha \neq 0, \beta}(2^n \cdot |\mathrm{cor}_E(\alpha, \beta)|)$ and we call it *maximal* if it is equal to the size of the domain of E, i.e., 2^n.

For E as above and $\alpha \in \mathbb{F}_2^n$, we say that

$$\Delta_\alpha E(x) \coloneqq E(x) + E(x + \alpha)$$

is the *(first-order) derivative* of E at point x along α. A *probability-one differential* over E is a tuple (α, β), with $\alpha \in \mathbb{F}_2^n, \beta \in \mathbb{F}_2^n$, for which $\Delta_\alpha E(x)$ is equal to β for all x. We call a probability-one differential *non-trivial* if $(\alpha, \beta) \neq (0, 0)$. The *differential uniformity* of E is defined as $\max_{\alpha \neq 0, \beta} |\{x \in \mathbb{F}_2^n \mid \Delta_\alpha E(x) = \beta\}|$ and we call it *maximal* if it is equal to the size of the domain of E.

A perfect linear approximation of a derivative with input mask zero, that is an equation of the form

$$\langle \beta, E(x) + E(x + \alpha) \rangle = c$$

holding for all x, defines a *linear structure* (β, α, c) of E, and we call it non-trivial if $\alpha \neq 0$. The following notation is in particular used when we discuss SPNs. For a convenient handling of the *addition of constants*, and in particular keys, we call

$$T\colon \mathbb{F}_2^n \to \mathbb{F}_2^n \text{ with } T_\alpha(x) = x + \alpha$$

the *translation by* α.

For $n = dm$ and an s-box $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$, we denote by $\bar{S}$ the *parallel application of the s-box* S, i.e.,

$$\bar{S}(x_1, \ldots, x_d) = (S(x_1), \ldots, S(x_d)) .$$

As we will later deal with more general decompositions, we need the notion of a direct sum of vector spaces. Given vector spaces $U_1, ..., U_d \subseteq \mathbb{F}_2^n$ such that $U_i \cap U_j = \{0\}$ for all $i \neq j$, we define $\bigoplus_i U_i \coloneqq \sum_i U_i$ and call $\bigoplus_i U_i$ the *direct sum* of the U_i. Recall that for every $x \in \bigoplus_i U_i$ there exist unique $x_i \in U_i$ such that $x = \sum_i x_i$.

We shall call the map (well-)defined by $x \mapsto x_i$ the *projection onto* U_i *(and along* $\bigoplus_{j \neq i} U_j$*)* and denote it by π_i^U, where $U = (U_1, ..., U_d)$. For convenience, we may also write $\pi_{l \neq i}^U$ instead of $\sum_{l \neq i} \pi_i^U$, effectively considering the direct sum of $\bigoplus_{l \neq i} U_l$ and U_i.

For a simple s-box layer, the U_i have the form $0^{(i-1)m} \times \mathbb{F}_2^m \times 0^{(d-i)m}$, meaning that they are aligned with the parallel application of d m-bit s-boxes. If we have such a canonical direct sum, and the spaces U_i are clear from the context, we may simply write π_i instead of π_i^U.

Finally, for a vector space $U \subseteq \mathbb{F}_2^n$ we denote by $U^\perp$ the *orthogonal space* of U, i.e.,

$$U^\perp = \{x \mid \langle x, u \rangle = 0 \ \forall u \in U\}.$$

3 Perfect Linear Approximations

Our main result is captured in Theorem 1 and leads to an algorithm that can exclude the existence of weak keys, i.e., keys for which there is a perfect linear approximation. We applied this algorithm to several ciphers and report the results in Table 1. For most of the ciphers, we exclude the existence of non-trivial perfect linear approximations for up to four rounds. For others, we rediscover perfect linear approximations which were previously known in the literature in an automatised fashion.

3.1 Unkeyed Permutations

We start with the rather simple case of an unkeyed permutation $E \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. Given oracle access to E, we want to decide whether there exists a non-trivial perfect linear approximation (α, β) for E, i.e., to decide whether there exist $\alpha, \beta \in \mathbb{F}_2^n \setminus \{0\}$ and a constant $c \in \mathbb{F}_2$ such that, for all $x \in \mathbb{F}_2^n$, we have $\langle \alpha, x \rangle = \langle \beta, E(x) \rangle + c$. If such a linear approximation exists, we also want to determine the masks α and β. Of course, multiple choices of (α, β) might be possible and if this is the case we might want to determine all solutions.

To find a perfect linear approximation, we can build a system of linear equations with variables α, β, c by querying E on some random choices for x. If this system has only the trivial solution, we conclude that there is no non-trivial

perfect linear approximation for E. On the other hand, a solution (α, β, c) does not necessarily imply a perfect linear approximation, unless E is queried for (almost) all $x \in \mathbb{F}_2^n$. But such false positives would imply a linear approximation with a high absolute correlation and hence would also be of cryptographic interest. Therefore, we do not analyze the possibility of false positives in detail.

Notice that this scenario is mostly interesting in the context of permutation-based cryptography. Hence, we exemplary applied this approach to the Ascon permutation [15] and, unsurprisingly, found that there is no non-trivial perfect linear approximation.

3.2 Two Rounds

We now analyse keyed permutations $E_k \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. We are interested for which (if any) keys k the permutation E_k has a non-trivial perfect linear approximation. We call such keys weak and, for given masks (α, β) we define the set of weak keys $W_E(\alpha, \beta)$ as

$$W_E(\alpha, \beta) = \{k \mid \mathrm{cor}_{E_k}(\alpha, \beta) = 1\} \cup \{k \mid \mathrm{cor}_{E_k}(\alpha, \beta) = -1\}.$$

Notice that this scenario does not only apply to block ciphers but also to cryptographic permutations again. In that case, instead of weak keys we would be interested in weak constants.

If E is (close enough to) a family of permutations drawn independently and uniformly from the set of all permutations, then applying the approach from Section 3.1 to each of those permutations is essentially the best we can do. Here, we consider permutations restricted to the form depicted in Figure 1, i.e., $E_k(x) = R_2(R_1(x) + k)$ where $R_1, R_2 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. The following lemma shows that if there is a perfect linear approximation (α, β) for E_k, then all trails in the corresponding linear hull are such that the correlation over the first permutation R_1 is the same as over the second permutation R_2 up to a sign.

Lemma 1. *Let $R_1, R_2 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be bijective and let $k \in \mathbb{F}_2^n$ be fixed. Then (α, β, c) is a perfect linear approximation for $E_k = R_2(R_1(x) + k)$ if and only if, for all $\gamma \in \mathbb{F}_2^n$, we have $cor_{R_1}(\alpha, \gamma) = (-1)^{\langle \gamma, k \rangle + c} cor_{R_2}(\gamma, \beta)$.*

Proof. Let us start with a perfect linear approximation (α, β, c), i.e.,

$$\langle \alpha, x \rangle = \langle \beta, E_k(x) \rangle + c = \langle \beta, R_2(R_1(x) + k) \rangle + c.$$

The statement follows by considering the definition of the correlation of R_1 and replacing the $\langle \alpha, x \rangle$ term with the right-hand side from above. That is, for all

$\gamma \in \mathbb{F}_2^n$ we have

$$\begin{aligned}\mathrm{cor}_{R_1}(\alpha,\gamma) &= 2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{\langle\alpha,x\rangle+\langle\gamma,R_1(x)\rangle}\\ &= 2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{\langle\beta,R_2(R_1(x)+k)\rangle+c+\langle\gamma,R_1(x)\rangle}\\ &= 2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{\langle\gamma,x+k\rangle+\langle\beta,R_2(x)\rangle+c}\\ &= (-1)^{\langle\gamma,k\rangle+c}\mathrm{cor}_{R_2}(\gamma,\beta).\end{aligned}$$

Conversely, if for all $\gamma \in \mathbb{F}_2^n$ it holds that

$$\mathrm{cor}_{R_1}(\alpha,\gamma) = (-1)^{\langle\gamma,k\rangle+c}\mathrm{cor}_{R_2}(\gamma,\beta)$$

then the claim follows by Parseval's relation (see, e.g., [9, Corollary 5]) since

$$\begin{aligned}\mathrm{cor}_{E_k}(\alpha,\beta) &= \sum_{\gamma\in\mathbb{F}_2^n}\mathrm{cor}_{R_1}(\alpha,\gamma)(-1)^{\langle\gamma,k\rangle}\mathrm{cor}_{R_2}(\gamma,\beta)\\ &= (-1)^c\cdot\sum_{\gamma\in\mathbb{F}_2^n}\mathrm{cor}_{R_1}(\alpha,\gamma)^2 = (-1)^c.\end{aligned}$$

□

From Lemma 1 it is clear that if there is a weak key for (α,β) with constant c, then the set of all weak keys $W_E(\alpha,\beta)$ is given by the solution to the linear system of equations given by $\langle\gamma,k\rangle = c + b_\gamma$ for all $\gamma \in \mathbb{F}_2^n$ such that $\mathrm{cor}_{R_1}(\alpha,\gamma) \neq 0$, where

$$b_\gamma \coloneqq \begin{cases}0 & \mathrm{cor}_{R_1}(\alpha,\gamma) = \mathrm{cor}_{R_2}(\gamma,\beta)\\ 1 & \mathrm{cor}_{R_1}(\alpha,\gamma) \neq \mathrm{cor}_{R_2}(\gamma,\beta)\end{cases}.$$

Hence, the weak keys form an affine subspace. Moreover, $W_E(\alpha,\beta)$ is closely related to the linear structures of $\langle\alpha,R_1^{-1}\rangle$ and $\langle\beta,R_2\rangle$. We record this in the following lemma.

Lemma 2. *Let $R_1, R_2 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be bijective and let $E_k(x) = R_2(R_1(x)+k)$. For a pair of input and output masks (α,β) such that $W_E(\alpha,\beta)$ is non-empty, let $k \in W_E(\alpha,\beta)$. Then, for every $u \in \mathbb{F}_2^n$, the following three statements are equivalent.*

(1) $(k+u) \in W_E(\alpha,\beta)$.
(2) u is a linear structure of $\langle\beta,R_2\rangle$.
(3) u is a linear structure of $\langle\alpha,R_1^{-1}\rangle$.

The proof is straightforward and given in Supplementary Material A.

3.3 SPNs

SPNs are arguably the most important design pattern in symmetric cryptography and hence are of special interest. Considering the special case of SPNs allows us to make exhaustive statements for up to four rounds. To illustrate this, recall our approach from Section 3.1. With this, we can, e.g., show that for the AES with some *fixed key* there is no non-trivial perfect linear approximation. In contrast to this, our approach from this section allows us to show that, e.g., for two and three rounds of AES, and for two to four rounds PRESENT there is *no weak key* at all.

We first explain our approach for two round SPNs and then show how the resulting algorithm transfers to three and in the case of AES-like ciphers also to four round SPNs. The results were already given in the introduction in Table 1. We discuss those in more detail in the corresponding paragraphs below.

Two Rounds. As an example, consider the most basic form of a two round SPN;[1] an SPN consisting of two parallel s-boxes, a key addition, a linear layer and another two parallel s-boxes as depicted in Figure 2. We are interested

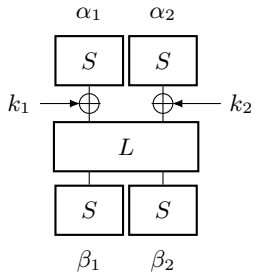

Fig. 2. A two-round SPN with two parallel s-boxes.

in perfect linear approximations $(\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2), c)$ for a weak key $k = (k_1, k_2)$. In other words, for all $x = (x_1, x_2) \in \mathbb{F}_2^n$ where n is twice the bit width of the s-box S, it holds that

$$\langle \alpha, x \rangle = \langle \beta, \bar{S}(L(\bar{S}(x) + k)) \rangle + c.$$

Now, our claim (which we prove in Theorem 1 more generally) is that the above equation implies that for all x

$$\langle \beta, \bar{S}(L((x_1, x_2))) \rangle = \langle \beta, \bar{S}(L((x_1, 0))) + \bar{S}(L((0, x_2))) + \bar{S}(L((0, 0))) \rangle$$

[1] For simplicity, we omit whitening keys and the linear layer in the final round. Adding those have no effect on the (non-)existence of perfect linear approximations.

which in turn implies an easy way to find all candidates for β by simply evaluating the equation above for some random x to build a system of linear equations. If there are no solutions $\beta \neq 0$ then there is no non-trivial perfect linear approximation. To understand why the claim holds, first notice that instead of inputs we can consider intermediate states directly after the key addition. Then, the upper part of the cipher still decomposes into two parallel s-boxes with key addition. Now the key insight is that the perfect linear approximation implies that the lower part, i.e., $\langle \beta, \bar{S} \circ L \rangle$ must also decompose into two parallel functions. We generalise this example to an arbitrary number of s-boxes in the theorem below.

Theorem 1. *Let $\bar{S}\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the parallel application of d s-boxes S and $L\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ linear. $E_k(x) = \bar{S}(L(\bar{S}(x) + k))$ has a perfect linear approximation (α, β, c) if and only if the following two assertions are both fulfilled*

1. *For all $x \in \mathbb{F}_2^n$ and for all $i \in \{1, 2, \ldots, d\}$, we have*

$$\langle \alpha_i, S^{-1}(x_i + k_i) \rangle = \langle \beta, \bar{S} \circ L(\pi_i(x)) \rangle + \sum_{\substack{j=1 \\ j \neq i}}^{d} \langle \alpha_j, S^{-1}(k_j) \rangle + c. \tag{2}$$

2. *For all $x \in \mathbb{F}_2^n$, we have*

$$\langle \beta, \bar{S} \circ L(x) \rangle = \begin{cases} \langle \beta, \sum_{i=1}^{d} (\bar{S} \circ L(\pi_i(x))) + \bar{S}(0) \rangle & d \text{ even} \\ \langle \beta, \sum_{i=1}^{d} \bar{S} \circ L(\pi_i(x)) \rangle & d \text{ odd} \end{cases}. \tag{3}$$

Proof. We start by assuming the perfect linear approximation (α, β, c) for E_k. That is, for all $x \in \mathbb{F}_2^n$, we have

$$\langle \alpha, x \rangle = \langle \beta, \bar{S} \circ L(\bar{S}(x) + k) \rangle + c,$$

and move one s-box layer and the key addition to the left-hand side:

$$\langle \alpha, \bar{S}^{-1}(x + k) \rangle = \langle \beta, \bar{S} \circ L(x) \rangle + c.$$

We make use of the fact that the s-box layer $\bar{S}$ consists of d parallel applications of the s-box S:

$$\sum_{i=1}^{d} \langle \alpha_i, S^{-1}(x_i + k_i) \rangle = \langle \beta, \bar{S} \circ L(x) \rangle + c. \tag{4}$$

Next, we consider the above equation for x with $x = \pi_i(x)$ and get, for all i,

$$\langle \alpha_i, S^{-1}(x_i + k_i) \rangle = \langle \beta, \bar{S} \circ L(\pi_i(x)) \rangle + c + \sum_{\substack{j=1 \\ j \neq i}}^{d} \langle \alpha_j, S^{-1}(k_j) \rangle. \tag{5}$$

Now we combine Equations (4) and (5) by replacing each term on the left-hand side of Equation (4) with right-hand side term from Equation (5). This yields

$$\begin{aligned}
\langle \beta, \bar{S} \circ L(x) \rangle + c &= \sum_{i=1}^{d} \left(\langle \beta, \bar{S} \circ L(\pi_i(x)) \rangle + c + \sum_{\substack{j=1 \\ j \neq i}}^{d} \langle \alpha_j, S^{-1}(k_j) \rangle \right) \\
&= \langle \beta, \sum_{i=1}^{d} \bar{S} \circ L(\pi_i(x)) \rangle + d \cdot c + (d-1) \cdot \sum_{j=1}^{d} \langle \alpha_j, S^{-1}(k_j) \rangle \\
&= \langle \beta, \sum_{i=1}^{d} \bar{S} \circ L(\pi_i(x)) \rangle + (2d-1) \cdot c + (d-1) \cdot \langle \beta, \bar{S}(0) \rangle \\
&= \begin{cases} \langle \beta, \sum_{i=1}^{d} (\bar{S} \circ L(\pi_i(x))) + \bar{S}(0) \rangle + c & d \text{ even} \\ \langle \beta, \sum_{i=1}^{d} \bar{S} \circ L(\pi_i(x)) \rangle + c & d \text{ odd} \end{cases},
\end{aligned}$$

where in the last but one step we used Eq. (4). This concludes the first part. Conversely, consider the sum of Eq. (2) over every value of i which yields

$$\begin{aligned}
\langle \alpha, \bar{S}^{-1}(x+k) \rangle &= \langle \beta, \sum_{i=1}^{d} \bar{S} \circ L(\pi_i(x)) \rangle + (d-1) \cdot \langle \alpha, \bar{S}^{-1}(k) \rangle + d \cdot c \\
&= \begin{cases} \langle \beta, \sum_{i=1}^{d} \bar{S} \circ L(\pi_i(x)) \rangle + \langle \alpha, \bar{S}^{-1}(k) \rangle & d \text{ even} \\ \langle \beta, \sum_{i=1}^{d} \bar{S} \circ L(\pi_i(x)) \rangle + c & d \text{ odd} \end{cases}.
\end{aligned}$$

Further, Eq. (2) for any i and $x = 0$ gives $\langle \alpha, \bar{S}^{-1}(k) \rangle = \langle \beta, \bar{S}(0) \rangle + c$ and hence we combine the above equation with Eq. (3) to get

$$\langle \alpha, \bar{S}^{-1}(x+k) \rangle = \langle \beta, \bar{S} \circ L(x) \rangle + c,$$

which concludes the proof. □

Notice that Theorem 1 does *not* directly lead to simple criteria for the s-box and linear layer. Instead it gives rise to efficient algorithms to find or exclude the existence of non-trivial perfect linear approximations. That is, from Theorem 1 it follows that for a perfect linear approximation (α, β) it is necessary that

$$\langle \beta, \bar{S} \circ L(x) + \sum_{i=1}^{d} \bar{S} \circ L(\pi_i(x)) \rangle = \begin{cases} \langle \beta, \bar{S}(0) \rangle & d \text{ even} \\ 0 & d \text{ odd} \end{cases}$$

holds for all $x \in \mathbb{F}_2^n$. Similar to the unkeyed case (Section 3.1), we can use this to build a system of linear equations. We record this in Algorithm 1. If there is no non-zero solution β, then we conclude that there is no non-trivial perfect linear approximation. Otherwise, we get candidate output masks which we examine further. Notice that we can apply the same algorithm to the inverse of the two-round SPN to get candidates for the input masks.

Algorithm 1 Search for perfect linear approximations for a two-round SPN

Input
E two round SPN $E\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ including the description of the s-box layer $\bar{S}$ with d parallel s-boxes and the linear layer L
Output
B list of candidates for output mask β of a perfect linear approximation
$M \leftarrow (n+5) \times n$ matrix
for $i = 1$ to $n+5$ **do**
  $x \leftarrow$ sample uniform random vector from $\mathbb{F}_2^n$
  $z \leftarrow \bar{S}(L(x))$
  for $j = 1$ to d **do**
    $z \leftarrow z + \bar{S}(L(\pi_j(x)))$
  end for
  if d even **then**
    $z \leftarrow z + \bar{S}(L(0))$
  end if
  replace i-th row of M with z
end for
return the (right) kernel of M

We applied[2] Algorithm 1 to a variety of ciphers and report the results in Table 1 together with our results on three and four rounds. We divide the results for two rounds into two groups. First, there are ciphers for which our algorithm shows that the only output mask candidate for a perfect linear approximation is $\beta = 0$, i.e., there is no non-trivial perfect linear approximation. As expected, this is the case for most of the examined ciphers.

There are also ciphers for which our automatized analysis indeed finds non-zero candidates for β. This is the case for Boomslang, CRAFT, Midori64, MANTIS[3] and SKINNY. For all of these ciphers, non-trivial perfect linear approximation over two rounds were known before. However, an automatized weak key search based on Eq. (2) reveals that some weak keys (or tweaks) were overlooked by the prior works. On closer inspection and with Lemma 2 in mind these additional findings are to no surprise as they correspond to linear structures of the s-boxes and their inverses. Hence, we omit a detailed description of those but briefly recap the prior works. Boomslang [2] was explicitly designed to contain a non-trivial perfect linear approximation. For CRAFT, the perfect linear approximations immediately follow from the representation as a Feistel cipher which was observed in [20]. For Midori64/MANTIS and SKINNY, the approximations were previously reported in [6] and [18] respectively.

Three and Four Rounds. There are two approaches to extend Algorithm 1 to three rounds. We can consider non-linear instead of linear equations or we

[2] See `https://doi.org/10.5281/zenodo.7934977`.
[3] Notice that for our analysis Midori64 and MANTIS are equivalent because their s-boxes and linear layers are identical.

can make use of superboxes. Combining both enables us to cover four rounds. The resulting variation of Theorem 1 and Algorithm 1 is rather straightforward and the key differences are given below.

First, we examine the approach based on superboxes which of course requires that the cipher has a superbox structure. Here we focus on AES-like designs. That is, the linear layer L can be represented as $L = SC \circ MC$ where MC is a mix column and SC a shuffle cells operation. With standard transformations, we write the three-round SPN as $E_k(x) = \bar{S}(L_2(\bar{Z}_{k^{(1)}}(x) + k^{(2)})))$ where $L_2 = SC \circ MC \circ SC$ and $\bar{Z}_{k^{(1)}} = \bar{S}(MC(\bar{S}(x) + k^{(1)}))$ is a keyed superbox layer. Recall Theorem 1 and notice it still applies if we replace the first s-box layer $\bar{S}$ with a keyed superbox layer $\bar{Z}_{k^{(1)}}$ and redefine π superbox-wise instead of s-box-wise.

The second approach is based on the idea of considering non-linear equations. On the one hand, this is more generic since it does not require a superbox structure but on the other hand it is computationally more demanding. Again consider a three round SPN $E_k = \bar{S}(L(\bar{S}(L(\bar{S}(x) + k^{(1)})) + k^{(2)}))$. Along the lines of Theorem 1, we first get

$$\langle \alpha, \bar{S}^{-1}(x + k^{(1)}) \rangle = \langle \beta, \bar{S}(L(\bar{S} \circ L(x)) + k^{(2)\prime}) \rangle + c$$

where $k^{(2)\prime} = L(k^{(2)})$ and then, for $H = L \circ \bar{S} \circ L$, we get that $\langle \beta, \bar{S}(H(x) + k^{(2)\prime}) \rangle$ is equal to

$$\begin{cases} \langle \beta, \sum_{i=1}^{d} (\bar{S}(H(\pi_i(x)) + k^{(2)'})) + \bar{S}(H(0) + k^{(2)\prime}) \rangle & d \text{ even} \\ \langle \beta, \sum_{i=1}^{d} \bar{S}(H(\pi_i(x)) + k^{(2)\prime}) \rangle & d \text{ odd} \end{cases}.$$

The resulting system contains non-linear equations in $k^{(2)\prime}$. But $\bar{S}$ is just the parallel application of s-boxes S, so the non-linearity corresponds to a single s-box and hence can be solved by standard techniques such as linearization, Gröbner bases or SAT solvers.

To cover four rounds, we combine both ideas from before, i.e., we consider superboxes and non-linear equations. Consider a four round SPN with superboxes Z as

$$\begin{aligned} E_k(x) &= \bar{S}(MC(\bar{S}(SC(MC(SC(\bar{S}(MC(\bar{S}(x) + k^{(1)})) + k^{(2)}))))) + k^{(3)\prime}) \\ &= \bar{S}(MC(\bar{S}(SC(MC(SC(\bar{Z}_{k^{(1)}}(x) + k^{(2)}))))) + k^{(3)\prime}). \end{aligned}$$

Then, we get $\langle \alpha, \bar{Z}^{-1}_{k^{(1)}}(x + k^{(2)}) \rangle = \langle \beta, \bar{S}(MC(\bar{S}(SC(MC(SC(x))))) + k^{(3)\prime}) \rangle + c$ and once again continue analogous to Theorem 1. But keep in mind that we swapped s-boxes for superboxes and hence redefine d to the number of superboxes and π accordingly.

We applied our algorithm for three and four rounds to the same ciphers as before (see Table 1). Some resulting systems were too complex to solve. Those are marked with $\perp$. Ciphers that are not AES-like were not tested for four rounds and hence the corresponding entries are marekd with -. Other than that, we can exlude the existence of weak keys for most ciphers either directly with the adapted versions of Algorithm 1 or with an additional weak key search based on

Eq. (2). Exceptions are four rounds of Boomslang, Midori64 and MANTIS. For those, the perfect approximation over two rounds are iterative and hence perfect for four rounds again.

4 Probability-One Differentials

In contrast to the linear case, until now, there are, to the best of our knowledge, no known non-trivial probability-one differentials over two rounds aside from trivial edge cases such as the s-boxes having maximal differential uniformity or the linear layer only working locally on one s-box. While it is easy to see that maximal differential uniformity is a condition for the s-boxes if the differential should hold for all keys (see Corollary 2), the same is not the case if it should only hold a subset of (weak) keys, as the following example will illustrate.

Example 1. Let us consider the 5-bit s-box defined by the following lookup table.

x	0x00	0x01	0x02	0x03	0x04	0x05	0x06	0x07	0x08	0x09	0x0a	0x0b	0x0c	0x0d	0x0e	0x0f
S(x)	0x1c	0x1b	0x1e	0x09	0x17	0x15	0x1d	0x04	0x19	0x00	0x08	0xa	0x0d	0x13	0x0f	0x11
x	0x10	0x11	0x12	0x13	0x14	0x15	0x16	0x17	0x18	0x19	0x1a	0x1b	0x1c	0x1d	0x1e	0x1f
S(x)	0x0c	0x12	0x0e	0x10	0x1f	0x16	0x05	0x07	0x1a	0x18	0xb	0x02	0x14	0x03	0x06	0x01

Note that S has differential uniformity 20 and linearity 24. But, together with the following linear layer L, $(\texttt{0x1d}^{\times 3}, \texttt{0x1d}^{\times 3})$ is a probability-one differential over two rounds.

$$L = \left(\begin{array}{ccccc|ccccc|ccccc}
1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
\hline
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
\hline
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0
\end{array}\right)$$

In a nutshell, this example was constructed by choosing S such that translating the input of S (resp. S^{-1}) by some constants is the same as an affine transformation A of S (resp. S^{-1}), i.e.,

$$S(x+\alpha) = A \circ S(x) \text{ and } S^{-1}(x+\alpha') = A \circ S^{-1}(x), \tag{6}$$

and choosing L such that this affine mapping A commutes with L. More details on this can be found in Supplementary Material B.1.[4]

Hence, the question arises under which conditions such a non-trivial differential with probability one can exist and whether we are able to find easy arguments to show non-existence. As we will see, conditions on the differential

[4] An implementation of this example is also provided together with the source code.

branch number of the linear layer, together with conditions on the s-boxes, e. g. non-trivial boomerang uniformity and/or all linear structures being trivial, are enough to show that no such differential can exist, see Corollaries 7 to 9.

To actually show our main result, Theorem 2, and the corresponding corollaries, we rely on recent advances on decomposing round functions into a linear and non-linear layer [19]. We will therefore provide the proof of Theorem 2 in a more abstract fashion, and later give a simpler interpretation of this result in Section 4.3.

First of all, let us take a look at some general implications of probability-one differentials by abstracting differentials as functionals. For this, we first need the definition of the graph of a function.

Definition 1 (Graph of a Function). *For two sets U, V and $F\colon U \to V$, we call*

$$\mathcal{G}_F \coloneqq \{(x, F(x)) \mid x \in U\} \subseteq U \times V$$

the graph *of F.*

It is easy to see that a function and its graph determine each other uniquely.

Then, differential cryptanalysis can be generalized to analyzing the evolution of graphs throughout the cipher E, i. e. for $(x, y) \in \mathcal{G}_F$ we consider the probability that $(E(x), E(y)) \in \mathcal{G}_G$ for two functions F and G. This has been coined *functional cryptanalysis* [5].

Definition 2 (Functional [5]). *For two finite sets U, V and $F\colon U \to U$ and $G\colon V \to V$, as well as $E\colon U \to V$, we call $F \xrightarrow[p]{E} G$ a* functional *of E of probability p if*

$$p = \frac{|\{(x, y) \in \mathcal{G}_F \mid (E(x), E(y)) \in \mathcal{G}_G\}|}{|U|}.$$

If $p = 1$, we will just write $F \xrightarrow{E} G$.

In particular any differential (α, β) over E with probability p is a functional $T_\alpha \xrightarrow[p]{E} T_\beta$. Note that we only consider the unkeyed case here, but the definition could easily be extended by simply taking the average probability over the key.

Lemma 3. *Let U, V be finite sets and $E\colon U \to V$ be bijective. Then, for any $F\colon U \to U$ and $G\colon V \to V$, the functional $F \xrightarrow{E} G$ holds (with probability one) if and only if $G = E \circ F \circ E^{-1}$.*

Proof. By definition, $F \xrightarrow{E} G$ if and only if, for any $x \in U$, the tuple $(E(x), E \circ F(x))$ is an element of the graph of G, i. e.

$$\forall x \in U\ \exists!\ y \in V\colon (E(x), E \circ F(x)) = (y, G(y)) \iff G(y) = E \circ F \circ E^{-1}(y).$$

Since E is bijective, the last equation completely defines G and therefore $G = E \circ F \circ E^{-1}$. □

In addition, any probability-one functional over multiple rounds can be seen as a trail of probability-one functionals, as the next corollary will show. But first, let us formally define a (probability-one) trail of functionals.

Definition 3 (Functional Trail (of Probability One)). *Let W_1, ..., W_{r+1} be finite sets and $H_1 \colon W_1 \to W_1$, ..., $H_{r+1} \colon W_{r+1} \to W_{r+1}$, as well as $R_1 \colon W_1 \to W_2$, $R_2 \colon W_2 \to W_3$, ..., $R_r \colon W_r \to W_{r+1}$. We call $H_1 \xrightarrow{R_1} H_2 \xrightarrow{R_2} ... \xrightarrow{R_r} H_{r+1}$ a* functional trail *(of probability one) over $R_r \circ ... \circ R_1$ if, for every $i = 1, ..., r$, $H_i \xrightarrow{R_i} H_{i+1}$ is a functional over R_i (of probability one).*

While functional trails can also be defined for probabilities of the functionals that are lower than one, one has to be careful about assuming independence of the transitions $H_i \xrightarrow{R_i} H_{i+1}$, as even the addition of independent keys would, in general, not suffice to achieve this independence. If, one the other hand, every transition happens deterministically, the whole trail has to hold deterministically.

Corollary 1. *Let U, V, W be finite sets and let $E \colon U \to W$ be bijective. Furthermore, let $F \colon U \to U$ and $H \colon W \to W$ such that $F \xrightarrow{E} H$. For any $R_1 \colon U \to V$ and $R_2 \colon V \to W$ with $E = R_2 \circ R_1$ we find a unique $G \colon V \to V$ such that $F \xrightarrow{R_1} G \xrightarrow{R_2} H$. Moreover, $G = R_1 \circ F \circ R_1^{-1} = R_2^{-1} \circ H \circ R_2$.*

Proof. We know from the previous lemma that $F \xrightarrow{E=R_2 \circ R_1} H$ is a functional with probability one if and only if

$$\begin{aligned} & R_2 \circ R_1 \circ F \circ R_1^{-1} \circ R_2^{-1} = H \\ \iff & R_1 \circ F \circ R_1^{-1} = R_2^{-1} \circ H \circ R_2. \end{aligned}$$

In addition, the lemma also tells us that $F \xrightarrow{R_1} G$ if and only if $G = R_1 \circ F \circ R_1^{-1}$, and $G \xrightarrow{R_2} H$ if and only if $H = R_2 \circ G \circ R_2^{-1}$. □

This can be iterated in case of E being the composition of more than two functions.

Remark 1. While the intuition for R_1 and R_2 should be that they represent consecutive rounds (or parts of rounds, e. g. for superboxes) of a cipher, they do not necessarily have to be, but could be any consecutive parts of a cipher such that $F \xrightarrow{R_2 \circ R_1} G$.

With this, it is easy to see that if a non-trivial probability-one differential should hold for all keys, there need to exist non-trivial probability-one differentials over R_1 and R_2 individually.

Lemma 4. *Let $F, G, R \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, R bijective, and let us define $R_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ as the map $x \mapsto R(x) + k$ for $k \in \mathbb{F}_2^n$. If $F \xrightarrow{R_k} G$ is a probability-one functional for all $k \in \mathbb{F}_2^n$, then G actually corresponds to the difference $G = T_{G(0)}$.*

Proof. Since $F \xrightarrow{R_k} G$ for all $k \in \mathbb{F}_2^n$, we know from Lemma 3 that this is equivalent to

$$F = R_k^{-1} \circ G \circ R_k$$

for all keys $k \in \mathbb{F}_2^n$. As the left-hand side is independent of k, and holds especially for zero, this gives us that, for all $x \in \mathbb{F}_2^n$,

$$\begin{aligned} & R^{-1} \circ G \circ R(x) = R_k^{-1} \circ G \circ R_k(x) = R^{-1}\left(G\left(R(x) + k\right) + k\right) \\ \iff & G(x) = G(x+k) + k. \end{aligned}$$

Hence, for $x = 0$ we get that $G(k) = k + G(0)$ holds for all $k \in \mathbb{F}_2^n$. □

Corollary 2. *Any probability-one differential over two rounds that holds for all keys is actually a trail of probability-one differentials over the individual rounds.*

In other words we rediscover that, for reasonable s-boxes, there cannot exist a non-trivial differential with probability one over two rounds that holds for all keys.

Note that the left- and right-hand side of the equation $R_1 \circ F \circ R_1^{-1} = R_2^{-1} \circ H \circ R_2$ from Corollary 1 only depend on R_1 and R_2 respectively. If R_1 is a simple s-box layer, and $F = T_\alpha$ for some α, this shows that $R_2^{-1} \circ H \circ R_2$ has in some sense to be aligned with those s-boxes. To make this more precise, we will utilize the results from [19].

4.1 Recent Results Regarding Round Function Decompositions

The basic idea of decomposing a round function into a linear and s-box layer is that we can write an s-box layer as the sum of independent functions defined by the s-boxes, i. e.

$$\begin{pmatrix} S_1(x_1) \\ S_2(x_2) \\ \vdots \\ S_d(x_d) \end{pmatrix} = \begin{pmatrix} S_1(x_1) \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ S_2(x_2) \\ \vdots \\ 0 \end{pmatrix} + \ldots + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ S_d(x_d) \end{pmatrix}.$$

Any linear layer will only change the subspaces induced by the s-boxes.

Definition 4 (Decomposition [19]). *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ bijective. Furthermore, let $U_1, \ldots, U_d$ and $V_1, \ldots, V_d$ be non-trivial[5] subspaces of $\mathbb{F}_2^n$ with $\bigoplus_i U_i = \mathbb{F}_2^n = \bigoplus_i V_i$, as well as $F_i \colon U_i \to V_i$ with*

$$F(x) = F\left(\sum_i \pi_i^U(x)\right) = \sum_i F_i \circ \pi_i^U(x).$$

We call $\{(U_i, V_i, F_i) \mid 1 \le i \le d\}$ a decomposition *of F.*

[5] More precisely, we allow the subspaces to be equal to $\mathbb{F}_2^n$ but not to be $\{0\}$.

As is shown in [19, Lemma 1], knowing the U_i is enough to recover the complete decomposition.

Lemma 5 (Induction of decomposition [19]). *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ bijective. Let further $U_1, ..., U_d$ be non-trivial subspaces of $\mathbb{F}_2^n$ with $\bigoplus_i U_i = \mathbb{F}_2^n$ and let us define $V_i \coloneqq F(U_i) + F(0)$. If the V_i are subspaces with $\bigoplus_i V_i = \mathbb{F}_2^n$ and if*

$$F = \sum_i F \circ \pi_i^U + (d+1) \cdot F(0)$$

then $D = \{(U_i, V_i, F_i) \mid 1 \leq i \leq d\}$ with $F_i \coloneqq F_{|U_i} + \pi_{l \neq i}^V \circ F(0)$ is a decomposition of F. In this case, we say that $\{U_i \mid 1 \leq i \leq d\}$ induces *the decomposition D.*

Additionally, let us recall some basic properties that are useful when working with decompositions.

Corollary 3 ([19]). *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ bijective and let $\{(U_i, V_i, F_i) \mid 1 \leq i \leq d\}$ be a decomposition of F. Then, for all i and all $x \in \mathbb{F}_2^n$, we have*

1. *$\pi_i^V \circ F = F_i \circ \pi_i^U$, and*
2. *$\Delta_{\pi_i^U(x)} F = \pi_i^V(\Delta_x F)$, and*
3. *$\Delta_{\pi_i^U(x)} F \in V_i$.*

We can also say something about the decomposition of composite functions.

Corollary 4. *Let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be bijective. Further, let $\{(U_i, V_i, F_i) \mid 1 \leq i \leq d\}$ be a decomposition of F, as well as $\{(V_i, W_i, G_i) \mid 1 \leq i \leq d\}$ be a decomposition of G. Then $\{(U_i, W_i, G_i \circ F_i) \mid 1 \leq i \leq d\}$ is a decomposition of $G \circ F$.*

Proof. Since $\{(V_i, W_i, G_i) \mid 1 \leq i \leq d\}$ is a decomposition of G, we have

$$G \circ F = \sum_i G_i \circ \pi_i^V \circ F = \sum_i G_i \circ F_i \circ \pi_i^U,$$

where the last equality follows from Corollary 3, which completes the proof. □

Finally, let us recall the implications of having two different decompositions. For this, let us recall Lemma 5 and 6, as well as Corollary 9 from [19] in condensed form.[6]

Lemma 6 ([19]). *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ bijective and let $\{(U_i, V_i, F_i) \mid 1 \leq i \leq d\}$ and $\{(W_i, X_i, G_i) \mid 1 \leq i \leq e\}$ be two decompositions of F. Then, we have that F_i is affine on $\mathrm{Im}(\pi_i^U \circ \pi_j^W \circ \pi_{l \neq i}^U)$ for every i, j. Furthermore, if it holds that $\mathrm{Im}(\pi_i^U \circ \pi_j^W \circ \pi_k^U) \neq \{0\}$ for some i, j and $k \neq i$ then*

1. *F_i has maximal differential uniformity, and*
2. *F_k has maximal linearity.*

Knowing this, we can finally move on to analysing the implications that $R_2^{-1} \circ H \circ R_2$ has two different decompositions, as implied by the probability-one differential.

[6] For convenience of the reader, we slightly reformulate them by making use of the fact that $\mathrm{Im}(\pi_i^U \circ \pi_j^W) \cap \mathrm{Im}(\pi_i^U \circ \pi_{k \neq j}^W) = \mathrm{Im}(\pi_i^U \circ \pi_j^W \circ \pi_{l \neq i}^U)$ (see [19, Corollary 8]).

4.2 Implications of Two Different Decompositions

Corollary 5. *Let $F, G, R\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be all bijective and let $\{(U_i, V_i, H_i) | 1 \leq i \leq d\}$ be a decomposition of R, as well as $F \xrightarrow{R} G$. Then $\{(U_i, U_i, F_i) | 1 \leq i \leq d\}$ is a decomposition of F if and only if $\{(V_i, V_i, G_i) | 1 \leq i \leq d\}$ is a decomposition of G, where F_i and G_i define each other by the equation $G_i = H_i \circ F_i \circ H_i^{-1}$.*

Proof. This is a direct consequence of Corollary 4 and Lemma 3. □

Remark 2. $\{(U_i, U_i, T_{\pi_i^U(\alpha)}) \mid 1 \leq i \leq d\}$ is always a decomposition of T_α (for any $\alpha \in \mathbb{F}_2^n$). Hence, for any differential (α, β) over $R_2 \circ R_1$ that holds with probability one, we can always decompose $R_1 \circ T_\alpha \circ R_1^{-1} = R_2^{-1} \circ T_\beta \circ R_2$ according to any decomposition of R_1, but also according to any decomposition of R_2.

Remark 3. Even if $\{(U_i, V_i, F_i) \mid 1 \leq i \leq d\}$ is a maximal decomposition[7] of R this does not mean that $\{(V_i, V_i, G_i) \mid 1 \leq i \leq d\}$ is a maximal decomposition of $R \circ T_\alpha \circ R^{-1}$. Trivial examples are the cases in which not all s-boxes are active, i. e. $\pi_i^U(\alpha) = 0$ for some i, as then $G_i \coloneqq F_i \circ T_{\pi_i^U(\alpha)} \circ F_i^{-1}$ is the identity and can be further decomposed.[8]

With this we can break down the question of the existence of a non-trivial probability-one differential over $R_2 \circ R_1$ into two parts.

Lemma 7. *Let $R_1, R_2\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ both be bijective. Then (α, β) is a probability-one differential over $R_2 \circ R_1$ if and only if for any decomposition $\{(U_i, V_i, H_i) \mid 1 \leq i \leq d\}$ of R_1 it holds that*

1. *$\{V_i \mid 1 \leq i \leq d\}$ induces a decomposition of $R_2^{-1} \circ T_\beta \circ R_2$, and*
2. *for any j it holds that $\left(R_1 \circ T_\alpha \circ R_1^{-1}\right)_{|V_i} = \left(R_2^{-1} \circ T_\beta \circ R_2\right)_{|V_i}$.*

Proof. Let us assume that (α, β) is a probability-one differential over $R_2 \circ R_1$, i. e. $T_\alpha \xrightarrow{R_2 \circ R_1} T_\beta$. By Corollary 1, this is equivalent to $R_1 \circ T_\alpha \circ R_1^{-1} = R_2^{-1} \circ T_\beta \circ R_2$. Hence, equality has especially to hold for any restriction. Additionally, we know that, for any decomposition $\{(U_i, V_i, H_i) \mid 1 \leq i \leq d\}$ of R_1, $\{V_i \mid 1 \leq i \leq d\}$ has to induce a decomposition of $R_1 \circ T_\alpha \circ R_1^{-1}$ and therefore of $R_2^{-1} \circ T_\beta \circ R_2$.

Now, let $\{(U_i, V_i, H_i) \mid 1 \leq i \leq d\}$ be a decomposition of R_1 such that $\{V_i \mid 1 \leq i \leq d\}$ induces a decomposition of $R_2^{-1} \circ T_\beta \circ R_2$ and for any j it holds that $\left(R_1 \circ T_\alpha \circ R_1^{-1}\right)_{|V_i} = \left(R_2^{-1} \circ T_\beta \circ R_2\right)_{|V_i}$. Since we know that $\{V_i \mid 1 \leq i \leq d\}$ also induces a decomposition of $R_1 \circ T_\alpha \circ R_1^{-1}$, we get that

$$\begin{aligned} R_1 \circ T_\alpha \circ R_1^{-1} &= \sum_i R_1 \circ T_\alpha \circ R_1^{-1} \circ \pi_i^V + (d+1) \cdot R_1 \circ T_\alpha \circ R_1^{-1}(0) \\ &= \sum_i R_2^{-1} \circ T_\beta \circ R_2 \circ \pi_i^V + (d+1) \cdot R_2^{-1} \circ T_\beta \circ R_2(0) \\ &= R_2^{-1} \circ T_\beta \circ R_2, \end{aligned}$$

[7] Intuitively, a maximal decomposition means that no s-box can be seen as the composition of two s-boxes. For a precise definition of a maximal decomposition, we refer the interested reader to [19].

[8] As long as $\dim(U_i) \neq 1$ of course, which would already mean that F_i would be affine.

where $R_1 \circ T_\alpha \circ R_1^{-1}(0) = R_2^{-1} \circ T_\beta \circ R_2(0)$ follows from the fact that $0 \in V_i$ for any choice of i. □

Note that, if α and β are both zero, those conditions are trivially true, but otherwise they may be not. We will later give a more palatable version of Condition 2, but for now, we will focus on Condition 1.

Recall that Lemma 6 tells us that, under some condition, $R_2^{-1} \circ T_\beta \circ R_2$ has maximal differential uniformity, meaning that (at least) one (first-order) derivative would be constant. This shows a direct link to the boomerang connectivity table (BCT).

Definition 5 ([10]). *Let $U, V \subseteq \mathbb{F}_2^n$ be vector spaces and $R\colon U \to V$ be bijective, then the* boomerang connectivity table (BCT) *is defined as*

$$BCT_F[\alpha, \beta] \coloneqq \left|\{x \in U | R^{-1}(R(x) + \beta) + R^{-1}(R(x + \alpha) + \beta) = \alpha\}\right|$$

for $\alpha \in U$, $\beta \in V$. Furthermore, the boomerang uniformity is defined as

$$\max_{\alpha \in U \setminus \{0\}, \beta \in V \setminus \{0\}} BCT_R[\alpha, \beta]$$

and we say that it is maximal if it is equal to $|U|$.

The following lemma makes the connection between the BCT and $R_2^{-1} \circ T_\beta \circ R_2$ having maximal differential uniformity more clear, and also provides a similar connection between $R_2^{-1} \circ T_\beta \circ R_2$ having maximal linearity and the existence of linear structures.

Lemma 8. *Let $U, V \subseteq \mathbb{F}_2^n$ be vector spaces and $R\colon U \to V$ be bijective. Then*

1. *for any $\beta \in V \setminus \{0\}$, $R^{-1} \circ T_\beta \circ R$ having maximal differential uniformity is equivalent to R having maximal boomerang uniformity (for output difference β). More precisely, $R^{-1} \circ T_\beta \circ R$ having maximal differential uniformity implies the existence of $\delta \in U \setminus \{0\}$ such that $BCT_R[\delta, \beta] = |U|$, which trivially implies $\Delta_\delta R^{-1} \circ T_\beta \circ R = \delta$, and*
2. *for any $\alpha \in U \setminus \{0\}$, $R \circ T_\alpha \circ R^{-1}$ having maximal linearity is equivalent to R having (at least) one linear structure (with difference α). More precisely, $R \circ T_\alpha \circ R^{-1}$ having maximal linearity implies the existence of $\gamma \in \mathbb{F}_2^n \setminus V^\perp$ such that $\langle \gamma, R(x) + R(x + \alpha)\rangle = c$ for any $x \in U$ and some $c \in \mathbb{F}_2$, which trivially implies $\langle \gamma, R \circ T_\alpha \circ R^{-1}(x)\rangle = \langle \gamma, x\rangle + c$ for any $x \in U$.*

Proof. First, let us assume that $R^{-1} \circ T_\beta \circ R$ has maximal differential uniformity, i. e. there exist $\delta, \hat{\delta} \in U \setminus \{0\}$ such that

$$R^{-1} \circ T_\beta \circ R(x) + R^{-1} \circ T_\beta \circ R(x + \delta) = \hat{\delta}.$$

If $\delta = \hat{\delta}$ would hold, then it would already follow that $\mathrm{BCT}_R[\delta, \beta] = |U|$. Hence, let us assume that $\delta \neq \hat{\delta}$. As $R^{-1} \circ T_\beta \circ R$ is an involution, it also holds that

$$R^{-1} \circ T_\beta \circ R(x) + R^{-1} \circ T_\beta \circ R(x + \hat{\delta}) = \delta$$

holds for all $x \in U$. Adding those two equations, and substituting x by $x + \delta$, this gives

$$R^{-1} \circ T_\beta \circ R(x) + R^{-1} \circ T_\beta \circ R(x + \delta + \hat{\delta}) = \delta + \hat{\delta}.$$

Now, let us assume that $R \circ T_\alpha \circ R^{-1}$ has maximal linearity, i. e. there exist $\gamma, \hat{\gamma} \in \mathbb{F}_2^n \setminus V^\perp$ such that, for $c = \langle \gamma, R \circ T_\alpha \circ R^{-1}(0) \rangle$, it holds that

$$\langle \gamma, R \circ T_\alpha \circ R^{-1}(x) \rangle = \langle \hat{\gamma}, x \rangle + c \; \forall x \in V.$$

Similar to above, we either have that $\hat{\gamma} = \gamma$, meaning that, by substituting x by $R(x)$

$$\langle \gamma, R(x) + R(x + \alpha) \rangle = c \; \forall x \in U,$$

or we use once more that $R \circ T_\alpha \circ R^{-1}$ is an involution and therefore

$$\langle \hat{\gamma}, R \circ T_\alpha \circ R^{-1}(x) \rangle = \langle \gamma, x \rangle + c \; \forall x \in V.$$

Hence, adding the equations leads to

$$\langle \gamma + \hat{\gamma}, R \circ T_\alpha \circ R^{-1}(x) \rangle = \langle \gamma + \hat{\gamma}, x \rangle \; \forall x \in V,$$

which completes the proof. □

With this, we can state our main result for the differential setting, of which we will provide a more digestible version in Corollary 6.

Theorem 2. *Let $R_1, R_2 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ all be bijective. Furthermore, let $\{U_1, U_2\}$ induce a decomposition of R_1^{-1} and let $\{(W_i, X_i, G_i) \mid 1 \leq i \leq e\}$ be a decomposition of R_2. Then (α, β) being a probability-one differential over $R_2 \circ R_1$ has the following implications (for any i).*

1. *If it holds that $\mathrm{Im}(\pi_i^W \circ \pi_1^U \circ \pi_{k \neq i}^W) = \{0\}$, and also $1 \leq \dim(W_i \cap U_1) \leq 2$, as well as $\pi_i^X(\beta) \neq 0$, then it has to hold that*
   (a) *$BCT_{G_i}[\delta, \pi_i^X(\beta)]$ is maximal for some $\delta \in (W_i \cap U_1) \setminus \{0\}$, and*
   (b) *$(\gamma, \pi_j^X(\beta), \langle \gamma, G_j^{-1} \circ T_{\pi_j^X(\beta)} \circ G_j(0) \rangle)$ is a non-trivial linear structure of G_i^{-1} for some $\gamma \in (W_{k \neq i} \oplus (W_i \cap U_2))^\perp \setminus \{0\}$.*

   If $\dim(W_i \cap U_1) = 1$, then δ and γ are unique.
2. *If it holds that $\mathrm{Im}(\pi_i^W \circ \pi_1^U \circ \pi_k^W) \neq \{0\}$ for some $k \neq i$ then it holds that*
   (a) *$\pi_i^X(\beta) = 0$ or $BCT_{G_i}[\delta, \pi_i^X(\beta)]$ is maximal for some $\delta \in W_i$, and*
   (b) *$\pi_k^X(\beta) = 0$ or $(\gamma, \pi_k^X(\beta), c)$ is a non-trivial linear structure of G_k^{-1} for some some $\gamma \in \mathbb{F}_2^n \setminus W_k^\perp$ and $c = \langle \gamma, G_k^{-1}(0) + G_k^{-1}(\pi_k^X(\beta)) \rangle$.*
3. *If it holds that $\mathrm{Im}(\pi_i^W \circ \pi_1^U \circ \pi_{k \neq i}^W) = W_i$ then the map $G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i$ is affine.*

Note that those implications are trivial if $\beta = 0$, but they can be quite strong for non-trivial probability-one differentials. Before we can prove this, we need the following lemma.

Lemma 9. *Let $U_1, U_2, W_1, W_2 \subseteq \mathbb{F}_2^n$ be subspaces with $U_1 \oplus U_2 = \mathbb{F}_2^n = W_1 \oplus W_2$. Then it holds that $\pi_1^W \circ \pi_1^U \circ \pi_2^W = 0$ if any only if $(W_1 \cap U_1) \oplus (W_1 \cap U_2) = W_1$.*

Proof. First, let us assume that $(W_1 \cap U_1) \oplus (W_1 \cap U_2) = W_1$. This means that we are able to find a basis $b_1, ..., b_n$ of $\mathbb{F}_2^n$ such that $\{b_1, ..., b_n\}$ contains a basis of U_1, W_1 and W_2. Since $\pi_1^W \circ \pi_1^U \circ \pi_2^W$ is a composition of linear functions and therefore linear, we will show that every basis vector b_l is mapped to 0. Let us start with looking at $\pi_2^W(b_l)$. We either have $b_l \in W_2$, and therefore $\pi_2^W(b_l) = b_l$, or $\pi_2^W(b_l)$ is already zero. Hence, let us assume that $b_l \in W_2$. Moving to π_1^U, we once more have that either $b_l \in U_1$, thus $\pi_1^U(b_l) = b_l$, or $\pi_1^U(b_l) = 0$. Again, let us assume that $b_l \in U_1$. But then we know that $\pi_1^W(b_l) = 0$, as $b_l \in W_2$ by assumption.

Now, let us assume that $\pi_1^W \circ \pi_1^U \circ \pi_2^W = 0$. According to [19, Corollary 8] this is equivalent to $\mathrm{Im}(\pi_1^W \circ \pi_1^U) \cap \mathrm{Im}(\pi_1^W \circ \pi_2^U) = \{0\}$. Hence, by [19, Corollary 7], $\pi_1^W \circ \pi_1^U = \pi_1^U \circ \pi_1^W$ and $\pi_1^W \circ \pi_2^U = \pi_2^U \circ \pi_1^W$. Similar to how it was done in the proof of [19, Lemma 3], this means that $\mathrm{Im}(\pi_1^W \circ \pi_1^U) = W_1 \cap U_1$ and $\mathrm{Im}(\pi_1^W \circ \pi_2^U) = W_1 \cap U_2$. Hence, $(W_1 \cap U_1) \oplus (W_1 \cap U_2) = W_1$. □

Proof of Theorem 2. Let us start with showing Item 2, i. e. let us assume that $\mathrm{Im}(\pi_i^W \circ \pi_1^U \circ \pi_k^W) \neq \{0\}$ for some $k \neq i$. From Lemma 6 we know that $G_i^{-1} \circ T_{\pi_i^W(\beta)} \circ G_i$ has maximal differential uniformity and $G_k^{-1} \circ T_{\pi_k^W(\beta)} \circ G_k$ has maximal linearity. Hence, the claim follows from Lemma 8.

Next, let us show Item 3, i. e. let us assume that $\mathrm{Im}(\pi_i^W \circ \pi_1^U \circ \pi_{k\neq i}^W) = W_i$. Then it directly follows from Lemma 6 that $G_i^{-1} \circ T_{\pi_i^W(\beta)} \circ G_i$ is affine on $\mathrm{Im}(\pi_i^W \circ \pi_1^U \circ \pi_{k\neq i}^W) = W_i$.

Finally, let us show Item 1, i. e. let us assume that $\mathrm{Im}(\pi_i^W \circ \pi_1^U \circ \pi_{k\neq i}^W) = \{0\}$ holds. By the previous lemma, we know that this is equivalent to $(W_i \cap U_1) \oplus (W_i \cap U_2) = W_i$. Note that, by Corollary 3, for any $w \in W_i$ we have that $\Delta_w R_2^{-1} \circ T_\beta \circ R_2(0) \in W_i$, and for any $v \in W_{k\neq i}$ we have $\Delta_v R_2^{-1} \circ T_\beta \circ R_2(0) \in W_{k\neq i}$. Also, by Corollary 1, for any $u \in U_1$ we have that

$$\Delta_u R_2^{-1} \circ T_\beta \circ R_2(0) = \Delta_u R_1 \circ T_\alpha \circ R_1^{-1}(0) \in U_1.$$

Hence, for any $x \in W_i \cap U_1$ we get that $\Delta_x R_2^{-1} \circ T_\beta \circ R_2(0) \in W_i \cap U_1$. Similar, for any $y \in W_i \cap U_2$ we get $\Delta_y R_2^{-1} \circ T_\beta \circ R_2(0) \in W_i \cap U_2$. Additionally, we know from [19, Lemma 4] that $\{W_{k\neq i}, W_i \cap U_1, W_i \cap U_2\}$ induces a decomposition of $R_2^{-1} \circ T_\beta \circ R_2$, i. e. if we denote the corresponding projections onto $W_i \cap U_1$ and $W_i \cap U_2$ by τ_1 and τ_2 respectively we get

$$\Delta_z R_2^{-1} \circ T_\beta \circ R_2(0) = \Delta_{\pi_{k\neq i}^W(z)} R_2^{-1} \circ T_\beta \circ R_2(0) + \sum_{j=1,2} \Delta_{\tau_j(z)} R_2^{-1} \circ T_\beta \circ R_2(0).$$

Those observations now implies that, for any $z \in \mathbb{F}_2^n$ and any j,

$$\tau_j \left(\Delta_z R_2^{-1} \circ T_\beta \circ R_2(0) \right) = \Delta_{\tau_j(z)} R_2^{-1} \circ T_\beta \circ R_2(0).$$

Moreover, by Corollary 3, for any $w \in W_i$, we have that $\Delta_w R_2^{-1} \circ T_\beta \circ R_2(0) = \Delta_w G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0)$, which means that, for any $w \in W_i$ and any j, we can

rewrite the equation above to

$$\tau_j\left(\Delta_w G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0)\right) = \Delta_{\tau_j(w)} G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0).$$

Now, let us assume that $\dim(W_i \cap U_1) \leq 2$. We know that the map $M\colon W_i \cap U_1 \to W_i \cap U_1$ defined by $x \mapsto \Delta_x G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0)$ is a bijection, and $M(0) = 0$. Together, this implies that this function must have algebraic degree one, and therefore has to be linear. But this means that, for any $w \in W_i$, we get that

$$\begin{aligned}\Delta_w G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0) &= \sum_{j=1,2} \Delta_{\tau_j(w)} G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0) \\ &= \Delta_{\tau_2(w)} G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0) + M \circ \tau_1(w).\end{aligned}$$

Hence, it is easy to see that for any $\delta \in (W_i \cap U_1) \setminus \{0\}$ the differential $(\delta, M(\delta))$ over $G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i$ holds with probability one, since $\tau_2(\delta) = 0$. Therefore, similar to the proof of Lemma 6, we either get $\delta = M(\delta)$, i. e. $\mathrm{BCT}_{G_i}[\delta, \pi_i^X(\beta)]$ is maximal, or we use that $G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i$ is an involution and get that $\mathrm{BCT}_{G_i}[\delta', \pi_i^X(\beta)]$ is maximal with $\delta' = M(\delta) + \delta \in (W_i \cap U_1) \setminus \{0\}$. Additionally, we know that, for any $w \in W_i$ and any $\hat{\gamma} \in (W_{k \neq i} \oplus (W_i \cap U_2))^\perp \setminus \{0\}$,

$$\begin{aligned}\langle \hat{\gamma}, \Delta_w G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0)\rangle &= \langle \hat{\gamma}, \Delta_{\tau_2(w)} G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0)\rangle + \langle \hat{\gamma}, M \circ \tau_1(w)\rangle \\ &= \langle \hat{\gamma}, M \circ \tau_1(w)\rangle = \langle (M \circ \tau_1)^T(\hat{\gamma}), w\rangle,\end{aligned}$$

as $\Delta_{\tau_2(w)} G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0) \in W_i \cap U_2$. Again, similar to the proof of Lemma 6, we either get $\hat{\gamma} = (M \circ \tau_1)^T(\hat{\gamma})$, or we consider $\gamma' = (M \circ \tau_1)^T(\hat{\gamma}) + \hat{\gamma} \in (W_{k \neq i} \oplus (W_i \cap U_2))^\perp \setminus \{0\}$. Hence, we know that, for some $\gamma \in (W_{k \neq i} \oplus (W_i \cap U_2))^\perp \setminus \{0\}$ and any $w \in W_i$,

$$\langle \gamma, G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(w)\rangle = \langle \gamma, w\rangle + \langle \gamma, G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i(0)\rangle,$$

and substituting w by $G_i^{-1}(w)$ completes the proof. □

Note that, by Lemma 8, $G_i^{-1} \circ T_{\pi_i^X(\beta)} \circ G_i$ being affine implies that G_i has maximal boomerang uniformity and G_i^{-1} has (at least) one linear structure. But it even implies more.

Lemma 10. *Let $U, V \subseteq \mathbb{F}_2^n$ be vector spaces and $R\colon U \to V$ be bijective. Furthermore, let $\beta \in V \setminus \{0\}$ such that $R^{-1} \circ T_\beta \circ R$ is affine and let $\alpha := R^{-1} \circ T_\beta \circ R(0)$, i. e. $L\colon U \to U$ with $L := R^{-1} \circ T_\beta \circ R + \alpha$ is linear. Then it holds that*

1. *(α, β) is a differential with probability $2^{-\dim(\mathrm{Im}(L+I))} \geq 2^{-\dim(U)/2}$ over R, where I denotes the identity, and*
2. *$BCT_R[\delta, \beta] \in \{0, |U|\}$ for all $\delta \in U$, and*
3. *$(\gamma, \beta, \langle \gamma, \alpha\rangle)$ is either a linear structure of R^{-1} or $cor_{R^{-1}+R^{-1}\circ T_\beta}(0, \gamma) = 0$.*

Proof. Let us start with the first statement. By the definition of L, we have, for all $x \in U$,

$$R^{-1} \circ T_\beta \circ R(x) + x + \alpha = (L + I) \cdot x,$$

which in turn means that

$$R^{-1}(x + \beta) + R^{-1}(x) + \alpha = (L + I) \cdot R^{-1}(x)$$

holds for all $x \in V$. In other words, $R^{-1}(x) + R^{-1}(x + \beta) = \alpha$ holds if and only if $R^{-1}(x) \in \ker(L + I)$. In addition, it is well known that $\dim(U) = \dim(\ker(I + L)) + \dim(\mathrm{Im}(I + L))$. Hence, (β, α) is a differential with probability $2^{\dim(\ker(L+I))-\dim(U)} = 2^{-\dim(\mathrm{Im}(L+I))}$ over R^{-1}, meaning that (α, β) is a differential with the same probability over R. In addition, it holds that $(I + L)^2 = I + L^2 = 0$ as L has to be an involution, i. e. $\mathrm{Im}(I + L) \subseteq \ker(I + L)$. Hence, $\dim(U) \geq 2 \cdot \dim(\mathrm{Im}(I + L))$, or equivalent $\dim(\mathrm{Im}(I + L)) \leq \frac{\dim(U)}{2}$.

Now, let us prove the second statement. Since $R^{-1} \circ T_\beta \circ R$ is affine, any derivative is constant and the equation $R^{-1} \circ T_\beta \circ R(x) + R^{-1} \circ T_\beta \circ R(x + \delta) = \delta$ is either fulfilled by every or no $x \in U$.

The last statement directly follows from

$$\begin{aligned}
2^{\dim(V)} \cdot \mathrm{cor}_{R^{-1}+R^{-1}\circ T_\beta}(0, \gamma) &= \sum_{x \in V} (-1)^{\langle \gamma, R^{-1}(x) + R^{-1} \circ T_\beta(x) \rangle} \\
&= \sum_{x \in V} (-1)^{\langle \gamma, R^{-1}(x) + L \circ R^{-1}(x) + \alpha \rangle} \\
&= (-1)^{\langle \gamma, \alpha \rangle} \sum_{x \in V} (-1)^{\langle (I+L)^T \cdot \gamma, R^{-1}(x) \rangle} \\
&= (-1)^{\langle \gamma, \alpha \rangle} \sum_{y \in U} (-1)^{\langle (I+L)^T \cdot \gamma, y \rangle} \\
&= \begin{cases} (-1)^{\langle \gamma, \alpha \rangle} \cdot 2^{\dim(U)} & \text{if } \gamma \in \ker\left((I + L)^T\right) \\ 0 & \text{if } \gamma \notin \ker\left((I + L)^T\right) \end{cases}
\end{aligned}$$

and the fact that $\dim(U) = \dim(V)$ as R is bijective. □

Next, we will provide more intuition on the result presented above and also give some easy to check conditions that allow to prove the non-existence of probability-one differentials over multiple rounds no matter the key. To make the arguments more easily applicable to standard descriptions of symmetric primitives, we will represent R_1 and R_2 each as an SPN round function in the remainder of this section.

4.3 A Less Technical Interpretation

Remember that a decomposition just means that we can write the functions R_1 (resp. R_2) as the composition of linear layer L_1' (resp. L_2), the parallel application of s-boxes N_1 (resp. N_2) and another linear layer L_1 (resp. L_2'), i. e. $R_1 = L_1 \circ$

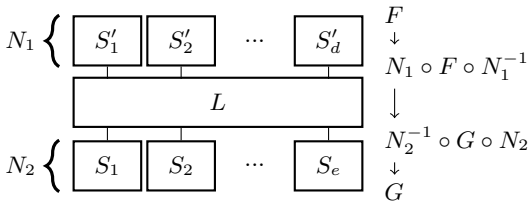

Fig. 3. Probability-one functional trail over a two round SPN

$N_1 \circ L'_1$ and $R_2 = L'_2 \circ N_2 \circ L_2$. Since the existence of a probability-one differential over $R_2 \circ R_1$ is invariant under linear transformations, we can, without loss of generality, assume that L'_1 and L'_2 are the identity. Also, we can see $L_2 \circ L_1$ as one linear layer L, meaning that we look at $N_2 \circ L \circ N_1$ instead of $R_2 \circ R_1$. Figure 3 shows this well known view of such a two round SPN. Here, we write $N_1 = S'_1 \times S'_2 \times ... \times S'_d$ and $N_2 = S_1 \times S_2 \times ... \times S_e$ where $S'_i \colon \mathbb{F}_2^{m'_i} \to \mathbb{F}_2^{m'_i}$ and $S_i \colon \mathbb{F}_2^{m_i} \to \mathbb{F}_2^{m_i}$, i. e. if we define $U_i \coloneqq 0^{\sum_{l<i} m'_l} \times \mathbb{F}_2^{m'_i} \times 0^{\sum_{l>i} m'_l}$ then $\{(U_i, U_i, 0^{\sum_{l<i} m'_l} \times S'_i \times 0^{\sum_{l>i} m'_l}) \mid 1 \leq i \leq d\}$ is a decomposition of N_1, and if we define $W_i \coloneqq 0^{\sum_{l<i} m_l} \times \mathbb{F}_2^{m_i} \times 0^{\sum_{l>i} m_l}$ then $\{(W_i, W_i, 0^{\sum_{l<i} m_l} \times S_i \times 0^{\sum_{l>i} m_l}) \mid 1 \leq i \leq e\}$ is a decomposition of N_2.

Let us assume that there exist $F, G \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $F \xrightarrow{N_2 \circ L \circ N_1} G$. We know from Corollary 1 that there exists an unique trail

$$F \xrightarrow{N_1} N_1 \circ F \circ N_1^{-1} \xrightarrow{L} N_2^{-1} \circ G \circ N_2 \xrightarrow{N_2} G,$$

and we know that the probability-one functional over L is equivalent to

$$N_2^{-1} \circ G \circ N_2 = L \circ N_1 \circ F \circ N_1^{-1} \circ L^{-1}. \tag{7}$$

If we assume that $\{W_i \mid 1 \leq i \leq e\}$ induces a decomposition of G (as it is the case for any translation by an output difference), then we know from Corollary 4 that $\{W_i \mid 1 \leq i \leq e\}$ also induces a decomposition of $N_2^{-1} \circ G \circ N_2$. Similar, assuming that $\{U_i \mid 1 \leq i \leq d\}$ induces a decomposition of F (as it is the case for any translation by an input difference), we know that $\{U_i \mid 1 \leq i \leq d\}$ induces a decomposition of $N_1 \circ F \circ N_1^{-1}$. Note that, by construction, the input and output spaces are identical for each of the two decompositions.

With that, we would like to give an alternative version of Theorem 2 that is plainly based on the linear layer L and the s-boxes of N_2. For this, let us recall how bijective affine transformations impact a decomposition.

Lemma 11 (Lemma 2 of [19]). *Let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be bijective and affine equivalent, i. e. $F = A \circ G\,(B + b) + a$ for invertible matrices $A, B \in \mathbb{F}_2^{n \times n}$ and constants $a, b \in \mathbb{F}_2^n$. Then $\{U_i | 1 \leq i \leq d\}$ induces a decomposition of F if and only if $\{B \cdot U_i | 1 \leq i \leq d\}$ induces a decomposition of G.*

Hence, $\{U_i \mid 1 \leq i \leq d\}$ inducing a decomposition of $N_1 \circ F \circ N_1^{-1}$ means that $\{L(U_i) \mid 1 \leq i \leq d\}$ induces a decomposition of $N_2^{-1} \circ G \circ N_2$, and that the corresponding projections onto $L(U_i)$ are $L \circ \pi_i^U \circ L^{-1}$. With that, we can reduce the properties imposed on compositions of the projections to ones imposed on the linear layer L. For this, let us write L and L^{-1} (or more precisely their matrix representation with respect to the standard basis) as block matrices, where the blocks are aligned with the s-boxes in N_1 and N_2, i. e.

$$L = \begin{pmatrix} L_{1,1} & \dots & L_{1,d} \\ \vdots & & \vdots \\ L_{e,1} & \dots & L_{e,d} \end{pmatrix} \text{ and } L^{-1} = \begin{pmatrix} \left(L^{-1}\right)_{1,1} & \dots & \left(L^{-1}\right)_{1,e} \\ \vdots & & \vdots \\ \left(L^{-1}\right)_{d,1} & \dots & \left(L^{-1}\right)_{d,e} \end{pmatrix}.$$

With that, the blocks of L and L^{-1} composed with the projections π_i^W and π_j^U are

$$\left(\pi_i^W \circ L \circ \pi_j^U\right)_{a,b} = \begin{cases} L_{i,j} & \text{if } (a,b) = (i,j) \\ 0 & \text{else} \end{cases}$$

and

$$\left(\pi_j^U \circ L^{-1} \circ \pi_l^W\right)_{a,b} = \begin{cases} \left(L^{-1}\right)_{j,l} & \text{if } (a,b) = (i,j) \\ 0 & \text{else} \end{cases}.$$

Hence,

$$\begin{aligned} &\left(\pi_i^W \circ L \circ \pi_j^U \circ L^{-1} \circ \pi_{l \neq i}^W\right)_{a,b} \\ &= \left(\sum_{l \neq i} \left(\pi_i^W \circ L \circ \pi_j^U\right) \circ \left(\pi_j^U \circ L^{-1} \circ \pi_l^W\right)\right)_{a,b} \\ &= \begin{cases} L_{i,j} \cdot \left(L^{-1}\right)_{j,b} & \text{if } a = i \text{ and } b \neq i \\ 0 & \text{else} \end{cases}. \end{aligned}$$

For convenience, let us denote row j of L^{-1} without block $\left(L^{-1}\right)_{j,i}$ by $\left(L^{-1}\right)_{j,l \neq i}$. Then our observations above mean that

1. $\mathrm{Im}(\pi_i^W \circ L \circ \pi_j^U \circ L^{-1} \circ \pi_{l \neq i}^W) = 0 \iff \forall l \neq i \colon L_{i,j} \cdot \left(L^{-1}\right)_{j,l} = 0$,
2. $\mathrm{Im}(\pi_i^W \circ L \circ \pi_j^U \circ L^{-1} \circ \pi_k^W) \neq 0 \iff L_{i,j} \cdot \left(L^{-1}\right)_{j,k} \neq 0$,
3. $\mathrm{Im}(\pi_i^W \circ L \circ \pi_j^U \circ L^{-1} \circ \pi_{l \neq i}^W) = W_i \iff L_{i,j} \cdot \left(L^{-1}\right)_{j,l \neq i}$ has full rank.

With that, we can reformulate Theorem 2 into the following corollary.

Corollary 6. *Let $N_1, N_2, L \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be as above. Then the existence of a probability-one differential $((\alpha_1, \dots, \alpha_d), (\beta_1, \dots, \beta_e))$ over $N_2 \circ L \circ N_1$ has the following implications (for any pair i, j).*

1. *If it holds that $L_{i,j} \cdot \left(L^{-1}\right)_{j,k \neq i} = 0$, and also $1 \leq \mathrm{rank}(L_{i,j}) \leq 2$, as well as $\beta_i \neq 0$, then it has to hold that*

   (a) $BCT_{S_i}[\delta, \beta_i]$ *is maximal for some* $\delta \in \mathrm{Im}(L_{i,j}) \setminus \{0\}$, *and*
   (b) $(\gamma, \beta_i, \langle \gamma, S_i^{-1} \circ T_{\beta_i} \circ S_i(0)) \rangle$ *is a linear structure of* S_i^{-1} *for some* $\gamma \in \ker\left((L_{i,k\neq j})^T\right) \setminus \{0\}$.

   If $\mathrm{rank}(L_{i,j}) = 1$, *then* δ *and* γ *are unique.*
2. *If it holds that* $L_{i,j} \cdot \left(L^{-1}\right)_{j,k} \neq 0$ *for some* $k \neq i$ *then it holds that*
   (a) $\beta_i = 0$ *or* $BCT_{S_i}[\delta, \beta_i]$ *is maximal for some* $\delta \in \mathbb{F}_2^{m_i}$, *and*
   (b) $\beta_k = 0$ *or* (γ, β_k, c) *is a linear structure of* S_i^{-1} *for some* $\gamma \in \mathbb{F}_2^{m_k}$ *and* $c = \langle \gamma, S_i^{-1}(0) + S_i^{-1}(\beta_k) \rangle$.
3. *If it holds that* $L_{i,j} \cdot \left(L^{-1}\right)_{j,k\neq i}$ *has full rank, then the map* $x \in \mathbb{F}_2^{m_i} \mapsto S_i^{-1}(S_i(x) + \beta_i)$ *is affine.*

Remark 4. Note that we do not make any assumptions about the s-boxes in N_1 other than the spaces U_i that they define. Hence, we can see any key/constant addition that happens right before (or right after) the linear layer as part of the s-boxes of N_1, as a simple translation does not affect those spaces.

Now, let us assume that all s-boxes are of equal size m, i. e. $m = m_i = m'_j$ for any i, j, as it is usually the case. Then we can argue based on the differential branch number of L.

Definition 6 (Differential Branch Number [12]). *Let* $w\colon (\mathbb{F}_2^m)^d \to \mathbb{N}$ *map a vector* $\begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}$ *to the number of non-zero coordinates* x_i. *For a linear map* $L\colon (\mathbb{F}_2^m)^d \to (\mathbb{F}_2^m)^d$ *the* differential branch number of L (over $\mathbb{F}_2^m$) *is defined as*

$$\mathcal{B}_d(L) \coloneqq \min_{x \neq 0} \left(w(x) + w(L(x))\right).$$

Let us also recall [1, Lemma 1].

Lemma 12 ([1]). *Let* L *be a* $dm \times dm$ *matrix, decomposed into* $m \times m$ *submatrices* $L_{i,j}$ *as above. Then* L *has differential branch number* b *(over* $\mathbb{F}_2^m$*) if and only if all* $i \times (d-b+i+1)$ *block submatrices of* L *have full rank for* $1 \leq i < b-1$. *Moreover,* L *has linear branch number* b *if and only if all* $(d-b+i-1) \times i$ *block submatrices of* L *have full rank for* $1 \leq i < b-1$.

If the differential branch number of L is at least 3, then Corollary 6 implies the following two corollaries.

Corollary 7. *Let us assume that* L *has differential branch number of at least* 3 *and every row of* L *has a block of full rank. If every s-box* $S\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$ *of the second non-linear layer has*

1. *differential uniformity smaller than* $2^{-m/2}$, *or*
2. *no column in the BCT such that each entry is either zero or* 2^m, *or*
3. *no linear structure* (γ, β, c) *such that* $cor_{S^{-1}+S^{-1}\circ T_\beta}(0, \gamma') \in \{-1, 0, 1\}$

then there cannot exist any non-trivial probability-one differential over two rounds.

Proof. Let us fix i. As L, and therefore L^{-1}, has differential branch number of at least 3, we know from the previous lemma that for any j the submatrix $\left(L^{-1}\right)_{j,l\neq i}$ has full rank. Hence, $L_{i,j} \cdot \left(L^{-1}\right)_{j,l\neq i}$ has full rank if and only if $L_{i,j}$ has full rank. By assumption, we know that for every i there exists a j such that $L_{i,j}$ has full rank, which means that we can apply Item 3 of Corollary 6, which, together with Lemma 10, completes the proof. □

Table 1 gives examples where this corollary can be used to directly show that there cannot exist a non-trivial probability-one differential, not matter the key.

Corollary 8. *If L has differential branch number of at least 3 and if the s-boxes of the second non-linear layer either all do not have*

1. *maximal boomerang uniformity, or*
2. *linear structures*

then there cannot exist any non-trivial probability-one differential over two rounds.

Proof. Let i and $l \neq i$ be arbitrary. Since L has differential branch number of at least 3, we know from the lemma above that, for any k, the matrices $L_{i,j\neq k}$ and $\left(L^{-1}\right)_{j\neq k,l}$ both have full rank, which means that

$$L_{i,j\neq k} \cdot \left(L^{-1}\right)_{j\neq k,l} = \sum_{j\neq k} L_{i,j} \cdot \left(L^{-1}\right)_{j,l}$$

must have full rank. But this implies that there exists a j such that $L_{i,j} \cdot \left(L^{-1}\right)_{j,l} \neq 0$, which means that we can apply Item 2 of Corollary 6. If now all s-boxes do not have maximal differential uniformity, we get that the output difference must be zero, i. e. there does not exist a probability-one differential over two rounds. Similar, if all s-boxes do not have linear structures, there also cannot exist a probability-one differential over two rounds. □

Examples of ciphers covered by this corollary are once more given in Table 1. We also get the following corollary.

Corollary 9. *If L is a bit-permutation that maps every output bit of one s-box to a different s-box and if each s-box of the second non-linear layer does not have maximal differential uniformity, then there cannot exist any non-trivial probability-one differential over two rounds.*

Proof. L being a bit-permutation means that its rows and columns are permutations of the standard basis. Together with the fact that L maps every output bit of one s-box to a different s-box this means that $\text{rank}(L_{i,j})$ is either zero or one. Every rank one block now must itself contain a vector of the standard basis (but of $\mathbb{F}_2^m$ instead of $\mathbb{F}_2^{dm}$), which means that the only non-zero elements in the images of the $L_{i,j}$ are standard basis vectors. Note that, as each row of L must have full rank, we actually get the complete standard basis. Hence, if we apply

Item 1 of Corollary 6, we get that there exists a β such that for any s-box S and any i, $\mathrm{BCT}_S[e_i, \beta]$ is maximal, i. e.

$$S^{-1} \circ T_\beta \circ S(x) + S^{-1} \circ T_\beta \circ S(x + e_i) = e_i \ \forall x \in \mathbb{F}_2^m, i.$$

It is now easy to see that, by adding such equations, we get that

$$S^{-1} \circ T_\beta \circ S(x) + S^{-1} \circ T_\beta \circ S(x + y) = y \ \forall x, y \in \mathbb{F}_2^m.$$

By fixing $x = 0$, this gives us

$$\begin{aligned} & S^{-1} \circ T_\beta \circ S(y) + y = S^{-1} \circ T_\beta \circ S(0) \ \forall y \in \mathbb{F}_2^m \\ \iff & S^{-1}(y + \beta) + S^{-1}(y) = S^{-1} \circ T_\beta \circ S(0) \ \forall y \in \mathbb{F}_2^m. \end{aligned}$$

In other words, if $\beta \neq 0$, $(\beta, S^{-1} \circ T_\beta \circ S(0))$ would be a probability-one differential over S^{-1}, meaning that S^{-1}, and therefore S would have maximal differential uniformity, which would be a contradiction to our assumption □

Examples where this corollary is applicable are PRESENT and GIFT, see Table 1.

While Corollaries 7 to 9 already cover a large variety of ciphers, there still exist some, like CRAFT, PRIDE and SKINNY, that are not already covered. For CRAFT and SKINNY, there exist some cells of the output that each only depend on a single cell of the input. As Theorem 2 is based on having two different decompositions, but as one cell of the output depending on only one input-cell means that parts of the two decompositions are identical, it is only reasonable that this theorem cannot directly be used to restrict the output differences for this cell. Still, Theorem 2 can be used to restrict the input and output differences that could potentially lead to a non-trivial probability-one differential to the ones depicted in Table 2 (more details, in addition to an algorithmic interpretation of Theorem 2,[9] are given in Supplementary Material B.2). In order to show that none of those candidates yield a probability-one differential, we can get additional conditions based on the second item of Lemma 7.

Corollary 10. *Let $N_1, N_2, L \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be as above. If $((\alpha_1, ..., \alpha_d), (\beta_1, ..., \beta_e))$ is a probability-one differential over $N_2 \circ L \circ N_1$ then it has to hold that*

$$L_{i,j} \cdot S'_j \left(\left(S'_j\right)^{-1}(x) + \alpha_j \right) + \sum_{k \neq j} L_{i,k} \cdot S'_k \left(\left(S'_k\right)^{-1}(0) + \alpha_k \right) = S_i^{-1} \left(S\left(L_{i,j} \cdot x\right) + \beta_i \right)$$

for any i, j and any $x \in \mathbb{F}_2^m$.

Proof. From Lemma 7 we know that, for any j, $\left(N_1 \circ T_{(\alpha_1,...,\alpha_d)} \circ N_1^{-1}\right)_{U_j} = \left(L^{-1} \circ N_2^{-1} \circ T \circ N_2 \circ L\right)_{U_j}$. If we multiply from the left by L this means that, for any i,

$$L_{i,j} \cdot S'_j \left(\left(S'_j\right)^{-1}(x) + \alpha_j \right) + \sum_{k \neq j} L_{i,k} \cdot S'_k \left(\left(S'_k\right)^{-1}(0) + \alpha_k \right) = S_i^{-1} \left(S\left(L_{i,j} \cdot x\right) + \beta_i \right).$$

□

[9] This algorithmic version of Theorem 2 is also part of the provided source code.

Table 2. In-/output difference candidates (by Theorem 2).

Cipher	Input Differences	Output Differences	Prob. One Differentials
CRAFT	$0^4 \times 0^4 \times \mathbb{F}_2^4 \times \mathbb{F}_2^4$	$0^4 \times 0^4 \times \mathbb{F}_2^4 \times \mathbb{F}_2^4$	None
PRIDE	$\{\texttt{0x0}, \texttt{0x1}, \texttt{0x8}\}^{16}$	$\{\texttt{0x0}, \texttt{0x1}, \texttt{0x8}\}^{16}$	None
SKINNY-64	$\mathbb{F}_2^4 \times 0^4 \times 0^4 \times 0^4$	$0^4 \times \mathbb{F}_2^4 \times 0^4 \times 0^4$	None
SKINNY-128	$\mathbb{F}_2^8 \times 0^8 \times 0^8 \times 0^8$	$0^8 \times \mathbb{F}_2^8 \times 0^8 \times 0^8$	None

Remark 5. Recall that we moved a potential key/constant addition in the s-boxes S'_j. Hence, instead of directly checking the equation above, one can instead check

$$\begin{aligned} & L_{i,j} \cdot \left(S'_j \left(\left(S'_j\right)^{-1} (x + \kappa) + \alpha_j \right) + S'_j \left(\left(S'_j\right)^{-1} (\kappa) + \alpha_j \right) \right) \\ =& S_i^{-1} \left(S \left(L_{i,j} \cdot x \right) + \beta_i \right) + S_i^{-1} \left(S \left(0 \right) + \beta_i \right) \end{aligned}$$

for any key/constant κ.

For CRAFT and SKINNY, the implications of this corollary are quite obvious, as all blocks $L_{i,j} \in \{0, I\}$, and therefore $\alpha_j \neq 0 \Rightarrow \beta_i \neq 0 \; \forall i$ s.t. $L_{i,j} = I$. As no non-zero difference from Table 2 fulfills this condition, this shows that there cannot exist a non-trivial probability-one differential for CRAFT and SKINNY. Similarly, Corollary 10 can be used to show that the differences from Table 2 for PRIDE are also not possible. For details on this, we refer the interested reader to Example 4 in the Supplementary Material B.2.

5 Conclusion

We presented algorithms (in the linear case) and conditions (in the differential case) to exclude the existence of weak keys for optimal distinguishers for a few rounds of SPN ciphers. There are several obvious questions that arise, most prominently to generalize to either more rounds or smaller probability or both. We expect that in particular studying non-optimal distinguishers immediately gets very complicated in general. However, we think that generalizing the probability-one differential case from two to more rounds is worth trying. For four rounds, continuing the track we laid out here, one would have to consider superboxes instead of s-boxes and one of the technical question becomes how to ensure that a superbox, i.e., two rounds of an SPN, does not have maximal boomerang uniformity.

From a technical perspective, the striking difference of the differential case, where we can give rather compact criteria, and the linear case, where we have to rely on algorithms to check the properties, can also be seen as a vectorial vs. Boolean variant of the uniqueness property. More precisely while for the vectorial case we can rely on Lemma 6, there does not seem to be a corresponding version for the Boolean case. More general, understanding under which condition

a Boolean function allows two essentially different compositions is an interesting future research topic on its own. In terms of questions for Boolean functions and s-boxes, we feel that the s-box property considered in Eq. (6) could be of independent interest in the design of s-boxes and many natural questions in the area of Boolean functions could be discussed in the future.

Acknowledgments. This work was funded by the by the projects *Analysis and Protection of Lightweight Cryptographic Algorithms* (432878529), *Symmetric Cipher Design with Inherent Physical Security* (406956718) and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foudation) under Germany's Excellence Strategy - EXC 2092 CASA – 390781972.

References

1. Albrecht, M.R., Driessen, B., Kavun, E.B., Leander, G., Paar, C., Yalçin, T.: Block ciphers - focus on the linear layer (feat. PRIDE). In: Garay, J.A., Gennaro, R. (eds.) Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I. Lecture Notes in Computer Science, vol. 8616, pp. 57–76. Springer (2014). https://doi.org/10.1007/978-3-662-44371-2_4, https://doi.org/10.1007/978-3-662-44371-2_4
2. Beierle, C., Beyne, T., Felke, P., Leander, G.: Constructing and deconstructing intentional weaknesses in symmetric ciphers. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13509, pp. 748–778. Springer (2022). https://doi.org/10.1007/978-3-031-15982-4_25, https://doi.org/10.1007/978-3-031-15982-4_25
3. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9815, pp. 123–153. Springer (2016). https://doi.org/10.1007/978-3-662-53008-5_5, https://doi.org/10.1007/978-3-662-53008-5_5
4. Beierle, C., Leander, G., Moradi, A., Rasoolzadeh, S.: CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks. IACR Trans. Symmetric Cryptol. **2019**(1), 5–45 (2019). https://doi.org/10.13154/tosc.v2019.i1.5-45, https://doi.org/10.13154/tosc.v2019.i1.5-45
5. Bellini, E., Makarim, R.H.: Functional cryptanalysis: Application to reduced-round xoodoo. IACR Cryptol. ePrint Arch. p. 134 (2022), https://eprint.iacr.org/2022/134
6. Beyne, T.: Block cipher invariants as eigenvectors of correlation matrices. J. Cryptol. **33**(3), 1156–1183 (2020). https://doi.org/10.1007/s00145-020-09344-1, https://doi.org/10.1007/s00145-020-09344-1
7. Beyne, T., Rijmen, V.: Differential cryptanalysis in the fixed-key model. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III. Lecture Notes in Computer

Science, vol. 13509, pp. 687–716. Springer (2022). https://doi.org/10.1007/978-3-031-15982-4_23, https://doi.org/10.1007/978-3-031-15982-4_23
8. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1990). https://doi.org/10.1007/3-540-38424-3_1, https://doi.org/10.1007/3-540-38424-3_1
9. Carlet, C. (ed.): Boolean Functions for Cryptography and Coding Theory. Cambridge University Press (2020). https://doi.org/10.1017/9781108606806, https://doi.org/10.1017/9781108606806
10. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: A new cryptanalysis tool. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II. Lecture Notes in Computer Science, vol. 10821, pp. 683–714. Springer (2018). https://doi.org/10.1007/978-3-319-78375-8_22, https://doi.org/10.1007/978-3-319-78375-8_22
11. Daemen, J.: Cipher and hash function design, strategies based on linear and differential cryptanalysis, PhD Thesis. K.U.Leuven (1995), http://jda.noekeon.org/
12. Daemen, J., Rijmen, V.: The wide trail design strategy. In: Honary, B. (ed.) Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2260, pp. 222–238. Springer (2001). https://doi.org/10.1007/3-540-45325-3_20, https://doi.org/10.1007/3-540-45325-3_20
13. Daemen, J., Rijmen, V.: Plateau characteristics. IET Inf. Secur. **1**(1), 11–17 (2007). https://doi.org/10.1049/iet-ifs:20060099, https://doi.org/10.1049/iet-ifs:20060099
14. Dinur, I., Dunkelman, O., Keller, N., Ronen, E., Shamir, A.: Efficient detection of high probability statistical properties of cryptosystems via surrogate differentiation. In: Advances in Cryptology - EUROCRYPT 2023, Lyon, France, April 23-27, 2023. Lecture Notes in Computer Science, vol. 14007. Springer (2023)
15. Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Ascon v1.2: Lightweight authenticated encryption and hashing. J. Cryptol. **34**(3), 33 (2021). https://doi.org/10.1007/s00145-021-09398-9, https://doi.org/10.1007/s00145-021-09398-9
16. Fourquet, R., Loidreau, P., Tavernier, C.: Finding good linear approximations of block ciphers and its application to cryptanalysis of reduced round DES. In: WCC 2009 - Workshop on Coding and Cryptography (2009), https://perso.univ-rennes1.fr/pierre.loidreau/articles/wcc_2009/wcc_2009.pdf
17. Guo, H., Sun, S., Shi, D., Sun, L., Sun, Y., Hu, L., Wang, M.: Differential attacks on CRAFT exploiting the involutory s-boxes and tweak additions. IACR Trans. Symmetric Cryptol. **2020**(3), 119–151 (2020). https://doi.org/10.13154/tosc.v2020.i3.119-151, https://doi.org/10.13154/tosc.v2020.i3.119-151
18. Kuijsters, D., Verbakel, D., Daemen, J.: Weak subtweakeys in SKINNY. IACR Cryptol. ePrint Arch. p. 1042 (2022), https://eprint.iacr.org/2022/1042
19. Lambin, B., Leander, G., Neumann, P.: Pitfalls and shortcomings for decompositions and alignment. In: Advances in Cryptology - EUROCRYPT 2023, Lyon, France, April 23-27, 2023. Lecture Notes in Computer Science, vol. 14007. Springer (2023)

20. Leander, G., Rasoolzadeh, S.: Weak tweak-keys for the CRAFT block cipher. IACR Trans. Symmetric Cryptol. **2022**(1), 38–63 (2022). https://doi.org/10.46586/tosc.v2022.i1.38-63, https://doi.org/10.46586/tosc.v2022.i1.38-63
21. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. Lecture Notes in Computer Science, vol. 765, pp. 386–397. Springer (1993). https://doi.org/10.1007/3-540-48285-7_33, https://doi.org/10.1007/3-540-48285-7_33
22. Nyberg, K., Knudsen, L.R.: Provable security against a differential attack. J. Cryptol. **8**(1), 27–37 (1995). https://doi.org/10.1007/BF00204800, https://doi.org/10.1007/BF00204800
23. Peyrin, T., Wang, H.: The MALICIOUS framework: Embedding backdoors into tweakable block ciphers. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III. Lecture Notes in Computer Science, vol. 12172, pp. 249–278. Springer (2020). https://doi.org/10.1007/978-3-030-56877-1_9, https://doi.org/10.1007/978-3-030-56877-1_9
24. Vaudenay, S.: Provable security for block ciphers by decorrelation. In: Morvan, M., Meinel, C., Krob, D. (eds.) STACS 98, 15th Annual Symposium on Theoretical Aspects of Computer Science, Paris, France, February 25-27, 1998, Proceedings. Lecture Notes in Computer Science, vol. 1373, pp. 249–275. Springer (1998). https://doi.org/10.1007/BFb0028566, https://doi.org/10.1007/BFb0028566

A Proof of Lemma 2

Proof. We show (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1). For the step (1) $\Rightarrow$ (2), we start with the two weak keys $k, (k+u) \in W_E(\alpha, \beta)$. That is, for all $x \in \mathbb{F}_2^n$ and some constants $c_1, c_2 \in \mathbb{F}_2$, we have

$$\langle \alpha, x \rangle = \langle \beta, R_2(R_1(x) + k) \rangle + c_1$$
$$\langle \alpha, x \rangle = \langle \beta, R_2(R_1(x) + k + u) \rangle + c_2.$$

Adding both equations and considering $R_1^{-1}(x)$ instead of x yields

$$\langle \beta, R_2(x+k) + R_2(x+k+u) \rangle = c_1 + c_2,$$

which shows that u is a linear structure of $\langle \beta, R_2 \rangle$. Next, to show (2) $\Rightarrow$ (3), we start with the weak key k for which it holds that

$$\langle \alpha, R_1^{-1}(x) \rangle = \langle \beta, R_2(x+k) \rangle + c_1.$$

Considering the linear structure u of $\langle \beta, R_2 \rangle$, we also have

$$\langle \alpha, R_1^{-1}(x) \rangle = \langle \beta, R_2(x+k+u) \rangle + c_1'.$$

Here, we substitute x by $x+u$ and again consider the sum of both equations to conclude that u is a linear structure of $\langle \alpha, R_1^{-1}(x) \rangle$. For the last step, we again consider the weak key k with

$$\langle \alpha, R_1^{-1}(x) \rangle = \langle \beta, R_2(x+k) \rangle + c_1.$$

With the linear structure u of $\langle \alpha, R_1^{-1}(x) \rangle$ in mind, it is apparent that

$$\langle \alpha, R_1^{-1}(x+u) \rangle = \langle \beta, R_2(x+k) \rangle + c_1''.$$

Now, we substitute x by $x+u$ and then x by $R_1(x)$ to get

$$\langle \alpha, x \rangle = \langle \beta, R_2(R_1(x) + k + u) \rangle + c_1''$$

and conclude that $(k+u)$ is a weak key too. □

B More Details on Probability-One Differentials over Two Rounds

B.1 Some Examples

Let us start with giving some more insights into Example 1. Recall that the s-box S and linear layer L are as follows.

x	0x00	0x01	0x02	0x03	0x04	0x05	0x06	0x07	0x08	0x09	0x0a	0x0b	0x0c	0x0d	0x0e	0x0f
S(x)	0x1c	0x1b	0x1e	0x09	0x17	0x15	0x1d	0x04	0x19	0x00	0x08	0xa	0x0d	0x13	0x0f	0x11
x	0x10	0x11	0x12	0x13	0x14	0x15	0x16	0x17	0x18	0x19	0x1a	0x1b	0x1c	0x1d	0x1e	0x1f
S(x)	0x0c	0x12	0x0e	0x10	0x1f	0x16	0x05	0x07	0x1a	0x18	0xb	0x02	0x14	0x03	0x06	0x01

$$L = \left(\begin{array}{ccccc|ccccc|ccccc} 1&1&0&1&0&1&1&1&0&1&1&1&1&1&0\\ 0&0&1&0&1&0&0&0&1&0&0&1&0&1&0\\ 0&1&0&0&1&0&1&1&1&0&0&0&1&1&0\\ 0&1&1&0&1&0&1&0&1&1&0&1&0&0&0\\ 0&0&1&1&0&0&0&0&0&1&0&1&1&1&1\\ \hline 0&0&1&1&1&1&0&0&0&1&1&1&1&1&0\\ 0&0&0&0&1&0&1&1&1&1&0&0&0&1&1\\ 0&0&0&0&1&0&0&0&1&1&0&1&1&1&1\\ 0&0&1&1&0&0&1&0&1&1&0&1&1&1&1\\ 0&0&1&0&1&0&1&0&0&1&0&1&0&0&0\\ \hline 1&0&0&1&1&1&0&0&1&0&0&0&0&0&0\\ 0&0&1&1&0&0&0&0&1&1&0&1&1&0&1\\ 0&1&0&1&0&0&1&1&1&1&0&1&1&0&1\\ 0&0&0&1&1&0&1&0&0&1&0&0&1&0&0\\ 0&1&0&0&0&0&0&1&1&1&0&1&1&1&0 \end{array}\right)$$

It is not hard to verify that $S^{-1} \circ T_{\texttt{0x1d}} \circ S = S \circ T_{\texttt{0x1d}} \circ S^{-1}$ is the affine map $x \in \mathbb{F}_2^5 \mapsto A \cdot x + a$ with

$$A = \begin{pmatrix} 1&1&1&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix} \text{ and } a = \begin{pmatrix} 1\\1\\1\\1\\1 \end{pmatrix}.$$

Here, `0x1d` denotes the vector

$$\begin{pmatrix} 1\\1\\1\\0\\1 \end{pmatrix}.$$

Note that it holds that for

$$\hat{A} \coloneqq \begin{pmatrix} A&0&0\\ 0&A&0\\ 0&0&A \end{pmatrix} \text{ and } \hat{a} \coloneqq \begin{pmatrix} a\\a\\a \end{pmatrix}$$

we have that $\hat{A} \cdot L = L \cdot \hat{A}$ and $\hat{a} = L \cdot \hat{a}$. In other words, the $\hat{a}$ is invariant under L and $\hat{A}$ commutes with L. But this means that, for any $x \in \mathbb{F}_2^{15}$,

$$\begin{aligned} \bar{S} \circ L \circ \bar{S}(x + \texttt{0x1d}^{\times 3}) =& \bar{S} \circ L \left(\hat{A} \circ \bar{S}(x) + \hat{a} \right) \\ =& \bar{S} \left(\hat{A} \circ L \circ \bar{S}(x) + \hat{a} \right) \\ =& \bar{S} \circ L \circ \bar{S}(x) + \texttt{0x1d}^{\times 3}. \end{aligned}$$

In other words, $(\texttt{0x1d}^{\times 3}, \texttt{0x1d}^{\times 3})$ is a probability-one differential over $\bar{S} \circ L \circ \bar{S}$. If we also consider key addition, i. e. we want $\bar{S} \circ L \circ T_k \circ \bar{S} \circ T_{\texttt{0x1d}} = T_{\texttt{0x1d}} \circ \bar{S} \circ L \circ T_k \circ \bar{S}$ to be fulfilled, then we need

$$\begin{aligned} & \bar{S} \circ L \left(\hat{A} \circ \bar{S}(x) + \hat{a} + k \right) = \bar{S} \left(\hat{A} \circ L \circ T_k \circ \bar{S}(x) + \hat{a} \right) && \forall x \in \mathbb{F}_2^{15} \\ \iff & L \left(\hat{A}(x) + \hat{a} + k \right) = \hat{A} \circ L(x + k) + \hat{a} && \forall x \in \mathbb{F}_2^{15} \\ \iff & k = \hat{A} \cdot k. \end{aligned}$$

In other words, the weak keys are all elements of $\mathbb{F}_2^{15}$ that are invariant under $\hat{A}$. Hence, it is easy to verify that the space of weak keys is the 3-times direct product of the space spanned by `0x10`, `0x0c`, `0x02` and `0x01`.

Next, let us look at an example where $S^{-1} \circ T_\beta \circ S$ is not affine, but S has maximal boomerang uniformity.

Example 2. Consider the S-Box $S : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ defined by

x	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
S(x)	0x8	0x0	0xa	0x2	0x3	0x5	0x4	0x7	0x6	0x9	0x1	0xb	0xc	0xd	0xe	0xf

and the linear layer

$$L = L^{-1} = \left(\begin{array}{cccc|cccc} 0&0&0&0&0&0&1&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ \hline 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \end{array}\right).$$

S has differential uniformity and linearity 12, but $\bar{S} \circ L \circ \bar{S}$ has a probability-one differential $(\texttt{0x0c}, \texttt{0x05})$. Note that S has maximal boomerang uniformity, e.g., $\mathrm{BCT}_S[\texttt{0xc}, \texttt{0x2}]$ is maximal.[10]

B.2 Algorithmic Version of Theorem 2

Note that Theorem 2 (or more precisely Corollary 6) can be trivially reformulated into an algorithm that returns a set containing all posssible output differences, see Algorithm 2.[11] By the nature of the theorem, it can only restrict the set of output differences that *could* lead to a probability-one differential. In other words, it can only show non-existence, if the returned set contains only the zero difference, but not all of the returned differences have to yield a probability-one differential, meaning that the returned set might contain false positives. Let us exemplify this on a SKINNY superbox.

Example 3 (Algorithm 2 applied to SKINNY). Recall that the SKINNY MixColumns matrix and its inverse are

$$L = \begin{pmatrix} I & 0 & I & I \\ I & 0 & 0 & 0 \\ 0 & I & I & 0 \\ I & 0 & I & 0 \end{pmatrix}, L^{-1} = \begin{pmatrix} 0 & I & 0 & 0 \\ 0 & I & I & I \\ 0 & I & 0 & I \\ I & 0 & 0 & I \end{pmatrix},$$

where I denotes the $m \times m$ identity matrix, with $m = 4$ or $m = 8$ depending on the version of SKINNY we are considering. Let us start with $(i, j) = (1, 1)$.

[10] For implementations of both examples we refer the reader to the source code we provide.

[11] This algorithm is also part of the source code we provide.

Algorithm 2 Search for output difference candidates

Input

L	linear layer as block-matrix
d	number of s-box
$S\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$	s-box
LS	linear structures of S^{-1}
BCT	boomerang connectivity table of S

Output

B	set containing all output differences that belong to probability-one differentials over two rounds

$B_i \leftarrow \mathbb{F}_2^m$ for $i = 1, ..., d$
for $(i, j) \in \{1, ..., d\}^2$ such that $L_{i,j} \neq 0$ **do**
  if $L_{i,j} \cdot \left(L^{-1}\right)_{j,l\neq i} = 0$ and $\operatorname{rank}(L_{i,j}) \leq 2$ **then**
    $B_i \leftarrow B_i \cap \{\beta \in \mathbb{F}_2^m \mid \exists \delta \in \operatorname{Im}(L_{i,j}) : \mathrm{BCT}[\delta, \beta] = 2^m\}$
    $B_i \leftarrow B_i \cap \{\beta \in \mathbb{F}_2^m \mid \exists \gamma \in \ker\left((L_{i,k\neq j})^T\right), c \in \mathbb{F}_2 \colon (\gamma, \beta, c) \in \mathrm{LS}\}$
  end if
  if $L_{i,j} \cdot \left(L^{-1}\right)_{j,l\neq i}$ has rank between 1 and $m-1$ **then**
    $B_i \leftarrow B_i \cap \{\beta \in \mathbb{F}_2^m \mid \exists \delta \in \mathbb{F}_2^m \colon \mathrm{BCT}[\delta, \beta] = 2^m\}$
    for $k \neq i$ such that $L_{i,j} \cdot \left(L^{-1}\right)_{j,k} \neq 0$ **do**
      $B_i \leftarrow B_i \cap \{\beta \in \mathbb{F}_2^m \mid \exists \gamma \in \mathbb{F}_2^m, c \in \mathbb{F}_2 \colon (\gamma, \beta, c) \in \mathrm{LS}\}$
    end for
  end if
  if $L_{i,j} \cdot \left(L^{-1}\right)_{j,l\neq i}$ has full rank **then**
    $B_i \leftarrow B_i \cap \{\beta \in \mathbb{F}_2^m \mid S^{-1} \circ T_\beta \circ S \text{ is affine}\}$
  end if
end for
return $B_1 \times ... \times B_d$

We have that $L_{1,1} = I$ and $\left(L^{-1}\right)_{1,l\neq 1} = \begin{pmatrix} I & 0 & 0 \end{pmatrix}$, which means that B_1 becomes $\{\beta \in \mathbb{F}_2^m \mid S^{-1} \circ T_\beta \circ S \text{ is affine}\}$. Using Lemma 10 it is easy to see that this already means $B_1 = \{0\}$. Similarly, using $(i,j) = (3,2)$ and $(i,j) = (4,1)$ shows that $B_3 = \{0\} = B_4$. As it is not possible to restrict those B_i's any further, let us skip all other iterations where $i \neq 2$ and instead continue with $i = 2$ and $j = 1$, which is the only j with $L_{2,j} \neq 0$. Again, $L_{2,1} = I$, but $\left(L^{-1}\right)_{1,l\neq 2} = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}$, meaning that we cannot restrict B_2 at all. Hence, the algorithm returns $0^m \times \mathbb{F}_2^m \times 0^m \times 0^m$.

Applying the algorithm to the inverse cipher yields $\mathbb{F}_2^m \times 0^m \times 0^m \times 0^m$. It is easy to see (for example by using Corollary 10) that the only pair of input and output difference that is compatible is the one where both differences are zero, which means that there does not exist a non-trivial probability-one differential over two rounds of SKINNY.

Next, let us show that the non-zero differences that are returned by Algorithm 2 for PRIDE are also all incompatile.

Example 4 (Algorithm 2 applied to PRIDE). The linear layer of PRIDE is depicted in Fig. 4. Note that the primary diagonal only contains the blocks

$$A = \begin{pmatrix} 0&0&0&0 \\ 0&1&0&0 \\ 0&0&0&0 \\ 0&0&0&1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix}.$$

Algorithm 2 tells us that $(\alpha_1, ..., \alpha_{16}), (\beta_1, ..., \beta_{16}) \in \{\texttt{0x0}, \texttt{0x1}, \texttt{0x8}\}^{16}$ are the only candidates that lead to a probability-one differential over s-box layer, linear layer and s-box layer. In addition, we know form Remark 5 that for all $x \in \mathbb{F}_2^4$ and all i, j

$$\begin{aligned} & L_{i,j} \cdot \left(S'_j\left(\left(S'_j\right)^{-1}(x+\kappa)+\alpha_j\right) + S'_j\left(\left(S'_j\right)^{-1}(\kappa)+\alpha_j\right)\right) \\ =& S_i^{-1}\left(S\left(L_{i,j}\cdot x\right)+\beta_i\right) + S_i^{-1}\left(S\left(0\right)+\beta_i\right) \end{aligned}$$

has to hold, which implies that it has especially hold for $i = j$. Hence, it is easy to verify[12] that this equation holds for none of the 128 possible choices of $L_{i,i} \in \{A, B\}$, $\kappa \in \mathbb{F}_2^4$ and $\alpha_i, \beta_i \in \{\texttt{0x1}, \texttt{0x8}\}$, which shows that there does not exist a non-trivial probability-one differential over two rounds of PRIDE.

[12] For convenience of the reader, we have implemented this step and provide it as part of our source code.

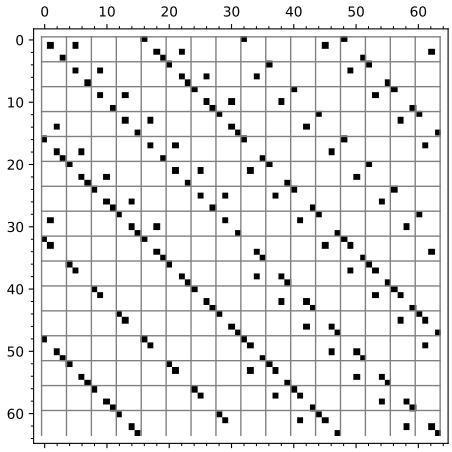

Fig. 4. Linear layer of PRIDE