Understanding Unexpected Fixed-Key Differential Behaviours: How to Avoid Major Weaknesses in Lightweight Designs (Extended Version)

Anne Canteaut[1] and Merlin Fruchon[2,1]

[1] Inria, Paris, France
[2] DGA, France

Abstract Many design strategies and differential attacks rely on the so-called hypothesis of stochastic equivalence, which states that the differential behaviour of a cipher for any fixed key can be approximated by its average behaviour over all keys. However, this assumption is known to be invalid in general. For instance, all two-round differential characteristics of AES are plateau, meaning that their probabilities highly depend on the key. While such discrepancies were traditionally expected to occur only for a small number of rounds, several counter-examples have been exhibited recently thanks to the quasi-differential framework.

This paper aims to show why the divergence between fixed-key and average behaviour can be even more pronounced and is definitely harder to anticipate when analyzing differentials, rather than individual characteristics, which is the quantity actually relevant in differential cryptanalysis. Indeed, when a differential aggregates many characteristics that do not satisfy the hypothesis of stochastic equivalence, several scenarios may arise: the sets of weak keys may be identical across all characteristics, resulting in a strong clustering effect, or entirely disjoint, eliminating any such effect. Focusing on (truncated) differentials that include plateau characteristics, we demonstrate how this mechanism explains the unexpected differential behaviour observed in Midori64 and Scream over an arbitrary number of rounds, as recently reported by Baudrin *et al.* We also clarify how this situation differs from invariant subspaces, except in a few specific cases. Furthermore, we identify the properties of the Sbox that give rise to this weakness and all vulnerable Sboxes among the optimal 4-bit functions.

Keywords. Differential cryptanalysis · Hypothesis of stochastic equivalence · Clustering effect · Invariant subspaces · Midori64.

1 Introduction

Differential cryptanalysis, introduced in 1990 by Biham and Shamir [BS91], is one of the oldest and most prominent cryptanalytic techniques in symmetric cryptography. Various design strategies, such as the wide-trail strategy [DR01] or a careful selection of the constituent Sboxes [Nyb12], have been successfully developed to ensure resistance against this type of attacks. Today, any new proposal is expected to demonstrate robustness against differential attacks. However, evaluating the resistance to differential cryptanalysis still relies on several hypotheses that may not hold always in practice. One such hypothesis is the *hypothesis of stochastic equivalence*, first introduced by Lai, Massey and Murphy [LMM91]. This hypothesis formalizes the idea that the behaviour of a cipher for (almost) all *fixed values of the expanded key* can be approximated by its *average* behaviour over all possible keys. Indeed, for key-alternating ciphers, the so-called *expected differential probability (EDP)* of a differential characteristic corresponds to the average of its fixed-key probabilities, where the average is taken over all possible expanded keys, i.e., over all possible sequences of independent round-keys.

Several practical scenarios where the hypothesis of stochastic equivalence does not hold have been known for a long time, for instance, for certain iterative 2-round characteristics on DES used by Biham and Shamir [Knu93]. Later, Daemen and Rijmen [DR07] identified and thoroughly studied a broad class of characteristics, called *plateau characteristics*, for which the hypothesis of stochastic equivalence fails. Indeed, these are characteristics whose fixed-key probability is either a constant or zero, depending on whether the

expanded key belongs to a specific set of weak keys or not. Notably, Daemen and Rijmen proved that, in any SPN using an Sbox with differential uniformity 4, all 2-round differential characteristics are plateau. Extending this analysis beyond 2 rounds was considered challenging, until Beyne and Rijmen recently introduced a novel framework, called *quasi-differentials* [BR22]. This framework provides an exact expression for the fixed-key probability of a differential characteristic. Although it involves matrices of size $2^{2n} \times 2^{2n}$, where n is the block size, it offers an elegant and powerful tool for enabling a far more accurate and insightful analysis of the differential behavior of symmetric primitives.

Another major difficulty in determining the complexity of differential attacks lies in the fact that the relevant quantity is not the probability of a specific *differential characteristic*, which corresponds to a sequence $(\Delta_0, \Delta_1, \ldots, \Delta_r)$ of intermediate differences across the successive rounds. In practice, only the input and output differences are accessible to an attacker. Consequently, the relevant quantity is the probability of the differential (Δ_0, Δ_r). It corresponds to the cumulative probability of all differential characteristics $(\Delta_0, \Delta_1, \ldots, \Delta_r)$ that begin with Δ_0 and end with Δ_r. In some cases, this probability is well approximated by that of a single dominant characteristic (or a few of them). But, there also several well-known cases where this is not the case and where the complexity of the attack is significantly lower than expected because several characteristics need to be taken into account, see e.g. [Abd13,CFG$^+$15,LPS21]. Crucially, when the hypothesis of stochastic equivalence does not hold, summing the expected differential probabilities of the individual characteristics to estimate the EDP of the overall differential is misleading. Indeed, many of the contributing characteristics may have nonzero EDPs, but each may be valid only for different weak-key sets. In such a case, there is no clustering effect, contrary to what might be incorrectly inferred from the individual EDPs. However, if all contributing characteristics happen to correspond to the same weak-key set, this could pose a potential threat.

The aim of this paper is to analyse such behaviours, and demonstrate why traditional analysis based on the EDP can lead to misleading results and incorrect intuitions. Studies of recent constructions intended for low-resources devices have revealed several unexpected fixed-key behaviours in ciphers designed according to state-of-the-art design principles. These findings have led to new types of attacks, such as invariant-subspace attacks [LAAZ11,LMR15,GJN$^+$16] or nonlinear-invariant attacks [TLS16,Bey18]. More intriguingly, as a corollary of their commutative cryptanalysis, Baudrin *et al.* revealed the existence of truncated differentials on Midori64 [BBI$^+$15] that hold *for an arbitrary number of rounds* with probability 2^{-16} for a certain set of weak expanded-keys [BFL$^+$23]. Interestingly, the corresponding set of weak expanded-keys contains, as a subset, the weak keys for which invariant subspaces have been previously found in [GJN$^+$16] and [Bey18]. However, it also includes some new weak-keys for which this differential behaviour was unknown and cannot be explained by traditional methods. A similar phenomenon is reported on Scream [GLS$^+$14].

We believe that understanding the origin of such unexpected behaviours, is extremely important. Indeed, the existence of an unexpected behaviour for a cipher that follows the state-of-the-art design principles, calls into question the security of a broader class of primitives. A common mitigation strategy is to adopt a more complex key schedule, in the hope that it will be incompatible with the potential weak expanded keys. However, this approach is not entirely satisfactory: complex key schedules come with an implementation overhead, whereas a simpler—often linear—key schedule is typically considered an efficient option, particularly in the context of lightweight cryptography.

Our contributions. Our main contribution is to clarify the phenomenon identified by Baudrin *et al.* on Midori64 and Scream, and to identify its origins. We show that this unexpected differential behaviour actually results from two distinct phenomena, depending on the weak expanded-keys involved. For some weak keys, specifically those previously identified by Guo *et al.* for Midori64, this truncated differential includes a plateau characteristic which has a high probability. However, for the vast majority of the weak expanded-keys, all constituent characteristics are plateau but have a very low probability (typically 2^{-62} or 2^{-63}) as the number of rounds increases. We then show that the number of such constituent plateau characteristics that are valid for at least one weak expanded-key is quite large. More importantly, due to the specific properties of Midori64's Sbox, all these characteristics are valid *for the same weak-keys*. We precisely identify the Sbox properties responsible for each phenomenon, and as an illustration, we show how

changing the Sbox significantly modifies the fixed-key differential behaviour. As a corollary, we prove that among all optimal 4-bit Sboxes [LP07], only those having 3 components of algebraic degree 2 may lead to the same behavior as observed on MIDORI64 by Baudrin *et al.* Most notably, some "Silver Sboxes" proposed by Guo *et al.* [GJN+16] as stronger alternatives to MIDORI64's Sbox due to their resistance to invariant subspaces, exhibit the exact same vulnerability as MIDORI64 with respect to the truncated differential.

Outline. The next section is dedicated to plateau characteristics. It mainly recalls the results of Daemen and Rijmen [DR07]. Thanks to the quasi-differential framework [BR22], it formalizes the case of some plateau characteristics over many rounds, in a way that provides an explicit description of the weak-key subspace and of the set of valid inputs. Section 3 then focuses on the fixed-key probability of a truncated differential when it aggregates many plateau characteristics that have the previously studied form. We analyse how the number of such characteristics, that are valid for at least one weak expanded-key, grows with the number of rounds. Moreover, we determine under which condition all these characteristics are valid for the same weak keys. Section 4 illustrates these theoretical results by analysing how the fixed-key truncated differential probability in MIDORI64 varies with the properties of the Sbox. The influence of the Sbox is then further examined in Section 5, where we identify all optimal 4-bit Sboxes exhibiting this weakness, including several Silver Sboxes recommended in [GJN+16]. Section 6 shows how the results in Section 3 extend to a more general setting, with a larger set of differences, and illustrates this on SCREAM and ISCREAM. Finally, Section 7 analyses the similarities and differences between our work and different techniques, including invariant-subspace attacks [LAAZ11,LMR15,GJN+16] and commutative cryptanalysis [BFL+23].

2 A Deeper Look at Plateau Characteristics

2.1 General Setting and Notation

In the paper, we consider an SPN cipher with block size $n := sm$. Its round function is defined as $\mathcal{R} := L \circ \boldsymbol{\mathcal{S}}$ where $L : \mathbb{F}_2^{sm} \to \mathbb{F}_2^{sm}$ is the linear layer and $\boldsymbol{\mathcal{S}}$ corresponds to the parallel application of m copies of the same s-bit Sbox $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$. At the beginning of each round, an n-bit round-key is xored to the internal state of the cipher. For r rounds, we denote by $K := (K_1, K_2, \ldots, K_{r-1})$ the *expanded key*, i.e., the vector of round keys where the initial and final whitening round keys are omitted.

In the following, we study the probability of an r-round differential characteristic $(\Delta_0, \ldots, \Delta_r)$. A *valid input* for this characteristic is a plaintext $x \in \mathbb{F}_2^n$ for which the following two sequences

$$\begin{cases} x_0 := x \\ \widetilde{x_0} := x + \Delta_0 \end{cases} \text{ and } \forall t \in \{0, \ldots, r-1\}, \begin{cases} x_{t+1} = \mathcal{R}(x_t) + K_{t+1} \\ \widetilde{x_{t+1}} = \mathcal{R}(\widetilde{x_t}) + K_{t+1} \end{cases}$$

satisfy $\widetilde{x_t} = x_t + \Delta_t$ for all $0 \le t \le r$.

For any expanded key $K = (K_1, \ldots, K_{r-1})$, we denote by $\mathsf{DP}[K](\Delta_0, \ldots, \Delta_r)$ the probability that the characteristic $(\Delta_0, \ldots, \Delta_r)$ is satisfied by the r-round cipher with key K. The expected differential probability (EDP) of $(\Delta_0, \ldots, \Delta_r)$ then corresponds to the average value of $\mathsf{DP}[K](\Delta_0, \ldots, \Delta_r)$, *i.e.*

$$\mathsf{EDP}(\Delta_0, \ldots, \Delta_r) = \sum_{K \in \mathbb{F}_2^{n(r-1)}} 2^{-n(r-1)} \mathsf{DP}[K](\Delta_0, \ldots, \Delta_r) \ .$$

While the expected differential probability of $(\Delta_0, \ldots, \Delta_r)$ is entirely determined by the differential probabilities of the Sbox, its fixed-key probability highly depends on the structure of the set on inputs satisfying the Sbox transitions. The following notation will be extensively used in the rest of the paper.

Definition 1 (Derivative). *For any $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$ and any $a \in \mathbb{F}_2^s$, the* derivative of S at a *is the function from $\mathbb{F}_2^s$ to $\mathbb{F}_2^s$ defined by $D_a S : x \mapsto S(x+a) + S(x)$.*

Notation 1 *For any $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$, and any differential (a, b), with $a, b \in \mathbb{F}_2^s$, we denote the input (resp. output) set of (a, b) as follows:*

$$\mathsf{XDDT}_S(a, b) := \{x \in \mathbb{F}_2^s \mid D_a S(x) = b\} \text{ and } \mathsf{YDDT}_S(a, b) := \{S(x) \mid x \in \mathsf{XDDT}_S(a, b)\} \ .$$

Moreover, $\mathsf{DDT}_S(a, b) := \#\mathsf{XDDT}_S(a, b) = \#\mathsf{YDDT}_S(a, b)$.

2.2 Planar and Super-Planar Differentials

The case where the input and output sets of a differential are (affine) subspaces is of particular interest as first pointed out by Daemen and Rijmen [DR07].

Definition 2 (Planar differential [DR07]). *A differential (a, b) for $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$ is said to be* planar *if both sets $\mathsf{XDDT}_S(a, b)$ and $\mathsf{YDDT}_S(a, b)$ are affine subspaces. In this case, we use the following notation:*

$$\mathsf{XDDT}_S(a, b) := x_0^{a,b} + \mathsf{U}_S(a, b) \text{ and } \mathsf{YDDT}_S(a, b) := y_0^{a,b} + \mathsf{V}_S(a, b)$$

where $y_0^{a,b} = S(x_0^{a,b})$.

As noted in [DR07], any differential (a, b) with $\mathsf{DDT}_S(a, b) \in \{2, 4, 2^s\}$ is planar, implying that all differentials of an Sbox with differential uniformity at most 4 are planar. We refine this notion and define the more restricted property of *super-planar differential*. This new property will actually enable us to determine the fixed-key probability of some characteristics over several rounds by composition.

Definition 3 (Super-planar differential). *Let (a, b) be a planar differential for $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$ with $\mathsf{XDDT}_S(a, b) = x_0^{a,b} + \mathsf{U}_S(a, b)$. Let*

$$\begin{aligned} \phi_{a,b} : \mathsf{U}_S(a, b) &\to \mathsf{V}_S(a, b) \\ \theta &\mapsto S(x_0^{a,b}) + S(x_0^{a,b} + \theta) = D_\theta S(x_0^{a,b}) \ . \end{aligned}$$

Then, (a, b) is super-planar *if one of the following equivalent conditions holds:*

(i) *The function $\phi_{a,b}$ is linear.*
(ii) *The set corresponding to the graph of $\phi_{a,b}$, i.e.,*

$$\mathsf{Z}_S(a, b) := \{(\theta, \phi_{a,b}(\theta)) \mid \theta \in \mathsf{U}_S(a, b)\} \tag{1}$$

is a linear subspace of $\mathsf{U}_S(a, b) \times \mathsf{V}_S(a, b)$.
(iii) *For all $\theta_1, \theta_2 \in \mathsf{U}_S(a, b)$, $D_{\theta_1} D_{\theta_2} S(x_0^{a,b}) = 0$.*

The equivalence between (i) and (iii) is derived from the following more general fact: for any θ_1, θ_2 and any $x \in \mathbb{F}_2^s$, $D_{\theta_1} S(x) + D_{\theta_2} S(x) + D_{\theta_1+\theta_2} S(x) = D_{\theta_1} D_{\theta_2} S(x)$.

We note that (iii) implies that any choice for the offset $x_0^{a,b}$ leads to the same function $\phi_{a,b}$. Indeed, for any other offset $z_0^{a,b} = x_0^{a,b} + u$, with $u \in \mathsf{U}_S(a, b)$, we have $D_\theta S(z_0^{a,b}) + D_\theta S(x_0^{a,b}) = D_u D_\theta S(x_0^{a,b}) = 0$, for all $\theta \in \mathsf{U}_S(a, b)$.

Super-planar differentials of S are therefore planar differentials such that S *is affine on* $\mathsf{XDDT}_S(a, b)$, because

$$S(\mathsf{XDDT}_S(a, b)) = S(x_0^{a,b} + \mathsf{U}_S(a, b)) = S(x_0^{a,b}) + \phi_{a,b}(\mathsf{U}_S(a, b)) \ .$$

Lemma 1. *Let (a, b) be any differential for S such that $\mathsf{DDT}_S(a, b) \in \{2, 4\}$. Then, (a, b) is super-planar. Most notably, if S has differential uniformity at most 4, all its* active *differentials are super-planar.*

Proof. We first observe that $\phi_{a,b}(0) = 0$ and $\phi_{a,b}(a) = b$.

The case $\mathsf{DDT}_S(a, b) = 2$ is trivial since $\phi_{a,b}$ is defined over a subspace of dimension 1, and is therefore linear.

When $\mathsf{DDT}_S(a, b) = 4$, we have $\mathsf{U}_S(a, b) = \langle a, \theta \rangle$ for some $\theta \in \mathsf{U}_S(a, b) \backslash \{0, a\}$, where $\langle v_1, \cdots, v_k \rangle$ denotes the linear space spanned by $v_1, \ldots, v_k$. Then,

$$\begin{aligned} \phi_{a,b}(a + \theta) &= S(x_0^{a,b}) + S(x_0^{a,b} + \theta + a) \\ &= S(x_0^{a,b}) + S(x_0^{a,b} + \theta) + S(x_0^{a,b} + \theta) + S(x_0^{a,b} + \theta + a) \\ &= \phi_{a,b}(\theta) + b = \phi_{a,b}(\theta) + \phi_{a,b}(a) \ . \end{aligned}$$

where the penultimate equality uses that $x_0^{a,b} + \theta \in \mathsf{XDDT}_S(a, b)$. □

It is important to note that any differential with probability one is planar but is *not* super-planar if $\deg S > 1$. Indeed, in this case, $\mathsf{U}_S(a,b) = \mathsf{V}_S(a,b) = \mathbb{F}_2^s$ and (iii) means that $S(0) + S(\theta_1) + S(\theta_2) + S(\theta_1 + \theta_2) = 0$ for all θ_1, θ_2, i.e. $x \mapsto S(x) + S(0)$ is linear.

Super-planar differentials may also occur for a higher value of $\mathsf{DDT}_S(a,b)$. For instance, the Sbox of iScream [GLS+14] has a super-planar differential (a,b) with $\mathsf{DDT}_S(a,b) = 8$.

Another simple but useful remark is that, when $\boldsymbol{\mathcal{S}} : \mathbb{F}_2^{sm} \to \mathbb{F}_2^{sm}$ corresponds to the Cartesian product of m functions of $S_j : \mathbb{F}_2^s \to \mathbb{F}_2^s$, then the differential (A,B) for $\boldsymbol{\mathcal{S}}$ is planar (resp. super-planar) if all constituent differentials are planar (resp. super-planar). Indeed, $\mathsf{XDDT}_{\boldsymbol{\mathcal{S}}}(A,B) = \prod_{j=1}^m \mathsf{XDDT}_{S_j}(A[j], B[j])$. The other subspaces $\mathsf{YDDT}_{\boldsymbol{\mathcal{S}}}(A,B)$, $\mathsf{U}_{\boldsymbol{\mathcal{S}}}(A,B)$, $\mathsf{V}_{\boldsymbol{\mathcal{S}}}(A,B)$ and, in the super-planar case, $Z_{\boldsymbol{\mathcal{S}}}(A,B)$ similarly equal the products of the subspaces corresponding to the constituent Sboxes.

2.3 Plateau Characteristics over Several Rounds

Plateau characteristics are a major type of differential characteristics whose fixed-key probabilities are distributed in a very structured way and significantly differ from the average.

Definition 4 (Plateau characteristic [DR07]). *A characteristic $(\Delta_0, \ldots, \Delta_r)$ for an iterative function over $\mathbb{F}_2^n$ is said to be* plateau *if there exists an integer $h \geq 0$ such that its fixed-key probability satisfies*

$$\mathsf{DP}[K](\Delta_0, \ldots, \Delta_r) \in \{0, 2^{-n+h}\} .$$

The number of expanded keys for which the characteristic is valid is then determined by the value of h and the EDP of the characteristic. Daemen and Rijmen proved that any SPN with a differentially 4-uniform Sbox, including the AES, is such that all its 2-round characteristics are plateau. However, extending such characteristics to more rounds and determining their probabilities is more complicated. The notion of quasi-differential matrix, later introduced by Beyne and Rijmen [BR22], provides a very useful tool that can be applied to this context.

Definition 5 (Quasi-differential transition matrix [BR22]). *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Its quasi-differential transition matrix is the $\left(2^{2n} \times 2^{2n}\right)$-matrix defined by*

$$D^F(v,b)(u,a) := 2^{-n} \sum_{x \in \mathsf{XDDT}_F(a,b)} (-1)^{v \cdot F(x) + u \cdot x}, \ \forall u, v, a, b \in \mathbb{F}_2^n ,$$

where $x \cdot y$ denotes the scalar product between x and y.

The entries of the quasi-differential transition matrix corresponding to a super-planar differential (a,b) have a very simple expression involving the input and output sets of (a,b), namely $\mathsf{XDDT}_F(a,b) = x_0^{a,b} + \mathsf{U}_F(a,b)$ and $\mathsf{YDDT}_F(a,b) = y_0^{a,b} + \mathsf{V}_F(a,b)$.

Lemma 2. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and (a,b) be a super-planar differential for F, $a, b \in \mathbb{F}_2^n \setminus \{0\}$. Then, for all $u, v \in \mathbb{F}_2^n$, we have*

$$D^F(v,b)(u,a) = \begin{cases} (-1)^{u \cdot x_0^{a,b} + v \cdot y_0^{a,b}} \mathsf{DDT}_F(a,b) \times 2^{-n} & \text{if } (u,v) \in \mathsf{Z}_F(a,b)^\perp \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathsf{Z}_F(a,b)$ is defined by (1). Moreover, if (a,b) is a planar differential,

- $D^F(v,b)(0,a) = (-1)^{v \cdot y_0^{a,b}} \mathsf{DDT}_F(a,b) 2^{-n} \mathbf{1}_{v \in \mathsf{V}_F(a,b)^\perp}$
- $D^F(0,b)(u,a) = (-1)^{u \cdot x_0^{a,b}} \mathsf{DDT}_F(a,b) 2^{-n} \mathbf{1}_{u \in \mathsf{U}_F(a,b)^\perp}$

where $\mathbf{1}_{x \in X}$ equals 1 if $x \in X$ and 0 otherwise.

The proof relies on the well-known fact that, for any vector space E,

$$\sum_{x\in E}(-1)^{c\cdot x} = \begin{cases} 2^{\dim(E)} & \text{if } c \in E^\perp \\ 0 & \text{otherwise.} \end{cases}$$

It is important to observe that the previous formula holds only for the entries of the quasi-differential matrix corresponding to an active differential, i.e., when a and b are nonzero. Indeed, the entries corresponding to $a = b = 0$ are given by the Walsh coefficients of the function.

While planar differentials for the Sbox lead to 2-round plateau characteristics, the result cannot be directly extended to a larger number of rounds. Daemen and Rijmen [DR07, Page 11] have pointed out that plateau characteristics can be composed in the particular case of an SPN with an Sbox with differential uniformity at most 4 when all the Sboxes are active. The following theorem refines this result, first by removing the constraint on the differential uniformity of the Sbox, which enables us to capture other situations, like in Scream. More importantly, we provide an explicit expression of the corresponding set of valid inputs, and of the expanded keys for which the characteristic is valid.

Theorem 1. *Let us consider a key-alternating cipher with linear layer L and nonlinear layer $\boldsymbol{\mathcal{S}} = (S, \dots, S)$. Let $(\Delta_0, \Delta_1, \dots, \Delta_r)$ be an r-round differential characteristic, $r \geq 2$, such that all constituent differentials for S, i.e.,*

$$\left(\Delta_t[j], L^{-1}(\Delta_{t+1})[j]\right),\ \forall 0 \leq t \leq r-1,\ \forall 1 \leq j \leq m$$

are planar, and all internal differentials, i.e. for $1 \leq t \leq r-2$, are super-planar. Then, $(\Delta_0, \Delta_1, \dots, \Delta_r)$ is plateau and satisfies

$$\mathsf{DP}[K](\Delta_0, \dots, \Delta_r) = \begin{cases} 2^{-n-\dim(W)} \prod_{t=0}^{r-1} \mathsf{DDT}_{\boldsymbol{\mathcal{S}}}\left(\Delta_t, L^{-1}(\Delta_{t+1})\right) & \text{if } K \in w_0 + W \\ 0 & \text{otherwise,} \end{cases}$$

with $w_0 := \left(x_0^{\Delta_t, L^{-1}(\Delta_{t+1})} + L(y_0^{\Delta_{t-1}, L^{-1}(\Delta_t)})\right)_{1\leq t\leq r-1}$ and W is the sum of the following r linear subspaces of $\mathbb{F}_2^{sm(r-1)}$

- $L\left(\mathsf{V}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1))\right) \times \{0\}^{sm(r-2)}$
- $\{0\}^{sm(t-1)} \times (I \times L)\left(\mathsf{Z}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1}))\right) \times \{0\}^{sm(r-2-t)}$ *for* $1 \leq t \leq r-2$
- $\{0\}^{sm(r-2)} \times \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r))$.

where $(F \times G)$ denotes the Cartesian product of two functions, i.e., the function which maps (x, y) to $(F(x), G(y))$, and $\mathsf{U}_{\boldsymbol{\mathcal{S}}}$, $\mathsf{V}_{\boldsymbol{\mathcal{S}}}$ and $\mathsf{Z}_{\boldsymbol{\mathcal{S}}}$ are defined in Def. 2 and 3.

Proof. By [BR22, Theorem 4.1], we have

$$\mathsf{DP}[K](\Delta_0, \dots, \Delta_r) = \sum_{u_1, u_2 \dots u_{r-1} \in \mathbb{F}_2^{ms}} \prod_{t=0}^{r-1} D^{\mathcal{R}_t}(u_{t+1}, \Delta_{t+1})(u_t, \Delta_t)$$

where $\mathcal{R}_t = \mathsf{Add}_{K_{t+1}} \circ L \circ \boldsymbol{\mathcal{S}}$ for $t \leq r-2$ and $\mathcal{R}_{r-1} = L \circ \boldsymbol{\mathcal{S}}$ since we do not consider the post-whitening key. Moreover, [BR22, Theorem 3.2] leads to $D^{\mathcal{R}_t} = D^{\mathsf{Add}_{K_{t+1}}} D^L D^{\boldsymbol{\mathcal{S}}}$. It follows that

$$D^{\mathcal{R}_t}(u_{t+1}, \Delta_{t+1})(u_t, \Delta_t) = (-1)^{K_{t+1}\cdot u_{t+1}} D^{\boldsymbol{\mathcal{S}}}(L^T(u_{t+1}), L^{-1}(\Delta_{t+1}))(u_t, \Delta_t)\ .$$

Let us consider a sequence of masks $(0, u, 0) := (0, u_1, u_2, \dots, u_{r-1}, 0)$. We apply Lemma 2 to the first and last rounds whose input (resp. output) mask is zero:

$$D^{\boldsymbol{\mathcal{S}}}(L^T(u_1), L^{-1}(\Delta_1))(0, \Delta_0) = (-1)^{s_0(u)} \mathsf{DDT}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1)) 2^{-sm} \times \mathbf{1}_{L^T(u_1) \in \mathsf{V}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1))^\perp}$$
$$D^{\boldsymbol{\mathcal{S}}}(0, L^{-1}(\Delta_r))(u_{r-1}, \Delta_{r-1}) = (-1)^{s_{r-1}(u)} \mathsf{DDT}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r)) 2^{-sm} \times \mathbf{1}_{u_{r-1} \in \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r))^\perp}\ ,$$

where

$$s_0(u) = L^T(u_1) \cdot y_0^{\Delta_0, L^{-1}(\Delta_1)} \text{ and } s_{r-1}(u) = u_{r-1} \cdot x_0^{\Delta_{r-1}, L^{-1}(\Delta_r)} .$$

Since all intermediate differences are super-planar, again by Lemma 2, we have for all $1 \leq t \leq r-2$,

$$\begin{aligned} D^{\boldsymbol{\mathcal{S}}}(L^T(u_{t+1}), L^{-1}(\Delta_{t+1}))(u_t, \Delta_t) &= (-1)^{s_t(u)} \mathsf{DDT}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1})) 2^{-sm} \times \mathbf{1}_{(u_t, L^T(u_{t+1})) \in \mathsf{Z}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1}))^\perp} \\ &= (-1)^{s_t(u)} \mathsf{DDT}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1})) 2^{-sm} \times \mathbf{1}_{(u_t, u_{t+1}) \in ((I \times L)(\mathsf{Z}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1}))))^\perp} \end{aligned}$$

$$\begin{aligned} \text{with } s_t(u) &= \left(u_t, L^T(u_{t+1})\right) \cdot \left(x_0^{\Delta_t, L^{-1}(\Delta_{t+1})}, y_0^{\Delta_t, L^{-1}(\Delta_{t+1})}\right) \\ &= (u_t, u_{t+1}) \cdot \left(x_0^{\Delta_t, L^{-1}(\Delta_{t+1})}, L\left(y_0^{\Delta_t, L^{-1}(\Delta_{t+1})}\right)\right) . \end{aligned}$$

It follows that the correlation of the quasi-differential trail associated to the sequence of masks u corresponds to the product

$$\pm \prod_{t=0}^{r-1} D^{\boldsymbol{\mathcal{S}}}(L^T(u_{t+1}), L^{-1}(\Delta_{t+1}))(u_t, \Delta_t)$$

and is nonzero if and only if $u := (u_1, u_2, \ldots, u_{r-1})$ belongs to the intersection of r linear subspaces, corresponding to the orthogonals of

- $L\left(\mathsf{V}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1))\right) \times \{0\}^{sm(r-2)}$
- $\{0\}^{sm(t-1)} \times (I \times L)\left(\mathsf{Z}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1}))\right) \times \{0\}^{sm(r-2-t)}$ for $1 \leq t \leq r-2$
- $\{0\}^{sm(r-2)} \times \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r))$.

Using that $(U \cap V)^\perp = U^\perp + V^\perp$, we deduce that the quasi-differential trail associated to u is valid if and only if $u \in W^\perp$. It follows that

$$\mathsf{DP}[K](\Delta_0, \ldots, \Delta_r) = 2^{-msr} \left(\prod_{t=0}^{r-1} \mathsf{DDT}_{\boldsymbol{\mathcal{S}}}\left(\Delta_t, L^{-1}(\Delta_{t+1})\right)\right) \sum_{u \in W^\perp} (-1)^{u \cdot K + s_0(u) + \ldots s_{r-1}(u)}.$$

Moreover,

$$u \cdot K + s_0(u) + s_1(u) + \ldots s_{r-1}(u) = \sum_{t=1}^{r-1} u_t \cdot \left(K_t + L\left(y_0^{\Delta_{t-1}, L^{-1}(\Delta_t)}\right) + x_0^{\Delta_t, L^{-1}(\Delta_{t+1})}\right) .$$

Therefore,

$$\sum_{u \in W^\perp} (-1)^{u \cdot K + s_0(u) + \ldots s_{r-1}(u)} = \begin{cases} 2^{\dim W^\perp} & \text{if all } K_t + L\left(y_0^{\Delta_{t-1}, L^{-1}(\Delta_t)}\right) + x_0^{\Delta_t, L^{-1}(\Delta_{t+1})} \in W \\ 0 & \text{otherwise,} \end{cases}$$

implying that

$$\mathsf{DP}[K](\Delta_0, \ldots, \Delta_r) = \begin{cases} 2^{-ms - \dim W} \left(\prod_{t=0}^{r-1} \mathsf{DDT}_{\boldsymbol{\mathcal{S}}}\left(\Delta_t, L^{-1}(\Delta_{t+1})\right)\right) & \text{if } K \in w_0 + W \\ 0 & \text{otherwise.} \end{cases}$$

□

Moreover, when the expanded key satisfies the conditions exhibited in the previous theorem, the set of the valid inputs of the characteristic can be explicitly described, as shown in the following proposition.

Proposition 1. *Let $(\Delta_0, \Delta_1, \ldots, \Delta_r)$ be an r-round differential characteristic, $r \geq 2$, satisfying the same conditions as in Theorem 1. If the expanded key is such that the characteristic is valid, then the set of valid inputs of the characteristic equals $\boldsymbol{\mathcal{S}}^{-1}(\widetilde{X_r})$ where $\widetilde{X_r}$ is a coset of the linear space*

$$X_r := \{x \in \mathsf{V}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1)) \mid L \circ \phi_{\Delta_{t-1}, L^{-1}(\Delta_t)} \circ \ldots \circ L \circ \phi_{\Delta_1, L^{-1}(\Delta_2)} \circ L(x) \\ \textit{belongs to } \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1})),\ \forall 1 \leq t \leq r-1\}.$$

Proof. We show by induction on $r \geq 2$ that the set of valid inputs of the r-round characteristic $(\Delta_0, \ldots, \Delta_r)$ is of the form $\boldsymbol{\mathcal{S}}^{-1}(\widetilde{X_r})$ where $\widetilde{X_r}$ is a coset of X_r, and that the images of the valid inputs before the r-th round form a coset of

$$L \circ \phi_{\Delta_{r-2}, L^{-1}(\Delta_{r-1})} \circ \ldots \circ L \circ \phi_{\Delta_1, L^{-1}(\Delta_2)} \circ L(X_r)\ .$$

For $r = 2$: it is well-known (see e.g. [DR07, Th. 1]) that the set formed by all images of the valid inputs after the first round, y, corresponds to the intersection between $K_1 + L(\mathsf{YDDT}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1)))$ and $\mathsf{XDDT}_{\boldsymbol{\mathcal{S}}}(\Delta_1, L^{-1}(\Delta_2))$. The set of all valid y is therefore a coset of the linear subspace

$$L(\mathsf{V}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1))) \cap \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_1, L^{-1}(\Delta_2))\ ,$$

which is equal to $L(X_2)$. Therefore, the valid inputs of the 2-round characteristic are the values of $\mathcal{R}^{-1}(c + L(X_2)) = \boldsymbol{\mathcal{S}}^{-1}(c' + X_2)$ for some offsets c, c', where $\mathcal{R} = L \circ \boldsymbol{\mathcal{S}}$.

Induction step: Consider a valid r-round characteristic. From the induction hypothesis, we know that the set of valid inputs of to the $(r-1)$-round characteristic $(\Delta_0, \ldots, \Delta_{r-1})$ is $\boldsymbol{\mathcal{S}}^{-1}(\widetilde{X_{r-1}})$, where $\widetilde{X}_{r-1}$ is a coset of X_{r-1}. Moreover, their images after the first $(r-2)$ rounds form a coset $\widetilde{Y_{r-1}}$ of

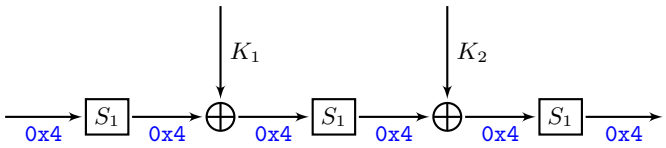
$$Y_{r-1} = L \circ \phi_{\Delta_{r-3}, L^{-1}(\Delta_{r-2})} \circ \ldots \circ L \circ \phi_{\Delta_1, L^{-1}(\Delta_2)} \circ L(X_{r-1}) \subset \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-2}, L^{-1}(\Delta_{r-1}))\ .$$

Since $(\Delta_{r-2}, L^{-1}(\Delta_{r-1}))$ is a super-planar differential for $\boldsymbol{\mathcal{S}}$ and the characteristic is valid, $\widetilde{Y_{r-1}}$ is non-empty and is included in $\mathsf{XDDT}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-2}, L^{-1}(\Delta_{r-1}))$. Therefore, we can choose $x_0^{\Delta_{r-2}, L^{-1}(\Delta_{r-1})} \in \widetilde{Y_{r-1}}$ so that $\widetilde{Y_{r-1}} = x_0^{\Delta_{r-2}, L^{-1}(\Delta_{r-1})} + Y_{r-1}$. Then,

$$\boldsymbol{\mathcal{S}}(\widetilde{Y_{r-1}}) = \boldsymbol{\mathcal{S}}(x_0^{\Delta_{r-2}, L^{-1}(\Delta_{r-1})}) + \phi_{\Delta_{r-2}, L^{-1}(\Delta_{r-1})}(Y_{r-1})$$

where $\phi_{\Delta_{r-2}, L^{-1}(\Delta_{r-1})}$ is linear. It follows that the images of $\boldsymbol{\mathcal{S}}^{-1}(\widetilde{X_{r-1}})$ after the first $(r-1)$ rounds form a coset of $L \circ \phi_{\Delta_{r-2}, L^{-1}(\Delta_{r-1})}(Y_{r-1})$. Moreover, any element $u + y$, $y \in L \circ \phi_{\Delta_{r-2}, L^{-1}(\Delta_{r-1})}(Y_{r-1})$ in this coset also satisfies the last-round differential if and only if it belongs to $\mathsf{XDDT}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r))$, or equivalently if $L \circ \phi_{\Delta_{r-2}, L^{-1}(\Delta_{r-1})}(y) \in \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r))$. It follows that any such element corresponds to an input in $\boldsymbol{\mathcal{S}}^{-1}(\widetilde{X_r})$ where $\widetilde{X_r}$ is a coset of X_r. □

Remark 1. For a given characteristic $(\Delta_0, \ldots, \Delta_r)$, the offset of the coset $\widetilde{X_r}$ of X_r defined in Prop. 1 may depend on the expanded key K in the weak-key set. For instance, let us consider 3 rounds of a toy cipher operating on 4 bits, whose round function S_1 is defined in Appendix A. Let us focus on the differential



characteristic $(\mathtt{0x4}, \mathtt{0x4}, \mathtt{0x4})$. We have $\mathsf{XDDT}_{S_1}(\mathtt{0x4}, \mathtt{0x4}) = \mathtt{0x3} + \langle \mathtt{0x4}, \mathtt{0xb} \rangle$, $\mathsf{YDDT}_{S_1}(\mathtt{0x4}, \mathtt{0x4}) = \mathtt{0x7} +$

$\langle \mathtt{0x4}, \mathtt{0x1} \rangle$ and $\mathsf{Z}_{S_1}(\mathtt{0x4}, \mathtt{0x4}) = \langle (\mathtt{0x4}, \mathtt{0x4}), (\mathtt{0xb}, \mathtt{0x1}) \rangle$. We deduce from Theorem 1 that the set of weak-keys is

$$\begin{aligned}\mathcal{K} &= (x_0^{\mathtt{0x4},\mathtt{0x4}} + y_0^{\mathtt{0x4},\mathtt{0x4}}, x_0^{\mathtt{0x4},\mathtt{0x4}} + y_0^{\mathtt{0x4},\mathtt{0x4}}) + W \\ &= (\mathtt{0x4}, \mathtt{0x4}) + \langle (\mathtt{0x4}, \mathtt{0x0}), (\mathtt{0x1}, \mathtt{0x0}), (\mathtt{0xb}, \mathtt{0x1}), (\mathtt{0x0}, \mathtt{0x4}), (\mathtt{0x0}, \mathtt{0xb}) \rangle.\end{aligned}$$

Moreover, $X_2 = \mathsf{V}_{S_1}(\mathtt{0x4}, \mathtt{0x4}) \cap \mathsf{U}_{S_1}(\mathtt{0x4}, \mathtt{0x4}) = \langle \mathtt{0x4} \rangle$. However, for $K = (\mathtt{0x5}, \mathtt{0x4})$, the set of valid inputs for the characteristic is $\{\mathtt{0x8}, \mathtt{0xc}\} = S_1^{-1}(\mathtt{0x2} + X_2)$ whereas for $K' = (\mathtt{0xf}, \mathtt{0x5})$, it equals $\{\mathtt{0x3}, \mathtt{0x7}\} = S_1^{-1}(\mathtt{0x3} + X_2)$.

In the case where the first-round and last-round differentials for S are also super-planar, the valid inputs of the characteristic form an affine subspace, which then propagates as a chain of subspaces across the r rounds, as observed in the following direct corollary. This corresponds to the notion of input-planar and output-planar characteristic in [DR07]. Obviously, the additional condition on the first-round and last-round differentials is necessary. For instance, the valid inputs of any 2-round characteristic in AES do not form an affine subspace.

Corollary 1. *Let $(\Delta_0, \Delta_1, \ldots, \Delta_r)$ be an r-round differential characteristic, $r \geq 2$, such that* all *constituent differentials for the Sbox S are super-planar. If the expanded key is such that the characteristic is valid, then there is a chain of affine subspaces of the same dimension that propagates across the r rounds where the linear part V_i of the subspace at the input of Round i, $0 \leq i < r$, is given by*

$$\begin{aligned}V_0 = \{x \in \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1)) \mid\ & L \circ \phi_{\Delta_{t-1}, L^{-1}(\Delta_t)} \circ \ldots \circ L \circ \phi_{\Delta_0, L^{-1}(\Delta_1)}(x) \\ & \textit{belongs to } \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1})),\ \forall 1 \leq t \leq r-1\}, \\ \textit{and } V_i = L \circ \phi_{\Delta_{i-1}, L^{-1}(\Delta_i)}(V_{i-1}) & \textit{ for all } 1 \leq i < r\ .\end{aligned}$$

Therefore, the number of valid inputs of an r-round plateau characteristic of the type analyzed in Prop. 1, 2^{d_r} (d_r is the dimension of the subspaces in Coro. 1) is a decreasing sequence satisfying $d_r \geq 1$ since the characteristic is valid. The usual situation is that this sequence decreases when r increases and d_r becomes constant and equal to 1 after a reasonable number of rounds, and Coro. 1 becomes trivial. It is worth noting that, in some particular cases, the minimal number of valid inputs for a valid plateau characteristic may be equal to $2^{d_{\min}}$ with $d_{\min} > 1$, as shown by Prop. 8 in Appendix C.

2.4 Plateau Characteristics and Invariant Subspaces

We now show that the situation, where the sequence $(d_r)_{r \geq 0}$ converges to a constant that exceeds $d_{\min}$, especially occurs when the linear layer of the cipher satisfies a particular property. This property is described in the following lemma that will be extensively used in the paper, since it highly influences the behaviour of the previously analyzed differential characteristics.

Lemma 3. *Let $L : (\mathbb{F}_{2^s})^m \to (\mathbb{F}_{2^s})^m$ be an $\mathbb{F}_{2^s}$-linear mapping defined by $M \in \mathcal{M}_m(\mathbb{F}_{2^s})$. Then, L is said to satisfy Property $(\mathcal{P})$ if one of the following equivalent conditions holds:*

- *all entries of M are in $\{0, 1\}$ and all rows of M have an odd Hamming weight.*
- *For any additive subgroup E of $\mathbb{F}_{2^s}$, $L(E^m) = E^m$ and for any $x \in \mathbb{F}_{2^s}$, $L(x^{\times m}) = x^{\times m}$.*

where $x^{\times m}$ denotes[1] the element $(x, x, \ldots, x)$ in $\mathbb{F}_{2^s}^m$.

Proof. Let $M \in \mathcal{M}_m(\mathbb{F}_{2^s})$ be a binary matrix such that all its rows have an odd Hamming weight and $x \in \mathbb{F}_{2^s}$. Then it is trivial that $Mx^{\times m} = x^{\times m}$. Moreover, let E be an additive subgroup of $\mathbb{F}_{2^s}$, $b \in E$, and let e_i denote the i-th vector of the canonical basis of $(\mathbb{F}_2)^m$. Then, for all $1 \leq i \leq m$, $M(be_i) = b\,(Me_i) \in E^m$. Therefore, $L(E^m) \subset E^m$ and since L is bijective, $L(E^m) = E^m$.

[1] In order to avoid confusion with exponentiation x^u in the field $\mathbb{F}_{2^s}$.

Conversely, suppose that for any additive subgroup E of $\mathbb{F}_{2^s}$, $L(E^m) = E^m$ and for all $x \in \mathbb{F}_{2^s}$, $L(x^{\times m}) = x^{\times m}$. If there exist $1 \leq i, j \leq m$ such that $M_{i,j} \notin \{0,1\}$, then $(Me_j)_i = M_{i,j} \notin \{0,1\}$. Then, $L(\mathbb{F}_2^m) \subsetneq \mathbb{F}_2^m$, which contradicts the hypothesis on L. Therefore, all $M_{i,j}$ are in $\{0,1\}$. Moreover,

$$(Mx^{\times m})_i = \left(\sum_{j=1}^{m} M_{i,j}\right) x = \begin{cases} 0 \text{ if } w_H(M[i]) \text{ is even} \\ x \text{ otherwise,} \end{cases}$$

where $M[i]$ denotes the i-th row of M. It implies that all $M[i]$ have an odd Hamming weight. □

The linear layers in MIDORI [BBI+15], SCREAM, ISCREAM [GLS+14], PRINCE [BCG+12] or MANTIS [BJK+16] satisfy Property $(\mathcal{P})$. The following lemma provides the expression of the images by such linear layers of the elements in affine subspaces of the form $\{a,b\}^m$.

Lemma 4. *Let $\{a,b\} \subset \mathbb{F}_2^s$ and $A \in \{a,b\}^m$. Let $L : (\mathbb{F}_{2^s})^m \to (\mathbb{F}_{2^s})^m$ be an $\mathbb{F}_{2^s}$-linear mapping satisfying $(\mathcal{P})$. Then, $L(A) \in \{a,b\}^m$, and for all $x \in \{a,b\}$,*

$$L\left(\left(\mathbf{1}_{A_j=x}\right)_{1\leq j\leq m}\right) = \left(\mathbf{1}_{L(A)_j=x}\right)_{1\leq j\leq m} ,$$

where $\mathbf{1}_{y=x} := 1$ if $y = x$ and 0 otherwise.

Proof. The fact that $\{a,b\}^m$ is invariant under L comes from Lemma 3 using that $\{a,b\}^m = a^{\times m} + \langle a+b\rangle^m$. Now, let M be the matrix such that $L(x) = Mx$. Let $1 \leq \ell \leq m$. Let us define $I_\ell := \{j \in [\![1,m]\!] \mid M_{\ell,j} = 1\}$. Then, for all $x \in \{a,b\}$,

$$\left[L\left(\left(\mathbf{1}_{A_j=x}\right)_{1\leq j\leq m}\right)\right]_\ell = \sum_{j\in I_\ell} \mathbf{1}_{A_j=x} \in \{0,1\} .$$

By Lemma 3, $\#I_\ell$ is odd, implying

$$\left[L\left(\left(\mathbf{1}_{A_j=x}\right)_{1\leq j\leq m}\right)\right]_\ell = 1 \iff \#\{j \in I_\ell \mid A_j = x\} \text{ is odd} \iff [L(A)]_\ell = x.$$

□

The following proposition now exhibits some differential characteristics for which the number of valid inputs does not decrease with the number of rounds and is strictly larger than 2.

Proposition 2. *Let us consider an SPN whose linear layer L satisfies Property $(\mathcal{P})$. Let (a,b) be a super-planar differential for S with $\mathsf{DDT}(a,b) = 2^\ell$ such that $\mathsf{XDDT}_S(a,b) = \mathsf{XDDT}_S(b,a)$. Then, for all $r \geq 2$ and all $\Delta_0 \in \{a,b\}^m$, there exist a differential characteristic $(\Delta_0, \Delta_1, \ldots, \Delta_r)$ and an affine key space $\mathcal{K} \subset \mathbb{F}_2^{sm(r-1)}$ of dimension $m(\ell r - \dim(\chi_r))$ such that, for any $K \in \mathcal{K}$,*

$$\mathsf{DP}[K](\Delta_0, \ldots, \Delta_r) = 2^{-m(s-\dim(\chi_r))}$$

where $\chi_r := \left\{x \in \mathsf{V}_S(a,b) \mid \forall 0 \leq i \leq r-2,\ \phi_{a,b}^i(x) \in \mathsf{U}_S(a,b)\right\}$. Moreover, for any $K \in \mathcal{K}$, the set of valid inputs for $(\Delta_0, \ldots, \Delta_r)$ is a coset of $\left(\phi_{a,b}^{-1}(\chi_r)\right)^m$.

In particular, when $\mathsf{U}_S(a,b) = \mathsf{V}_S(a,b)$, we have $\mathcal{K} = \left(x_0^{a,b} + y_0^{a,b} + \mathsf{U}_S(a,b)\right)^{m(r-1)}$ and, for any weak key, the set of valid inputs equals $\mathsf{XDDT}_S(a,b)^m$ and is an invariant subspace for the cipher.

Proof. The differences Δ_t, for $1 \leq t \leq r$, are successively determined from Δ_0 as follows. For any $\Delta_t \in \{a,b\}^m$, we choose Δ_{t+1} such that, for all $1 \leq j \leq m$, $L^{-1}(\Delta_{t+1})[j] \in \{a,b\}$ and satisfies $\Delta_t[j] = L^{-1}(\Delta_{t+1})[j] + a + b$. Since $L^{-1}(\Delta_{t+1}) \in \{a,b\}^m$ and L satisfies $(\mathcal{P})$, Lemma 4 implies that $\Delta_{t+1} \in \{a,b\}^m$. Since $\mathsf{XDDT}_S(a,b) = \mathsf{XDDT}_S(b,a)$, (b,a) is also super-planar and we have $\mathsf{U}_S(a,b) = \mathsf{U}_S(b,a) := \mathsf{U}_S$,

$\mathsf{V}_S(a,b) = \mathsf{V}_S(b,a) := \mathsf{V}_S$, $\phi_{a,b} = \phi_{b,a} := \phi$ and $\mathsf{Z}_S(a,b) = \mathsf{Z}_S(b,a) := \mathsf{Z}_S$. We can also choose the offsets such that $x_0^{a,b} = x_0^{b,a} := x_0$ and thus $y_0^{a,b} = y_0^{b,a} := y_0$. Therefore, we deduce from Theorem 1 that $(\Delta_0, \dots, \Delta_r)$ is a valid characteristic for $K := (K_t)_{1 \le t \le r-1}$ if and only if $K \in w_0 + W_{r-1}$ where

$$w_0 := (x_0^{\times m} + L(y_0^{\times m}))^{\times r-1} = (x_0 + y_0)^{\times m(r-1)}$$

$$\text{and } W_{r-1} := \left[L(\mathsf{V}_S^m) \times \{0\}^{sm(r-2)}\right] + \sum_{t=1}^{r-2} \left[\{0\}^{sm(t-1)} \times (I \times L)(\mathsf{Z}_S^m) \times \{0\}^{sm(r-2-t)}\right] + \left[\{0\}^{sm(r-2)} \times \mathsf{U}_S^m\right]$$

$$= (\Omega_{r-1})^m \ ,$$

$$\text{with } \Omega_{r-1} := \left(\mathsf{V}_S \times \{0\}^{s(r-2)}\right) + \sum_{t=1}^{r-2} \left(\{0\}^{s(t-1)} \times \mathsf{Z}_S \times \{0\}^{s(r-2-t)}\right) + \left(\{0\}^{s(r-2)} \times \mathsf{U}_S\right).$$

Therefore, $\mathcal{K} = (x_0 + y_0)^{\times m(r-1)} + \Omega_{r-1}^m$ and, when $(K_t)_{1 \le t \le r-1} \in \mathcal{K}$, we have

$$\mathsf{DP}[K](\Delta_0 \dots \Delta_r) = 2^{-ms - \dim W_{r-1}} \prod_{t=0}^{r-1} (\mathsf{DDT}_S(a,b))^m = 2^{m(\ell r - s - \dim \Omega_{r-1})} \tag{2}$$

By grouping spaces together, we then deduce the form of Ω_{r-1} depending on the parity of r:

$$\Omega_{2t-1} = \mathsf{V}_S \mathsf{Z}_S^{t-1} + \mathsf{Z}_S^{t-1} \mathsf{U}_S$$
$$\Omega_{2t} = \mathsf{V}_S \mathsf{Z}_S^{t-1} \mathsf{U}_S + \mathsf{Z}_S^t$$

for all $t \ge 1$. It follows that

$$\begin{aligned} \dim(\Omega_{2t-1}) &= \dim(\mathsf{V}_S \mathsf{Z}_S^{t-1}) + \dim(\mathsf{Z}_S^{t-1} \mathsf{U}_S) - \dim(\left(\mathsf{V}_S \mathsf{Z}_S^{t-1}\right) \cap \left(\mathsf{Z}_S^{t-1} \mathsf{U}_S\right)) \\ &= 2t\ell - \dim(\left(\mathsf{V}_S \mathsf{Z}_S^{t-1}\right) \cap \left(\mathsf{Z}_S^{t-1} \mathsf{U}_S\right)) \ . \end{aligned}$$

Similarly, $\dim(\Omega_{2t}) = (2t+1)\ell - \dim(\left(\mathsf{V}_S \mathsf{Z}_S^{t-1} \mathsf{U}_S\right) \cap \mathsf{Z}_S^t)$. Let us now prove that

$$\left(\mathsf{V}_S \mathsf{Z}_S^{t-1}\right) \cap \left(\mathsf{Z}_S^{t-1} \mathsf{U}_S\right) = \left\{(\phi^i(x))_{0 \le i \le 2t-2} \mid x \in \chi_{2t}\right\} = \left(\mathsf{V}_S \mathsf{Z}_S^{t-1} \mathsf{U}_S\right) \cap \mathsf{Z}_S^t \ .$$

We will prove the first equality for $r = 2t$ by double inclusion. By definition,

$$\mathsf{Z}_S = \{(x, \phi_{a,b}(x)) \mid x \in \mathsf{U}_S\} \subset \mathsf{U}_S \times \mathsf{V}_S \ .$$

Let $x \in \chi_{2t}$. By definition, $\phi^0(x) = x \in \mathsf{V}_S$. The previous remark leads to $(\phi^i(x))_{1 \le i \le 2t-2} \in \mathsf{Z}_S^{t-1}$. Similarly, $(\phi^i(x))_{0 \le i \le 2t-3} \in \mathsf{Z}_S^{t-1}$ and $\phi^{2t-2}(x) = \phi^{r-2}(x) \in \mathsf{U}_S$ by definition of χ_{2t}. Therefore,

$$(\phi^i(x))_{0 \le i \le 2t-2} \in \left(\mathsf{V}_S \mathsf{Z}_S^{t-1}\right) \cap \left(\mathsf{Z}_S^{t-1} \mathsf{U}_S\right).$$

Conversely, let $x := (x_0, \dots, x_{2t-2}) \in \left(\mathsf{V}_S \mathsf{Z}_S^{t-1}\right) \cap \left(\mathsf{Z}_S^{t-1} \mathsf{U}_S\right)$. Then $x_0 \in \mathsf{U}_S \cap \mathsf{V}_S$. Moreover, if for some $j \in [\![0, 2t-3]\!]$, $x_{j+1} \ne \phi(x_j)$, then $(x_j, x_{j+1}) \notin \mathsf{Z}_S$. If j is even, $x \notin \mathsf{Z}_S^{t-1} \mathsf{U}_S$, and if j is odd $x \notin \mathsf{V}_S \mathsf{Z}_S^{t-1}$. Therefore, $x = (\phi^j(x_0))_{0 \le j \le 2t-2}$ and $x_0 \in \chi_{2t}$. This achieves the proof of the first equality in the case r even, the case r odd is proved similarly. Formula (2) then leads to

$$\mathsf{DP}[K](\Delta_0, \dots, \Delta_r) = 2^{\ell m r - ms - m(r\ell - \dim \chi_r)} = 2^{-m(s - \dim \chi_r)} \ .$$

Now, from Prop. 1, for any $K \in \mathcal{K}$, the set of valid inputs for the characteristic is equal to $\boldsymbol{\mathcal{S}}^{-1}(\widetilde{X_r})$ where $\widetilde{X_r}$ is a coset of $X_r := \{x \in \mathsf{V}_S^m \mid \left((L \circ \phi)^i \circ L\right)(x) \in \mathsf{U}_S^m, \ \forall 0 \le i \le r-2\}$. Using that $L(\mathsf{U}_S^m) = \mathsf{U}_S^m$, we deduce that $X_r = \chi_r^m$. Since, (a,b) is super-planar, we have that $\boldsymbol{\mathcal{S}}^{-1}(\widetilde{X_r})$ is a coset of $\left(\phi^{-1}(\chi_r)\right)^m$ which proves the result in the general case.

Now, when $\mathsf{U}_S = \mathsf{V}_S$, we have $\chi_r = \mathsf{U}_S \cap \mathsf{V}_S = \mathsf{U}_S = \mathsf{V}_S$ which has dimension ℓ and is invariant under ϕ. Hence, the set of valid inputs is a coset of U_S^m which is included in $\mathsf{XDDT}_S(a,b)^m$. Therefore, the set of valid inputs is exactly $\mathsf{XDDT}_S(a,b)^m$. Furthermore, $\Omega_{r-1} = \mathsf{U}_S^{r-1}$ and $\mathcal{K} = (x_0 + y_0)^{\times m(r-1)} + \mathsf{U}_S^{m(r-1)}$. Then, $(L \circ \boldsymbol{\mathcal{S}})(\mathsf{XDDT}_S(a,b)^m) = y_0^{\times m} + \mathsf{U}_S^m$ and $\mathsf{Add}_{K_t}\left(y_0^{\times m} + \mathsf{U}_S(a,b)^m\right) = x_0^{\times m} + \mathsf{U}_S^m = \mathsf{XDDT}_S(a,b)^m$ which proves that $\mathsf{XDDT}_S(a,b)^m$ is invariant under the round-function $\mathsf{Add}_{K_t} \circ \mathcal{R}$ if $K_t \in (x_0 + y_0)^{\times m} + \mathsf{U}_S^m$. Note that, if $K_t \notin (x_0 + y_0)^{\times m} + \mathsf{U}_S^m$ then $\mathsf{Add}_{K_t}\left(y_0^{\times m} + \mathsf{U}_S^m\right) = c_0 + \mathsf{U}_S^m$ for some $c_0 \notin x_0^{\times m} + \mathsf{U}_S^m$, and the subspace does not propagate. □

The simplest case in which the previous proposition applies is when there exists a super-planar differential for S with the same input and output differences, $a = b$ in Prop. 2. Then, $\mathsf{XDDT}_S(a,b) = \mathsf{XDDT}_S(b,a)$ and 0 and a are included in both $\mathsf{U}_S(a,a)$ and $\mathsf{V}_S(a,a)$, and therefore in χ_r because $\phi_{a,a}(a) = a$. It follows that $\dim \chi_r \geq 1$ and that the iterative characteristic $(a^{\times m}, \ldots, a^{\times m})$ is plateau with $\mathsf{DP}[K](a^{\times m}, \ldots, a^{\times m}) \geq 2^{-m(s-1)}$ for $K \in \mathcal{K}$.

The case of Midori64. The invariant subspaces in MIDORI64 exhibited by Guo *et al.* [GJN+16] for a certain set of weak expanded-keys actually correspond to the valid inputs of some iterative differential characteristic of the form $(a^{\times m}, \ldots, a^{\times m})$ whose probability is independent of the number of rounds. Let us consider two such examples:

- For $a = \mathtt{0xf}$, the Sbox of MIDORI64 satisfies

$$\mathsf{XDDT}_S(\mathtt{0xf}, \mathtt{0xf}) = \mathsf{YDDT}_S(\mathtt{0xf}, \mathtt{0xf}) = \mathtt{0x2} + \langle \mathtt{0xa}, \mathtt{0xf} \rangle.$$

  The hypotheses of Prop. 2 are then satisfied. Moreover, for any r, $\mathsf{U}_S(\mathtt{0xf}, \mathtt{0xf}) = \mathsf{V}_S(\mathtt{0xf}, \mathtt{0xf}) = \chi_r = \langle \mathtt{0xa}, \mathtt{0xf} \rangle$ and has dimension 2. It follows that the expanded key K is a weak key if all round keys belong to

$$\left(x_0^{\mathtt{0xf},\mathtt{0xf}} + y_0^{\mathtt{0xf},\mathtt{0xf}} + \langle \mathtt{0xa}, \mathtt{0xf} \rangle\right)^{16} = \langle \mathtt{0xa}, \mathtt{0xf} \rangle^{16}.$$

  For these weak expanded keys, the characteristic $(\mathtt{0xf}^{\times 16}, \ldots, \mathtt{0xf}^{\times 16})$ has probability $2^{-2m} = 2^{-32}$.
- For $a = \mathtt{0x1}$, we have $\mathsf{XDDT}_S(\mathtt{0x1}, \mathtt{0x1}) = \mathsf{YDDT}_S(\mathtt{0x1}, \mathtt{0x1}) = \mathtt{0x8} + \langle \mathtt{0x1} \rangle$. Then, $\chi_r = \langle \mathtt{0x1} \rangle$ for any r, and if each round key belongs to χ_r^m, the characteristic $(\mathtt{0x1}^{\times 16}, \ldots, \mathtt{0x1}^{\times 16})$ has probability $2^{-3m} = 2^{-48}$.

As observed in [GJN+16], the space formed by the weak expanded-keys for the second characteristic is compatible with the key schedule proposed by the designers of MIDORI64 while this is not the case for the first iterative characteristic. It is worth noting that we also derive that these characteristics are plateau, which means that their probability is equal to zero when the expanded key does not belong to the weak-key space. This implies for instance that, because of MIDORI64 key schedule, the characteristic $(\mathtt{0xf}^{\times 16}, \ldots, \mathtt{0xf}^{\times 16})$ has probability 0 for all keys in $\mathbb{F}_2^{128}$ when we consider MIDORI64 with its key schedule.

The case of iScream. Another important remark is that Prop. 2 is not reduced to characteristics of the form $(\Delta, \Delta, \ldots, \Delta)$. In [LMR15], the authors present different types of invariant-subspace attacks. In particular, they exhibit six affine subspaces of dimension 3 invariant under the 8-bit Sbox of ISCREAM. Four of them are actually equal to $\mathsf{XDDT}_S(a,b)$ for some super-planar differentials (a,b), and for these pairs we have $\mathsf{XDDT}_S(a,b) = \mathsf{XDDT}_S(b,a)$. Since the Sbox of ISCREAM is involutive, we have $\mathsf{U}_S(b,a) = \mathsf{V}_S(a,b)$. Moreover, the linear layer of ISCREAM satisfies Property $(\mathcal{P})$. Thus, Prop. 2 applies and if the round keys all belong to the same affine subspace of dimension $\ell \times m = 48$, $\mathsf{XDDT}_S(a,b)^{16}$ is an invariant subspace for the whole cipher, as pointed out by [LMR15]. In terms of differential characteristic, it corresponds to plateau characteristics $(\Delta_0, \ldots, \Delta_r)$ with $\Delta_t \in \{a,b\}^m$ such that $\mathsf{DP}[K](\Delta_0, \ldots, \Delta_r) = 2^{-m(s-3)} = 2^{-80}$.

An example in which $\mathsf{U}_S(a,b) \neq \mathsf{V}_S(a,b)$. Prop. 2 also applies when $\mathsf{U}_S(a,b) \neq \mathsf{V}_S(a,b)$. For instance, the Sbox S_1 defined in App. A satisfies $\mathsf{XDDT}_{S_1}(\mathtt{0x4},\mathtt{0x4}) = \mathtt{0x3} + \langle \mathtt{0x4}, \mathtt{0xb} \rangle$ and $\mathsf{YDDT}_{S_1}(\mathtt{0x4},\mathtt{0x4}) = \mathtt{0x7} + \langle \mathtt{0x4}, \mathtt{0x1} \rangle$. Therefore $\chi_r = \langle \mathtt{0x4} \rangle$ has dimension 1 for any r. If this Sbox was used instead of MIDORI64's Sbox, the resulting cipher would have a weak-key space $\mathcal{K}$ of dimension $m \times (\ell r - \dim(\chi_r)) = 16 \times (2r-1)$ such that, for the expanded keys in $\mathcal{K}$, the differential characteristic $(\mathtt{0x4}^{\times 16}, \mathtt{0x4}^{\times 16}, \ldots, \mathtt{0x4}^{\times 16})$ has probability $2^{-16(4-1)} = 2^{-48}$. Note that here, $\mathcal{K}$ is not of the form $\mathcal{A}^{r-1}$ for any affine subspace $\mathcal{A}$.

The existence of such differential characteristics is rather rare and can be checked by searching for affine subspaces that propagate through the cipher. Moreover, the proportion of weak expanded keys is limited since it is equal to $\mathsf{EDP}(\Delta_0, \ldots, \Delta_r)/\mathsf{DP}[K](\Delta_0, \ldots, \Delta_r)$ with $K \in \mathcal{K}$. However, as usual in differential cryptanalysis, the relevant quantity is not the probability of a characteristic but the probability of a differential, which may include a very large number of valid characteristics.

3 Fixed-Key Truncated Differentials of Constant Probability

Following [DR07], the previous section has exhibited situations where a large family of plateau characteristics exist for an arbitrary number of rounds. By definition, none of these characteristics satisfy the hypothesis of stochastic equivalence. What happens for a given *differential*, composed of such plateau characteristics, is then unclear. Indeed, each of the constituent characteristics is valid for a given set of weak expanded-keys, but the weak keys may be the same for the different characteristics or not. In other words, we wonder whether there is a (possibly strong) clustering effect, or not, when the key is fixed.

In this section, we focus on truncated differentials of the form $\{\alpha, \beta\}^m$, where (α, β) is a super-planar differential for the Sbox satisfying some specific property. Indeed, the truncated differentials reported by Baudrin *et al.* [BFL+23] for an arbitrary number of rounds of MIDORI64 have this particular form. However, all results in this section can be generalized to truncated differentials (a, b) with $a, b \in \mathcal{A}$ for a larger set of differences $\mathcal{A}$. We chose to detail this generalization in Section 6 and to keep the current section as simple as possible. Indeed, the case $\mathcal{A} = \{\alpha, \beta\}$ already captures the nature of the different (and unexpected) behaviours of fixed-key truncated differentials composed of plateau characteristics.

In this section, we will focus on the differentials satisfying the following property, which holds for several practical ciphers.

Definition 6. *A differential (α, β) for $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$ with $\alpha \neq \beta$ is said to be a* square differential *for S if it satisfies the following conditions:*

1. *(α, α), (α, β), (β, α), (β, β) are super-planar differentials.*
2. *$\mathsf{U}_S(\alpha, \alpha) = \mathsf{U}_S(\alpha, \beta) := \mathsf{U}_S(\alpha)$ and $\mathsf{U}_S(\beta, \alpha) = \mathsf{U}_S(\beta, \beta) := \mathsf{U}_S(\beta)$.*
3. *$\mathsf{U}_S(\alpha) + \langle x_0^{\alpha,\beta} + x_0^{\alpha,\alpha} \rangle = \mathsf{U}_S(\beta) + \langle x_0^{\beta,\beta} + x_0^{\beta,\alpha} \rangle := E$*
4. *$\forall (x, y) \in \{\alpha, \beta\}^2, \mathsf{V}_S(x, y) \subset E$*

If, additionally, $\forall (x, y) \in \{\alpha, \beta\}^2, y_0^{x,y} + x_0^{y,\alpha} \in (y_0^{\alpha,\alpha} + x_0^{\alpha,\alpha}) + E$ then (α, β) is said to be a perfect square differential.

These conditions might seem very restrictive, but hold for several practical ciphers: Table 2 in App. B provides examples of square differentials for some known Sboxes. Moreover, we will see later that, in many cases, some of the requirements are consequences of some others. For example, if S is an involution, all square differentials are perfect square differentials. Indeed, in that case $y_0^{x,y} \in x_0^{y,x} + \mathsf{U}_S(y)$. It follows that

$$y_0^{x,y} + x_0^{y,\alpha} \in (x_0^{y,x} + x_0^{y,\alpha}) + \mathsf{U}_S(y) = \begin{cases} \mathsf{U}_S(y) \subset E & \text{if } x = \alpha \\ x_0^{y,\beta} + x_0^{y,\alpha} + \mathsf{U}_S(y) = E & \text{if } x = \beta \end{cases}$$

by definition of E.

The following three properties of square differentials will be useful for proving the main result.

Lemma 5. *Let (α, β) a super-planar differential for S such that $\mathsf{U}_S(\alpha, \beta) = \mathsf{U}_S(\alpha, \alpha) := \mathsf{U}_S(\alpha)$. Then $\mathsf{U}_S(\alpha)$ and $\langle x_0^{\alpha,\beta} + x_0^{\alpha,\alpha} \rangle$ are in direct sum, implying that $\dim E = \dim \mathsf{U}_S(\alpha) + 1$.*

Proof. If $x_0^{\alpha,\beta} + x_0^{\alpha,\alpha} \in \mathsf{U}_S(\alpha)$ then $x_0^{\alpha,\alpha} \in x_0^{\alpha,\beta} + \mathsf{U}_S(\alpha) = \mathsf{XDDT}_S(\alpha, \beta)$. This is impossible since $\mathsf{XDDT}_S(\alpha, \alpha)$ and $\mathsf{XDDT}_S(\alpha, \beta)$ are disjoint. □

Lemma 6. *Let (α, β) be a square differential for S. Then, for all $x, y \in \{\alpha, \beta\}$,*

$$\mathsf{Z}_S(x, y) + (\{0\}^s \times E) = \mathsf{U}_S(x, y) \times E. \tag{3}$$

Proof. Any element in $\mathsf{Z}_S(x, y) + (\{0\}^s \times E)$ can be written $(\theta, \phi_{x,y}(\theta) + e)$ for some $\theta \in \mathsf{U}_S(x, y)$ and $e \in E$. We deduce that it belongs to $\mathsf{U}_S \times E$ if and only if $\{\phi_{x,y}(\theta) \mid \theta \in \mathsf{U}_S(x, y)\} = \mathsf{V}_S(x, y)$ is included in E, which corresponds to Condition 4 in Def. 6. Moreover, the two linear spaces have the same dimension, $\dim \mathsf{U}_S(x, y) + \dim E$, implying that there are equal if and only if $\mathsf{V}_S(x, y) \subset E$. □

Lemma 7. *Let us consider an SPN whose linear layer L satisfies Property $(\mathcal{P})$. Let (α, β) be a square differential for S and $(\Delta_0, \ldots, \Delta_r)$ be a r-round characteristic with $\Delta_t \in \{\alpha, \beta\}^m$ for all $0 \leq t \leq r$. Then, the linear part of the subspace formed by the weak expanded keys, $W_{r-1}(\Delta_0, \ldots, \Delta_r)$, is independent of Δ_r.*

Proof. The only subspace in the definition of W_{r-1} in Theorem 1 that may depend on Δ_r is $\mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r))$. But Condition 2 in Definition 6 implies that $\mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r)) = \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1})$. □

The following lemma now shows that, in the particular case of square differentials, there is a relation between the linear part of the weak-key space W_r for which an $(r+1)$-round characteristic $(\Delta_0, \ldots, \Delta_r, \Delta_{r+1})$ is valid, and the linear part of the weak-key space W_{r-1} for $(\Delta_0, \ldots, \Delta_r)$.

Lemma 8. *Let us consider an SPN whose linear layer L satisfies Property $(\mathcal{P})$. Let (α, β) be a square differential for S and $(\Delta_0, \ldots, \Delta_{r+1})$ be a $(r+1)$-round characteristic with $\Delta_t \in \{\alpha, \beta\}^m$ for all $0 \leq t \leq r+1$. Then, if $r \geq 2$,*

$$\left(\{0\}^{sm(r-1)} \times \prod_{j=1}^{m} \left\langle x_0^{\Delta_r[j],\alpha} + x_0^{\Delta_r[j],\beta} \right\rangle \right) + W_r = W_{r-1} \times E^m \ .$$

Moreover, for a two-round characteristic,

$$\prod_{j=1}^{m} \left\langle x_0^{\Delta_1[j],\alpha} + x_0^{\Delta_1[j],\beta} \right\rangle + W_1 = E^m$$

Proof. On the one hand, we have by Condition 3 in Def. 6

$$\mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_1) + \prod_{j=1}^{m} \left\langle x_0^{\Delta_1[j],\alpha} + x_0^{\Delta_1[j],\beta} \right\rangle = E^m \ .$$

From Theorem 1, we know that

$$W_1 = L(\mathsf{V}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1))) + \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_1, L^{-1}(\Delta_2)) \subset E^m + \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_1) \ ,$$

because of Condition 4. in Definition 6. It follows that

$$\prod_{j=1}^{m} \left\langle x_0^{\Delta_1[j],\alpha} + x_0^{\Delta_1[j],\beta} \right\rangle + W_1 \subset E^m$$

and we also have that

$$E^m \subset \prod_{j=1}^{m} \left\langle x_0^{\Delta_1[j],\alpha} + x_0^{\Delta_1[j],\beta} \right\rangle + W_1$$

since $\mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_1) \subset W_1$. This proves the result in the case $r = 1$.

Now, for $r \geq 2$, since $L(E^m) = E^m$,

$$\begin{aligned}\mathcal{E} &= \left[(I \times L)\left(\mathsf{Z}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r))\right)\right] + \left[\{0\}^{sm} \times E^m\right] \\ &= (I \times L)\left(\mathsf{Z}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r)) + \{0\}^{sm} \times E^m\right) \\ &= (I \times L)(\mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}) \times E^m) = L(\mathsf{U}_S(\Delta_{r-1})) \times E^m \ ,\end{aligned}$$

where the last equality comes from Lemma 6. Let W'_{r-1} denote the sum of the first $(r-1)$ subspaces defining W_{r-1} in Th. 1, i.e.,

$$W_{r-1} = W'_{r-1} + \left(\{0\}^{sm(r-2)} \times \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1})\right) \ .$$

Then, we have

$$\begin{aligned}\mathcal{E}' &= \left(\{0\}^{sm(r-1)} \times \prod_{j=1}^{m} \left\langle x_0^{\Delta_r[j],\alpha} + x_0^{\Delta_r[j],\beta} \right\rangle\right) + W_r \\ &= \left(W'_{r-1} \times \{0\}^{sm}\right) + \{0\}^{sm(r-2)} \times \left[(I \times L)\left(\mathsf{Z}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}, L^{-1}(\Delta_r))\right)\right] + \left[\{0\}^{sm(r-1)} \times E^m\right] \\ &= \left(W'_{r-1} \times \{0\}^{sm}\right) + (\mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_{r-1}) \times E^m) = W_{r-1} \times E^m \ .\end{aligned}$$

□

The following result considers an SPN with $(r+1)$ rounds and a given key. It determines the number of $(r+1)$-round characteristics with all differences in $\{a, b\}^m$ that are valid for this specific key and share the same first r differences.

Proposition 3. *Let us consider an SPN with $(r+1)$ rounds, $r \geq 1$, whose linear layer L satisfies Property $(\mathcal{P})$. Let (α, β) a square differential for S with $\mathsf{DDT}_S(\alpha, \beta) = 2^\ell$. Let $K = (K_1, \ldots, K_r)$ be an expanded key and $(\Delta_0, \ldots, \Delta_r)$ with all $\Delta_t \in \{\alpha, \beta\}^m$ be an r-round characteristic which is valid for the first $(r-1)$ round keys. Then,*

$$\Gamma_r := \{\Delta_{r+1} \in \{\alpha, \beta\}^m \mid (\Delta_0, \ldots, \Delta_r, \Delta_{r+1}) \text{ is a valid characteristic for } K\}$$

is an affine subspace. It is non-empty if and only if

$$L^{-1}(K_r)[j] \in \left(y_0^{\Delta_{r-1}[j], L^{-1}(\Delta_r)[j]} + x_0^{L^{-1}(\Delta_r)[j],\alpha}\right) + E, \ \forall 1 \leq j \leq m \ .$$

In that case, it has dimension

$$\dim \Gamma_r = \begin{cases} \dim(W_r) - \dim(W_{r-1}) - \ell m & \text{if } r \geq 2 \\ \dim(W_1) - \ell m & \text{if } r = 1 \end{cases} \tag{4}$$

Proof. By Th. 1, $(\Delta_0, \ldots, \Delta_r, \Delta_{r+1})$, is valid for K if and only if

$$(0, \ldots, 0, x_0^{\Delta_r, L^{-1}(\Delta_{r+1})}) \in K + \widetilde{w_0} + W_r$$

$$\text{where } \widetilde{w_0}[t] := \begin{cases} x_0^{\Delta_t, L^{-1}(\Delta_{t+1})} + L(y_0^{\Delta_{t-1}, L^{-1}(\Delta_t)}) & \text{if } 1 \leq t \leq r-1 \\ L(y_0^{\Delta_{r-1}, L^{-1}(\Delta_r)}) & \text{if } t = r. \end{cases}$$

Moreover, $K + \widetilde{w_0} + W_r$ does not depend on Δ_{r+1} by Lemma 7. Let

$$\begin{aligned} \psi_{\Delta_r} : \{\alpha, \beta\}^m &\to \mathbb{F}_2^{sm} \\ B &\mapsto x_0^{\Delta_r, B} \ . \end{aligned}$$

Then, the values of Δ_{r+1} in Γ_r correspond to the intersection between $\left(\{0\}^{sm(r-1)} \times \mathsf{Im}(\psi_{\Delta_r})\right)$ and $K + \widetilde{w_0} + W_r$. This intersection does not depend on the choice of the offset $x_0^{\Delta_r,B}$ since any other offset $z_0^{\Delta_r,B}$ belongs to $x_0^{\Delta_r,B} + \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_r)$ and then $(0,\dots,0,z_0^{\Delta_r,B}) + (0,\dots,0,x_0^{\Delta_r,B})$ lies in W_r.

We have

$$\mathsf{Im}(\psi_{\Delta_r}) = \prod_{j=1}^{m} \left\{ x_0^{\Delta_r[j],\alpha}, x_0^{\Delta_r[j],\beta} \right\},$$

which is an affine subspace whose linear part is $\prod_{j=1}^{m} \left\langle x_0^{\Delta_r[j],\alpha} + x_0^{\Delta_r[j],\beta} \right\rangle$. Therefore, ψ_{Δ_r} is an isomorphism from $\alpha^{\times m} + \langle \alpha + \beta \rangle^m$ to $\mathsf{Im}(\psi_{\Delta_r})$. Then:

$$\Gamma_r = L \circ \psi_{\Delta_r}^{-1} \left\{ \pi_r \left(\left(\{0\}^{sm(r-1)} \times \mathsf{Im}(\psi_{\Delta_r}) \right) \cap (K + \widetilde{w_0} + W_r) \right) \right\} \tag{5}$$

where π_r denotes the last coordinate of an element in $(\mathbb{F}_2^{sm})^r$. Since ψ_{Δ_r} is an isomorphism, Γ_r is an affine subspace and Γ_r is non-empty if and only if

$$\left(\{0\}^{sm(r-1)} \times \mathsf{Im}(\psi_{\Delta_r}) \right) \cap (K + \widetilde{w_0} + W_r) \neq \emptyset \,,$$

or equivalently,

$$K + \widetilde{w_0} \in \left(\{0\}^{sm(r-1)} \times \mathsf{Im}(\psi_{\Delta_r}) \right) + W_r$$

Choosing $Q := (0,\dots,0,x_0^{\Delta_r,\alpha^{\times m}})$ as an offset of $\left(\{0\}^{sm(r-1)} \times \mathsf{Im}(\psi_{\Delta_r})\right)$, the above condition is equivalent to

$$K + \widetilde{w_0} + Q \in \left(\{0\}^{sm(r-1)} \times \prod_{j=1}^{m} \left\langle x_0^{\Delta_r[j],\alpha} + x_0^{\Delta_r[j],\beta} \right\rangle \right) + W_r = W_{r-1} \times E^m$$

by Lemma 8. By assumption, $(\Delta_0,\dots,\Delta_r)$ is a valid characteristic for $(K_1,\dots,K_{r-1})$, which means that the first $(r-1)$ coordinates of $(K + \widetilde{w_0} + Q)$ satisfy the previous condition. It follows that the condition is equivalent to

$$K_r \in L(y_0^{\Delta_{r-1},L^{-1}(\Delta_r)}) + x_0^{\Delta_r,\alpha^{\times m}} + E^m \,.$$

Applying L^{-1}, it is also equivalent to

$$L^{-1}(K_r) \in y_0^{\Delta_{r-1},L^{-1}(\Delta_r)} + L^{-1}\left(x_0^{\Delta_r,\alpha^{\times m}} \right) + E^m \,.$$

By Lemma 4, $L^{-1}\left(x_0^{\Delta_r,\alpha^{\times m}} \right) = x_0^{L^{-1}(\Delta_r),\alpha^{\times m}}$. Looking at each coordinate, the condition then corresponds to

$$L^{-1}(K_r)[j] \in \left(y_0^{\Delta_{r-1}[j],L^{-1}(\Delta_r)[j]} + x_0^{L^{-1}(\Delta_r)[j],\alpha} \right) + E, \ \forall 1 \leq j \leq m \,.$$

When this condition holds, using again Lemma 8, we have when $r \geq 2$

$$\begin{aligned}
\dim(\Gamma_r) &= \dim\left(\left(\{0\}^{sm(r-1)} \times \prod_{j=1}^{m} \left\langle x_0^{\Delta_r[j],\alpha} + x_0^{\Delta_r[j],\beta} \right\rangle \right) \cap W_r \right) \\
&= m + \dim(W_r) - \dim\left(\left(\{0\}^{sm(r-1)} \times \prod_{j=1}^{m} \left\langle x_0^{\Delta_r[j],\alpha} + x_0^{\Delta_r[j],\beta} \right\rangle \right) + W_r \right) \\
&= m + \dim(W_r) - \dim(W_{r-1}) - m\dim(E) \\
&= m(1 - \dim(E)) + \dim(W_r) - \dim(W_{r-1}) = -m\ell + \dim(W_r) - \dim(W_{r-1})
\end{aligned}$$

where the last equality is derived from Lemma 5. For $r = 1$, we use the expression of W_1 given in Lemma 8 and get

$$\begin{aligned}\dim(\Gamma_1) &= m + \dim(W_1) - \dim\left(\prod_{j=1}^{m} \left\langle x_0^{\Delta_1[j],\alpha} + x_0^{\Delta_1[j],\beta} \right\rangle + W_1\right) \\ &= m + \dim(W_1) - m\dim(E) = -m\ell + \dim(W_1)\ .\end{aligned}$$

□

Therefore, the previous proposition shows that, starting from a given r-round characteristic $(\Delta_0, \ldots, \Delta_r)$ with all $\Delta_t \in \{\alpha, \beta\}^m$, only two situations can occur, depending on whether the last round-key K_r satisfies a condition involving Δ_{r-1} and Δ_r. Either this characteristic cannot be extended to a longer characteristic with differences in $\{\alpha, \beta\}^m$, or it can be extended to many such $(r+1)$-round characteristics and in that case the set of possible extensions forms an affine subspace of $\{a, b\}^m$.

Now, we show that, in the particular case of a *perfect* square differential, the condition on K_r required for extending $(\Delta_0, \ldots, \Delta_r)$ one round further does not depend on the characteristic. Therefore, for a given expanded key, either there exists no valid r-round characteristic with differences in $\{\alpha, \beta\}^m$, or there exist many of them since *any* valid characteristic $(\Delta_0, \ldots, \Delta_r)$ can be extended.

Corollary 2. *Let us consider an SPN whose linear layer L satisfies Property $(\mathcal{P})$. Let (α, β) a* perfect *square differential for S with $\mathsf{DDT}_S(\alpha, \beta) = 2^\ell$. Then, for any expanded key K in $(x_0^{\alpha,\alpha} + y_0^{\alpha,\alpha} + E)^{mr}$ and for any $\Delta_0 \in \{\alpha, \beta\}^m$,*

$$\sum_{\Delta_1, \ldots, \Delta_r \in \{\alpha,\beta\}^m} \mathsf{DP}[K](\Delta_0, \ldots, \Delta_r) = 2^{-m(s-\ell-1)}\ .$$

Proof. Let N_r, for $r \geq 1$, be the number of inputs satisfying an r-round characteristic with differences in $\{\alpha, \beta\}^m$ and starting from Δ_0. We will prove that $N_r = 2^{m(\ell+1)}$ for all $r \geq 1$. First, for $r = 1$, we have

$$N_1 = \sum_{\Delta_1 \in \{\alpha,\beta\}^m} \prod_{j=1}^{m} \mathsf{DDT}_{\boldsymbol{\mathcal{S}}}(\Delta_0[j], L^{-1}(\Delta_1[j])) = \sum_{\Delta_1 \in \{\alpha,\beta\}^m} 2^{\ell m} = 2^{m(\ell+1)}\ .$$

Let us now define

$$\mathcal{C}_r(K) := \{\Delta_1, \ldots, \Delta_r \in \{\alpha, \beta\}^m \mid (\Delta_0, \Delta_1, \ldots, \Delta_r) \text{ is valid for } K\}\ .$$

Using the same notation as in the previous proof, we have

$$\mathcal{C}_{r+1}(K_1, \ldots, K_r) = \mathcal{C}_r(K_1, \ldots, K_{r-1}) \times \Gamma_r\ .$$

Since $K_r \in (x_0^{\alpha,\alpha} + y_0^{\alpha,\alpha} + E)^m$ and L satisfies $(\mathcal{P})$, we have $L^{-1}(K_r) \in (x_0^{\alpha,\alpha} + y_0^{\alpha,\alpha} + E)^m$. Therefore, for all $1 \leq j \leq m$,

$$L^{-1}(K_r)[j] \in y_0^{\Delta_{r-1}[j], L^{-1}(\Delta_r)[j]} + x_0^{L^{-1}(\Delta_r)[j],\alpha} + E$$

because (α, β) is a *perfect* square differential for S. Hence, by Prop. 3, $\Gamma_r \neq \emptyset$ and its dimension is given by (4). Let us denote $K' := (K_1, \ldots, K_{r-1})$. Then, using Lemma 7, we deduce that,

$$\begin{aligned}N_{r+1} &= \sum_{\Delta_1, \ldots, \Delta_{r+1} \in \mathcal{C}_{r+1}(K', K_r)} 2^{-\dim(W_r)} \prod_{t=0}^{r} \mathsf{DDT}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1})) \\ &= 2^{\ell m(r+1)} \sum_{\Delta_1, \ldots, \Delta_{r+1} \in \mathcal{C}_{r+1}(K', K_r)} 2^{-\dim(W_r)} \\ &= 2^{\ell m(r+1)} \sum_{\Delta_1, \ldots, \Delta_r \in \mathcal{C}_r(K')} 2^{-\dim(W_r)+\dim(\Gamma_r)} \\ &= 2^{\ell m(r+1)} \sum_{\Delta_1, \ldots, \Delta_r \in \mathcal{C}_r(K')} 2^{-\dim(W_{r-1})-\ell m} \\ &= N_r\ .\end{aligned}$$

Remark 2. While all results presented in this section assume that the linear layer of the cipher satisfies $(\mathcal{P})$, requiring $L(E^m) = E^m$ and $L(\{\alpha,\beta\}^m) = \{\alpha,\beta\}^m$ would have been sufficient. However, we believe that it is unlikely to occur if L does not satisfy $(\mathcal{P})$.

4 Examples of Different Fixed-Key Behaviours

As an illustration of the previous results, we study the fixed-key probabilities of truncated differentials obtained by aggregating all characteristics with differences in a given set $\{\alpha,\beta\}^m$. We start from MIDORI64 whose linear layer satisfies Property $(\mathcal{P})$ and then see how the properties of the underlying differential (α,β) for S affect the general fixed-key behaviour of the truncated probability.

4.1 Case of a Perfect Square Differential: Midori64

We consider the same differential as in [BFL+23]: $\alpha = \texttt{0xa}$ and $\beta = \texttt{0xf}$. Then,

$$\mathsf{DDT}_S(\texttt{0xa},\texttt{0xa}) = \mathsf{DDT}_S(\texttt{0xa},\texttt{0xf}) = \mathsf{DDT}_S(\texttt{0xf},\texttt{0xa}) = \mathsf{DDT}_S(\texttt{0xf},\texttt{0xf}) = 4\ .$$

Moreover, $(\texttt{0xa},\texttt{0xf})$ is a square differential in the sense of Def. 6 since

$$\begin{aligned}
\mathsf{XDDT}_S(\texttt{0xa},\texttt{0xa}) &= \texttt{0x3} + \langle \texttt{0x7},\texttt{0xa}\rangle \quad \text{and} \quad \mathsf{YDDT}_S(\texttt{0xa},\texttt{0xa}) = \texttt{0x3} + \langle \texttt{0x7},\texttt{0xa}\rangle \\
\mathsf{XDDT}_S(\texttt{0xa},\texttt{0xf}) &= \texttt{0xc} + \langle \texttt{0x7},\texttt{0xa}\rangle \quad \text{and} \quad \mathsf{YDDT}_S(\texttt{0xa},\texttt{0xf}) = \langle \texttt{0xa},\texttt{0xf}\rangle \\
\mathsf{XDDT}_S(\texttt{0xf},\texttt{0xa}) &= \langle \texttt{0xa},\texttt{0xf}\rangle \quad \text{and} \quad \mathsf{YDDT}_S(\texttt{0xf},\texttt{0xa}) = \texttt{0xc} + \langle \texttt{0x7},\texttt{0xa}\rangle \\
\mathsf{XDDT}_S(\texttt{0xf},\texttt{0xf}) &= \texttt{0x2} + \langle \texttt{0xa},\texttt{0xf}\rangle \quad \text{and} \quad \mathsf{YDDT}_S(\texttt{0xf},\texttt{0xf}) = \texttt{0xd} + \langle \texttt{0xa},\texttt{0xf}\rangle\ ,
\end{aligned}$$

where the offset y_0 of YDDT_S corresponds to the image by S of the offset of XDDT_S. We can then easily check that all conditions in Def. 6 hold. Most notably,

$$\mathsf{U}_S(\texttt{0xa}) + \langle x_0^{\texttt{0xa},\texttt{0xf}} + x_0^{\texttt{0xa},\texttt{0xa}}\rangle = \mathsf{U}_S(\texttt{0xf}) + \langle x_0^{\texttt{0xf},\texttt{0xf}} + x_0^{\texttt{0xf},\texttt{0xa}}\rangle = \langle \texttt{0x7},\texttt{0xa},\texttt{0xf}\rangle := E\ .$$

Then, according to Prop. 3, any valid r-round characteristic with differences in $\{\texttt{0xa},\texttt{0xf}\}^m$ can be extended for some weak round-keys K_r.

Now, we check that $(\texttt{0xa},\texttt{0xf})$ is also a *perfect* square differential. Indeed, we compute the four values $y_0^{\delta_0,\delta_1} + x_0^{\delta_1,\texttt{0xa}}$ for $\delta_0,\delta_1 \in \{\texttt{0xa},\texttt{0xf}\}$ in the table below and check that these values belong to E. Note that the values in the table depend on the choice of $x_0^{\delta_0,\delta_1}$ for each (δ_0,δ_1). However, their coset in E is always independent of that choice because $\mathsf{U}_S(\alpha)$ and $\mathsf{U}_S(\beta)$ are included in E.

δ_0 \ δ_1	α	β
α	0x0	0xa
β	0xf	0xd

Because (α,β) is perfect, Coro. 2 applies and shows that the weak round-keys K_r for which a valid r-round characteristic $(\Delta_0,\ldots,\Delta_r)$ can be extended are the same for all $(\Delta_0,\ldots,\Delta_r)$. This situation is depicted on Fig. 1 in the case of a reduced version of MIDORI64 with block size 16, named Column-MIDORI, which corresponds to MIDORI64 restricted to a single column. Fig. 1 represents, for a given randomly chosen weak expanded key, all 11-round valid characteristics $(\Delta_0,\Delta_1,\ldots,\Delta_{11})$ with all $\Delta_t \in \{\texttt{0xa},\texttt{0xf}\}^4$ starting from given Δ_0,Δ_1 chosen at random in $\{\texttt{0xa},\texttt{0xf}\}^4$. The nodes at the t-th level in the tree, $0 \le t \le 11$, starting from the top, represent the different t-round valid characteristics with differences in $\{\texttt{0xa},\texttt{0xf}\}^4$. In other words, the $(t+1)$-th level is deduced from the t-th level by computing Γ_t as in Prop. 3.

In the generic case there are two growth regimes. On the first 5 or 6 rounds, the tree width grows a lot. But starting from Round 7, the width stays constant because each valid characteristic has at least 2 valid

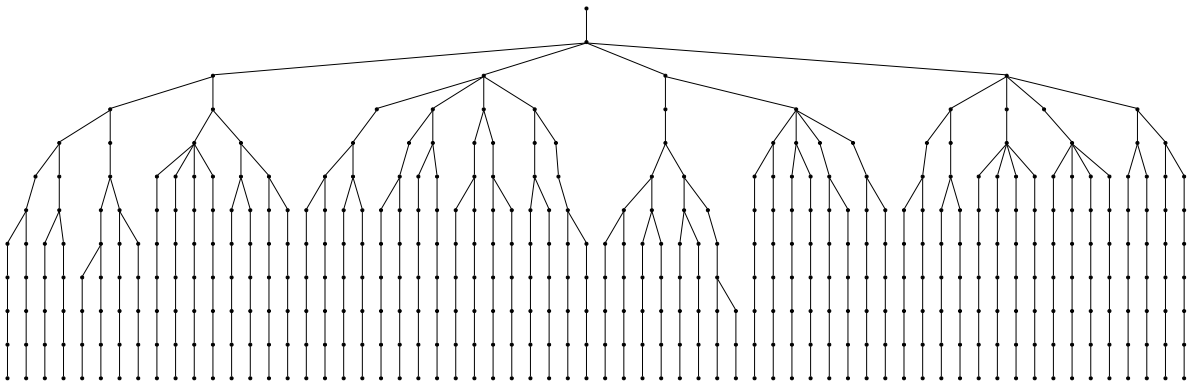


Figure1: Representation of the valid characteristics $(\Delta_0, \ldots, \Delta_{11})$ with all $\Delta_t \in \{\texttt{0xa}, \texttt{0xf}\}^4$ starting from given $\Delta_0, \Delta_1 \in \{\alpha, \beta\}^4$ for 11 rounds of Column-MIDORI, and for a random weak expanded key.

inputs. In the case of MIDORI64, Prop. 8 in App. C applies and shows that this minimum number is 4, instead of 2 in the general case.

In other words, there are exactly 2^8 valid inputs for the single-round characteristic (Δ_0, Δ_1). But then, these inputs are split up into the sets of valid inputs of different 2-round characteristics $(\Delta_0, \Delta_1, \Delta_2)$. And when the set of valid inputs of a characteristic has size 4, it cannot be divided anymore. Then, in this example, for 9 rounds and more, we obtain a total of 64 characteristics, each having exactly 4 valid inputs.

There are some particular cases where the truncated differential derived from all characteristics with differences in $\{\texttt{0xa}, \texttt{0xf}\}^{16}$ has the same probability, but corresponds to a very different configuration. Indeed, if all round keys belong to the subspace of weak round-keys equal to $\langle \texttt{0xa,0xf} \rangle^{16}$, then the tree of all valid characteristics starting from $\Delta_0 = \Delta_1 = \texttt{0xf}^{\times 16}$ is a filiform tree. It consists of the single iterative characteristic $(\texttt{0xf}^{\times 16}, \texttt{0xf}^{\times 16}, \texttt{0xf}^{\times 16}, \ldots)$, meaning that all the 2^{32} elements of $\mathsf{XDDT}(\Delta_0, L^{-1}(\Delta_1))$ satisfy the same entire characteristic. This situation corresponds to Prop. 2 and to the invariant subspaces exhibited in [GJN+16] as explained at the end of Section 2.4.

With Sbox S_1. Now, we consider a variant of MIDORI64 in which we use the Sbox S_1 defined in App. A. For this Sbox, $(\texttt{0x4}, \texttt{0xf})$ is a perfect square differential, hence the general behaviour is the same as in the case of MIDORI64, *even if the Sbox is not involutive*. Indeed, for any $\Delta_0 \in \{\texttt{0x4}, \texttt{0xf}\}^m$, the truncated differential beginning with Δ_0 has probability equal to 2^{-16} when only characteristics with intermediate differences in $\{\texttt{0x4}, \texttt{0xf}\}^m$ are considered. But, this cipher differs from the previous one for two reasons:

- The minimal number of valid inputs of a differential characteristic whose differences lie in $\{\texttt{0x4}, \texttt{0xf}\}^m$ is 2, while it was 4 in MIDORI64. This is because Prop. 8 does not apply.
- There is no characteristic having a high probability. Indeed, the highest probability of a characteristic whose differences lie in $\{\texttt{0x4}, \texttt{0xf}\}^m$ is 2^{-3m} whereas it was 2^{-2m} in MIDORI64. Invariant subspaces of dimension 32 as the ones found in [GJN+16] do not exist. This comes from the fact that for $x \in \{\texttt{0x4}, \texttt{0xf}\}$, $\dim(\mathsf{U}_{S_1}(x, x) \cap \mathsf{V}_{S_1}(x, x)) = 1$.

As for MIDORI64, Fig. 2 represents, for a given randomly chosen weak expanded key, all 11-round valid characteristics $(\Delta_0, \Delta_1, \ldots, \Delta_{11})$ with all $\Delta_t \in \{\texttt{0x4}, \texttt{0xf}\}^4$ starting from given Δ_0, Δ_1 chosen at random in $\{\texttt{0x4}, \texttt{0xf}\}^4$. As in Fig. 1, we observe two growth regimes. But, there are more characteristics than in the original Column-MIDORI: since the minimum number of inputs for a given characteristic is divided by 2, the number of valid characteristics after 11 rounds is twice bigger.

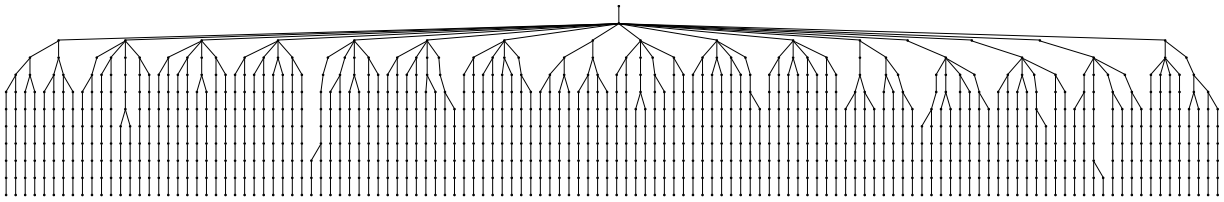


Figure2: Representation of the valid characteristics $(\Delta_0, \ldots, \Delta_{11})$ with all $\Delta_t \in \{\texttt{0x4}, \texttt{0xf}\}^4$ starting from given $\Delta_0, \Delta_1 \in \{\alpha, \beta\}^4$ for 11 rounds of Column-MIDORI with Sbox S_1, and for a random weak expanded-key.

4.2 Case of a Square but Not Perfect Differential

With Rectangle Sbox. We now replace MIDORI64 Sbox by the Sbox used in RECTANGLE [ZBL+14,ZBL+15] specified in Appendix A. It can be checked that (α, β) with $\alpha := \texttt{0x5}$ and $\beta := \texttt{0x9}$ is a square differential for S with

$$\mathsf{DDT}_S(\texttt{0x5}, \texttt{0x5}) = \mathsf{DDT}_S(\texttt{0x5}, \texttt{0x9}) = \mathsf{DDT}_S(\texttt{0x9}, \texttt{0x5}) = \mathsf{DDT}_S(\texttt{0x9}, \texttt{0x9}) = 2\ .$$

Indeed, we have

$$\begin{array}{llll} \mathsf{XDDT}_S(\texttt{0x5}, \texttt{0x5}) = \texttt{0x2} + \langle \texttt{0x5} \rangle & \text{and} & \mathsf{YDDT}_S(\texttt{0x5}, \texttt{0x5}) = \texttt{0xc} + \langle \texttt{0x5} \rangle, \\ \mathsf{XDDT}_S(\texttt{0x5}, \texttt{0x9}) = \texttt{0xe} + \langle \texttt{0x5} \rangle & \text{and} & \mathsf{YDDT}_S(\texttt{0x5}, \texttt{0x9}) = \texttt{0x4} + \langle \texttt{0x9} \rangle, \\ \mathsf{XDDT}_S(\texttt{0x9}, \texttt{0x5}) = \texttt{0x6} + \langle \texttt{0x9} \rangle & \text{and} & \mathsf{YDDT}_S(\texttt{0x9}, \texttt{0x5}) = \texttt{0x7} + \langle \texttt{0x5} \rangle, \\ \mathsf{XDDT}_S(\texttt{0x9}, \texttt{0x9}) = \texttt{0x3} + \langle \texttt{0x9} \rangle & \text{and} & \mathsf{YDDT}_S(\texttt{0x9}, \texttt{0x9}) = \texttt{0xa} + \langle \texttt{0x9} \rangle. \end{array}$$

Moreover, $E = \langle \texttt{0x5}, \texttt{0x9} \rangle$.

This differential is not a perfect square differential, as shown in the following table providing the values of $y_0^{\delta_0,\delta_1} + x_0^{\delta_1,\texttt{0x5}}$ for all $\delta_0, \delta_1 \in \{\texttt{0x5}, \texttt{0x9}\}$. Elements in red lie in E, those in blue lie in $\texttt{0x2} + E$. Hence, the set of weak round-keys is defined by the disjoint union of these two cosets of E: $\mathcal{K} = (E \cup (\texttt{0x2} + E))^m$.

δ_0 \ δ_1	α	β
α	0xe	0x2
β	0x5	0xc

From Prop. 3, we know that a valid $(r-1)$-round characteristic $(\Delta_0, \ldots, \Delta_{r-1})$ can be extended to some r-round characteristic if and only if, for each $1 \le j \le m$, one of the following two conditions holds

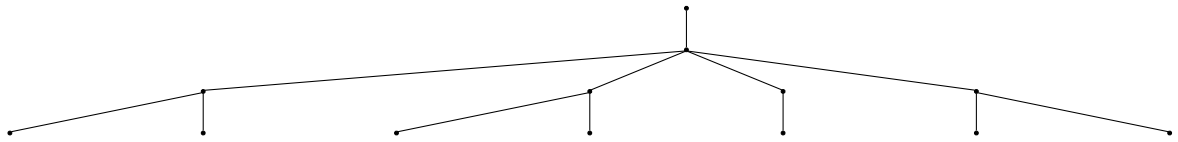
$$\begin{array}{c} L^{-1}(K_{r-1})[j] \in E \text{ and } \Delta_{r-2}[j] = \texttt{0x9} \\ \text{or } L^{-1}(K_{r-1})[j] \in (\texttt{0x2} + E) \text{ and } \Delta_{r-2}[j] = \texttt{0x5}\ . \end{array}$$

It follows that, for any given $(K_1, \ldots, K_{r-1})$ in the set of weak expanded keys, there is a single $(r-2)$-round characteristic $(\Delta_0, \ldots, \Delta_{r-2})$ such that $(\Delta_0, \ldots, \Delta_{r-2}, \Delta_{r-1}, \Delta_r)$ is valid for some $\Delta_{r-1}, \Delta_r \in \{\texttt{0x5}, \texttt{0x9}\}^m$. In other words, all valid r-round characteristics with differences in $\{\texttt{0x5}, \texttt{0x9}\}^m$ share the same $(\Delta_0, \ldots, \Delta_{r-2})$.

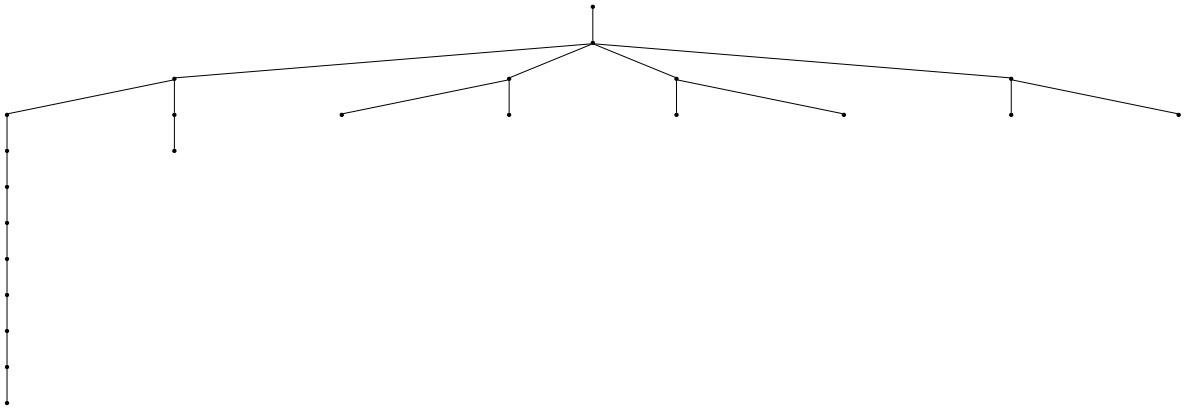
As before, we consider a randomly chosen weak expanded key. We choose for Δ_0 and Δ_1 the values determined by K_1 and K_2. Then, at Round 3, there are several valid characteristics $(\Delta_0, \Delta_1, \Delta_2, \Delta_3)$. For the majority of the weak expanded keys, these characteristics cannot be extended since none of the valid values of Δ_2 is compatible with the condition for $\Gamma_3 \neq \emptyset$, namely

$$\begin{array}{c} L^{-1}(K_3)[j] \in E \text{ and } \Delta_2[j] = \texttt{0x9} \\ \text{or } L^{-1}(K_3)[j] \in (\texttt{0x2} + E) \text{ and } \Delta_2[j] = \texttt{0x5}\ . \end{array}$$

Figure3: Representation of the valid characteristics $(\Delta_0, \ldots, \Delta_{11})$ with all $\Delta_t \in \{\texttt{0x5}, \texttt{0x9}\}^4$ starting from the unique possible $\Delta_0, \Delta_1 \in \{\alpha, \beta\}^4$ for 11 rounds of Column-MIDORI with RECTANGLE Sbox.



(a) For a random weak expanded key.



(b) For a particular well-chosen weak expanded key.

This generic situation is depicted by Fig. 3a.

But, for a few weak expanded keys, there exist differential characteristics $(\Delta_0, \Delta_1, \Delta_2, \Delta_3)$ that can be extended. This situation is described by Fig. 3b. Here, we start from a set of 2^4 valid inputs for (Δ_0, Δ_1). This set is then divided into the input sets of 8 different 3-round characteristics, each of size 2. Obviously, these sets cannot be divided further, but only some of the characteristics can be extended. This implies that, after 5 rounds and more, there is a single valid characteristic with differences in $\{\texttt{0x5}, \texttt{0x9}\}^4$ and this characteristic has only two valid inputs.

With *Luffa* v1 Sbox. We now replace MIDORI64 Sbox by the Sbox used in *Luffa* v1 [CSW08] specified in Appendix A. It can be checked that (α, β) with $\alpha := \texttt{0x7}$ and $\beta := \texttt{0xf}$ is a square differential for S with

$$\mathsf{DDT}_S(\texttt{0x7}, \texttt{0x7}) = \mathsf{DDT}_S(\texttt{0x7}, \texttt{0xf}) = \mathsf{DDT}_S(\texttt{0xf}, \texttt{0x7}) = \mathsf{DDT}_S(\texttt{0xf}, \texttt{0xf}) = 2\ .$$

Indeed, we have

$$\begin{array}{llll} \mathsf{XDDT}_S(\texttt{0x7}, \texttt{0x7}) = \texttt{0xa} + \langle \texttt{0x7} \rangle & \text{and} & \mathsf{YDDT}_S(\texttt{0x7}, \texttt{0x7}) = \texttt{0x6} + \langle \texttt{0x7} \rangle, \\ \mathsf{XDDT}_S(\texttt{0x7}, \texttt{0xf}) = \texttt{0x2} + \langle \texttt{0x7} \rangle & \text{and} & \mathsf{YDDT}_S(\texttt{0x7}, \texttt{0xf}) = \texttt{0xb} + \langle \texttt{0xf} \rangle, \\ \mathsf{XDDT}_S(\texttt{0xf}, \texttt{0x7}) = \texttt{0x6} + \langle \texttt{0xf} \rangle & \text{and} & \mathsf{YDDT}_S(\texttt{0xf}, \texttt{0x7}) = \texttt{0x8} + \langle \texttt{0x7} \rangle, \\ \mathsf{XDDT}_S(\texttt{0xf}, \texttt{0xf}) = \texttt{0x1} + \langle \texttt{0xf} \rangle & \text{and} & \mathsf{YDDT}_S(\texttt{0xf}, \texttt{0xf}) = \texttt{0xd} + \langle \texttt{0xf} \rangle. \end{array}$$

Moreover, $E = \langle \texttt{0x7}, \texttt{0xf} \rangle$.

This differential is not a perfect square differential, as shown in the following table which provides the values of $y_0^{\delta_0,\delta_1} + x_0^{\delta_1,\texttt{0x7}}$ for all $\delta_0, \delta_1 \in \{\texttt{0x7}, \texttt{0xf}\}$. The values in red in the table belong to $\texttt{0x4} + E$, those in

blue, belong to $\texttt{0x2} + E$. It follows that the set of weak round-keys is defined by the disjoint union of these two cosets of E: $\mathcal{K} := ((\texttt{0x2} + E) \cup (\texttt{0x4} + E))^m$.

δ_0 \ δ_1	α	β
α	0xc	0xd
β	0x2	0xb

At first glance, this case seems then similar to the previous one, but it is actually different. Indeed, we now deduce from Prop. 3 the following result. For any given expanded key with all round keys in $\mathcal{K}$, and for each choice of $\Delta_0 \in \{\texttt{0x7}, \texttt{0xf}\}^m$, a given $(r-1)$-round characteristic $(\Delta_0, \ldots, \Delta_{r-1})$ can be extended to some $(\Delta_0, \ldots, \Delta_{r-1}, \Delta_r)$ if and only if, for each $1 \leq j \leq m$, one of two conditions hold

$$L^{-1}(\Delta_{r-1})[j] = \Delta_{r-2}[j] \quad \text{and} \quad L^{-1}(K_{r-1})[j] \in (\texttt{0x4} + E)$$
$$\text{or } L^{-1}(\Delta_{r-1})[j] = \Delta_{r-2}[j] \oplus \texttt{0x8} \quad \text{and} \quad L^{-1}(K_{r-1})[j] \in (\texttt{0x2} + E)\ .$$

Like in the previous examples, we consider an expanded key with all round-keys randomly chosen in $\mathcal{K}^4$. Unlike in the previous case, we can choose any $\Delta_0 \in \{\alpha, \beta\}^m$, K_1 then fixes the value of Δ_1. This way, we ensure that $\Gamma_2 \neq \emptyset$. For most of the weak expanded keys, the characteristics $(\Delta_0, \Delta_1, \ldots, \Delta_2)$ can not be further extended. This case is described by Fig. 4. Similarly to the previous case, for a few expanded keys in the weak key set, there are characteristics that can be extended for several rounds.

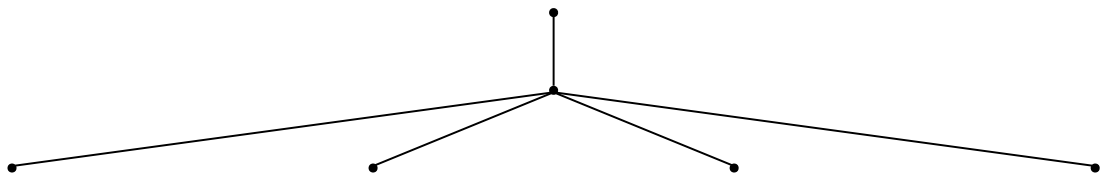


Figure4: Representation of the valid characteristics $(\Delta_0, \ldots, \Delta_{11})$ with all $\Delta_t \in \{\texttt{0x7}, \texttt{0xf}\}^4$ starting from a random Δ_0 and the unique possible $\Delta_1 \in \{\alpha, \beta\}^4$ for 11 rounds of Column-MIDORI64 with *Luffa* v1 Sbox and for a random expanded key the weak key space.

5 Identifying the Weak Sboxes

We have seen that the existence of weak keys, for which differential characteristics aggregate and lead to a high truncated differential probability, as in the case of MIDORI64, comes from the structure of the linear layer and from the existence of *perfect square differentials* for the Sbox. At first glance and as discussed in [GJN+16], it seems that the fact that MIDORI64's Sbox is involutive is the main cause of such differentials. However, in Section 4.1, we studied an optimal 4-bit Sbox that is not involutive and nevertheless has the same weakness.

In order to identify the Sboxes that have perfect square differentials, it is much more convenient to study this property up to some equivalence relation, since optimal Sboxes are classified up to equivalence, e.g. [LP07,DC07] for 4-bit Sboxes. Moreover, it is well-known that the differential properties of an Sbox can be derived from those of any Sbox in its equivalence class. In the following, we mainly focus on *affine equivalence* which is used for 4-bit Sboxes in [LP07].

Definition 7 (Affine equivalence). *Two Sboxes from $\mathbb{F}_2^s$ to $\mathbb{F}_2^s$ are said to be* affine equivalent *if there exist two affine bijections on $\mathbb{F}_2^s$, A_1 and A_2, such that $S_2 = A_2 \circ S_1 \circ A_1$.*

It is well-known that the differential properties of Sboxes within the same affine-equivalence class are related, as pointed out by the following lemma.

Lemma 9. *Let S_1, S_2 two s-bit Sboxes such that $S_2 = A_2 \circ S_1 \circ A_1$. Then,*

$$\mathsf{XDDT}_{S_2}(a,b) = A_1^{-1}\left(\mathsf{XDDT}_{S_1}(L_1(a), L_2^{-1}(b))\right)$$
$$\text{and } \mathsf{YDDT}_{S_2}(a,b) = A_2\left(\mathsf{YDDT}_{S_1}(L_1(a), L_2^{-1}(b))\right) ,$$

where L_1 and L_2 are the linear parts of A_1 and A_2. Moreover, $(L_1(a), L_2^{-1}(b))$ is a super-planar differential for S_1 if and only if (a,b) is super-planar for S_2.

Proof. Let $x \in \mathsf{XDDT}_{S_2}(a,b)$. Left-composing by A_2^{-1}, we get:

$$S_2(x+a) + S_2(x) = b \iff S_1(L_1(x) + L_1(a) + c_1) + S_1(L_1(x) + c_1) = L_2^{-1}(b) .$$

Therefore, $x \in \mathsf{XDDT}_{S_2}(a,b)$ is equivalent to $A_1(x) \in \mathsf{XDDT}_{S_1}(L_1(a), L_2^{-1}(b))$. In other words, $\mathsf{XDDT}_{S_2}(a,b) = A_1^{-1}\left(\mathsf{XDDT}_{S_1}(L_1(a), L_2^{-1}(b))\right)$. Moreover,

$$\begin{aligned}\mathsf{YDDT}_{S_2}(a,b) &= S_2\left(\mathsf{XDDT}_{S_2}(a,b)\right) = A_2 \circ S_1\left(\mathsf{XDDT}_{S_1}(L_1(a), L_2^{-1}(b))\right) \\ &= A_2\left(\mathsf{YDDT}_{S_1}(L_1(a), L_2^{-1}(b))\right) .\end{aligned}$$

Now, (a,b) is a super-planar differential for S_2 if and only if

$$\{(x, S_2(x)) \mid x \in \mathsf{XDDT}_{S_2}(a,b)\} = (A_1^{-1} \times A_2)\left(\{(y, S_1(y)) \mid y \in \mathsf{XDDT}_{S_1}(L_1(a), L_2^{-1}(b))\}\right)$$

is an affine space *i.e* if and only if $(L_1(a), L_2^{-1}(b))$ is super-planar for S_1. □

A square differential for a given Sbox then corresponds, for an affine-equivalent Sbox, to four related differentials that have the following structure.

Definition 8. *A 4-tuple (a_1, a_2, b_1, b_2) is called a* rectangle of differentials *of weight ℓ for S if the following conditions hold:*

1. *(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2) are super-planar differentials for S with $\mathsf{DDT}_S(a_i, b_j) = 2^\ell$, for all $1 \le i, j \le 2$.*
2. *$\mathsf{U}_S(a_1, b_1) = \mathsf{U}_S(a_1, b_2) := \mathsf{U}_S(a_1)$ and $\mathsf{U}_S(a_2, b_1) = \mathsf{U}_S(a_2, b_2) := \mathsf{U}_S(a_2)$.*
3. *$\mathsf{U}_S(a_1) + \langle x_0^{a_1,b_1} + x_0^{a_1,b_2}\rangle = \mathsf{U}_S(a_2) + \langle x_0^{a_2,b_1} + x_0^{a_2,b_2}\rangle$*
4. *$\dim\left(\mathsf{V}_S(a_1,b_1) + \mathsf{V}_S(a_1,b_2) + \mathsf{V}_S(a_2,b_1) + \mathsf{V}_S(a_2,b_2)\right) \le \ell + 1$.*

The next proposition shows that square differentials for a given Sbox can be derived from a rectangle of differentials for an affine-equivalent Sbox. It can be used either for checking whether an Sbox admits square differentials from a representative in its equivalence class, or for constructing an Sbox having square differentials from an Sbox with a rectangle of differentials.

Proposition 4. *Let S_1, S_2 two s-bit Sboxes such that $S_2 = A_2 \circ S_1 \circ A_1$. Then (a_1, a_2, b_1, b_2) is a rectangle of differentials of weight ℓ for S_1 if and only if*

$$(L_1^{-1}(a_1), L_1^{-1}(a_2), L_2(b_1), L_2(b_2))$$

is a rectangle of differentials of weight ℓ for S_2.

Most notably, $(L_1^{-1}(a_1), L_1^{-1}(a_2))$ is a square differential for S_2 if and only if $(L_1 \circ L_2)(\{b_1, b_2\}) = \{a_1, a_2\}$, and for all $1 \le i, j \le 2$,

$$(L_1 \circ L_2)(\mathsf{V}_{S_1}(a_i, b_j)) \subset \mathsf{U}_{S_1}(a_1) + \langle x_0^{a_1,b_1} + x_0^{a_1,b_2}\rangle .$$

Proof. Let us consider (a_1, a_2, b_1, b_2) a rectangle of differentials for S_1. It is sufficient to prove that

$$(L_1^{-1}(a_1), L_1^{-1}(a_2), L_2(b_1), L_2(b_2))$$

is one for S_2. From Lemma 9, $(L_1^{-1}(a_1), L_1^{-1}(a_2), L_2(b_1), L_2(b_2))$ satisfies Condition 2 in Def. 8 for S_2. Moreover, for all $1 \leq i, j \leq 2$, $\mathsf{U}_{S_2}(L_1^{-1}(a_i), L_2(b_j)) = L_1^{-1}(\mathsf{U}_{S_1}(a_i, b_j))$ and $\mathsf{V}_{S_2}(L_1^{-1}(a_i), L_2(b_j)) = L_2(\mathsf{V}_{S_1}(a_i, b_j))$. Therefore, Conditions 2 and 4 also hold. Let us now prove Condition 3: $\mathsf{U}_S(a_1) + \langle x_0^{a_1,b_1} + x_0^{a_1,b_2} \rangle$ is the linear part of

$$x_0^{a_1,b_1} + \mathsf{U}_S(a_1) + \langle x_0^{a_1,b_1} + x_0^{a_1,b_2} \rangle = \mathsf{XDDT}_{S_1}(a_1, b_1) \uplus \mathsf{XDDT}_{S_1}(a_1, b_2)$$

Hence Condition 3. is equivalent to the fact that $\mathsf{XDDT}_{S_1}(a_1, b_1) \uplus \mathsf{XDDT}_{S_1}(a_1, b_2)$ and $\mathsf{XDDT}_{S_1}(a_2, b_1) \uplus \mathsf{XDDT}_{S_1}(a_2, b_2)$ are cosets of the same vector space. Using again Lemma 9, it implies that $\mathsf{XDDT}_{S_2}(L_1^{-1}(a_1), L_2(b_1)) \uplus \mathsf{XDDT}_{S_2}(L_1^{-1}(a_1), L_2(b_2))$ and $\mathsf{XDDT}_{S_2}(L_1^{-1}(a_2), L_2(b_1)) \uplus \mathsf{XDDT}_{S_2}(L_1^{-1}(a_2), L_2(b_2))$ are cosets of the same vector space, which is equivalent to Condition 3. for $(L_1^{-1}(a_1), L_1^{-1}(a_2), L_2(b_1), L_2(b_2))$.

Obviously, a necessary condition for $(L_1^{-1}(a_1), L_1^{-1}(a_2))$ to be a square differential for S_2 is that $(L_1 \circ L_2)(\{b_1, b_2\}) = \{a_1, a_2\}$. In this case, the first three conditions in Def. 6 are satisfied. It then means that $(L_1^{-1}(a_1), L_1^{-1}(a_2))$ is a square differential if and only if

$$\mathsf{V}_{S_2}(L_1^{-1}(a_i), L_2(b_j)) \subset \mathsf{U}_{S_2}(L_1^{-1}(a_1)) + \langle x_0^{L_1^{-1}(a_1), L_2(b_1)} + x_0^{L_1^{-1}(a_1), L_2(b_2)} \rangle.$$

This is equivalent to

$$L_2(\mathsf{V}_{S_1}(a_i, b_j)) \subset L_1^{-1}\left(\mathsf{U}_{S_1}(a_1) + \langle x_0^{a_1,b_1} + x_0^{a_1,b_2} \rangle\right),$$

that means $(L_1 \circ L_2)(\mathsf{V}_{S_1}(a_i, b_j)) \subset \mathsf{U}_{S_1}(a_1) + \langle x_0^{a_1,b_1} + x_0^{a_1,b_2} \rangle$. □

Remark 3. Given a rectangle of differentials (a_1, a_2, b_1, b_2) for S_1, we can always find two bijective linear mappings L_1 and L_2 such that the conditions of Prop. 4 hold. Indeed, by Condition 4. in Def. 8, $\Sigma := \mathsf{V}_{S_1}(a_1, b_1) + \mathsf{V}_{S_1}(a_1, b_2) + \mathsf{V}_{S_1}(a_2, b_1) + \mathsf{V}_{S_1}(a_2, b_2)$ is a linear space of dimension lower or equal to the dimension of $\mathsf{U}_{S_1}(a_1) + \langle x_0^{a_1,b_1} + x_0^{a_1,b_2} \rangle$. Moreover, we have $\langle b_1, b_2 \rangle \subset \Sigma$. Let $\mathcal{B}$ be a basis of Σ whose first two vectors are b_1 and b_2. Similarly, there exist a basis $\widetilde{\mathcal{B}}$ of $\mathsf{U}_{S_1}(a_1) + \langle x_0^{a_1,b_1} + x_0^{a_1,b_2} \rangle$ whose first two vectors are a_1 and a_2 Choosing $L_1 \circ L_2$ such that $(L_1 \circ L_2)(\{b_1, b_2\}) = \{a_1, a_2\}$ and for all $v \in \mathcal{B} \backslash \{b_1, b_2\}$, $(L_1 \circ L_2)(v) \in \widetilde{\mathcal{B}} \backslash \{a_1, a_2\}$ is sufficient for the conditions of Prop. 4 to hold.

Focus on Optimal 4-bit Sboxes

It is well-known that the best differential uniformity and linearity for 4-bit Sboxes are equal to 4 and 8, respectively. The Sboxes reaching these two values are said to be optimal, and correspond to 16 affine-equivalence classes [LP07]. These classes may differ regarding several properties. Most notably, the subspace of their quadratic components, i.e., $\{\lambda \in \mathbb{F}_2^4 \mid x \mapsto \lambda \cdot S(x) \text{ has degree at most } 2\}$ may have dimension $0, 1$ or 2 depending on the class considered. Then, the existence of rectangles of differentials is related to this dimension as follows.

Proposition 5. *Let S be a 4-bit optimal Sbox. Then, the following assertions are equivalent:*

- *S has 3 quadratic components;*
- *S admits one rectangle of differentials of weight 2;*
- *S admits three distinct rectangles of differentials of weight 2.*

This fact can be observed by studying the 16 affine-equivalence representatives exhibited in [LP07].

Moreover, since any square differential for S with $\mathsf{DDT}_S(\alpha, \beta) = 4$ can be derived from a rectangle of differentials for a representative in the affine-equivalence class, it can be checked that any such square differential is a perfect square differential, and leads to the same weakness as MIDORI64 Sbox.

Proposition 6. *Let S be an optimal 4-bit Sbox and (α, β) be a square differential of weight 2 for S. Then (α, β) is a perfect square differential.*

As an example, the security criteria defined in [GJN+16, Section 5.6] for the best possible resistance to invariant-subspace attacks has led to the conclusion that the Sbox should be selected within five affine-equivalence classes. However, among those five classes, two correspond to classes satisfying the property defined in Prop. 5. Therefore, some optimal Sboxes in these two equivalent classes admit perfect square differentials, and using these Sboxes instead of MIDORI64's Sbox, would not avoid the weakness exhibited in Coro. 2. For instance, using Prop. 4, we were able to build an Sbox S_2 that admits $(\texttt{0x2}, \texttt{0x3})$ as a perfect square differential and is affine equivalent to S_{ilver}, the fifth *silver Sbox* given in [GJN+16]. These Sboxes are defined in Appendix A.

6 Generalization to a Larger Set of Differentials

6.1 General Setting

Definition 9 (Good set of differences). *A subset $\mathcal{A}$ of elements in $\mathbb{F}_2^s$ is said to be* a good set of differences of weight ℓ *for $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$ if all differentials $(a, b) \in \mathcal{A} \times \mathcal{A}$ are super-planar differentials with $\mathsf{DDT}_S(a, b) = 2^\ell$ and if there exists a vector space E, called the associated subspace, such that*

1. *For all $(a, b) \in \mathcal{A} \times \mathcal{A}$, $\mathsf{V}_S(a, b) \subset E$.*
2. *For all $a \in \mathcal{A}$, $\biguplus_{b\in\mathcal{A}} \mathsf{XDDT}_S(a, b) = x_0^{a,a} + E$.*

This definition generalizes the notion of square differentials: a square differential, as defined in Def. 6, is a particular case of a good set of differences of size 2. Most notably, if $\mathcal{A}$ is a good set of differences, then Eq. (3) in Lemma 6 holds for all $(x, y) \in \mathcal{A}^2$.

Now, we can prove an analogue of Prop. 3 in Section 3, on the number of $(r + 1)$-round characteristics with all differences in $\mathcal{A}^m$ that are valid for this specific key and share the same first r differences.

Proposition 7. *Let us consider an SPN with $(r + 1)$ rounds, $r \geq 1$, with Sbox S and linear layer L. Let $\mathcal{A}$ be a set of good differences of weight ℓ for S with associated subspace E, such that $L(\mathcal{A}^m) = \mathcal{A}^m$ and $L(E^m) = E^m$. Let $K := (K_1, \ldots, K_r)$ be an expanded key and $(\Delta_0, \ldots, \Delta_r)$ with all $\Delta_t \in \mathcal{A}^m$ be an r-round characteristic which is valid for the first $(r - 1)$ round keys. Then*

$$\Gamma_r := \{\Delta_{r+1} \in \mathcal{A}^m \mid (\Delta_0, \ldots, \Delta_r, \Delta_{r+1}) \text{ is a valid characteristic for } K\}$$

is non-empty if and only if

$$K_r \in L(y_0^{\Delta_{r-1}, L^{-1}(\Delta_r)}) + x_0^{\Delta_r, \Delta_r} + E^m \ .$$

In that case, the subspaces $W_{r-1}(\Delta_0, \ldots, \Delta_r)$ and $W_r(\Delta_0, \ldots, \Delta_{r+1})$ formed by the weak expanded keys for the r-round (resp. $(r + 1)$-round) characteristic satisfy:

$$\sum_{\Delta_{r+1}\in\Gamma_r} 2^{\ell m(r+1)-\dim(W_r(\Delta_0,\ldots,\Delta_{r+1}))} = 2^{\ell mr-\dim(W_{r-1}(\Delta_0,\ldots,\Delta_r))} \ .$$

Proof. Let $\Delta_{r+1} \in \mathcal{A}^m$. By Theorem 1,

$$\begin{aligned} \Delta_{r+1} \in \Gamma_r &\iff (0, \ldots, 0, x_0^{\Delta_r, L^{-1}(\Delta_{r+1})}) \in K + \widetilde{w_0} + W_r \\ &\iff \Big(\{0\}^{sm(r-1)} \times \mathsf{XDDT}_{\boldsymbol{S}}(\Delta_r, L^{-1}(\Delta_{r+1}))\Big) \bigcap (K + \widetilde{w_0} + W_r') \neq \emptyset \end{aligned}$$

where

$$\widetilde{w_0}[t] := \begin{cases} x_0^{\Delta_t, L^{-1}(\Delta_{t+1})} + L(y_0^{\Delta_{t-1}, L^{-1}(\Delta_t)}) & \text{if } 1 \leq t \leq r-1 \\ L(y_0^{\Delta_{r-1}, L^{-1}(\Delta_r)}) & \text{if } t = r \end{cases}$$

and W_r' denotes the sum of the first r subspaces defining W_r in Th. 1, i.e.,

$$W_r = W_r' + \Big(\{0\}^{sm(r-1)} \times \mathsf{U}_{\boldsymbol{S}}(\Delta_r, L^{-1}(\Delta_{r+1}))\Big) \ .$$

Then, Γ_r is not empty if and only if

$$\biguplus_{\Delta_{r+1}\in\mathcal{A}^m} \Big(\{0\}^{sm(r-1)} \times \mathsf{XDDT}_{\boldsymbol{\mathcal{S}}}(\Delta_r, L^{-1}(\Delta_{r+1}))\Big) \bigcap (K + \widetilde{w_0} + W'_r) \tag{6}$$

is not empty. By property 2. of Def. 9, the left-hand term in this intersection is equal to

$$\{0\}^{sm(r-1)} \times \left(x_0^{\Delta_r,\Delta_r} + E^m\right) .$$

Therefore, Γ_r is not empty if and only if

$$(0,\ldots,0,x_0^{\Delta_r,\Delta_r}) + K + \widetilde{w_0} \in \{0\}^{sm(r-1)} \times E^m + W'_r.$$

Eq. (3) together with the fact that $L(E^m) = E^m$ implies that

$$\{0\}^{sm(r-1)} \times E^m + W'_r = W_{r-1} \times E^m . \tag{7}$$

Hence, the above condition is equivalent to

$$\begin{aligned}(K_t)_{1\le t\le r-1} &\in \left(x_0^{\Delta_t,L^{-1}(\Delta_{t+1})} + L(y_0^{\Delta_{t-1},L^{-1}(\Delta_t)})\right)_{1\le t\le r-1} + W_{r-1}\\ K_r &\in L(y_0^{\Delta_{r-1},L^{-1}(\Delta_r)}) + x_0^{\Delta_r,\Delta_r} + E^m .\end{aligned}$$

The first condition is satisfied since $(\Delta_t)_{1\le t\le r}$ is a valid characteristic for $(K_t)_{1\le t\le r-1}$. The second condition is exactly the one stated in the proposition.

Now, when Γ_r is not empty,

$$\{0\}^{sm(r-1)} \times \left(x_0^{\Delta_r,\Delta_r} + E^m\right) \bigcap (K + \widetilde{w_0} + W'_r)$$

is a non-empty affine space. Its dimension is equal to

$$\dim(E^m) + \dim(W'_r) - \dim(\{0\}^{sm(r-1)} \times E^m + W'_r) = \dim(W'_r) - \dim(W_{r-1})$$

where the last equality stems from Equation (7). Now, in order to compute $\dim(W'_r)$, let us show that the sum defining W'_r is a direct sum. To do so, let us consider $v_0 \in \mathsf{V}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1))$, and for $1 \le t \le r-1$, $u_t \in \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1}))$ such that

$$\big(L(v_0) + u_1, L\circ\phi_{\Delta_1,L^{-1}(\Delta_2)}(u_1) + u_2, \ldots, L\circ\phi_{\Delta_{r-2},L^{-1}(\Delta_{r-1})}(u_{r-2}) + u_{r-1}, L\circ\phi_{\Delta_{r-1},L^{-1}(\Delta_r)}(u_{r-1})\big)$$

is the all-zero vector in $\mathbb{F}_2^{nr}$. Then, looking at the last coordinate, we obtain

$$L\circ\phi_{\Delta_{r-1},L^{-1}(\Delta_r)}(u_{r-1}) = 0$$

which implies $u_{r-1} = 0$ since L and $\phi_{\Delta_{r-1},L^{-1}(\Delta_r)}$ are isomorphisms. Now, looking at the $(r-1)$-th coordinate, we get $L\circ\phi_{\Delta_{r-2},L^{-1}(\Delta_{r-1})}(u_{r-2}) = 0$ which leads to $u_{r-2} = 0$. We can then show by induction that $u_t = 0$ for all $1 \le t \le r-1$. Then, the condition on the first coordinate becomes $L(v_0) = 0$ which implies $v_0 = 0$. This proves that W'_r is indeed a direct sum of r vector spaces of dimension ℓm. Therefore, $\dim(W'_r) = \ell r m$. On the other hand, Equation (6) yields

$$\sum_{\Delta_{r+1}\in\Gamma_r} 2^{\dim(\mathcal{E}_r(\Delta_0,\Delta_1,\ldots,\Delta_{r+1}))} = 2^{\ell m r - \dim(W_{r-1})}$$

where $\mathcal{E}_r(\Delta_0,\Delta_1,\ldots,\Delta_{r+1}) = \big(\{0\}^{sm(r-1)} \times \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_r, L^{-1}(\Delta_{r+1}))\big) \bigcap W'_r$. Finally, recall that $\{0\}^{sm(r-1)} \times \mathsf{U}_S(\Delta_r, L^{-1}(\Delta_{r+1})) + W'_r = W_r$. Therefore,

$$\begin{aligned}\dim(\mathcal{E}_r) &= \dim(\mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_r, L^{-1}(\Delta_{r+1}))) + \dim(W'_r) - \dim(W_r)\\ &= \ell m(r+1) - \dim(W_r) .\end{aligned}$$

□

The situation is therefore similar to the case of square differentials. Starting from a given r-round characteristic $(\Delta_0, \ldots, \Delta_r)$ with all $\Delta_t \in \mathcal{A}^m$, two situations can occur, depending on whether the last round-key K_r satisfies a condition involving Δ_{r-1} and Δ_r. Either this characteristic cannot be extended to a longer characteristic with differences in $\mathcal{A}^m$, or it can be extended to many such $(r+1)$-round characteristics. As a consequence, the following generalization of Coro. 2 states that if the set of good differentials satisfies an additional condition, which generalizes the notion of *perfect square differentials*, the condition on K_r required for extending $(\Delta_0, \ldots, \Delta_r)$ one round further is the same for all characteristics.

Corollary 3. *Let us consider an SPN with Sbox S and linear layer L. Let $\mathcal{A}$ be a set of good differences of weight ℓ for S with associated subspace E, such that $L(\mathcal{A}^m) = \mathcal{A}^m$ and $L(E^m) = E^m$. Assume that for any $\Delta, \Delta' \in \mathcal{A}^m$,*

$$L(y_0^{\Delta, L^{-1}(\Delta')}) + x_0^{\Delta', \Delta'} \in \theta + E^m$$

for some offset $\theta \in \mathbb{F}_2^{sm}$. Then, for any expanded key K in $(\theta + E^m)^r$ and for any $\Delta_0 \in \mathcal{A}^m$, we have

$$\sum_{\Delta_1, \ldots, \Delta_r \in \mathcal{A}^m} \mathsf{DP}[K](\Delta_0, \ldots, \Delta_r) = \left(2^{-(s-\ell)} \# \mathcal{A}\right)^m .$$

Proof. Let us prove the result by induction. Let us denote by N_r the number of inputs satisfying an r-round characteristic with differences in $\mathcal{A}^m$ and starting from Δ_0. We will prove that $N_r = \left(2^\ell \times \#\mathcal{A}\right)^m$ for all $r \geq 1$.

First, for $r = 1$, we have

$$N_1 = \sum_{\Delta_1 \in \mathcal{A}^m} \prod_{j=1}^{m} \mathsf{DDT}_{\boldsymbol{s}}(\Delta_0[j], L^{-1}(\Delta_1[j])) = \sum_{\Delta_1 \in \mathcal{A}^m} 2^{\ell m} = \left(2^\ell \times \#\mathcal{A}\right)^m .$$

For the induction part, let $r \geq 1$ and suppose that $N_r = \left(2^\ell \times \#\mathcal{A}\right)^m$. By Th. 1,

$$N_{r+1} = \sum_{\Delta_1 \in \mathcal{A}^m} \sum_{\Delta_2 \in \Gamma_1} \cdots \sum_{\Delta_{r+1} \in \Gamma_r} 2^{\ell m(r+1) - \dim(W_r)} .$$

By Prop. 7, $\Gamma_r \neq \emptyset$ and

$$\sum_{\Delta_{r+1} \in \Gamma_r} 2^{km(r+1) - \dim(W_r)} = 2^{\ell m r - \dim(W_{r-1})(\Delta_0, \ldots, \Delta_r)} .$$

Then, we deduce from the induction hypothesis that $N_{r+1} = N_r = (2^\ell \times \mathcal{A})^m$. □

6.2 Truncated Differentials for Scream and iScream

Using commutative cryptanalysis, Baudrin *et al.* [BFL+23] observed that Scream exhibits a behaviour similar to Midori64, namely the existence of fixed-key truncated differentials whose probabilities are independent of the number of rounds. This phenomenon is captured by the previous result for a suitable set of differences forming an affine subspace of dimension 3. A comparable differential behaviour can also be identified in iScream, although the techniques of [BFL+23] no longer apply. Let S_3 (resp. S_4) denote the S-box of Scream (resp. iScream), and L_3 (resp. L_4) its linear layer. Both L_3 and L_4 satisfy Property $(\mathcal{P})$. However, the approach of [BFL+23] does not apply to iScream, since there exist no non-trivial affine bijections $B, C : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $B \circ S_4 = S_4 \circ C$. This can be checked, as suggested by the authors, using the function `self_affine_equivalent_mappings` from the `sboxU` library.[2] Now, let $\mathcal{A}_3 := \texttt{0x21} + \langle \texttt{0x10,0x40,0x80} \rangle$ and $\mathcal{A}_4 := \texttt{0x94} + \langle \texttt{0x01,0x02,0x08} \rangle$. Then it can be easily checked that $\mathcal{A}_3$ (resp. $\mathcal{A}_4$) is a good set of differences for S_3 (resp. S_4) with associated subspace $E_3 := \langle \texttt{0x01,0x10,0x20,0x40,0x80} \rangle$ (resp. $E_4 := \langle \texttt{0x90,0x08,0x04,0x02,0x01} \rangle$). Moreover, let us show that Scream satisfies the condition exhibited in Coro. 3. To that purpose, we will need the following observations:

[2] `https://github.com/lpp-crypto/sboxU`

(1) $\forall (a,b) \in \mathcal{A}_3^2, \mathsf{U}_{S_3}(a,b) = \mathsf{V}_{S_3}(b,a)$ and $y_0^{b,a} \in \mathtt{0x01} + x_0^{a,b} + \mathsf{U}_S(a,b)$.
(2) $\forall (a,b,c) \in \mathcal{A}_3^3, x_0^{a+b+c,a+b+c} + E_3 = x_0^{a,a} + x_0^{b,b} + x_0^{c,c} + E_3$.

These observations allow us to prove the following lemma which corresponds exactly to the condition exhibited in Coro. 3.

Lemma 10. *For all $\Delta, \Delta' \in \mathcal{A}_3^{16}$, $L_3(y_0^{\Delta, L_3^{-1}(\Delta')}) + x_0^{\Delta',\Delta'} \in E_3^{16}$.*

Proof.

$$L_3(y_0^{\Delta, L_3^{-1}(\Delta')}) + x_0^{\Delta',\Delta'} \in E_3^{16} \iff y_0^{\Delta, L_3^{-1}(\Delta')} + L_3^{-1}(x_0^{\Delta',\Delta'}) \in E_3^{16}$$

By Observation (1) above,

$$y_0^{\Delta, L_3^{-1}(\Delta')} + E_3^{16} = (\mathtt{0x01})^{\times 16} + x_0^{L_3^{-1}(\Delta'),\Delta} + E_3^{16} = x_0^{L_3^{-1}(\Delta'),\Delta} + E_3^{16}$$

Now, let us prove that $L_3^{-1}(x_0^{\Delta'}) + x_0^{L_3^{-1}(\Delta')} \in E_3^{16}$. Using the Observation (2) above, we can prove by induction that

$$\forall k \geq 1,\ \forall (a_1, a_2, \ldots, a_{2k+1}) \in \mathcal{A}_3,\ x_0^{\sum_{j=1}^{2k+1} a_j} + \sum_{j=1}^{2k+1} x_0^{a_j} \in E_3. \tag{8}$$

Indeed, Observation (2) corresponds to the case $k = 1$ and for the induction step, we use the following writing:

$$\sum_{j=1}^{2k+1} x_0^{a_j} = \sum_{j=1}^{2k-1} x_0^{a_j} + x_0^{a_{2k}} + x_0^{a_{2k+1}}$$

and apply the same observation with $a = \sum_{j=1}^{2k-1} a_j$, $b = a_{2k}$ and $c = a_{2k+1}$. Finally, let $1 \leq j \leq 16$ and $I_j := \{1 \leq k \leq 16 \mid M^{-1}_{j,k} = 1\}$ where $M \in \mathcal{M}_{16}(\mathbb{F}_{2^s})$ is the matrix canonically associated to L_3. Since L_3 satisfies $(\mathcal{P})$, so does L_3^{-1}. Therefore, all entries in M^{-1} are in $\{0,1\}$ and $\#I_j$ is odd. The j-th coordinate of $L_3^{-1}(x_0^{\Delta'}) + x_0^{L_3^{-1}(\Delta')}$ is

$$\sum_{k \in I_j} x_0^{\Delta'_k} + x_0^{\sum_{k \in I_j} \Delta'_k},$$

where Δ'_k denotes the k-th coordinate of Δ'. Equation (8) shows that it belongs to E_3. □

Lemma 10 implies that the weak-key sets are the same for all differentials in $\mathcal{A}_3 \times \mathcal{A}_3$, which leads to a truncated differential of probability 2^{-48} for Scream. Namely, combining Lemma 10 with Coro. 3 we show that, for an arbitrary number $r \geq 1$ of rounds,

$$\forall \Delta_0 \in \mathcal{A}_3^{16},\ \forall K \in E_3^{16(r-1)} \sum_{\Delta_1, \ldots, \Delta_r \in \mathcal{A}_3^m} \mathsf{DP}[K](\Delta_0, \ldots, \Delta_r) = 2^{-48}\ .$$

Concerning iScream, Observation (1) holds but Observation (2) does not. Consequently, the differential characteristics involved in the cluster are valid for different weak-keys, implying that there is no fixed-key clustering. Therefore, our analysis provides an explanation for the origin of these two differential behaviours, despite their apparent similarity at first glance.

7 Similarities and Differences with Other Concepts

Since Midori64 already suffers from many different types of attacks, including invariants [GJN+16,TLS16,Bey18] and commutative cryptanalysis [BFL+23], it is worth understanding whether the phenomenon we have analysed, namely a clustering of plateau characteristics having the same weak keys, is related to these other notions.

7.1 Super-Planar Plateau Characteristics and Invariant Subspaces

As detailed in Coro. 1, the plateau characteristics studied in Th. 1 imply the existence of chains of affine subspaces that propagate across the cipher. This property differs from the notion of *subspace trail*, defined in [GRR16] and analyzed in [LTW18], which is a stronger property than a subspace chain. In a subspace trail, each coset of a given subspace is mapped to a coset of the output subspace. If the subspaces in Coro. 1 formed a subspace trail, all expanded keys would have the same behaviour, which is not the case for plateau characteristics.

It may happen that the chain of affine subspaces associated to a plateau characteristic corresponds to an invariant subspace, as identified in Prop. 2 when $\mathsf{U}_S(a,b) = \mathsf{V}_S(a,b)$. In this particular case, $\mathsf{XDDT}_S(a,b)$ is an invariant subspace for the Sbox. This is what happens in MIDORI64 for a subset of the weak keys we consider [GJN+16]. However, in general, the chains of subspaces corresponding to the characteristics in Th. 1 are not related to an invariant subspace.

Conversely, an invariant subspace does not always define the valid inputs of a plateau characteristic. For example, $\mathcal{A}_0^{16}$, with $\mathcal{A}_0 := \mathtt{0x18} + \langle \mathtt{0x01}, \mathtt{0x64}, \mathtt{0x86} \rangle$, is an invariant subspace of ISCREAM for 2^{48} weak keys [LMR15]. However, the input set of a differential characteristic is always included in a set $\mathsf{XDDT}_{\boldsymbol{\mathcal{S}}}(A,B)$ for some nonzero differences A and B, which is not the case of $\mathcal{A}_0^{16}$.

7.2 Clusters of Plateau Characteristics, Invariant Subspaces and Truncated Differentials

The differential behaviour we have identified shares with invariant subspaces and commutative cryptanalysis the property that it defines a fixed-key truncated differential for r rounds, of the form

$$\sum_{\Delta_r \in \mathcal{D}} \mathsf{DP}[K](\Delta_0, \Delta_r) \geq 2^{-ms+k} \tag{9}$$

for a subspace W^r of weak keys, where ms is the block size of the cipher.

In the case of an invariant subspace, e.g. if $\mathcal{R}(a+V) = b+V$, then the truncated differential we derive includes all output differences in $\mathcal{D} = V$ and $k = \dim W = \dim V$. If V is defined as an invariant under several rounds, but is not invariant under the round function, $\mathcal{D}$ and k in (9) remain the same, but the weak-key set is not of the form W^r anymore (see [Bey18]).

When considering a square differential (α, β) for the Sbox as in Section 3, the output difference in (9) varies in $\mathcal{D} = \{\alpha, \beta\}^m$ and $k = \dim W = m(\ell+1)$ where $\mathsf{DDT}_S(\alpha,\beta) = 2^\ell$. In the more general situation of a good set of differences, we still have that $k = \dim W = m\ell + \log_2(\#\mathcal{D})$. Therefore, k is always strictly greater than the dimension of $\mathcal{D}$, while both values are equal when the truncated differential is derived from an invariant subspace. This shows that these two phenomena are distinct.

An argument pointing out the difference between our work and nonlinear invariants is that MIDORI64 with Sbox S_2, defined in App. A, has the same behaviour as the genuine MIDORI64 as shown at the end of Section 5. However, neither S_2 nor its powers S_2^i for $i \leq 4$, admit a quadratic invariant. Therefore, the truncated differential we present does not stem from a quadratic invariant of the round function nor from a two-round invariant, as those identified in [Bey18]. Moreover, the weak-key set identified by Coro. 2 differs from those found in [Bey18], and is strictly larger than those in [TLS16].

Obviously, as already noted in [LTW18] in the case of subspace trails, the notion of truncated differentials is more general than the differential behaviour we analyse (and than the notion of invariant subspaces).

7.3 Clusters of Plateau Characteristics and Commutative Cryptanalysis

We now show that our results capture the truncated differentials derived from commutative cryptanalysis [BFL+23] as soon as the corresponding differentials for the Sbox are super-planar. As in [BFL+23], we only focus on commutants that are built from a small affine bijection A that commutes with the Sbox.[3] Let $\mathcal{A} := c_A + \mathsf{Im}(\mathsf{Id} + L_A)$ and $E := \mathsf{Ker}(\mathsf{Id} + L_A)$ where L_A is the linear part of A and $c_A := A + L_A$.

[3] The linear commutants that are independent of the Sbox, as in [LMR15,CFG+17], are of a different nature.

Lemma 11. *$\forall a \in \mathcal{A},\ \{x \in \mathbb{F}_2^s \mid S(x) + S(x+a) \in \mathcal{A}\}$ is a coset of E. Moreover,*

$$\biguplus_{a\in\mathcal{A}} \{x \in \mathbb{F}_2^s \mid S(x) + S(x+a) \in \mathcal{A}\} = \mathbb{F}_2^s$$

Proof. First, we observe that $x + A(x) = a$ iff $(\mathsf{Id} + L_A)(x) = a + c_A$. Therefore, since $\{x \mid x + A(x) = a\}$ is not empty, it is a coset of $E := \mathsf{Ker}(\mathsf{Id} + L_A)$ with offset x_a. Moreover, we have $\biguplus_{a\in\mathcal{A}} x_a + E = \mathbb{F}_2^s$ since $\dim(\mathcal{A}) + \dim(E) = s$.
Now, for all $a \in \mathcal{A}$, $\{x \mid x + A(x) = a\} \subset \{x \in \mathbb{F}_2^s \mid S(x) + S(x+a) \in \mathcal{A}\}$. Indeed, if $x + A(x) = a$ then $S(x) + S(x+a) = S(x) + S(A(x)) = (\mathsf{Id} + A)(S(x)) \in \mathcal{A}$.
Finally, if there exists $a_0 \in \mathcal{A}$ such that $\{x \mid x + A(x) = a_0\} \subsetneq \{x \mid S(x) + S(x+a_0) \in \mathcal{A}\}$, then we would have

$$\mathbb{F}_2^s \subsetneq \biguplus_{a\in\mathcal{A}} \{x \mid S(x) + S(x+a) \in \mathcal{A}\}$$

which is a contradiction. □

Corollary 4. *If all pairs (α, β) of elements of $\mathcal{A}$ are super-planar differentials for S with $\mathsf{DDT}_S(\alpha, \beta) = 2^\ell$, then $\mathcal{A}$ is a good set of differentials as defined in Def 9. In the particular case where $\dim \mathcal{A} = 1$, $\mathcal{A}$ is a square differential.*

Proof. $\mathcal{A}$ is a good set of differentials if the following two conditions hold:

1. For all $(a, b) \in \mathcal{A} \times \mathcal{A}$, $\mathsf{V}_S(a, b) \subset E$.
2. For all $a \in \mathcal{A}, \biguplus_{b\in\mathcal{A}} \mathsf{XDDT}_S(a, b) = x_0^{a,a} + E$.

The second one is a direct application of Lemma 11. For the first one, we observe that $S^{-1} \circ (A \circ S) \circ S^{-1} = S^{-1} \circ (S \circ A) \circ S^{-1}$, *i.e.*, $S^{-1} \circ A = A \circ S^{-1}$. Therefore, from Lemma 11, $\forall b \in \mathcal{A}, \biguplus_{a\in\mathcal{A}} \mathsf{XDDT}_{S^{-1}}(b, a) = x_b + E$. It follows that, $\mathsf{YDDT}_S(a, b) = \mathsf{XDDT}_{S^{-1}}(b, a) \subset x_b + E$. Hence, $\mathsf{V}_S(a, b) \subset E$.

Let us now focus on $\mathcal{A} = \{a_0, a_1\}$ and on Conditions 2 and 3 in Def. 6, since the other two conditions trivially hold. From Lemma 11, $\mathsf{XDDT}_S(a, a_0) \uplus \mathsf{XDDT}_S(a, a_1) = x_a + E$, hence $\dim(E) = \ell + 1$. Let us write $\mathsf{XDDT}_S(a, a_0) = x_0 + \langle(\theta_i)_{1\le i\le \ell}\rangle$ and $\mathsf{XDDT}_S(a, a_1) = x_1 + \langle(\delta_i)_{1\le i\le \ell}\rangle$. Since $\mathsf{XDDT}_S(a, a_0)$ and $\mathsf{XDDT}_S(a, a_1)$ are disjoint, $x_0 + x_1 \notin \langle(\theta_i)_{1\le i\le \ell}, (\delta_i)_{1\le i\le \ell}\rangle$. Moreover, since E is a linear space,

$$\langle x_0 + x_1, (\theta_i)_{1\le i\le \ell}, (\delta_i)_{1\le i\le \ell}\rangle \subset E\ .$$

The dimension of the left-hand side is

$$1 + \dim \langle(\theta_i)_{1\le i\le \ell}, (\delta_i)_{1\le i\le \ell}\rangle \ge 1 + \ell = \dim(E)\ .$$

This implies $\langle(\theta_i)_{1\le i\le \ell}\rangle = \langle(\delta_i)_{1\le i\le \ell}\rangle$ *i.e*, $\mathsf{U}_S(a, a_0) = \mathsf{U}_S(a, a_1)$ (Condition 2) and that $E = \langle x_0 + x_1\rangle + \mathsf{U}_S(a)$ (Condition 3). □

Commutation with the linear layer. We now show that if the linear layer L commutes with A^m, then it satisfies the hypotheses of Coro. 3. Indeed, the only requirement is that E^m and $\mathcal{A}^m$ are invariant under L (this also holds for the particular case of Coro. 2, as observed in Rmk. 2). These two conditions can be deduced from the following observation, stated in [Bau24, Lemma 5.12]: $A^{\times m} \circ L = L \circ A^{\times m}$ iff $L_A^{\times m} \circ L = L \circ L_A^{\times m}$ and $L(c_A^{\times m}) = c_A^{\times m}$.

Therefore, it follows that the fixed-key truncated differentials derived from commutative trails built from a matrix A commuting with the Sbox and such that A^m commutes with the linear layer, all correspond to a cluster of plateau characteristics and are captured by our work. The only additional condition we need is that the involved differentials are super-planar.

Remark 4. Compared to [BFL+23], we require that all pairs in $\mathcal{A}$ are super-planar differentials. This condition always holds when the Sbox has differential uniformity at most 4 and when $0 \notin \mathcal{A}$. This last requirement equivalently means that $c_A \neq 0$. But when $c_A = 0$, $A = L_A$ is linear and E is an invariant subspace of the cipher. This is the case of the commutative trail for MIDORI128 (without key-schedule) exhibited in [BFL+23]. This subspace is invariant under the linear and the Sbox layers.

Most importantly, our work captures more ciphers than the ones covered by the commutative trails described in [BFL+23]. For instance, as detailed in Section 6, it enables us to show that SCREAM and ISCREAM both present similar clusters of plateau characteristics, but that the associated weak-keys are the same of all characteristics in SCREAM, and are different in ISCREAM.

8 Conclusions and Future Work

Our work emphasizes that when the hypothesis of stochastic equivalence does not hold, estimating the expected differential probability of an overall differential by summing the EDPs of its individual characteristics can be misleading. By focusing on (truncated) differentials composed of plateau characteristics, we are able to characterize and explain the distinct fixed-key behaviours of MIDORI64, SCREAM and ISCREAM with respect to certain truncated differentials. Identifying this mechanism is particularly relevant, as the associated weak expanded-keys of MIDORI64 are not detected by other known attacks, such as invariant-subspace attacks. Gaining insight into this *a priori* unpredictable differential behaviour is therefore crucial. Ignoring it could raise concerns about the security of other lightweight ciphers that relies solely on conventional EDP-based reasoning.

Our analysis has two major limitations: it is restricted to ciphers whose linear layers let some particular subspaces invariant. This holds in particular for the linear layers with a binary matrix satisfying the so-called Property ($\mathcal{P}$), as those of MIDORI, SCREAM, ISCREAM, PRINCE or MANTIS. It is also limited to differential characteristics where all internal differentials for the Sbox are super-planar, otherwise these characteristics won't be plateau. In practice, when the Sbox has differential uniformity at most 4, this condition equivalently means that *all internal Sboxes are active*. Generalizing this to non-plateau characteristics would require determining the fixed-key probabilities of characteristics that do not present such a strong structure. The quasi-differential framework offers a promising avenue in this context, but deriving meaningful expressions for a large set of characteristics remains challenging, especially because it not only involves the differential properties of the Sboxes, but also their Walsh spectra. The omission of the concrete key schedule in our analysis should not be viewed as a limitation. Quite the opposite, it enables a two-step design approach: first, identifying potential weaknesses in the expanded-key model, and then developing a key schedule that mitigates them. Guaranteeing the absence of weak expanded keys is an attractive design principle, as it provides greater flexibility in the choice of key-schedule algorithms.

Acknowledgements. This work was supported by PEPR Cybersécurité, project Cryptanalyse (22-PECY-0010) and by the French DGA. The authors warmly thank Jules Baudrin and Léo Perrin for stimulating discussions, and the anonymous reviewers for their insightful comments, which contributed to improving the quality of this work.

References

ABC+19. Alexandre Adomnicai, Thierry P. Berger, Christophe Clavier, Julien Francq, Paul Huynh, Virginie Lallemand, Kévin Le Gouguec, Marine Minier, Léo Reynaud, and Gaël Thomas. Lilliput-AE: a new lightweight tweakable block cipher for authenticated encryption with associated data. Submission to the NIST Lightweight Cryptography Standardization Process `https://csrc.nist.rip/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/LILLIPUT-AE-spec.pdf`, 2019.

Abd13. Mohamed Ahmed Abdelraheem. Estimating the probabilities of low-weight differential and linear approximations on PRESENT-like ciphers. In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *ICISC 12*, volume 7839 of *LNCS*, pages 368–382. Springer, Berlin, Heidelberg, November 2013.

Bau24. Jules Baudrin. *Algebraic properties of symmetric ciphers and of their non-linear components*. PhD thesis, Sorbonne Université, 2024. `https://theses.fr/api/v1/document/2024SORUS547`.

BBI+15. Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 411–436. Springer, Berlin, Heidelberg, November / December 2015.

BCG+12. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knežević, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 208–225. Springer, Berlin, Heidelberg, December 2012.

Bey18. Tim Beyne. Block cipher invariants as eigenvectors of correlation matrices. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 3–31. Springer, Cham, December 2018.

BFL+23. Jules Baudrin, Patrick Felke, Gregor Leander, Patrick Neumann, Léo Perrin, and Lukas Stennes. Commutative cryptanalysis made practical. *IACR Trans. Symm. Cryptol.*, 2023(4):299–329, 2023.

BJK+16. Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 123–153. Springer, Berlin, Heidelberg, August 2016.

BR22. Tim Beyne and Vincent Rijmen. Differential cryptanalysis in the fixed-key model. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part III*, volume 13509 of *LNCS*, pages 687–716. Springer, Cham, August 2022.

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

CFG+15. Anne Canteaut, Thomas Fuhr, Henri Gilbert, María Naya-Plasencia, and Jean-René Reinhard. Multiple differential cryptanalysis of round-reduced PRINCE. In Carlos Cid and Christian Rechberger, editors, *FSE 2014*, volume 8540 of *LNCS*, pages 591–610. Springer, Berlin, Heidelberg, March 2015.

CFG+17. Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jérémy Jean, and Jean-René Reinhard. Cryptanalysis of NORX v2.0. *IACR Trans. Symm. Cryptol.*, 2017(1):156–174, 2017.

CSW08. Christophe De Cannière, Hisayoshi Sato, and Dai Watanabe. Hash function *Luffa*: Specification. Submission to NIST `https://www.hitachi.com/rd/yrl/crypto/luffa/round1archive/Luffa_Specification.pdf`, 2008.

DC07. Christophe De Cannière. *Analysis and Design of Symmetric Encryption Algorithms*. PhD thesis, Katholieke Universiteit Leuven, 2007.

DR01. Joan Daemen and Vincent Rijmen. The wide trail design strategy. In Bahram Honary, editor, *8th IMA International Conference on Cryptography and Coding*, volume 2260 of *LNCS*, pages 222–238. Springer, Berlin, Heidelberg, December 2001.

DR07. Joan Daemen and Vincent Rijmen. Plateau characteristics. *IET information security*, 1(1):11–17, 2007.

GJN+16. Jian Guo, Jérémy Jean, Ivica Nikolic, Kexin Qiao, Yu Sasaki, and Siang Meng Sim. Invariant subspace attack against Midori64 and the resistance criteria for S-box designs. *IACR Trans. Symm. Cryptol.*, 2016(1):33–56, 2016.

GLS+14. Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici, François Durvaux, Lubos Gaspar, and Stéephanie Kerckhof. SCREAM & iSCREAM: Side-channel resistant authenticated encryption with masking. Submission to the Caesar competition `https://competitions.cr.yp.to/round1/screamv1.pdf`, 2014.

GRR16. Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace trail cryptanalysis and its applications to AES. *IACR Trans. Symm. Cryptol.*, 2016(2):192–225, 2016.

KLPR10. Lars R. Knudsen, Gregor Leander, Axel Poschmann, and Matthew J. B. Robshaw. PRINTcipher: A block cipher for IC-printing. In Stefan Mangard and François-Xavier Standaert, editors, *CHES 2010*, volume 6225 of *LNCS*, pages 16–32. Springer, Berlin, Heidelberg, August 2010.

Knu93. Lars R. Knudsen. Iterative characteristics of DES and s^2-DES. In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 497–511. Springer, Berlin, Heidelberg, August 1993.

LAAZ11. Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A cryptanalysis of PRINTcipher: The invariant subspace attack. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 206–221. Springer, Berlin, Heidelberg, August 2011.

LMM91. Xuejia Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 17–38. Springer, Berlin, Heidelberg, April 1991.

LMR15. Gregor Leander, Brice Minaud, and Sondre Rønjom. A generic approach to invariant subspace attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 254–283. Springer, Berlin, Heidelberg, April 2015.

LP07. Gregor Leander and Axel Poschmann. On the classification of 4 bit S-boxes. In Claude Carlet and Berk Sunar, editors, *WAIFI 2007*, pages 159–176, Berlin, Heidelberg, 2007. Springer.

LPS21. Gaëtan Leurent, Clara Pernot, and André Schrottenloher. Clustering effect in Simon and Simeck. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 272–302. Springer, Cham, December 2021.

LTW18. Gregor Leander, Cihangir Tezcan, and Friedrich Wiemer. Searching for subspace trails and truncated differentials. *IACR Trans. Symm. Cryptol.*, 2018(1):74–100, 2018.

Nyb12. Kaisa Nyberg. "Provable" security against differential and linear cryptanalysis (invited talk). In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 1–8. Springer, Berlin, Heidelberg, March 2012.

SMS19. Sumanta Sarkar, Kalikinkar Mandal, and Dhiman Saha. Sycon v1.0. Submission to Lightweight Cryptographic Standards `https://csrc.nist.gov/csrc/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/sycon-spec.pdf`, 2019.

TLS16. Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear invariant attack - practical attack on full SCREAM, iSCREAM, and Midori64. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 3–33. Springer, Berlin, Heidelberg, December 2016.

ZBL+14. Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, and Ingrid Verbauwhede. RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms. Cryptology ePrint Archive, Report 2014/084, 2014.

ZBL+15. Wentao Zhang, Zhenzhen Bao, Dongdai Lin, Vincent Rijmen, Bohan Yang, and Ingrid Verbauwhede. RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. *Sci. China Inf. Sci.*, 58(12):1–15, 2015.

A Specifications of the Sboxes Analysed in the Paper

Table1: Specifications of the 4-bit Sboxes used in the paper, in hexadecimal notation.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
MIDORI64	c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6
RECTANGLE	6	5	c	a	1	e	7	9	b	0	3	d	8	f	4	2
Luffa v1	7	d	b	a	c	4	8	3	5	f	6	0	9	1	2	c
S_1	4	8	1	7	9	0	e	3	6	5	f	d	2	a	c	b
S_2	b	9	a	8	7	c	4	e	5	0	6	2	d	1	3	f
S_{ilver}	0	1	2	d	4	7	f	6	8	b	e	3	a	c	5	9

B Some Examples of Square Differentials in Sboxes from the Literature

Table2: Examples of Square Differentials.

Sbox	s	ℓ	(α, β)	Involution?	Perfect?
MIDORI64	4	2	(0xa, 0xf)	Yes	Yes
RECTANGLE	4	1	(0x5, 0x9)	No	No
Luffa v1	4	1	(0x7, 0xf)	No	No
PRINTCIPHER [KLPR10]	3	1	(0x1, 0x7)	No	No
SYCON [SMS19]	5	1	(0x5, 0x7)	No	No
LILLIPUT-AE [ABC+19]	8	2	(0x06, 0x46)	No	Yes

C Minimal Probability of Valid Characteristics

Obviously, any valid characteristic has at least 2 valid inputs. Therefore, its probability cannot be lower than 2^{-ms+1} where ms is the block size. However, we show that this bound may be larger for the characteristic with differences in $\{\alpha, \beta\}^m$ when the square differential (α, β) satisfies some additionnal property. This situation occurs for instance in MIDORI64.

Proposition 8. *Let us consider an SPN whose linear layer L satisfies Property $(\mathcal{P})$. Let (α, β) be a square differential for S with $\mathsf{DDT}_S(\alpha, \beta) = 2^\ell$ and such that*

1. $\mathsf{U}_S(\alpha) = \mathsf{V}_S(\alpha)$ *and* $\mathsf{U}_S(\beta) = \mathsf{V}_S(\beta)$
2. $\phi_{\alpha,\beta} \circ \phi_{\beta,\alpha} = \mathsf{Id}_{\mathsf{U}_S(\alpha)}$
3. $\phi^2_{\beta,\beta} = \mathsf{Id}_{\mathsf{U}_S(\beta)}$ *and* $\phi^2_{\alpha,\alpha} = \mathsf{Id}_{\mathsf{U}_S(\alpha)}$
4. $\phi_{\alpha,\beta} = \phi_{\alpha,\alpha} \circ \phi_{\alpha,\beta} \circ \phi_{\beta,\beta}$

Let $K \in \mathbb{F}_2^{sm(r-1)}$ be an expanded key and $(\Delta_0, \ldots, \Delta_r)$ with all $\Delta_t \in \{\alpha, \beta\}^m$, be a valid characteristic for K. Then, $(\Delta_0, \ldots, \Delta_r)$ has at least 2^ℓ valid inputs.

Proof. For all $u \in \mathsf{U}_S(\alpha)$, we define $\theta^{(0)}_u : \{\alpha, \beta\} \to \mathbb{F}_2^4$ by

$$\theta^{(0)}_u(\alpha) = u \text{ and } \theta^{(0)}_u(\beta) = (\phi_{\alpha,\beta} \circ \phi_{\alpha,\alpha})(u) \ .$$

Similarly, we define $\theta_u^{(1)} : \{\alpha, \beta\} \to \mathbb{F}_2^4$ by

$$\theta_u^{(1)}(\alpha) = \phi_{\alpha,\alpha}(u) \text{ and } \theta_u^{(1)}(\beta) = \phi_{\alpha,\beta}(u) \ .$$

By definition, we have for $i \in \{0, 1\}$ and $x \in \{\alpha, \beta\}$, $\theta_u^{(i)}(x) \in \mathsf{U}_S(x) = \mathsf{V}_S(x)$. From Prop. 1, the number of valid inputs for the characteristic is equal to the cardinality of

$$\begin{aligned} X_r := \{x \in \mathsf{V}_{\boldsymbol{\mathcal{S}}}(\Delta_0, L^{-1}(\Delta_1)) \mid & \ L \circ \phi_{\Delta_{t-1},L^{-1}(\Delta_t)} \circ \ldots \circ L \circ \phi_{\Delta_1,L^{-1}(\Delta_2)} \circ L(x) \\ & \text{belongs to } \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1})),\ \forall 1 \leq t \leq r-1\}. \end{aligned}$$

Now, let us show that $x \in X_r$ implies that the elements $x + (\theta_u^{(1)}(L^{-1}(\Delta_1[j])))_{1 \leq j \leq m}$, for all $u \in \mathsf{U}_S(\alpha)$, belong to X_r too. To do so, we will use the following two facts:

- For any $A \in \{\alpha, \beta\}^m$, $L\left((\theta_u^{(i)}(A[j]))_{1 \leq j \leq m}\right) = (\theta_u^{(i)}(L(A)[j]))_{1 \leq j \leq m}$.
- For all $u \in \mathsf{U}_S(\alpha)$, for all $(x, y) \in \{\alpha, \beta\}^2$, we have

$$(\phi_{x,y} \circ \theta_u^{(i \mod 2)})(x) = \theta_u^{(i+1 \mod 2)}(y).$$

The first one is a direct application of Lemma 4 and the second one follows from the assumptions of the proposition. For $1 \leq t \leq r-1$ let us denote

$$\Psi_t := L \circ \phi_{\Delta_{t-1},L^{-1}(\Delta_t)} \circ \ldots \circ L \circ \phi_{\Delta_1,L^{-1}(\Delta_2)} \circ L \ .$$

Then, the above facts yield

$$\Psi_t\left(x + (\theta_u^{(1)}(L^{-1}(\Delta_1[j])))_{1 \leq j \leq m}\right) = \Psi_t(x) + (\theta_u^{(t \mod 2)}(\Delta_t[j]))_{1 \leq j \leq m}.$$

Therefore, if $x \in X_r$, then for all $1 \leq t \leq r-1$, $\Psi_t(x) \in \mathsf{U}_{\boldsymbol{\mathcal{S}}}(\Delta_t, L^{-1}(\Delta_{t+1}))$. Combining this fact with the above equation leads to

$$x + (\theta_u^{(1)}(L^{-1}(\Delta_1[j])))_{1 \leq j \leq m} \in \ X_r.$$

Finally, each distinct $u \in \mathsf{U}_S(\alpha)$ gives a distinct $(\theta_u^{(1)}(L^{-1}(\Delta_1[j])))$, therefore, there are at least $\#\mathsf{U}_S(\alpha) = 2^\ell$ valid inputs for the characteristic. □