Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer

Lorenzo Grassi[1], Christian Rechberger[2] and Markus Schofnegger[2]

[1] Digital Security Group, Radboud University, Nijmegen
[2] IAIK, Graz University of Technology, Austria
l.grassi@cs.ru.nl,firstname.lastname@iaik.tugraz.at

Abstract. Designing cryptographic permutations and ciphers using a substitution-permutation network (SPN) approach where the non-linear part does not cover the full state has recently gained attention due to favourable implementation characteristics in various scenarios.

For word-oriented partial SPN schemes with a fixed linear layer, our goal is to better understand how the details of the linear layer affect the security of the construction. In this paper we derive conditions which allow either to set up or to prevent attacks based on infinitely long truncated differentials with probability 1. Our analysis is rather broad compared to earlier independent work on this problem, since we consider *(1)* both invariant and non-invariant/iterative trails, and *(2)* trails with and without active S-boxes.

For these cases, we provide rigorous sufficient and necessary conditions for the matrix that defines the linear layer in order to prevent the analyzed attacks. On the practical side, we present a tool which is able to determine whether a given linear layer is vulnerable based on these results. Further, we propose a sufficient condition for the linear layer that – if satisfied – ensures that no infinitely long truncated differential exists. This condition is related to the degree and the irreducibility of the minimal polynomial of the matrix that defines the linear layer.

Besides P-SPN schemes, our observations may also have a crucial impact on the recent Hades design strategy, which mixes rounds with full S-box layers and rounds with partial S-box layers.

Keywords: Partial SPN · Linear Layer · Subspace Trails · Hades Schemes

Contents

1 Introduction 2

1.1 Choosing the Linear Layer in Partial SPN Schemes 2

1.2 Our Contribution and Related Work 3

2 Preliminaries 5

2.1 Partial SPN Schemes 5

2.2 Invariant Subspaces and Subspace Trails 6

2.3 Decomposition Theorem & Frobenius Normal Form 8

3 Infinitely Long Invariant Subspace Trails for P-SPN Schemes (Inactive S-Boxes) 10

3.1 Preliminary Results 10

3.2 Infinitely Long Invariant Subspace Trails via Eigenspaces of M 11

3.3 A Necessary and Sufficient Condition for the Existence of Infinitely Long Invariant Subspace Trails (with Inactive S-boxes) 12

4 Iterative Subspace Trails with Inactive S-Boxes 14

4.1 Linear Layers with Low Multiplicative Order 15

4.2 Linear Layer with Low-Degree Minimal Polynomial 16

5 Practical Tests (Inactive S-Boxes) 18

5.1 Algorithm for Detecting Weak Matrices 18

5.2 Percentage of Weak Linear Layers 19

6 Infinitely Long Subspace Trails for P-SPN Schemes (Active S-Boxes) 20

6.1 Preliminary: Subspace Trails and Truncated Differentials 20

6.2 Infinitely Long Invariant Subspace Trails with Active S-Boxes via the Eigenspaces of M 20

6.3 A Necessary and Sufficient Condition for the Existence of Infinitely Long Invariant Subspace Trails with Active S-boxes 22

6.4 Infinitely Long Iterative Subspace Trails with Active S-Boxes 24

7 Practical Tests (Active S-Boxes) 25

7.1 Related Strategies in the Literature 25

7.2 Algorithms for Detecting “Weak” Matrices 26

7.3 Percentage of “Weak” Linear Layers 27

8 Conclusion and Open Problems 29

8.1 Preventing Infinitely Long Subspace Trails – A Sufficient Condition 29

8.2 Open Problems 31

A Related Work 34

B 2-Round Iterative Subspace Trail – Details 35

C Truncated and Impossible Differentials 37

C.1 Subspace Trails and Truncated Differentials 37

C.2 Truncated Differentials with Probability Smaller than 1 38

C.3 Impossible Differentials 39

D Infinitely Long Iterative Subspace Trails with Active S-Boxes 39

E Results Using our Tool and More Examples of Subspace Trails with Active S-Boxes 40
E.1 Starkad and Poseidon Matrices 40
E.2 Zorro Matrix 41
E.3 Examples of Infinitely Long Subspace Trails (Active S-Boxes) 42

1 Introduction

Modern cryptography developed many techniques that go well beyond solving traditional confidentiality and authenticity problems in two-party communications. Among many others, this includes practical applications of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge (ZK) proofs using symmetric primitives. Designs for these applications are usually led by the idea that linear operations are more efficient than non-linear ones in these scenarios. This fact is also true in the context of masking, a widespread countermeasure against side-channel attacks (SCA) in which all the computations are performed on shared secrets.

Driven by all these application areas, many new symmetric primitives have recently been proposed to reduce the multiplicative complexity in various ways. They include masking-friendly designs like PICARO [42], Zorro [23], LS-designs [30], several FHE-friendly symmetric encryption schemes such as LowMC [4], FLIP [40], Kreyvium [17], and Rasta [22], some MPC-friendly block ciphers such as MiMC [3, 29], GMiMC [2] and HadesMiMC [26] (and its hash variant Poseidon [24]), and some primitives dedicated to proof systems such as Jarvis and Friday [6], *Vision* and *Rescue* [5].

1.1 Choosing the Linear Layer in Partial SPN Schemes

Some of the recalled designs (e.g., LowMC, Zorro, and Poseidon) reach the goal of minimizing the total number of multiplications by making use of rounds with a partial S-box layer. These designs are called partial substitution-permutation network (P-SPN) schemes. They are a variant of SPN schemes, in which a plaintext block is transformed into a ciphertext block by applying several alternating *rounds* of substitution boxes and permutations to provide confusion and diffusion. For an SPN cipher over $\mathbb{F}^t$, the substitution layer usually consists of t parallel (independent) non-linear functions called S-boxes. The permutation layer is in most cases a linear operation defined by the multiplication of the state with a $t \times t$ matrix.

In the case of a partial substitution-permutation network (P-SPN), part of the substitution layer is replaced with an identity mapping, leading to substantial practical advantages in many applications in which the cost of a non-linear operation is significantly higher than the cost of a linear one. This approach has been proposed for the first time by Gérard et al. [23] at CHES 2013. A concrete instantiation of their methodology is Zorro [23], a 128-bit lightweight AES-like cipher which reduces the number of S-boxes per round from 16 to only 4 (to compensate, the number of rounds has been increased to 24). A similar approach has then been considered by Albrecht et al. [4] in the recent design of a family of block ciphers called LowMC proposed at Eurocrypt 2015. LowMC is a family of block ciphers based on an SPN structure which combines an incomplete S-box layer with a strong linear layer in order to guarantee security and to be competitive in applications like MPC, FHE, or ZK.

While Zorro uses the same linear layer in all rounds, LowMC uses different pseudo-random linear layers for each round. Both these two strategies have their advantages and disadvantages. For example, even if the second strategy may provide security against statistical attacks (as discussed in [4]), it has some drawbacks. First, the computation time or memory may become a problem, even when considering the optimizations proposed in [33, 20]. Secondly, the security analysis against other attacks may become harder, since the linear layer is different in each round. Moreover, a poor choice of the linear layers may not provide security against statistical attacks, as shown concretely in [21].[1] Finally, the

[1] In particular, the fact that the designers of LowMC allow to instantiate it using a pseudo-random source that is not cryptographically secure is risky, since using an over-simplified source for pseudo randomness may give a malicious party additional control over the LowMC instantiation, and may allow finding weak instances much faster than exhaustively searching for them.

possibility to have different matrices at every round can be exploited in order to insert a backdoor, as recently shown in [41] in the case of a tweakable version of LowMC.

More generically, a considerable disadvantage of partial SPN schemes is that many strategies proposed in the literature for SPN schemes for providing security are no longer applicable and have to be replaced by more ad-hoc approaches. This includes the well-known *wide trail strategy* [19], which is one of the main approaches used in order to achieve provable security against various statistical attacks, as the differential [14, 15] and linear [39] ones. Instead of choosing larger S-boxes with strong properties, the wide trail strategy aims to design the linear round transformations in such a way that the minimum number of active S-boxes over multiple rounds is increased. However, this strategy can only work in the case in which the S-box layer is full (or almost full), i.e., it is not directly applicable to most partial SPN schemes. In the case of `Zorro`, the heuristic argument proposed by the designers turned out to be insufficient, as Wang et al. [45] (and later on Bar-On et al. [9]) found iterative differential and linear characteristics that were missed by the heuristic and used them to break full `Zorro`. Similarly, the authors of LowMC chose the number of rounds in order to guarantee that no differential or linear characteristic can cover the whole cipher with non-negligible probability. However, they do not provide similarly strong security arguments against other attack vectors including algebraic attacks, and key-recovery attacks on LowMC have thus been found [21].

1.2 Our Contribution and Related Work

Automated characteristic search tool and dedicated key-recovery algorithms for SP networks with partial non-linear layers have been presented in [9]. In there, the authors propose generic techniques for differential and linear cryptanalysis of SP networks with partial non-linear layers. As a main result, this tool can be used in order to understand how many rounds a *given* scheme requires in order to be secure. However, focusing on the matrix that defines the linear layer, it is not clear which properties it must satisfy in order to prevent infinitely long subspace trails.

Focusing on partial SPN schemes with a fixed linear layer (e.g., `Zorro`), our goal is to understand *which properties a linear layer has to fulfill in order to prevent the existence of infinitely long truncated differentials with prob. 1* [35], or equivalently *infinitely long subspace trails* [27, 28] (i.e., the existence of a non-trivial subspace $\mathcal{U} \subseteq \mathbb{F}^t$ of inputs that is mapped into a proper (affine) subspace of the state space over any number of rounds).

Infinitely Long Subspace Trails: Necessary & Sufficient Conditions for P-SPN Schemes. Specifically, we present sufficient and necessary conditions that a matrix must satisfy in order to guarantee security against infinitely long (non-trivial) subspace trails. In more details, we analyze

(1) the case of *inactive S-boxes* in which the input difference of the S-box is equal to zero (see Section 3 - Section 4), and

(2) the case of *active S-boxes* in which the input difference of the S-box can take any possible value (see Section 6).

In both cases, we show that an infinitely long subspace trail exists *if and only if* the invertible fixed matrix that defines the linear layer satisfies some particular properties, and we show how to construct such an infinitely long subspace trail if it exists. Our results are independent of the details of the S-box (with the only exception that the S-box has no non-trivial linear structure), of the round keys, and of the round constants.

In the particular case in which the matrix is diagonalizable, the infinitely long subspace trail (if existent) is always related to the eigenspaces of the matrix. This is not surprising, since the relation between the eigenvalues and eigenvectors of the linear layer matrix and the existence of an infinitely long (invariant) subspace trail is already known in the literature. Such a relation was e.g. pointed out by Abdelraheem et al. [1], and later on generalized by Beyne in [11]. In more detail, Abdelraheem et al. found such a result by analyzing the invariant subspace trails of PRINTcipher (which was presented one year before in [36]), while Beyne found such a result as a generalization and improvement of the non-linear invariant subspace attack on Midori-64 [44]. In particular, in [11] *a connection between the eigenvalues of the correlation matrix that defines the round function and the existence of an invariant subspace trail* is made. More details are given in Appendix A. However, we point out that all these results focus on SPN schemes and on invariant subspaces only. As a consequence, this analysis heavily depends both on the effect of the key (namely, the invariant subspace only holds in the case of weak keys) and in general on the details of the S-box, which is not the case here. The existence of such an invariant subspace can be prevented by carefully choosing the round constants, as shown in [10].

More generally, the infinitely long subspace trails (if existent) are always related to the invariant subspaces of the matrix M that defines the linear layer, namely the subspaces $\mathcal{X}$ that remains invariant when applying the matrix multiplication: $M \cdot \mathcal{X} = \mathcal{X}$. These subspaces can be found via the *primary decomposition theorem*, which allows to split the full space $\mathbb{F}^t$ into a direct sum of invariant and independent subspaces for M. This is possible by computing the Frobenius normal form of the matrix (as recalled in Section 2).

We emphasize that we do not focus on invariant subspace trails only, since a non-trivial infinitely long subspace trail is not necessarily invariant. In particular, such a subspace trail is invariant if it is related to the invariant subspaces of M, and not invariant if it is related to the invariant subspaces of M^l for $l \geq 2$. In this last case, we call the subspace trail iterative. In both cases, examples are provided to present and support the results.

To summarize, both in the case of inactive and active S-boxes, we present rigorous *necessary and sufficient conditions which guarantee that no infinitely long (invariant and iterative) subspace trail exists.* As a final result, we are able to present a *sufficient* (but in general not necessary) condition for the linear layer that – if satisfied – ensures that no infinitely long truncated differential exists. This condition is related to the degree and the irreducibility of the minimal polynomial of the matrix that defines the linear layer.

Dedicated Tool. Together with our theoretical observations, we also provide practical `Sage` implementations based on our results. Given a square matrix, the tool and the underlying algorithms are able to detect the structural vulnerabilities described in this paper (invariant and iterative trails), both in the case of inactive and active S-boxes and for binary and prime fields.

The tool is split into three different algorithms to cover all our results. The vulnerability of a single matrix can be evaluated quickly. In order to get a better understanding of the number of vulnerable matrices for given dimensions and field sizes, we applied our tool to large sets of pseudo-randomly sampled matrices. These tests show that the number of vulnerable matrices is in general small (and slightly larger than 10% only in a few particular cases). Details about the tool and the results are given in Section 5 and Section 7.

Impact on Hades-Like Schemes. Finally, our results have an impact on the Hades strategy as well [26]. The main property of this strategy is to mix rounds external with full S-box layers and middle rounds with partial S-box layers in order to minimize the total number of multiplications. The rounds with full S-box layers are used for the security against differential and linear attacks, while the purpose of the middle rounds is to provide security against algebraic attacks by increasing the degree of the overall scheme.

In [26], the authors define the linear layer as a multiplication of the state with a fixed MDS matrix, and no other properties have to be fulfilled by the linear layer. It follows that in the case of a "weak" MDS matrix (i.e., a matrix that does not satisfy the properties proposed in this work), an attacker can potentially choose an input space of texts for which no S-box is activated in the rounds with partial S-box layers. In such a case, the security of the corresponding design may potentially be lower. For the particular matrices used in [24], vulnerabilities related to the multiplicative order were shown in [12, 34].[2] Our results allow to solve this problem easily.

2 Preliminaries

Notation. We denote subspaces with calligraphic letters (e.g., $\mathcal{S}$). Further, we use the superscript notation together with parentheses to differentiate subspaces with similar properties (e.g., $\mathcal{S}^{(i)}$). By $\mathcal{S}^c$ we denote the complementary subspace of $\mathcal{S}$. We recall that two cosets $\mathcal{S}+a$ and $\mathcal{S}+b$ are equivalent if and only if $a-b \in \mathcal{S}$. Matrices are denoted by non-calligraphic letters. The entry of a vector $x \in \mathbb{F}^t$ is denoted by $x[i]$ for $i \in \{1, \ldots, t\}$, while the entry of a matrix M in the j-th column of the i-th row is denoted by $M_{i,j}$.

We denote by $\{e_1, \ldots, e_t\}$ the unit vectors of $\mathbb{F}^t$ (i.e., e_i has a single 1 in the i-th word). Given an arbitrary subspace $\mathcal{X} \subseteq \mathbb{F}^t$ and a matrix M, let $M \cdot \mathcal{X} := \{M \cdot x \mid x \in \mathcal{X}\}$. We use the symbol $\oplus$ to denote the direct sum of two spaces. Finally, the span $\langle v, w \rangle$ is always defined w.r.t. the space $\mathbb{F}$, that is, $\langle v, w \rangle = \{\alpha \cdot v + \beta \cdot w \mid \alpha, \beta \in \mathbb{F}\}$.

2.1 Partial SPN Schemes

In this paper, we will focus on partial SPN ciphers and permutations over $\left((\mathbb{F}_q)^t, +, \cdot\right)$, where $q \geq 2$ is a prime power.[3] Before going on, we highlight that all our results are independent of the round keys and constants. For this reason, in the following we do not clearly distinguish between ciphers and permutations, and we occasionally just refer to them using the term *schemes*.

Partial SPN (P-SPN) Schemes. We denote the application of r rounds of a P-SPN cipher by $E_k^r : \mathbb{F}^t \to \mathbb{F}^t$, where $k \in \mathbb{F}^t$ is a fixed secret key and $t \in \mathbb{N}$ denotes the number of cells. For every input $x = (x_1, \ldots, x_t) \in \mathbb{F}^t$, the encryption is defined by $E_k^r(x) = (F_r \circ \cdots \circ F_1)\left(x + k^{(0)}\right)$, where $F_i : \mathbb{F}^t \to \mathbb{F}^t$ is defined as $F_i(x) = R(x) + k^{(i)}$ for a round key $k^{(i)}$ and for each $i \in \{1, \ldots, r\}$. In the case of an unkeyed P-SPN permutation, the secret round keys are just replaced by public round constants.

We denote by R the composition of the S-box and the linear layer, i.e., we have $R : \mathbb{F}^t \to \mathbb{F}^t$ with

$$R(x) = (M \circ S)(x) = M(S_1(x_1), \ldots, S_s(x_s), x_{s+1}, \ldots, x_t), \tag{1}$$

where $S_i : \mathbb{F} \to \mathbb{F}$ for $i \in \{1, \ldots, s\}$ is a non-linear permutation.[4] Finally, $M \in \mathbb{F}^{t \times t}$ denotes an invertible non-trivial linear layer defined by the multiplication with a matrix, i.e., $(M(x))_j = \sum_i M_{i,j} \cdot x_i$, where $M_{i,j} \in \mathbb{F}$ for $i \in \{1, \ldots, t\}$ and $j \in \{1, \ldots, t\}$.

Definition 1. A linear layer $M \in \mathbb{F}^{t \times t}$ is *non-trivial* if it ensures full diffusion (in the sense that each word of the output depends on each word of the input and vice versa) after a *finite* number of rounds.

All word-wise (aligned) P-SPN schemes can be written in this way. Morever, in this paper we assume that the s S-boxes are applied to the first s words. Note that given any

[2] The multiplicative order of a matrix M is the smallest (positive integer) exponent $k \geq 1$ such that $M^k = \mu I$, where $\mu \in \mathbb{F}$ and I is the identity matrix.

[3] In the case in which $q = 2$, the field corresponds to $({\mathbb{F}_2}^t, \oplus, \cdot)$, where $\oplus$ corresponds to the `XOR` sum. In order to avoid confusion between the `XOR` sum and the direct sum, we use the symbol $\oplus$ to denote the direct sum only, and we use the symbol $+$ to denote the sum over the field $\mathbb{F}_q$.

[4] Note that this implies that $t - s$ input words are unaffected by the S-box layer, and indeed this is the only difference to classical SPN schemes.

P-SPN scheme, it is always possible to find an equivalent representation s.t. the S-boxes are applied to the first s words.

We further assume that the number of S-boxes s is smaller than $\lceil t/2 \rceil$. This implies that the choice of the linear layer is crucial for guaranteeing that at least one S-box is active after a *finite* number of rounds.[5]

Hades-Like Schemes. The recently proposed HADES strategy [26] combines both SPN and partial SPN schemes. In particular, the initial R_f and the final R_f rounds contain full S-box layers, for a total of $R_F = 2R_f$ rounds with full S-box layers. However, in the middle of the construction, R_P rounds with partial S-box layers are used. Roughly speaking, R_F rounds provide security against statistical attacks, while R_P rounds increase the overall degree of the function in an attempt to prevent algebraic attacks.

Assumption on the S-Box. In this paper, we only work with S-boxes that do not have any linear structures. That is, for an S-box S over $\mathbb{F}$, we assume that it is not possible to find $\mathcal{U}, \mathcal{V} \subset \mathbb{F}$ s.t. *for each* $u \in \mathbb{F}$ there exists $v \in \mathbb{F}$ s.t. $S(\mathcal{U} + u) = \mathcal{V} + v$. If the S-box has no non-trivial linear structures, there are only two essential subspace trails ($\{0\} \to \{0\}$ and $\mathbb{F} \to \mathbb{F}$) when working at word level, as was shown in [38]. Under this assumption, one can work independently of the details of the S-box. For example, both the AES S-box and the cube one ($x \mapsto x^3$) satisfy this assumption.

2.2 Invariant Subspaces and Subspace Trails

2.2.1 Invariant Subspace Attack

The invariant subspace attack, introduced in [36] and reconsidered e.g. in [37], is based on the possibility to set up an invariant subspace trail, defined as follows.

Definition 2 (*Invariant Subspace Trails*)**.** Let K_{weak} be a set of keys and $k \in K_{\text{weak}}$, with $k = \left(k^{(0)}, \ldots, k^{(r)}\right)$, where $k^{(j)}$ is the j-th round key. For $k \in K_{\text{weak}}$, the subspace $\mathcal{I}$ generates an invariant subspace trail of length r for the round function $R_k(\cdot) = R(\cdot) + k$ if for each $i \in \{1, \ldots, r\}$ there exists a non-empty set $A_i \subseteq \mathcal{I}^c$ for which

$$\forall a_i \in A_i : \exists a_{i+1} \in A_{i+1} \text{ s.t. } R_{k^{(i)}}(\mathcal{I} + a_i) = R(\mathcal{I} + a_i) + k^{(i)} = \mathcal{I} + a_{i+1}.$$

All keys in the set K_{weak} are weak keys.

Let us remark the main difference for invariant subspace attacks when working with partial SPN ciphers instead of SPN ones. In this last case and to the best of our knowledge, the sets A_i are (almost always) non-trivial subsets of $\mathbb{F}^t$. However, due to the fact that the non-linear layer is not full, this restriction is not mandatory in the case of partial SPN schemes. For this reason, in the following we work independently of the details of the S-box, and we assume that $A_i = \mathbb{F}^t$ for each i and that the set K_{weak} is equal to the set of all possible keys.

2.2.2 Subspace Trail Attack

Subspace trails were first defined in [27], and they are strictly related to truncated differential attacks, as shown in [38].

[5] In the case in which a fixed linear layer matrix M is used, let $2 \leq \beta \leq t + 1$ be its branch number. If $2t - 2s < \beta$, then at least $\beta + 2s - 2t \geq 1$ S-boxes are active in every two consecutive rounds. Note that this can never happen if $s < \lceil t/2 \rceil$ (equivalently, $s \leq \lceil t/2 \rceil - 1$), since $2t - 2s \geq t + 2 > \beta$.

Definition 3 (*Subspace Trails*)**.** Let $(\mathcal{U}_1, \ldots, \mathcal{U}_{r+1})$ denote a set of $r+1$ subspaces with $\dim(\mathcal{U}_i) \leq \dim(\mathcal{U}_{i+1})$. If for each $i \in \{1, \ldots, r\}$ and for each a_i there exists $a_{i+1} \in \mathcal{U}_{i+1}^c$ such that

$$R^{(i)}(\mathcal{U}_i + a_i) \subseteq \mathcal{U}_{i+1} + a_{i+1},$$

then $(\mathcal{U}_1, \ldots, \mathcal{U}_{r+1})$ is a *subspace trail* of length r for the function $F(\cdot) = R^{(r)}_{k^{(r)}} \circ \cdots \circ R^{(1)}_{k^{(1)}}(\cdot)$. If the relations hold with equality, the trail is called a *constant-dimensional subspace trail.*

Iterative (Constant-Dimensional) Subspace Trails. We now introduce the concept of infinitely long iterative (constant-dimensional) subspace trails.

Definition 4 (*Iterative Subspace Trails*)**.** Let $\{\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_l\}$ be a constant-dimensional subspace trail for l rounds. We call this subspace trail an *infinitely long iterative (constant-dimensional) subspace trail of period l* for the considered scheme if it repeats itself an infinite number of times, i.e., if

$$\{\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_l, \mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_l, \ldots, \mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_l, \ldots\}$$

is an infinitely long subspace trail.

Clearly, an invariant subspace trail is also an iterative subspace trail for the case of P-SPN schemes (under the previous assumptions), while not every iterative subspace trail is also an invariant subspace trail. At the same time, the following result holds.

Proposition 1. *Working over $\mathbb{F}^t$, let $\{\mathcal{V}_1, \ldots, \mathcal{V}_l\}$ be an infinitely long iterative subspace trail of period l. If $\dim(\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle) < t$, then $\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle$ generates an infinitely long invariant subspace trail.*

Proof. The subspace $\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle$ is invariant since each coset of $\mathcal{V}_i$ is mapped into a coset of $\mathcal{V}_{i+1}$ (where the subindex is taken modulo $l+1$). □

While, to the best of our knowledge, no example of infinitely long iterative constant-dimensional subspace trails for SPN ciphers is given in the literature, a poor choice of the linear layer allows to find them for the case of P-SPN schemes.

Truncated Differential Trails. Before going on, we briefly mention the link between truncated differential trails and subspace trails. Differential attacks [14] exploit the fact that pairs of plaintexts with certain differences yield other differences in the corresponding ciphertexts with a probability distribution that is different from that one would expect from a random permutation. A variant of this attack/distinguisher is the truncated differential one [35], in which the attacker can predict only part of the difference between pairs of texts. Using the subspace terminology, given pairs of plaintexts that belong to the same coset of a subspace $\mathcal{X}$, one considers the probability that the corresponding ciphertexts belong to the same coset of a subspace $\mathcal{Y}$ to set up an attack (see e.g. [16] for details). In particular, note that two texts are in the same coset of a given subspace if and only if their difference belongs to such a subspace:

$$x, y \in \mathcal{V} + v \quad \text{if and only if} \quad x - y \in \mathcal{V}.$$

The relation between truncated differential trails and subspace trails has been studied in details in [38, 16]. Finally, impossible differential and truncated impossible differential attacks based on differentials that hold with probability 0 have been studied in [13].

2.3 Decomposition Theorem & Frobenius Normal Form

Finally, we recall several notions from linear algebra useful for presenting our results, starting with the concept of eigenvalues/eigenspaces.

Definition 5. Given $M \in \mathbb{F}^{t\times t}$, the subspace $\mathcal{P} = \langle \rho_1, \ldots, \rho_d\rangle \in \mathbb{F}^t$ is the (right) eigenspace of M for the eigenvalue λ if the condition $M\cdot\rho_i = \lambda\cdot\rho_i$ is satisfied $\forall i \in \{1,\ldots,d\}$.

Definition 6. M is a diagonalizable matrix if and only if there exists an (invertible) matrix $P \in \mathbb{F}^{t\times t}$ s.t. $P^{-1}\cdot M\cdot P = D = \text{diag}(\lambda_1,\ldots,\lambda_t)$ is a diagonal matrix.

Definition 7. A field $\mathbb{F}$ is *algebraically closed* if every non-constant polynomial in $\mathbb{F}[x]$ has a root in $\mathbb{F}$.

As is well-known, not all matrices are diagonalizable. At the same time, when working over a field $\mathbb{F}$ that is *algebraically closed*, there always exists an invertible matrix $P \in \mathbb{F}^{t\times t}$ such that $J := P^{-1}\cdot M\cdot P$ is in the Jordan form. The Jordan form of a square matrix is equal to

$$J = \begin{bmatrix} J_1 & 0 & \ldots & 0 & 0 \\ 0 & J_2 & \ldots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & J_{l-1} & 0 \\ 0 & 0 & \ldots & 0 & J_l \end{bmatrix}, \qquad \text{where } J_i := \begin{bmatrix} j_1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & j_2 & 1 & \ldots & 0 & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & 0 & \ldots & j_{t_i-2} & 1 & 0 \\ 0 & 0 & \ldots & 0 & j_{t_i-1} & 1 \\ 0 & 0 & \ldots & 0 & 0 & j_{t_i} \end{bmatrix} \tag{2}$$

are square matrices in $\mathbb{F}^{t_i\times t_i}$ s.t. $\sum_{i=1}^{l} t_i = t$ (and $t_i \geq 1$) and where $1 \leq l \leq t$. The Jordan form of a given matrix can be exploited to easily compute the characteristic and the minimal polynomial of this matrix.

Definition 8. Let M be an invertible matrix over $\mathbb{F}^t$. The characteristic polynomial $\psi(x) \in \mathbb{F}[x]$ is defined as $\psi(x) = \det(M - x\cdot I)$. The minimal polynomial $\phi(x) \in \mathbb{F}[x]$ is the monic polynomial of minimal degree s.t.

1. $\phi(M)\cdot v = 0^t$ for each $v \in \mathbb{F}^t$, and
2. if $p(x)$ is annihilating (in the sense that $p(M)\cdot v = 0^t$ for each $v \in \mathbb{F}^t$), then $\phi(x)$ divides $p(x)$.

By definition, $\det(M) = \psi(0)$. Moreover,

- the minimal polynomial divides the characteristic polynomial (which implies that $\deg(\phi), \deg(\psi) \leq t$), and
- an eigenvalue of the matrix is a root of both the minimal and of the characteristic polynomial, and vice-versa (namely, each root is an eigenvalue).

Proposition 2 ([32, Prop. 1 & Prop. 2])**.** *Let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix with minimal polynomial $\phi(x)$. There exists (at least) one vector $v \in \mathbb{F}^t$ s.t.*

$$v, M\cdot v, M^2\cdot v, \ldots, M^{\deg(\phi)-1}\cdot v$$

are linearly independent.

Among other things , the Jordan form matrix can be exploited to split the full space $\mathbb{F}^t$ in subspaces that are independent and invariant through the matrix M. However, since we work over $\mathbb{F}_q^t$ for finite q and since *no finite field can be algebraically closed*[6], it is possible

[6] If $a_1, a_2, \ldots, a_N$ are all the elements of a finite field $\mathbb{F}$, then the polynomial $(x - a_1)\cdot(x - a_2)\cdot\cdots\cdot(x - a_N) + 1$ has no root in $\mathbb{F}$.

that the Jordan normal form does not exist. Here we recall a generalization of the Jordan normal form, known as the Frobenius normal form, that can be computed even if the field is not algebraically closed.

Definition 9. Let $M \in \mathbb{F}^{t\times t}$. The Frobenius normal form of M is the matrix $F \in \mathbb{F}^{t\times t}$ for which there exists an invertible matrix $Q \in \mathbb{F}^{t\times t}$ s.t.

$$F = Q \times M \times Q^{-1} = \text{diag}(C_1, C_2, \dots, C_l) = \begin{bmatrix} C_0 & 0 & \dots & 0 & 0 \\ 0 & C_1 & \dots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & C_{l-1} & 0 \\ 0 & 0 & \dots & 0 & C_l \end{bmatrix}$$

for $1 \le l \le t$, where

- $C_i \in \mathbb{F}^{t_i \times t_i}$ is the (invertible) companion matrix

$$C_i = \begin{bmatrix} 0 & 0 & \dots & 0 & -c_{0,i} \\ 1 & 0 & \dots & 0 & -c_{1,i} \\ 0 & 1 & \dots & 0 & -c_{2,i} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & -c_{t_i-1,i} \end{bmatrix}$$

  associated to the monic polynomial $p_i(x) = c_{0,i} + c_{1,i} \cdot x + c_{2,i} \cdot x^2 + \dots + c_{t_i-1,i} \cdot x^{t_i-1} + x^{t_i}$,

- for each $1 \le i \le l-1$ the polynomial p_i divides the polynomial p_{i+1}, and

- p_l is the minimal polynomial $\phi(x)$ of M and $\psi(x) = \prod_{i=1}^{l} p_i(x)$ is the characterestic polynomial of M.

In particular, note that given a companion matrix C_i over $\mathbb{F}^{t_i}$, then $\mathbb{F}^{t_i} = \langle e_1 \rangle_{C_i}$, since $p_i(e_1) = e_2, p_i(e_2) = e_3, \dots, p_i(e_{t_i-1}) = e_{t_i}$ and $p_i(e_{t_i}) = -c_{0,i} \cdot e_1 - c_{1,i} \cdot e_2 + \dots - c_{t_i-1,i} \cdot e^{t_i}$.

As already mentioned, such normal form can be exploited in order to decompose the full space $\mathbb{F}^t$ in subspaces that are invariant through M, as recalled in the following theorem.

Definition 10. Let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix, and let $\mathcal{V} \subseteq \mathbb{F}^t$ be a subspace. $\mathcal{V}$ is said to be *M-invariant* if and only if $M \cdot \mathcal{V} = \mathcal{V}$. Moreover, if $\mathcal{V}$ is an M-invariant subspace of $\mathbb{F}^t$, then

- $\mathcal{V}$ is said to be *directly indecomposable* if there are *no* non-trivial subspaces $\mathcal{V}_1, \mathcal{V}_2 \subseteq \mathcal{V}$ s.t. $\mathcal{V} = \mathcal{V}_1 \oplus \mathcal{V}_2$, and
- $\mathcal{V}$ is said to be *cyclic* if $\exists v \in \mathcal{V}$ s.t. $\mathcal{V} = \langle v, M \cdot v, M^2 \cdot v, \dots, M^l \cdot v, \dots \rangle \equiv \langle v \rangle_M$.

Theorem 1 (Primary Decomposition Theorem [31, Sect. 6.4] - [32, Theorem 3])**.** *Let M be an invertible matrix in $\mathbb{F}^{t\times t}$. Let $\phi(x) \in \mathbb{F}[x]$ be its minimal polynomial s.t.*

$$\phi(x) = [p_1(x)]^{\alpha_1} \cdot [p_2(x)]^{\alpha_2} \cdot \dots \cdot [p_m(x)]^{\alpha_m},$$

where $\alpha_i \ge 1$ and p_i, p_j are monic, irreducible, and relatively prime. The subspace $\mathbb{F}^t$ can be rewritten as a direct sum[7] *decomposition*

$$\mathbb{F}^t = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \dots \oplus \mathcal{A}_m, \tag{3}$$

[7] Recall that $\mathcal{V} = \mathcal{V}_1 \oplus \mathcal{V}_2$ if and only if $\forall v \in \mathcal{V}$ there exist $v_i \in \mathcal{V}_i$ s.t. $v = v_1 \oplus v_2$.

where for each $j \in \{1, \dots, m\}$

$$\mathcal{A}_j := \ker([p_j(A)]^{\alpha_j}) := \{x \in \mathbb{F}^t \mid [p_j(A)]^{\alpha_j} \cdot x = \underbrace{0 \,||\, 0 \,||\, \cdots \,||\, 0}_{\equiv 0^t}\}$$

(where $\ker(X)$ is the kernel of the matrix $X \in \mathbb{F}^{t\times t}$) such that

(1) $\mathcal{A}_i$ are linearly independent (in the sense that $\mathcal{A}_i \cap \mathcal{A}_j = \{0\}$ for $i \neq j$),

(2) $\mathcal{A}_i$ are M-invariant for each i, and

(3) the minimal polynomial of a linear operator M_i induced on $\mathcal{A}_i$ by M is $p_i(x)^{\alpha_i}$.

Note that the previous decomposition does not imply that there are no non-trivial subspaces of $\mathcal{A}_i$ that are M-invariant. For example, consider a 3×3 matrix $M = \text{diag}(1, 1, 2)$. In such a case the minimal polynomial is $\phi(x) = (x - 1) \cdot (x - 2)$, and $\mathbb{F}^3 = \mathcal{A}_1 \oplus \mathcal{A}_2$, where $\mathcal{A}_1 = \langle e_1, e_2\rangle$ and $\mathcal{A}_2 = \langle e_3\rangle$. At the same time, while $\mathcal{A}_2$ is “irreducible”, it is easy to find subspaces of $\mathcal{A}_1$ that are invariant through M, namely all subspaces of the form $\mathcal{A}'_1 = \langle \alpha \cdot e_1 + \beta \cdot e_2\rangle$ for $\alpha, \beta \in \mathbb{F}$.

3 Infinitely Long Invariant Subspace Trails for P-SPN Schemes (Inactive S-Boxes)

Focusing on P-SPN schemes which use the same linear layer in each round (e.g., `Zorro` [23]), here we study the properties that the matrix that defines the linear layer must satisfy in order to prevent infinitely long invariant subspace trails (with no active S-boxes).

3.1 Preliminary Results

Due to the fact that the non-linear layer is only partial in P-SPN schemes, parts of the state go through the S-box layer unchanged. In particular, if the non-linear layer consists of $s \geq 1$ S-boxes (applied to the first s words) and $t - s \geq 1$ identity functions, it is always possible to find an initial subspace such that no S-box is active (at least) in the first $\left\lfloor \frac{t-s}{s} \right\rfloor$ rounds. By choosing texts in the same coset of $\mathcal{S} = \langle v_1, \dots, v_{\dim(\mathcal{S})}\rangle$ such that

$$\forall i \in \left\{1, \dots, \left\lfloor \frac{t-s}{s} \right\rfloor\right\} : \qquad (M^{i-1} \cdot v_j)[1, 2, \dots, s] = 0 \,||\, 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s$$

for each $j \in \{1, \dots, \dim(\mathcal{S})\}$ and where $M^0 = I$ be the identity matrix, no S-box is active in the first $\left\lfloor \frac{t-s}{s} \right\rfloor$ rounds. We formalize this result in the following definition.

Definition 11. Consider the case of a P-SPN scheme over $\mathbb{F}^t$ with $1 \leq s < t$ S-boxes applied to the first s words defined as in Eq. (1). Let $\mathcal{S}^{(i)}$ be defined as

$$\mathcal{S}^{(i)} = \left\{v \in \mathbb{F}^t \;\middle|\; (M^j \cdot v)[1, \dots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s, j < i\right\}, \tag{4}$$

where $\mathcal{S}^{(0)} = \mathbb{F}^t$, and where $\dim\left(\mathcal{S}^{(i)}\right) \geq t - i \cdot s$. Then $\mathcal{S}^{(i)}$ generates a subspace trail for the first i (consecutive) rounds with no active S-boxes. Further, note that $\mathcal{S}^{(i+1)} \subseteq \mathcal{S}^{(i)}$.

Lemma 1. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes applied to the first s words defined as in Eq. (1), let $\mathcal{S}^{(i)}$ be defined as in Definition 11. Then, for each $i \geq 1$,*

$$\mathcal{S}^{(i+1)} = \left\{v \in \mathcal{S}^{(i)} \;\middle|\; (M \cdot v)[1, \dots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s\right\} \subseteq \mathcal{S}^{(i)}.$$

Proof. Given $\mathcal{S}^{(1)} = \langle e_{s+1}, \ldots, e_t \rangle$, note that $(M \cdot x)[1, \ldots, s] = 0 \mid\mid \cdots \mid\mid 0 \in \mathbb{F}^s$ if and only if $M \cdot x \in \langle e_{s+1}, e_{s+2}, \ldots, e_t \rangle = \mathcal{S}^{(1)}$, or equivalently $x \in \mathcal{S}^{(1)} \cap (M^{-1} \cdot \mathcal{S}^{(1)})$. Working recursively, it follows that $\mathcal{S}^{(i+1)} = \mathcal{S}^{(i)} \cap (M^{-1} \cdot \mathcal{S}^{(i)})$, which is equivalent to

$$\mathcal{S}^{(i+1)} = \mathcal{S}^{(1)} \cap (M^{(-1)} \cdot \mathcal{S}^{(1)}) \cap (M^{(-2)} \cdot \mathcal{S}^{(1)}) \cap \cdots \cap (M^{(-i)} \cdot \mathcal{S}^{(1)}). \qquad \square$$

In the case in which $\dim \left(\mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor \right)} \right) \geq s$, the previous definition can naturally be extended to more rounds, as stated in the following.

Proposition 3. *Consider the case of a P-SPN scheme over $\mathbb{F}^t$ with $1 \leq s < t$ S-boxes applied to the first s words as in Eq. (1), and let $\mathcal{S}^{(i)}$ be defined as before. Let $\mathfrak{R} \geq \left\lfloor \frac{t-s}{s} \right\rfloor$ s.t. $\dim \left(\mathcal{S}^{(\mathfrak{R})} \right) \geq 1$ and $\dim \left(\mathcal{S}^{(\mathfrak{R}+1)} \right) = 0$. For each $r \leq \mathfrak{R}$, the collection*

$$\left\{ \mathcal{S}^{(r)}, M \cdot \mathcal{S}^{(r)}, M^2 \cdot \mathcal{S}^{(r)}, \ldots, M^{r-1} \cdot \mathcal{S}^{(r)} \right\}$$

is a subspace trail for the first r rounds (with no active S-boxes).

This well-known result (see e.g. [4, Sect. 5.1] or [23, Sect. 4.1]) does not require any assumption about the matrix M that defines the linear layer. In the following, we will explore in which cases it is possible to set up an infinitely long subspace trail. In order to do this, we start by reconsidering some results already published in the literature.

3.2 Infinitely Long Invariant Subspace Trails via Eigenspaces of M

As it is well-known in the literature (see e.g. the results presented in [1, 11] and recalled in Appendix A), one possible strategy to set up invariant subspace trails is to analyze the eigenspaces of the matrix M that defines the linear layer.

Proposition 4. *Given a P-SPN scheme with s S-boxes per round defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix. Let $\lambda_1, \ldots, \lambda_\tau$ be its eigenvalues and let $\mathcal{P}_1, \ldots, \mathcal{P}_\tau$ be the corresponding eigenspaces. Let*

$$\mathcal{I} = \left\langle \mathcal{P}_1 \cap \left\langle e_{s+1}, \ldots, e_t \right\rangle, \ldots, \mathcal{P}_\tau \cap \left\langle e_{s+1}, \ldots, e_t \right\rangle \right\rangle.$$

If $1 \leq \dim(\mathcal{I}) < t$, then $\mathcal{I}$ generates a (non-trivial) infinitely long invariant subspace trail (with no active S-boxes).

Equivalently, let $\mathcal{I}$ be defined as $\mathcal{I} = \left\langle \mathcal{P}'_1, \ldots, \mathcal{P}'_\tau \right\rangle$, where $\mathcal{P}'_i \subseteq \mathcal{P}_i$ is a subspace of $\mathcal{P}_i$ for $i \in \{1, \ldots, \tau\}$. If $\mathcal{I} \cap \left\langle e_{s+1}, \ldots, e_t \right\rangle = \mathcal{I}$, it generates an infinitely long invariant subspace trail. This equivalent definition will be used in the following, and we emphasize that this result provides only a *sufficient* condition.

Proof. To prove the previous result, we have to show that for each $a \in \mathbb{F}^t$ there exists b s.t. $M \circ S(\mathcal{I} + a) = \mathcal{I} + b$. Hence, we omit the key and constant additions since they only change the coset. First of all, note that no S-box is active since $\mathcal{I} \subseteq \left\langle e_{s+1}, \ldots, e_t \right\rangle$, and thus only the coset changes through the S-box layer. Secondly, since $\mathcal{P}_i$ is an eigenspace of the linear layer M for each $i \in \{1, \ldots, \tau\}$, it follows that $\mathcal{P}_i \cap \left\langle e_{s+1}, \ldots, e_t \right\rangle$ remains invariant through it. The result follows immediately. $\square$

It is crucial to work independently on the eigenspaces of M. Indeed, consider the case in which $\mathcal{P}_1 = \langle v \rangle$, $\mathcal{P}_2 = \langle w \rangle$, and $\left\langle \mathcal{P}_1, \mathcal{P}_2 \right\rangle \cap \langle e_{s+1}, \ldots, e_t \rangle = \left\langle v + \alpha w \right\rangle$. Given $x \in \left\langle \mathcal{P}_1, \mathcal{P}_2 \right\rangle \cap \langle e_{s+1}, \ldots, e_t \rangle$, $M \cdot x$ does not belong to such a subspace since $M \cdot (v + \alpha w) = \lambda_v \cdot \left(v + \alpha \cdot \frac{\lambda_w}{\lambda_v} \cdot w \right)$, where $\lambda_w \neq \lambda_v$.

Examples. Consider a P-SPN scheme over $\mathbb{F}^4$ with $s = 1$. If the 4×4 matrix M is

$$M = \begin{pmatrix} 4 & 4 & 5 & 1 \\ 1 & 3 & 5 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 4 & 4 \end{pmatrix},$$

then $\mathcal{I} = \langle (0, 1, -1, 1)^T \rangle$ generates an infinitely long invariant subspace trail. Indeed, note that $(0, 1, -1, 1)^T$ is an eigenvector of M and $\langle (0, 1, -1, 1)^T \rangle \cap \langle e_2, e_3, e_4 \rangle = \langle (0, 1, -1, 1)^T \rangle$. Hence, this is a concrete example of the result given in the previous theorem, and it is independent of the branch number of M. Indeed, such a 4×4 matrix can even be an MDS matrix for sufficiently large p.[8]

As a second example, if $M = \text{circ}(2, 3, 1, 1)$, the only eigenspaces are given by $\langle (1, 1, 1, 1)^T \rangle$ and $\langle (1, -1, 1, -1)^T \rangle$ (with eigenvalues equal to 7 and -1, respectively). Neither of them satisfies the results of the theorem just given. Hence, there exist matrices which provide security against invariant subspace trails with inactive S-boxes, even though they have eigenspaces. This is also true for the most generic case of iterative subspace trails with active S-boxes.

3.3 A Necessary and Sufficient Condition for the Existence of Infinitely Long Invariant Subspace Trails (with Inactive S-boxes)

As shown in Section 2.3, a subspace does not have to be an eigenspace of the matrix in order to be invariant. In particular, as we have seen in Theorem 1, the space $\mathbb{F}^t$ can be rewritten as a direct sum decomposition

$$\mathbb{F}^t = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \cdots \oplus \mathcal{A}_m, \tag{5}$$

where – among other properties – all subspaces $\mathcal{A}_i$ are M-invariant. Hence, the previous result can be generalized by replacing the eigenspaces of the matrix with the subspaces $\mathcal{A}_i$, which lead us to a necessary and sufficient condition. In order to do that, we first present the following result.

Theorem 2. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix. A subspace $\mathcal{I}$, where $1 \leq \dim(\mathcal{I}) < t$, generates an infinitely long invariant subspace trail (with no active S-boxes) if and only if $\mathcal{I} \subseteq \mathcal{S}^{(1)}$ and $\mathcal{I} = (M \cdot \mathcal{I})$. In particular, $\mathcal{I} \subseteq \mathcal{S}^{(1)} \cap \left(M \cdot \mathcal{S}^{(1)}\right)$.*

Proof. We work with differences. That is, instead of proving that each coset of $\mathcal{I}$ is mapped into a coset of $\mathcal{I}$ after one round, we are going to prove that given two elements in the same coset of $\mathcal{I}$ (namely, an input difference in $\mathcal{I}$), then the corresponding output elements are still in the same coset of $\mathcal{I}$ (namely, the output difference lies in $\mathcal{I}$), i.e., $\text{Prob}(R(x) - R(y) \in \mathcal{I} \mid x - y \in \mathcal{I}) = 1$. We use this approach in the entire paper.

The fact that a subspace $\mathcal{I} \subseteq \mathcal{S}^{(1)}$ s.t. $\mathcal{I} = M \cdot \mathcal{I}$ generates an infinitely long invariant subspace trail (with no active S-boxes) is trivial. Indeed, the definition of $\mathcal{S}^{(1)}$ (which implies that no S-box is active) together with the fact that $\mathcal{I} = M \cdot \mathcal{I}$ implies the result. Vice-versa, here we show that given an infinitely long invariant subspace trail $\mathcal{I}$ (with no active S-boxes), it must satisfy $\mathcal{I} \subseteq \mathcal{S}^{(1)}$ and $\mathcal{I} = M \cdot \mathcal{I}$. To do this, observe that all pairs of texts which do not activate any S-box in the next round are in the same coset of $\mathcal{S}^{(1)}$ (by its definition). Focusing on the linear layer, note that a subspace $\mathcal{X}$ is invariant if and only if $M \cdot \mathcal{X} = \mathcal{X}$. The result follows immediately.

Finally, we prove that $\mathcal{I} \subseteq \mathcal{S}^{(1)} \cap \left(M \cdot \mathcal{S}^{(1)}\right)$. Since $\mathcal{I} \subseteq \mathcal{S}^{(1)}$, it follows that $(M \cdot \mathcal{I}) \subseteq (M \cdot \mathcal{S}^{(1)})$, where M is a linear operation. As a result, $\mathcal{I} \subseteq (M \cdot \mathcal{S}^{(1)})$ since $\mathcal{I} = M \cdot \mathcal{I}$. □

[8] It is an MDS matrix for e.g. $p = 4\,206\,590\,407$, which results in a block size of approximately 128 bits.

Theorem 3. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix. Let $\phi(x)$ be the minimal polynomial of M s.t. $\phi(x) = [p_1(x)]^{\alpha_1} \cdot [p_2(x)]^{\alpha_2} \cdot \cdots \cdot [p_m(x)]^{\alpha_m}$, where $\alpha_i \geq 1$ and p_i, p_j are monic, irreducible, and relatively prime. Let $\{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be the primary decomposition of $\mathbb{F}^t$ w.r.t. the matrix M, as defined in Theorem 1, i.e., a collection of independent subspaces in $\mathbb{F}^t$ which are M-invariant and s.t. $\mathbb{F}^t = \bigoplus_i \mathcal{A}_i$. Let $\{\mathcal{X}_1, \ldots, \mathcal{X}_m\}$ be a collection of subspaces defined as*

$$\mathcal{X}_i := \mathcal{A}_i \cap \langle e_{s+1}, \ldots, e_t\rangle. \tag{6}$$

A subspace $\mathcal{I}$, where $1 \leq \dim(\mathcal{I}) < t$, generates an infinitely long invariant subspace trail (with no active S-boxes) if and only if

$$\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\rangle,$$

where $\mathcal{P}_i \subseteq \mathcal{X}_i$ is an M-invariant subspace. In particular, $\mathcal{P}_i \subseteq \mathcal{X}_i \cap (M \cdot \mathcal{X}_i)$.

In the following, note that the condition $\mathcal{A}_i \cap \langle e_{s+1}, \ldots, e_t\rangle$ can be replaced by the condition $\mathcal{A}_i \cap \mathcal{S}^{(1)}$.

Proof. Proving that $\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\rangle$ generates an infinitely long invariant subspace trail (with no active S-boxes) is trivial. Indeed, by definition of $\mathcal{P}_i$, no S-box is active (since $\mathcal{P}_i \subseteq \mathcal{X}_i \subseteq \langle e_{s+1}, \ldots, e_t\rangle$ for $i \in \{1, \ldots, m\}$). The fact that $\mathcal{I}$ is M-invariant follows from the fact that all $\mathcal{P}_i$ are M-invariant subspaces of $\mathcal{X}_i$ (by assumption). Hence, every input difference in $\mathcal{I}$ is mapped into an output difference in $\mathcal{I}$.

Vice-versa, assume that $\mathcal{I}$ generates an infinitely long invariant subspace trail with inactive S-boxes. Let

$$\mathcal{P}_i := \mathcal{A}_i \cap \mathcal{I}.$$

Obviously, all $\mathcal{P}_i$ are subspaces. First of all, note that all $\mathcal{P}_i$ are subspaces of $\langle e_{s+1}, \ldots, e_t\rangle$, since no S-box is active by definition of $\mathcal{I}$. Indeed, if there exists a non-trivial $\mathcal{P}_i$ s.t. $\mathcal{P}_i \cap \langle e_1, \ldots, e_s\rangle \neq \{0\}$, then eventually at least one S-box would be active (since $\mathcal{I}$ generates an infinitely long subspace trail), which contradicts the assumption that no S-box is active. Moreover, note that $\mathcal{P}_i$ is M-invariant. Indeed, if $x \in \mathcal{P}_i$, then $M \cdot x$ belongs to $\mathcal{A}_i$ for $j \geq 0$ (since $\mathcal{A}_i$ is M-invariant) and to $\mathcal{I}$ for $j \geq 1$ (since it generates an infinitely long subspace trail), which implies that $M \cdot x \in \mathcal{P}_i$. Finally, $\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\rangle$ since $\mathcal{A}_i \cap \mathcal{A}_j = \{0\}$ for $i \neq j$, and since $\mathbb{F}^t = \bigoplus_i \mathcal{A}_i$.

As a last thing, $\mathcal{P}_i \subseteq \mathcal{X}_i \cap (M \cdot \mathcal{X}_i)$ follows from the fact that $\mathcal{P}_i \subseteq \mathcal{X}_i$ and $\mathcal{P}_i = M \cdot \mathcal{P}_i$, as in the proof of Theorem 2. □

Proposition 5. *Under the assumptions of the previous theorem, let $\mathcal{X}_i^{(0)} := \mathcal{A}_i \cap \langle e_{s+1}, \ldots, e_t\rangle$. For $j \geq 1$, we define*

$$\mathcal{X}_i^{(j)} = \mathcal{X}_i^{(j-1)} \cap M \cdot \mathcal{X}_i^{(j-1)}.$$

Let $l_i \geq 0$ be the smallest (finite) integer s.t. $\mathcal{X}_i^{(l_i)} = \mathcal{X}_i^{(l_i+1)}$. The biggest M-invariant subspace $\mathcal{P}_i$ of $\mathcal{X}_i$ that satisfies the previous theorem is equal to $\mathcal{X}_i^{(l_i)}$.

Proof. All $\mathcal{X}_i^{(j)}$ are subspaces of $\mathcal{X}_i^{(0)} \subseteq \mathcal{A}_i$, where $\mathcal{A}_i$ is invariant under M by construction. Hence, either $\dim(\mathcal{X}_i^{(j)}) < \dim(\mathcal{X}_i^{(j-1)})$ or $\dim(\mathcal{X}_i^{(j)}) = \dim(\mathcal{X}_i^{(j-1)})$. If $\dim(\mathcal{X}_i^{(j)}) = \dim(\mathcal{X}_i^{(j-1)})$, then $\mathcal{X}_i^{(j)} = \mathcal{X}_i^{(j-1)}$. Indeed, note that $\dim(\mathcal{X}_i^{(j-1)} \cap M \cdot \mathcal{X}_i^{(j-1)}) = \dim(\mathcal{X}_i^{(j-1)})$ if and only if $\mathcal{X}_i^{(j-1)} = M \cdot \mathcal{X}_i^{(j-1)}$, which implies that $\mathcal{X}_i^{(j)} = \mathcal{X}_i^{(j-1)}$. By construction, this is the biggest M-invariant subspace of $\mathcal{A}_i \cap \langle e_{s+1}, \ldots, e_t\rangle$.

Finally, note that the index l_i s.t. $\mathcal{X}_i^{(j)} = \mathcal{X}_i^{(j+1)}$ for each $j \geq l_i$ is always finite. Indeed, in the case in which $\dim(\mathcal{X}_i^{(j)}) < \dim(\mathcal{X}_i^{(j-1)})$ for each $j < l_i$, we have that $\mathcal{X}_i^{(j)} = \{0\}$ for each $j \geq l_i$. Otherwise there exists l_i s.t. $\mathcal{X}_i^{(j)} = \mathcal{X}_i^{(j+1)} \neq \{0\}$ for each $j \geq l_i$. In both cases, l_i is at most equal to the dimension of $\mathcal{X}_i^{(0)}$, since at each step the dimension of $\mathcal{X}_i^{(j)}$ either remains constant or decreases by 1. □

Corollary 1. *The infinitely long invariant subspace trail with inactive S-boxes presented in Proposition 4 satisfies Theorem 3. The two results are equivalent if the matrix is diagonalizable.*

Proof. The invariant subspace considered in Proposition 4 is equal to the one considered in Theorem 3 under the condition

$$\mathcal{P}_i = \begin{cases} \mathcal{X}_i & \text{if } \mathcal{X}_i \text{ is an eigenspace of } M, \\ \{0\} & \text{otherwise.} \end{cases}$$

This concludes the proof. □

Before going on, we highlight that Theorem 3 and Proposition 4 are not equivalent, in the sense that there are matrices M that admit infinitely long invariant subspace trails which are independent of their eigenspaces. A concrete example is given by the Cauchy matrix M generated as in [24] (recalled in Section 4.1) for $t = 24$ and $\mathbb{F}_{2^n}$, where $n = 63$. As shown in [34, Page 20], the subspace $\mathcal{S}^{(5)}$ defined as in Eq. (4) satisfies $M \cdot \mathcal{S}^{(5)} = \mathcal{S}^{(5)}$ and $(M \cdot x)[1] = 0$ for all $x \in \mathcal{S}^{(5)}$. At the same time, the subspace $\mathcal{S}^{(5)}$ is not related to any eigenspaces of M^j for $j \in \{1, \ldots, 5\}$.

4 Iterative Subspace Trails with Inactive S-Boxes

The previous results can be generalized to obtain a necessary and sufficient condition regarding the existence of infinitely long iterative subspace trails with inactive S-boxes.

Proposition 6. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix. A subspace $\mathcal{I}$, where $1 \leq \dim(\mathcal{I}) < t$, generates an infinitely long iterative (non-invariant) subspace trail of period $l \geq 2$ (with no active S-boxes) if and only if $\mathcal{I} \subseteq \mathcal{S}^{(l)}$ and $\mathcal{I} = \left(M^l \cdot \mathcal{I}\right)$. In particular, $\mathcal{I} \subseteq \mathcal{S}^{(l)} \cap \left(M^l \cdot \mathcal{S}^{(l)}\right)$.*[9]

The proof is a simple generalization of the one given for Theorem 2.

Proposition 7. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix. Let $\{\mathcal{A}_1^{(l)}, \mathcal{A}_2^{(l)}, \ldots, \mathcal{A}_m^{(l)}\}$ be the primary decomposition of $\mathbb{F}^t$ w.r.t. the matrix M^l, as defined in Theorem 1, that is, a collection of independent subspaces in $\mathbb{F}^t$ that are M^l-invariant and s.t. $\mathbb{F}^t = \bigoplus_i \mathcal{A}_i^{(l)}$. For each $l \geq 2$, let $\{\mathcal{X}_1, \ldots, \mathcal{X}_m\}$ be a collection of subspaces defined as*

$$\mathcal{X}_i := \mathcal{A}_i^{(l)} \cap \mathcal{S}^{(l)}.$$

A subspace $\mathcal{I}$, where $1 \leq \dim(\mathcal{I}) < t$, generates an infinitely long iterative subspace trail (with no active S-boxes) of period $l \geq 2$ if and only if

$$\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m \rangle,$$

where $\mathcal{P}_i \subseteq \mathcal{X}_i$ is a subspace that is M^l-invariant. In particular, $\mathcal{P}_i \subseteq \mathcal{X}_i \cap \left(M^l \cdot \mathcal{X}_i\right)$.

Proof. The proof of this result is equivalent to the one given in Theorem 3. In particular,

- the condition $\mathcal{P}_i \subseteq \mathcal{S}^{(l)}$ guarantees that no S-box is active in $\{\mathcal{I}, M \cdot \mathcal{I}, \ldots, M^{l-1} \cdot \mathcal{I}\}$ by definition of $\mathcal{S}^{(l)}$, and
- the subspace $\mathcal{I}$ is l-round invariant, since each subspace $\mathcal{A}_i^{(l)}$ is M^l-invariant. □

[9] In order to simplify the notation, we use $\mathcal{I}$ to denote either an invariant subspace trail or an iterative subspace trail. The period of the trail is clear from the context.

Connection to the Existence of Invariant Subspace Trails. One may wonder if there exists an example of a P-SPN scheme for which there exists no invariant subspace trail, but at the same time there exists an iterative subspace trail with inactive S-boxes. As we are going to show, this is not possible.

Proposition 8. *Consider a P-SPN scheme with s S-boxes defined as in Eq. (1). An iterative subspace trail with inactive S-boxes can only exist if there exists an invariant subspace trail with inactive S-boxes.*

Proof. As shown in Proposition 1, let $\{\mathcal{V}_1, \ldots, \mathcal{V}_l\}$ be an infinitely long *iterative* subspace trail of period l (with inactive S-boxes). If $\dim(\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle) < t$, then $\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle$ generates an infinitely long *invariant* subspace trail. Hence, if $\dim(\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle) = t$, it would be possible that an iterative subspace trail with inactive S-boxes exists and at the same time no invariant subspace trail exists. However, note that $\dim(\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle) = t$ can *never* occur in the case of inactive S-boxes. Indeed, since $\mathcal{V}_i \subseteq \langle e_{s+1}, \ldots, e_t \rangle$ for each $i \in \{1, ..., l\}$ (to guarantee that no S-box is active), it follows that $\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle \subseteq \langle e_{s+1}, \ldots, e_t \rangle$ can never generate the full space $\mathbb{F}^t$ (indeed, $\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle \cap \langle e_1, \ldots, e_s \rangle = \{0\}$). □

This does not mean that iterative subspace trails with inactive S-boxes are useless. Indeed, let $\{\mathcal{V}_1, \ldots, \mathcal{V}_l\}$ be an infinitely long iterative subspace trail of period l (with inactive S-boxes). If $\dim(\mathcal{V}_i) < \dim(\langle \mathcal{V}_1, \ldots, \mathcal{V}_l \rangle)$ (note: *strictly* less), then the data cost of setting up the iterative subspace trail may be smaller than the cost of setting up an invariant subspace trail. This can be crucial in scenarios in which there is a limitation on the data allowed for an attack.

4.1 Linear Layers with Low Multiplicative Order

Here we propose a first example of a matrix that generates an infinitely long iterative (non-invariant) subspace trail.

Proposition 9. *Given a P-SPN scheme over $\mathbb{F}^t$ defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix. If there exists $l \in \{2, \ldots, \mathfrak{R}\}$ (where $\mathfrak{R} \geq \left\lfloor \frac{t-s}{s} \right\rfloor$ is defined as in Proposition 3) and $\mu \in \mathbb{F} \setminus \{0\}$ such that $M^l = \mu \cdot I$ (i.e., M has a multiplicative order of l), where $I \in \mathbb{F}^{t \times t}$ is the identity matrix, then $\mathcal{S}^{(l)}$ generates an infinitely long iterative subspace trail of period l.*

Proof. To prove the result, it is sufficient to see that $\left\{\mathcal{S}^{(l)}, M \cdot \mathcal{S}^{(l)}, \ldots, M^{l-1} \cdot \mathcal{S}^{(l)}\right\}$ is an iterative subspace trail with no active S-boxes. This is a consequence of the fact that $M^l \cdot \mathcal{S}^{(l)} = \mu \cdot I \cdot \mathcal{S}^{(l)} = \mathcal{S}^{(l)}$, and because no S-boxes are active by the definition of $\mathcal{S}^{(l)}$. □

Cauchy Matrices in [24] – An Example from the Literature. A concrete example has recently been pointed out by Keller et al. [34] and by Beyne et al. [12]. In these papers, the authors focus on the Cauchy matrix $M \in (\mathbb{F}_{2^n})^{t \times t}$ proposed in [24] and defined as

$$M_{i,j} = \frac{1}{x_i + x_j + r}, \tag{7}$$

where $x_i = i - 1$ for $i \in \{1, \ldots, t\}$ and $t \leq r \leq p - t$. Such a matrix is used as the linear layer of some HADES-like permutations, namely STARKAD$^\pi$ and POSEIDON$^\pi$ [24]. In [46, Sect. 3.2] and in [34, 12], the authors prove that if $t = 2^\tau$, the previous matrix has a multiplicative order equal to 2, namely that M^2 is a multiple of the identity.[10] Hence, the previous result applies perfectly to this case.

[10] In [12], the authors generalize the result by assuming that $\{x_1, x_2, \ldots, x_t\}$ forms a closed subgroup of $GF(2^n)$. By definition of x_i, this is always the case for STARKAD$^\pi$ if t is a power of 2.

4.2 Linear Layer with Low-Degree Minimal Polynomial

As we have just seen, a matrix M has a low multiplicative order if there exists a small l s.t. $M^l = \mu \cdot I$, or equivalently $M^l - \mu \cdot I = 0$. Given the polynomial $p(x) = x^l - \mu$, it is easy to see that $p(\cdot)$ annihilates the entire space, since

$$\forall v \in \mathbb{F}^t : p(M) \cdot v = (M^l - \mu I) \cdot v = 0^{t\times t} \cdot v = 0^t.$$

Hence, $p(\cdot)$ divides the minimal polynomial of M. A generalization of the previous result is given in the following proposition.

Proposition 10. *Given a P-SPN scheme over $\mathbb{F}^t$ defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix. Let ϕ be the minimal polynomial of M, and let l be its degree. Assume l is "low", namely l satisfies $2 \le l \le \mathfrak{R}$ (where $\mathfrak{R} \ge \left\lfloor \frac{t-s}{s} \right\rfloor$ is defined as in Proposition 3). Moreover, let $1 \le h \le l$ be a divisor of l (and let $l' \ge 1$ s.t. $l = l' \cdot h$). Assume that the minimal polynomial is of the form*

$$\phi(x) = x^l + \sum_{i=1}^{l'-1} \alpha_{i\cdot h} \cdot x^{i\cdot h} + \alpha_0, \tag{8}$$

i.e., only monomials whose exponents are a multiple of h appear. Let us define $\mathcal{I}$ as

$$\mathcal{I} = \langle \mathcal{S}^{(l)}, M^h \cdot \mathcal{S}^{(l)}, M^{2h} \cdot \mathcal{S}^{(l)}, \ldots, M^{l-h} \cdot \mathcal{S}^{(l)} \rangle,$$

where $\mathcal{S}^{(l)}$ is defined as in Eq. (4). If $1 \le \dim(\mathcal{I}) < t$, $\mathcal{I}$ generates an infinitely long iterative subspace trail of period h (invariant if $h = 1$) with no active S-boxes.

Note that the special case $h = l$ corresponds to the one presented in Proposition 9.

Proof. The proof is similar to the one already presented in Proposition 9, noting that:

1. $\forall i = 0, 1, \ldots, h-1$: $M^i \cdot \mathcal{I} \in \langle M^i \cdot \mathcal{S}^{(l)}, M^{h+i} \cdot \mathcal{S}^{(l)}, M^{2h+i} \cdot \mathcal{S}^{(l)}, \ldots, M^{l-h+i} \cdot \mathcal{S}^{(l)} \rangle$.
2. $M^h \cdot \mathcal{I} \in \langle \mathcal{S}^{(l)}, M^h \cdot \mathcal{S}^{(l)}, M^{2h} \cdot \mathcal{S}^{(l)}, \ldots, M^{l-h} \cdot \mathcal{S}^{(l)} \rangle$ follows from the fact that $\phi(M) = 0$ (hence, $M^l = -\sum_{i=0}^{l'-1} \alpha_{i\cdot h} \cdot M^{i\cdot h}$).

The fact that no S-box is active follows from the definition of $\mathcal{S}^{(l)}$. □

4.2.1 A Concrete Example: The Starkad Matrix

A concrete example for this case is given by the matrix used for Starkad over $\mathbb{F}_{2^{63}}$ with $t = 24$, built by using the definition given in Eq. (7) in Section 4.1. Indeed, the minimal polynomial of this matrix is

$$\phi_{\text{Starkad}}(x) = x^6 + \alpha_4 \cdot x^4 + \alpha_2 \cdot x^2 + \alpha_0$$

for particular $\alpha_4, \alpha_2, \alpha_0 \in \mathbb{F}_{2^{63}}$. Following Proposition 10, we see that $l = 6$, $h = 2$, $l' = 3$. An iterative subspace trail can thus be constructed, as also shown in [34].

4.2.2 A Generic Example via the Eigenspaces of M^l

Finally, we show a concrete example of a matrix that satisfies the previous result. Consider a matrix M whose minimal polynomial is defined as in Eq. (8), that is, $\phi(x) = \sum_{i=0}^{l'} \alpha_{i\cdot h} \cdot x^{i\cdot h}$, and assume $h \ge 2$. This polynomial is related to $\phi'(y) = \sum_{i=0}^{l'} \alpha_{i\cdot h} \cdot y^i$ by replacing y with x^h. By definition, note that if ϕ is the minimal polynomial of M, ϕ' is a multiple of the minimal polynomial of M^h. Moreover, remember that every solution $\hat{y}$ of ϕ' (namely, such that $\phi'(\hat{y}) = 0$) is an eigenvalue of M^l and that each solution $\hat{x}$ of ϕ is an eigenvalue of M.

Since we are working over a finite field $\mathbb{F}$ (which is not algebraically closed), given a zero $\hat{y}$ of ϕ' as before, it is possible that there is no $\hat{x}$ that satisfies $(\hat{x})^h = \hat{y}$. In other words, it is possible that there exists an eigenspace of the matrix M^l that is not an eigenspace of M. In more details, if $\mathcal{E}$ is an eigenspace of M with eigenvalue λ, then $\mathcal{E}$ is also an eigenspace of M^l with eigenvalue λ^l, i.e.,

$$M \cdot \mathcal{E} = \lambda \cdot \mathcal{E} \implies M^l \cdot \mathcal{E} = \lambda^l \cdot \mathcal{E}.$$

Working over a space which is not algebraically closed, the other direction is not true in general. These facts can be exploited to present a more generic example of an iterative subspace trail, as given in the following lemma.

Lemma 2. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix. Let $\lambda_1^{(l)}, \dots, \lambda_\tau^{(l)}$ be the eigenvalues of M^l for some $l \geq 1$, and let $\mathcal{P}_1^{(l)}, \dots, \mathcal{P}_\tau^{(l)}$ be their corresponding eigenspaces (where $\tau \leq t$). The subspace $\mathcal{I}$ defined as $\mathcal{I} := \left\langle \mathcal{S}^{(l)} \cap \mathcal{P}_1^{(l)}, \mathcal{S}^{(l)} \cap \mathcal{P}_2^{(l)}, \dots, \mathcal{S}^{(l)} \cap \mathcal{P}_\tau^{(l)} \right\rangle$ generates an infinitely long iterative subspace trail of period l with no active S-box.*

Proof. The proof of this result is analogous to the one proposed for Proposition 9. In particular, it is sufficient to note that no S-box is active due to the definition of $\mathcal{S}^{(l)}$ (see Eq. (4)), and that the subspace trail is iterative with a period equal to l since $\mathcal{I}^{(l)}$ is constructed via the eigenspaces of M^l. □

We point out that this result includes the case in which the matrix has a low multiplicative order.

Corollary 2. *Lemma 2 implies the result presented in Proposition 9.*

Proof. Assume there exists l such that $M^l = \mu \cdot I$. Then $e_1, \dots, e_t$ are all eigenvectors of M^l with eigenvalue μ. Moreover, let $\mathcal{S}^{(l)}$ be the subspace constructed as in Eq. (4) such that no S-box is active in the first l rounds. Since $\langle e_1, \dots, e_t \rangle$ is an eigenspace of M^l corresponding to the eigenvalue μ, it follows that $\mathcal{S}^{(l)}$ is an invariant subspace of M^l. Hence, due to the previous considerations, $\left\{\mathcal{S}^{(l)}, M \cdot \mathcal{S}^{(l)}, M^2 \cdot \mathcal{S}^{(l)}, \dots, M^{l-1} \cdot \mathcal{S}^{(l)}\right\}$ is an infinitely long iterative (constant-dimensional) subspace trail. □

We remark that the two conditions are not equivalent (namely, Proposition 9 does in general not imply Lemma 2), as shown in the following concrete example.

Example. Consider the circulant matrix $M = \text{circ}(a, b, c, d)$ over $\mathbb{F}^4$. Its eigenvalues are

$$a + b + c + d, \quad \pm\sqrt{a^2 + b^2 - 2ac + c^2 - 2bd + d^2}, \quad a - b + c - d,$$

while the eigenvalues of M^2 are $(a + b + c + d)^2$, $a^2 + b^2 - 2ac + c^2 - 2bd + d^2$, and $(a-b+c-d)^2$. Since $x \mapsto x^2$ is not a permutation over $\mathbb{F}_p$ for a prime $p \geq 3$ (see Hermite's criterion), there exist a, b, c, d, s.t. $a^2 + b^2 - 2ac + c^2 - 2bd + d^2$ is not a square. Hence, for certain values of $a, b, c, d \in \mathbb{F}_p$, it is possible that M has two eigenvalues, while M^2 has always four eigenvalues.[11] This fact can be exploited in order to construct a matrix M that is not a multiple of the identity and for which an infinitely long iterative subspace trail exists. Given a P-SPN scheme over $(\mathbb{F}_p)^5$ with $s = 1$, a concrete example of such a matrix is

$$M = \begin{pmatrix} x & y & w & y & w \\ z_0 & a & b & c & d \\ z_1 & b & c & d & a \\ z_2 & c & d & a & b \\ z_3 & d & a & b & c \end{pmatrix}$$

[11] E.g., given $(a, b, c, d) = (1, 1, 2, 3)$, $a^2 + b^2 - 2ac + c^2 - 2bd + d^2$ is a square in $\mathbb{F}_{11}$, but not in $\mathbb{F}_{13}$.

Algorithm 1: Determining the existence of invariant infinitely long subspace trails without active S-boxes, using Theorem 3 and Proposition 5.

```
Data: P-SPN scheme over $\mathbb{F}^t$ with $s$ S-boxes applied to the first $s$ words (where
      the S-box has no linear structure).
Result: 1 if an invariant infinitely long subspace trail exists, 0 otherwise.
Obtain $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$ using Theorem 1.
for $i \leftarrow 1$ to $m$ do
    $\mathcal{A}_i \leftarrow \mathcal{A}_i \cap \langle e_{s+1}, \ldots, e_t \rangle$.
    while $\dim(\mathcal{A}_i) > 0$ do
        if $\mathcal{A}_i = M \cdot \mathcal{A}_i$ then
            break
        $\mathcal{A}_i \leftarrow M \cdot \mathcal{A}_i$.
$\mathcal{I} \leftarrow \langle \mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m \rangle$.
if $\dim(\mathcal{I}) > 0$ then
    return 1: Discard the matrix $M$ (due to existence of an invariant subspace
      trail generated by $\mathcal{I}$ – Theorem 3).
return 0: No infinitely long subspace trail found.
```

for particular values of $a, b, c, d, x, y, w, z_j \in \mathbb{F}_p$ s.t. *(1)* the matrix is invertible and it provides full diffusion (at word level after a finite number of rounds) for cryptographic purposes and *(2)* the circulant matrix $\text{circ}(a, b, c, d)$ has only two eigenvalues.

The iterative (non-invariant) subspace trail is thus given by $\{\mathcal{I} = \langle (0, 0, 1, 0, -1)^T \rangle, M \cdot \mathcal{I} = \langle (0, b-d, c-a, d-b, a-c)^T \rangle\}$, where $M^2 \cdot \mathcal{I} = \mathcal{I}$ and where $M^2 \neq \mu \cdot I$ for each $\mu \in \mathbb{F}_p$ (we refer to Appendix B for more details).

5 Practical Tests (Inactive S-Boxes)

In this section, we first present an algorithm which can be used to find vulnerabilities and to detect weak matrices (w.r.t. the attacks presented before). Moreover, we test several matrices over $\mathbb{F}_p$ and over $\mathbb{F}_{2^n}$ to give an idea of the number of these matrices.

5.1 Algorithm for Detecting Weak Matrices

In order to find the vulnerabilities, we use the results given in Theorem 3 and Proposition 5. In more detail, we first decompose the full space into (potentially smaller) M-invariant subspaces, that is, $\mathbb{F}^t = \bigoplus_{i=1}^m \mathcal{A}_i$, where this decomposition results from Theorem 1. For this purpose, we need the minimal polynomial of the matrix obtained by the Frobenius normal form. We then take the intersection of these subspaces with the unit vectors at the identity positions of the non-linear layer, i.e., $\mathcal{X}_i^{(0)} = \mathcal{A}_i \cap \langle e_{s+1}, \ldots, e_t \rangle$. Now we apply Proposition 5 to each of these $\mathcal{X}_i^{(0)}$, which means reducing the dimensions of these subspaces until the dimension becomes either zero or until the subspace has a nonzero dimension and does not change when applying the matrix multiplication. These final subspaces are $\mathcal{P}_i$ for $i \in \{1, \ldots, m\}$. We now build the space

$$\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m \rangle$$

and report that the matrix is vulnerable w.r.t. infinitely long invariant subspace trails if and only if $\dim(\mathcal{I}) > 0$. The detailed steps are shown as a pseudo code in Algorithm 1.

We emphasize that, while Algorithm 1 only detects infinitely long invariant subspace trails, this is sufficient in order to also prevent infinitely long iterative subspace trails. We refer to Proposition 8 for more details.

Table 1: Percentage of vulnerable matrices for Algorithm 1 and orders t, when considering prime fields $\mathrm{GF}(p)$.

$\lceil \log_2(p) \rceil$ t	8 3	4 4	6 4	16 4	8 8	12 8	16 8	8 12
Vulnerable (%) *(Random Invertible)*	0.46	8.94	2.06	< 0.01	0.51	0.03	< 0.01	0.50
Vulnerable (%) *(MDS, Random Cauchy)*	0.49	6.12	2.03	< 0.01	0.49	0.03	< 0.01	0.52

Computational Cost of Algorithm 1. The complexity of computing the Frobenius normal form is an element of $\mathcal{O}(t^3)$ for a $t \times t$ matrix [43]. Moreover, since $m \leq t$ and since the dimension of each $\mathcal{A}_i$ can be reduced at most t times, the complexity of the loop is an element of $\mathcal{O}(t^2)$. Hence, the computational cost is an element of $\mathcal{O}(t^3 + t^2) = \mathcal{O}(t^3)$.

Implementation. We make our implementation available online.[12] This tool can be used to detect vulnerabilities of given matrices over prime field or binary fields.

Computational Cost in Practice. In our practical runtime tests, we focus on prime fields $\mathrm{GF}(p)$. To give some concrete numbers, for $\lceil \log_2(p) \rceil = 16$, the test for a single matrix takes about 4 milliseconds for $t = 4$, while it takes about 30 milliseconds for $t = 16$ (using an Intel Xeon E5-2699v4 with a maximum clock frequency of 3.60 GHz). Moreover, note that the algorithm is easily parallelizable. Indeed, Proposition 5 can be applied to each $\mathcal{A}_i$ separately.

5.2 Percentage of Weak Linear Layers

We implemented Algorithm 1 in `Sage` and used it to get an idea of the percentage of matrices that are vulnerable to the attack without active S-boxes presented in Section 3.

Different Classes of Matrices. For concrete use cases, we set $s = 1$ and we focus on two scenarios, namely random invertible matrices and random Cauchy matrices.[13] As the source for randomness we use `Sage`'s random engine in both cases (and for choosing e.g. the prime numbers). In the first scenario, we create a matrix space, sample random matrices, and finally determine if they are invertible. In the second scenario, we generate Cauchy matrices using random (and valid) starting sequences. We tested all matrices using both prime fields and binary fields, focusing on square matrices of order $t \in \{3, 4, 8, 12\}$ and on fields with a size of $n \in \{4, 6, 8, 12, 16\}$ (and $\lceil \log_2(p) \rceil \in \{4, 6, 8, 12, 16\}$ for prime fields). Moreover, we tested our algorithm on the concrete matrices used to instantiate Starkad and Poseidon. We present these results in Appendix E.1.

Concrete Results. The sample size for all tests was set to 100 000 and the results are given in Table 1 and Table 2. We can immediately see that the choice of p (or n) has a significant impact on the number of vulnerable matrices. Specifically, increasing p (or n) tends to result in a higher probability for a matrix to be secure against the attacks

[12] `https://extgit.iaik.tugraz.at/krypto/linear-layer-tool`

[13] We recall that $M \in \mathbb{F}^{t\times t}$ is a Cauchy matrix if there exists $\{x_i, y_i\}_{i=1}^t$ s.t. $M_{i,j} = \frac{1}{x_i + y_j}$, where for each $i \neq j : x_i \neq x_j$, $y_i \neq y_j$, $x_i + y_j \neq 0$. Cauchy matrices are MDS matrices.

Table 2: Percentage of vulnerable matrices for Algorithm 1 and orders t, when considering binary fields GF(2^n).

n t	8 3	4 4	6 4	16 4	8 8	12 8	16 8	8 12
Vulnerable (%) *(Random Invertible)*	0.37	6.26	1.50	< 0.01	0.40	0.03	< 0.01	0.41
Vulnerable (%) *(MDS, Random Cauchy)*	0.39	5.14	1.48	< 0.01	0.41	0.02	< 0.01	0.37

presented here. We can observe that this is also true when keeping $N = n \cdot t$ constant. For example, $(n, t) = (16, 4)$ results in a very different probability compared to $(n, t) = (8, 8)$ (similar for $(n, t) = (8, 3)$ and $(n, t) = (6, 4)$, or for $(n, t) = (12, 8)$ and $(n, t) = (8, 12)$).

However, even for small fields, a secure matrix can easily be found by just testing a small number of matrices with our tool.

6 Infinitely Long Subspace Trails for P-SPN Schemes (Active S-Boxes)

Until now, we focused on the case in which no S-box is active. Here, we analyze the scenario in which S-boxes are active.

6.1 Preliminary: Subspace Trails and Truncated Differentials

We first present a generic result regarding the minimum number of rounds for which it is possible to set up a subspace trail with a probability of 1.

Proposition 11. *Given a partial SPN scheme over $\mathbb{F}^t$ with $s < \lceil t/2 \rceil$ S-boxes defined as in Eq. (1), there exists a subspace trail with prob. 1 on at least $2 \cdot \left\lfloor \frac{t-s}{s} \right\rfloor$ rounds, defined by*

$$\left\{ \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, M \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, \ldots, M^{\left\lfloor \frac{t-s}{s} \right\rfloor - 1} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, \mathcal{A}^{(1)}, \ldots, \mathcal{A}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)} \right\},$$

where $\mathcal{S}^{(i)}$ is defined as in Eq. (4) and where $\mathcal{A}^{(i)} := \left\langle M(e_1), \ldots, M(e_s), M \cdot \mathcal{A}^{(i-1)} \right\rangle$ for $i \geq 1$ (where $\mathcal{A}^{(0)} := M^{\left\lfloor \frac{t-s}{s} \right\rfloor - 1} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}$).

As for Proposition 3, this well-known result (whose proof can be found in Appendix C) only depends on the number of S-boxes, and no assumption on the matrix M is made. Similar to the case presented in Section 3.1, note that depending on the details of the linear layer, a longer subspace trail of dimension 1 can be set up.

6.2 Infinitely Long Invariant Subspace Trails with Active S-Boxes via the Eigenspaces of M

Using the approach from Section 3.2, here we present some simple examples of infinitely long invariant subspace trails with active S-boxes based on the eigenspaces of the matrix M. For this purpose, let us first introduce the concept of “compatible” subspaces.

Definition 12. Let $s \in \{1, \ldots, t-1\}$ be an integer. Let $\mathcal{V} \subseteq \mathbb{F}^t$ be a subspace and let $I \subseteq \{1, \ldots, s\}$. We say that the subspace $\mathcal{V}$ is *I-compatible* if and only if

- if $I = \emptyset$, then $\mathcal{V} \subseteq \langle e_{s+1}, \ldots, e_t \rangle$;

- if $I = \{\iota_1, \iota_2, \ldots, \iota_{|I|}\}$, then
  1. $\mathcal{V} \subseteq \langle e_{\iota_1}, \ldots, e_{\iota_{|I|}}, e_{s+1}, \ldots, e_t \rangle$;
  2. $\langle e_{\iota_1}, \ldots, e_{\iota_{|I|}} \rangle \subseteq \mathcal{V}$.

If there exists $I \subseteq \{1, \ldots, s\}$ s.t. $\mathcal{V}$ is I-compatible, then I is unique, in the sense that $\mathcal{V}$ is not J-compatible for any $J \neq I$. At the same time, note that it is possible that there is no I s.t. $\mathcal{V}$ is I-compatible. For example, working over $(\mathbb{F}_p)^t$ for a prime $p \geq 3$ and $t \geq 3$, consider the subspace $\mathcal{V} = \langle e_1 + 2 \cdot e_2 \rangle$. If $s = 1$, we can immediately see that there is no I s.t. the subspace $\mathcal{V}$ is I-compatible.

Proposition 12. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix. Let $\lambda_1, \ldots, \lambda_\tau$ be the eigenvalues of M, and let $\mathcal{P}_1, \ldots, \mathcal{P}_\tau$ be the corresponding eigenspaces (where $\tau \leq t$). Let $I = \{\iota_1, \ldots, \iota_{|I|}\} \subseteq \{1, \ldots, s\}$ be the indices of the active S-boxes (where $I \neq \emptyset$), and let*

$$\mathcal{I} = \langle \mathcal{P}'_1, \ldots, \mathcal{P}'_\tau \rangle,$$

where $\mathcal{P}'_h$ is a subspace[14] of $\mathcal{P}_h$ for $h \in \{1, \ldots, \tau\}$. If $1 \leq \dim(\mathcal{I}) < t$ and if $\mathcal{I}$ is I-compatible, then $\mathcal{I}$ generates an infinitely long invariant subspace trail with active S-boxes.

Proof. Since $\mathcal{I}$ is I-compatible, the first condition in Definition 12 ensures that the l-th S-box is not active if $l \notin I$. For each i-th active S-box, where $i \in I$, the second condition in Definition 12 implies that the entire space $\langle e_i \rangle$ is included in $\mathcal{I}$. The consequence is that, when applying the S-box, the subspace remains the same.

As for the results given in the previous sections, this subspace remains invariant through the linear layer since it is defined via the eigenspaces of M. Hence, $\mathcal{I}$ results in an infinitely long invariant subspace trail. □

Note that the number of active S-boxes in the previous subspace trail is proportional to the number of rounds (so, potentially "infinite"). As before, we emphasize that, in general, the previous observation provides only a sufficient condition.

Example. Given a P-SPN scheme with $s = 1$, consider the following 4×4 matrix M defined over $\mathbb{F}$:

$$M = \begin{pmatrix} 0 & (1 - M_{1,3} \cdot b - M_{1,4} \cdot c)/a & M_{1,3} & M_{1,4} \\ a & (-M_{2,3} \cdot b - M_{2,4} \cdot c)/a & M_{2,3} & M_{2,4} \\ b & (-M_{3,3} \cdot b - M_{3,4} \cdot c)/a & M_{3,3} & M_{3,4} \\ c & (-M_{4,3} \cdot b - M_{4,4} \cdot c)/a & M_{4,3} & M_{4,4} \end{pmatrix}, \tag{9}$$

where $a \neq 0$. A proper choice of a, b, c and $M_{\cdot,\cdot}$ provides invertibility and "full diffusion" (at word level after a finite number of rounds) for cryptographic purposes. The subspace

$$\mathcal{I} = \langle e_1 = (1, 0, 0, 0)^T, v = (0, a, b, c)^T \rangle,$$

where $M \cdot e_1 = v$ and $M \cdot v = e_1$, is invariant under the round transformation for any number of rounds. Indeed, since the first word can take every value and because the S-box is applied only to this word, $\mathcal{I}$ remains invariant (note that the S-box is active). Hence, this is a concrete example of an infinitely long invariant subspace trail with active S-boxes, where $\mathcal{P}_1 = \langle v + e_1 \rangle$ and $\mathcal{P}_2 = \langle v - e_1 \rangle$ are the eigenspaces of the matrix M that satisfy the conditions given in the previous theorem (we refer to Appendix E.3 for other examples).

Lastly, we remark that matrices of the form Eq. (9) are currently used in the literature. For example, the circulant almost-MDS matrix over $\mathbb{F}_{2^n}$ defined as circ(0,1,1,1) is used in Midori [8] and QARMA[7].

[14] We start with eigenspaces since any such constructed input space is invariant when ignoring the S-boxes. By imposing additional conditions for the active S-boxes we finally arrive at subspaces of eigenspaces.

6.3 A Necessary and Sufficient Condition for the Existence of Infinitely Long Invariant Subspace Trails with Active S-boxes

As done before, the natural step is to replace the eigenspace of M with subspaces that are M-invariant. As a main result, in this section we present a necessary and sufficient condition that allows to discard "weak" matrices with respect to invariant subspaces with active/inactive S-boxes.

Theorem 4. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix and assume that the S-box has no (non-trivial) linear structure. Let $I \subseteq \{1,\ldots,s\}$ be the positions of the active S-boxes (note that $I = \emptyset$ is also possible, that is, we do not require $|I| \geq 1$). A subspace $\mathcal{I}$ with $1 \leq \dim(\mathcal{I}) < t$ generates an infinitely long invariant subspace trail (with active S-boxes if $|I| \geq 1$) if and only if $\mathcal{I}$ is both M-invariant and I-compatible.*

Proof. The case $I = \emptyset$ corresponds to the case analyzed in Theorem 2. Hence, here we assume $|I| \geq 1$ (where $I = \{i_1, i_2, \ldots, i_{|I|}\}$).

Our approach is based on the strategy proposed for Theorem 3 and Proposition 12. We first show that an M-invariant and I-compatible subspace generates an infinitely long invariant subspace trail with active S-boxes. The proof is almost equal to the one given for Proposition 12. The only difference is that the condition that $\mathcal{I}$ is related to the eigenspaces of M is replaced by the more generic assumption that $\mathcal{I}$ is an M-invariant subspace. At the same time, since $\mathcal{I}$ is I-compatible (i.e., $\langle e_{i_1}, e_{i_2}, \ldots, e_{i_{|I|}}\rangle \subseteq \mathcal{I}$ and $\mathcal{I} \subseteq \langle e_{i_1}, e_{i_2}, \ldots, e_{i_{|I|}}, e_{s+1}, \ldots, e_t\rangle$), every i-th S-box is active if and only if $i \in I$, and inactive otherwise. We recall that for an active S-box the input difference can take each possible value in $\mathbb{F}$, and for an inactive S-box the input difference is equal to zero.

Vice-versa, assume that a subspace $\mathcal{I}$ generates an infinitely long invariant subspace trail with active S-boxes. First of all, this can happen if and only if it satisfies the condition $\mathcal{I} = M \cdot \mathcal{I}$. Indeed, by contradiction, if there exists $x \in \mathcal{I}$ s.t. $M \cdot x \notin \mathcal{I}$, then $\mathcal{I}$ would not be invariant. Moreover, since the subspace trail is invariant and with active S-boxes, each S-box can only be either constant or active. In particular, only two scenarios are possible. Either the input difference (and the output difference) of the S-box is equal to zero[15] or the input (and the output) of the S-box is active. Since the S-box does not have any linear structure, other cases are not compatible with the hypothesis of an invariant subspace trail with active S-boxes. Hence, there must exist $I \subseteq \{1,\ldots,s\}$ s.t. $\mathcal{I}$ is I-compatible. □

As expected, the result presented in Proposition 12 satisfies the previous theorem. This is due to the fact that the subspace $\mathcal{I}$ defined in Proposition 12 is related to the eigenspaces of M, which satisfy the condition $\mathcal{I} = M \cdot \mathcal{I}$. We formulate the following corollary.

Corollary 3. *The infinitely long subspace trail with active S-boxes presented in Proposition 12 satisfies Theorem 4.*

As previously done for the case of inactive S-boxes, we will now generalize Proposition 12 by replacing the eigenspaces with the generic invariant subspaces of M.

Theorem 5. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix. Assume that the S-box has no (non-trivial) linear structure. Let $\phi(x)$ be the minimal polynomial of M s.t. $\phi(x) = [p_1(x)]^{\alpha_1} \cdot [p_2(x)]^{\alpha_2} \cdot \cdots \cdot [p_m(x)]^{\alpha_m}$, where $\alpha_i \geq 1$ and p_i, p_j are monic, irreducible, and relatively prime. Let $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m\}$ be the primary decomposition of $\mathbb{F}^t$ w.r.t. the matrix M, as defined in Theorem 1.*

A subspace $\mathcal{I}$, where $1 \leq \dim(\mathcal{I}) < t$, generates an infinitely long invariant subspace trail with active S-boxes only in positions $I = \{i_1, \ldots, i_{|I|}\} \subseteq \{1, 2, \ldots, s\}$ (that is, where

[15] Equivalently, the input and the output of the S-box are constant.

the i-th S-box is active if and only if $i \in I$) if and only if

$$\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m \rangle,$$

where $\mathcal{P}_i$ is an M-invariant subspace of $\mathcal{A}_i \cap \langle e_{i_1}, e_{i_2}, \ldots, e_{i_{|I|}}, e_{s+1}, \ldots, e_t \rangle$ such that $\mathcal{I}$ is I-compatible.

Proof. The proof of this theorem is a consequence of the result given in Theorem 4 and in Theorem 1. In particular, due to the argument given in Theorem 4, we immediately see that $\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m \rangle$, where $\mathcal{I}$ is both M-invariant and I-compatible, generates an infinitely long invariant subspace trail with active S-boxes.

Vice-versa, if a subspace generates an infinitely long invariant subspace trail with active S-boxes, then it must be M-invariant and I-compatible, due to Theorem 4 and due to the fact that the S-box has no non-trivial linear structure. The particular shape of $\mathcal{I}$ is due to Theorem 1. Following the proof of Theorem 3, let

$$\mathcal{P}_i := \mathcal{A}_i \cap \mathcal{I}.$$

All $\mathcal{P}_i$ are M-invariant subspaces. In particular, we have that $\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m \rangle$ since all $\mathcal{A}_i$ are independent (in the sense that $\mathcal{A}_i \cap \mathcal{A}_j = \{0\}$) and since $\mathbb{F}^t = \bigoplus_i \mathcal{A}_i$. □

We emphasize that in general it is not trivial to give a precise "description/shape" of the subspaces $\mathcal{P}_i$. This is due to the fact that we have two conditions, first all $\mathcal{P}_i$ have to be M-invariant and secondly the full subspace $\mathcal{I}$ must be I-compatible. For example, there may be two subspaces $\mathcal{A}_i, \mathcal{A}_j$ such that they are both M-invariant and such that

- neither $\mathcal{A}_i$ nor $\mathcal{A}_j$ are I-compatible, but
- $\langle \mathcal{A}_i, \mathcal{A}_j \rangle$ is I-compatible.

In such a case, the span $\langle \mathcal{A}_i, \mathcal{A}_j \rangle$ can generate an infinitely long invariant subspace with active S-boxes, but not the two subspaces $\mathcal{A}_i, \mathcal{A}_j$. As a concrete example working over $\mathbb{F}_p^t$ for a prime $p \gg 1$ and $t \geq 3$, consider the subspace $\mathcal{V} = \langle e_1 + 2 \cdot e_2 \rangle$ and $\mathcal{W} = \langle e_1 - e_2 \rangle$, and assume that they are both M-invariant for a particular matrix M. If $s = 1$, it is not hard to see that neither $\mathcal{V}$ nor $\mathcal{W}$ are I-compatible, while $\langle \mathcal{V}, \mathcal{W} \rangle = \langle e_1, e_2 \rangle$ is obviously $\{1\}$-compatible. Hence, while in the case of inactive S-boxes we can work independently on the subspaces $\mathcal{A}_i$ (obtained as the decomposition of the $\mathbb{F}^t$), here it is not possible.

A special (trivial) case of the previous theorem is given in the following corollary.

Corollary 4. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix. Let $\phi(x)$ be the minimal polynomial of M s.t. $\phi(x) = [p_1(x)]^{\alpha_1} \cdot [p_2(x)]^{\alpha_2} \cdot \cdots \cdot [p_m(x)]^{\alpha_m}$ where $\alpha_i \geq 1$ and p_i, p_j are monic, irreducible, and relatively prime. Let $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m\}$ be the primary decomposition of $\mathbb{F}^t$ w.r.t. the matrix M. If there exists $I \subseteq \{1, \ldots, s\}$ and a subspace $\mathcal{A}_i$ s.t. $\mathcal{A}_i$ is I-compatible, then $\mathcal{A}_i$ generates an infinitely long invariant subspace trail with active S-boxes.*

An Example for Showing the Difference Between Inactive and Active S-Boxes. Finally, one may ask if there exist P-SPN schemes which are vulnerable to subspace trails with active S-boxes, but not to trails with inactive S-boxes. Assuming a P-SPN scheme with $s = 1$, an example for a matrix fulfilling these properties is given by the 4 × 4 MDS matrix

$$M = \begin{pmatrix} 3 & 1 & 1 & 2 \\ 3 & 4 & 2 & 1 \\ 2 & 1 & 3 & 4 \\ 4 & 1 & 4 & 1 \end{pmatrix}$$

over $\mathbb{F}_p$ for large $p \gg 1$ (e.g., where $p = 4\,145\,377\,273$ and $\lceil \log_2(p') \rceil = 32$). In such a case, $\mathcal{I} = \left\langle (1,0,0,0)^T, (0,1,0,2)^T, (0,0,1,p-1)^T \right\rangle$ generates an infinitely long invariant subspace trail with active S-boxes. Using our proposed tool, it is possible to see that no infinitely long invariant or iterative subspace trail with inactive S-boxes exists.

6.4 Infinitely Long Iterative Subspace Trails with Active S-Boxes

As a final step, we generalize the previous results in order to cover the case of iterative subspace trails with active S-boxes.

Theorem 6. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix and assume that the S-box has no (non-trivial) linear structure. Let $l \geq 1$ be the period of the iterative subspace trail. For each $j \in \{1,2,\dots,l\}$, let $I_j \subseteq \{1,\dots,s\}$ be the positions of the active S-boxes (note that $I_j = \emptyset$ is also possible, that is, we do not require $|I_j| \geq 1$) at the $(r+1)$-th round for $r = j \mod l$.*

A subspace $\mathcal{I}$ of dimension $1 \leq \dim(\mathcal{I}) < t$ generates an infinitely long iterative subspace trail (with active S-boxes if at least one I_j satisfies $|I_j| \geq 1$) of period l if and only if

(1) $M^j \cdot \mathcal{I}$ is I_j-compatible for $j \in \{0,1,\dots,l-1\}$, and

(2) $\mathcal{I}$ is M^l-invariant.

Proof. This result is a generalization of Theorem 4. In particular, $\mathcal{I}$ forms an l-round invariant subspace trail, i.e., a trail that is equal every l rounds. Hence, all l-round iterative subspace trails are of the form $\{\mathcal{I}, M\cdot\mathcal{I}, M^2\cdot\mathcal{I},\dots,M^{l-1}\cdot\mathcal{I}\}$. Since we assume that the S-box has no (non-trivial) linear structure, such a trail has active S-boxes if and only if the first condition (namely, there exists I_j s.t. $M^{j-1}\cdot\mathcal{I}$ is I_j compatible) is satisfied. □

We highlight that the active S-boxes are not forced to be in an active position (it is also possible that no S-box is active in some rounds). Moreover, the following result holds.

Theorem 7. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix. Assume that the S-box has no (non-trivial) linear structure. Let $l \geq 2$, and let $\{\mathcal{A}_1^{(l)}, \mathcal{A}_2^{(l)}, \dots, \mathcal{A}_m^{(l)}\}$ be the primary decomposition of $\mathbb{F}^t$ w.r.t. the matrix M^l, as defined in Theorem 1.*

A subspace $\mathcal{I}$, where $1 \leq \dim(\mathcal{I}) < t$, generates an infinitely long iterative subspace trail of period $l \geq 2$ with active S-boxes only in positions $I_j = \{i_{1,j},\dots,i_{|I_j|,j}\} \subseteq \{1,\dots,s\}$ in the j-th round (where j is taken modulo l) if and only if

$$\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_m \rangle,$$

where $\mathcal{P}_i$ is an M^l-invariant subspace of $\mathcal{A}_i^{(l)} \cap \langle e_{i_{1,0}}, e_{i_{2,0}}, \dots, e_{i_{|I_0|,0}}, e_{s+1}, \dots, e_t \rangle$ s.t.

$$\forall j \in \{0,1,\dots,l-1\}: \quad (M^j \cdot \mathcal{I}) \text{ is } I_j\text{-compatible.}$$

The proof is a simple generalization of the one given for Theorem 5 based on Theorem 6.

Examples. Given a P-SPN scheme with $s = 1$, consider again the 4×4 matrix M defined in Eq. (9). The subspace $\mathcal{I} = \left\langle e_1 = (1,0,0,0)^T \right\rangle$ generates an infinitely long iterative subspace trail with active S-boxes (of period 2) of the form

$$\left\{ \mathcal{I} = \left\langle e_1 = (1,0,0,0)^T \right\rangle, M\cdot\mathcal{I} = \left\langle (0,a,b,c)^T \right\rangle \right\},$$

where $I_{2i} = \{1\}$ and $I_{1+2i} = \emptyset$ for each $i \geq 0$.

For a second example, consider the case of a P-SPN scheme over $(\mathbb{F}_{2^n})^4$ with $s = 1$ and $M = \text{circ}(0, 1, 1, 1)$. Clearly, both $\left\langle (0, 1, 1, 0)^T \right\rangle$ and $\left\langle (0, 1, 0, 1)^T \right\rangle$ are invariant subspace trails with inactive S-boxes. As shown before, $\left\langle (1, 0, 0, 0)^T , (0, 1, 1, 1)^T \right\rangle$ is an invariant subspace trail with active S-boxes, while $\left\langle (1, 0, 0, 0)^T \right\rangle$ is an iterative (non-invariant) subspace trail with active S-boxes. By combining them, it is possible to set up new iterative subspace trails with active S-boxes, e.g., $\mathcal{I} = \left\langle (1, 0, 0, 0)^T , (0, 1, 1, 0)^T , (0, 1, 0, 1)^T \right\rangle$. A generalization of this result is presented in Appendix E.3.2.

About Iterative Subspace Trails with Active S-Boxes

Due to the results presented in Proposition 8, one may ask if there exist non-trivial iterative subspace trails with active S-boxes, namely P-SPN schemes for which there exist iterative subspace trails with active S-boxes but no subspace trails with inactive S-boxes or invariant subspace trails with active S-boxes. As shown in the following, such schemes exist even if they are "rare". Just to give a concrete example, consider a P-SPN scheme over $\mathbb{F}_p^3$ (for $s = 1$ and $t = 3$), where the linear layer is defined by the matrix

$$M = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -2 & 1 \\ 1 & -4 & 2 \end{pmatrix}. \tag{10}$$

The (non-trivial) subspace trail

$$\left\{ \mathcal{V}_0 = \langle (1, 0, 0)^T \rangle, \mathcal{V}_1 = M \cdot \mathcal{V}_0 = \langle (0, 1, 1)^T \rangle, \mathcal{V}_2 = M^2 \cdot \mathcal{V}_0 = \langle (0, 1, 2)^T \rangle \right\}$$

is iterative (since $\mathcal{V}_0$ is a proper subspace of $\mathbb{F}_p^3$ and $\mathcal{V}_0 = M^3 \cdot \mathcal{V}_0$) with active S-boxes. Since $\dim(\langle \mathcal{V}_0, \mathcal{V}_1, \mathcal{V}_2 \rangle) = 3$, it is not possible to set up an invariant subspace trail via the previous iterative subspace trail. Moreover, using the results and the tools presented in the paper, it is possible to show that (e.g., for $p = 251$) no invariant subspace trail (either with active or inactive S-boxes) can cover an infinite number of rounds.

7 Practical Tests (Active S-Boxes)

The results given in Theorem 5 to Theorem 7 seem hard to exploit in practice. A direct construction of the infinitely long subspace trail with active S-boxes is indeed missing. Without that, the cost of evaluating all subspaces $\mathcal{I}$ would likely be too large, since one has to compute all possible subspaces of $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$. Here, we fix this problem by proposing two algorithms, namely one for the case of infinitely long invariant subspace trails and one for the case of iterative trails (both with active S-boxes). Further, we test several matrices over $\mathbb{F}_p$ and over $\mathbb{F}_{2^n}$ to get an idea of the number of "weak" matrices.

Before going on, we emphasize again that we work under the assumption that the S-box has no linear structure. This assumption is crucial in order to have only two cases, namely the case in which the input of the S-box is constant and the case in which the input of the S-box is active (namely, the input can take any possible value). Since the S-box is a permutation, these two cases remain unchanged through the S-box. In other words, if the input is neither constant nor active, all information is lost when applying the S-box. This is not the case if the S-box has a linear structure.

7.1 Related Strategies in the Literature

In order to find invariant or iterative subspaces with active S-boxes, we decided to adapt algorithms already existing in the literature for our goal, that is the one proposed in [37]

Algorithm 2: Determining the existence of infinitely long invariant subspace trails with *active* S-boxes.

```
Data: P-SPN scheme over $\mathbb{F}^t$ with $s$ S-boxes applied to the first $s$ words (where
      the S-box has no linear structure).
Result: 1 if (invariant) infinitely long invariant subspace trail with active S-boxes
        is found, 0 otherwise.
foreach $I_s \subseteq \{1, 2, \ldots, s\}$ s.t. $|I_s| \geq 1$ (where $I_s := \{\iota_1, \ldots, \iota_{|I_s|}\}$) do
    $\mathcal{I} \leftarrow \langle e_{\iota_1}, \ldots, e_{\iota_{|I_s|}} \rangle$.
    foreach $i \in I_s$ do
        $v \leftarrow e_i$.
        do
            $\delta \leftarrow \dim(\mathcal{I})$.
            $v \leftarrow M \cdot v$.
            $\mathcal{I} \leftarrow \langle \mathcal{I}, v \rangle$.
            if $\dim(\mathcal{I}) = t$  or  $\mathcal{I} \cap \langle e_{\iota_1}, \ldots, e_{\iota_{|I_s|}}, e_{s+1}, \ldots, e_t \rangle \neq \mathcal{I}$ then
                break (move to next $I_s$)
        while $\dim(\mathcal{I}) > \delta$
    return 1: infinitely long invariant subspace trail with active S-boxes found: $\mathcal{I}$
     with active S-boxes in $I_s$.
return 0: No infinitely long invariant subspace trail with active S-boxes found.
```

for the detection of invariant subspace trails and the one proposed in [25] for the detection of weak-key subspace trails.

Let us focus on the algorithm proposed in [37]. Given an SPN-like permutation, the goal is to find a subspace $\mathcal{U}$ and an offset u that is invariant under the keyless round function $R(\cdot)$, namely $R(\mathcal{U} + u) = \mathcal{U} + v$ for a certain v. In the case of an SPN cipher, it is sufficient to choose the round key $k \in K_{\text{weak}} = \mathcal{U} + (u - v)$ if one aims to keep the coset invariant (depending on the key schedule, such a subspace trail can cover either a finite or an infinite number of rounds).

The approach described in [37, Lemma 1] serves as the basis for our algorithms. Starting by first guessing one possible offset u of the subspace to be found and fixing $v = R(u)$, the idea is then to guess a one-dimensional subspace $\mathcal{A}_0$ and to increase the space by computing

$$\mathcal{A}_{i+1} = \langle R(\mathcal{A}_i + u) - v, \mathcal{A}_i \rangle.$$

If $\mathcal{A}_{i+1} = \mathcal{A}_i$ for some $i > 0$, the attacker has found such an invariant subspace. If this is not the case, the attacker keeps increasing the dimension of the subspace until the space reaches the full dimension.

7.2 Algorithms for Detecting "Weak" Matrices

Infinitely Long Invariant Subspace Trails with Active S-Boxes. Our main algorithm is based on the idea proposed in [37] and briefly recalled in Section 7.1. In particular, the procedure is as follows.

1. We choose an initial subspace $\mathcal{I}$ generated by the unit vectors at the active S-box positions defined in I_s.

2. Now, similar to the approach described in [37], we keep increasing the dimension of the subspace until it stabilizes. For this purpose, we keep adding $M^j \cdot e_i$ for the active S-box positions for $j \geq 1$. Indeed, note that if we require that $\mathcal{I} = M \cdot \mathcal{I}$ and if $x \in \mathcal{I}$, it follows that $M^j \cdot x \in \mathcal{I}$.

3. If for every active S-box position i there exists an $j_i \geq 1$ such that $M^{j_i+h} \cdot e_i \in \mathcal{I}$ for $h \geq 1$, then

$$\mathcal{I} = \left\langle e_{\iota_1}, M \cdot e_{\iota_1}, \ldots, M^j \cdot e_{\iota_1}, \ldots, e_{\iota_{|I|}}, M \cdot e_{\iota_{|I|}}, \ldots, M^j \cdot e_{\iota_{|I|}} \right\rangle \tag{11}$$

generates an infinitely long invariant subspace trail for the S-box positions in I_s, where $j = \max(j_i)$. However, if this condition is not fulfilled for some i, then

$$\dim(\langle \mathcal{I}, M \cdot e_i, \ldots, M^{j_i} \cdot e_i, M^{j_i+1} \cdot e_i \rangle) = 1 + \dim(\langle \mathcal{I}, M \cdot e_i, \ldots, M^{j_i} \cdot e_i \rangle),$$

and hence the dimension of $\mathcal{I}$ increased by 1. If the condition is never fulfilled, the largest possible dimension t will be reached after a finite number of iterations. In this case, it follows that no infinitely long invariant subspace trail with active S-boxes exists (apart from the trivial one) for the particular set of active S-box positions I_s chosen in the first step.

A pseudo code for this procedure is given in Algorithm 2.

Note that in the first step, an input space has to be chosen based on some particular unit vectors. In the original approach proposed in [37], this quickly becomes too expensive due to the large number of unit vectors in the non-linear parts of the designs being considered. However, in our setting we focus on word-based designs, and further the number of S-boxes s is often small (e.g., $s = 1$ for HadesMiMC/Poseidon). Hence, we are able to determine if an invariant subspace trail with active S-boxes exists by evaluating all possibilities in a reasonable amount time – an advantage that is not necessarily related our algorithm, but to the setting we consider.

Computational Cost of Algorithm 2. Here we analyze the computational cost of Algorithm 2 in terms of loop iterations. First, consider the loop starting in the second line, and note that there are $2^s - 1$ non-empty subsets of $\{1, \ldots, s\}$. The second loop is iterated $|I_s|$ times for each of these subsets. For the Do-While loop, there are two possible cases. Either it finishes if the dimension of the new $\mathcal{I}$ is equal to the dimension of the old $\mathcal{I}$, or the dimension of $\mathcal{I}$ increased in the last iteration. Observe that the loop ends when $\dim(\mathcal{I}) = t$, and hence this loop is iterated at most $t - 1$ times. Consequently, the runtime of Algorithm 2 is an element in $\mathcal{O}(2^s st)$. Note that this runtime, even though being exponential in s, is not a major issue in the schemes we consider, since in these schemes the number of S-boxes per round (i.e., s) tends to be small.

Computational Cost in Practice. We used the same hardware as for the practical tests in Section 5.2, i.e., an Intel Xeon E5-2699v4 with a maximum clock frequency of 3.60 GHz. Again, we evaluate the performance of Algorithm 2 when using matrices over prime fields and for $n = 16$, $t \in \{4, 12\}$. For $t = 4$, Algorithm 2 takes about 3 milliseconds. For $t = 12$, Algorithm 2 takes about 16 milliseconds.

Infinitely Long Iterative Subspace Trails with Active S-Boxes. A similar algorithm can also be used to search for infinitely long iterative subspace trails with active S-boxes. Following the observations from Theorem 6, in this case we need to replace the single set I_s by l potentially different sets $I_1, I_2, \ldots, I_l$, where l is the period of the iterative subspace trail and where each of these sets denotes the positions of active S-boxes in a specific round. A pseudo code for this approach is given in Algorithm 3.

7.3 Percentage of "Weak" Linear Layers

Similar to the case for Algorithm 1, we estimate the percentage of "weak" linear layers with respect to Algorithm 2 and Algorithm 3. We refer to Section 5.2 for a description

Table 3: Percentage of vulnerable matrices using Algorithm 1, Algorithm 2, Algorithm 3, and orders t, when considering prime fields $GF(p)$. We denote by "Sx" and "Vx" the security and vulnerability w.r.t. to Algorithm x, respectively (e.g., S1 denotes security w.r.t. Algorithm 1, while V2 denotes vulnerability w.r.t. Algorithm 2). For Algorithm 3, we use a maximum period of $l = 2t$.

$\lceil \log_2(p) \rceil$	8	4	6	16	8	12	16	8
t	3	4	4	4	8	8	8	12
Random Invertible								
% (V2)	0.48	8.94	2.02	< 0.01	0.47	0.03	< 0.01	0.51
% (V2 $\wedge$ S1)	0.48	7.46	1.94	< 0.01	0.46	0.03	< 0.01	0.51
% (V2 $\vee$ V1)	0.94	16.41	4.00	< 0.01	0.97	0.06	< 0.01	1.01
% (V3 $\wedge$ S2)	< 0.01	0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01
% (V3 $\wedge$ S1 $\wedge$ S2)	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01
% (V3 $\vee$ V2 $\vee$ V1)	0.94	16.41	4.00	< 0.01	0.97	0.06	< 0.01	1.01
MDS, Random Cauchy								
% (V2)	0.51	6.12	1.84	< 0.01	0.53	0.04	< 0.01	0.48
% (V2 $\wedge$ S1)	0.50	5.29	1.76	< 0.01	0.52	0.04	< 0.01	0.47
% (V2 $\vee$ V1)	0.99	11.41	3.79	< 0.01	1.01	0.07	< 0.01	0.99
% (V3 $\wedge$ S2)	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01
% (V3 $\wedge$ S1 $\wedge$ S2)	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01
% (V3 $\vee$ V2 $\vee$ V1)	0.99	11.41	3.79	< 0.01	1.01	0.07	< 0.01	0.99

Table 4: Percentage of vulnerable matrices using Algorithm 1, Algorithm 2, Algorithm 3, and orders t, when considering binary fields $GF(2^n)$. We denote by "Sx" and "Vx" the security and vulnerability w.r.t. to Algorithm x, respectively (e.g., S1 denotes security w.r.t. Algorithm 1, while V2 denotes vulnerability w.r.t. Algorithm 2). For Algorithm 3, we use a maximum period of $l = 2t$.

n	8	4	6	16	8	12	16	8
t	3	4	4	4	8	8	8	12
Random Invertible								
% (V2)	0.38	6.25	1.56	< 0.01	0.42	0.02	< 0.01	0.41
% (V2 $\wedge$ S1)	0.38	5.54	1.51	< 0.01	0.42	0.02	< 0.01	0.40
% (V2 $\vee$ V1)	0.75	11.80	3.01	< 0.01	0.82	0.04	< 0.01	0.81
% (V3 $\wedge$ S2)	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01
% (V3 $\wedge$ S1 $\wedge$ S2)	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01
% (V3 $\vee$ V2 $\vee$ V1)	0.75	11.80	3.01	< 0.01	0.82	0.04	< 0.01	0.81
MDS, Random Cauchy								
% (V2)	0.40	5.13	1.51	< 0.01	0.36	0.03	< 0.01	0.42
% (V2 $\wedge$ S1)	0.39	4.10	1.44	< 0.01	0.36	0.03	< 0.01	0.41
% (V2 $\vee$ V1)	0.79	9.24	2.92	< 0.01	0.77	0.05	< 0.01	0.79
% (V3 $\wedge$ S2)	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01
% (V3 $\wedge$ S1 $\wedge$ S2)	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01	< 0.01
% (V3 $\vee$ V2 $\vee$ V1)	0.79	9.24	2.92	< 0.01	0.77	0.05	< 0.01	0.79

about the matrices we used for our tests. Again, our sample size is 100 000 and we focus on the case $s = 1$. To also get a better understanding of the differences between the results provided by our algorithms, we made the following distinctions:

(1) matrices which are vulnerable w.r.t. Algorithm 2,
(2) matrices which are vulnerable w.r.t. Algorithm 2 and secure w.r.t. Algorithm 1,
(3) matrices which are vulnerable w.r.t. Algorithm 3 and secure w.r.t. Algorithm 2,
(4) matrices which are vulnerable w.r.t. Algorithm 3 and secure w.r.t. Algorithm 1 and Algorithm 2.

Table 3 and Table 4 show the results for matrices over $\mathrm{GF}(p)$ and $\mathrm{GF}(2^n)$ respectively. We can immediately see that the numbers are not very different from the numbers obtained by testing Algorithm 1. Indeed, a similar amount of matrices seems to be vulnerable with respect to Algorithm 2. Interestingly, when first excluding matrices detected by Algorithm 1, the percentage is in most cases slightly lower but the difference is negligible. This fact suggests that using only one of the two algorithms is not sufficient in order to find all vulnerabilities.

Moreover, when looking at the numbers obtained by testing Algorithm 3, we can see the "rarity" of matrices which are vulnerable w.r.t. Algorithm 3, but not vulnerable w.r.t. the other two algorithms (see also Section 6.4). Indeed, for our sample size, the percentage for these matrices was close to zero.

8 Conclusion and Open Problems

In this paper, we presented necessary and sufficient conditions that a (highly non-trivial) linear layer must satisfy in order to prevent the existence of infinitely long subspace trail attacks.

8.1 Preventing Infinitely Long Subspace Trails – A Sufficient Condition

To conclude the paper, we propose a sufficient condition on the matrix M that defines the P-SPN scheme that – if satisfied – ensures that no infinitely long (invariant/iterative) subspace trail (with active/inactive S-boxes) exists. This condition only involves the details of the minimal polynomial of the matrix, and it is independent of the number of S-boxes per round. At the same time, we emphasize that it is only a sufficient condition. Hence, there exist matrices which do not satisfy it but which provide security against the approaches discussed in this paper.

Proposition 13. *Let ϕ be the minimal polynomial of a matrix M. Assume that ϕ is irreducible. For each $v \in \mathbb{F}^t$ and for each monic polynomial $\phi'(x) \in \mathbb{F}[x]$ s.t. $\phi'(M) \cdot v = 0$ it follows that $\phi' = \phi$.*

Proof. As we have seen in Proposition 2, there must exist at least one vector $v \in \mathbb{F}^t$ s.t. $v, M \cdot v, M^2 \cdot v, \ldots, M^{\deg(\phi)-1} \cdot v$ are linearly independent. Assume there exists a vector $w \in \mathbb{F}^t$ s.t. $\phi'(M) \cdot w = 0$ for a certain polynomial ϕ' for which $\deg(\phi') < \deg(\phi)$. In such a case, $w, M \cdot w, \ldots, M^{\deg(\phi)-1} \cdot w$ are not linearly independent. In particular, the subspace $\mathcal{W} = \langle w, M \cdot w, \ldots, M^{\deg(\phi')-1} \cdot w\rangle$ is a proper M-invariant subspace of $\mathbb{F}^t$. Due to [32, Prop. 2], it follows that $\phi\big|_{\mathcal{W}} = \phi'$ divides ϕ. However, this is not possible, since ϕ is irreducible. It follows that each monic polynomial $\phi'(x) \in \mathbb{F}[x]$ s.t. $\phi'(M) \cdot v = 0$ has the same degree as ϕ.

Next, we have to prove that $\phi' = \phi$. Assume as before there exists $v \in \mathbb{F}^t$ s.t. $\phi'(M) \cdot v = 0$ for a certain monic polynomial ϕ' where $d = \deg(\phi') = \deg(\phi)$ and $\phi' \neq \phi$. It follows that there are two linear combinations of $v, M \cdot v, \ldots, M^d \cdot v$ that are equal to zero, one induced by ϕ' and one induced by ϕ (note that they are different since $\phi' \neq \phi$ and since the two polynomials are monic, that is, ϕ' is not a multiple of ϕ). Hence, there exists a linear combination of $v, M \cdot v, \ldots, M^{d-1} \cdot v$ that is equal to zero.[16] Thus, there

[16] E.g., if $\sum_{i=0}^{d} \alpha_i(M^i v) = 0$ and $\sum_{i=0}^{t} \beta_i(M^i w) = 0$, then $\sum_{i=0}^{d-1}(\alpha_i\beta_d - \beta_i\alpha_d)(M^i v) = 0$.

Table 5: Percentage of MDS matrices fulfilling the requirement given in Proposition 14.

Cauchy MDS matrices over $\mathbb{F}_p$								
$\lceil \log_2(p) \rceil$	8	4	6	16	8	12	16	8
t	3	4	4	4	8	8	8	12
Secure (%)	33.79	26.52	24.66	25.23	13.42	12.89	12.42	8.10
Cauchy MDS matrices over $\mathbb{F}_{2^n}$								
n	8	4	6	16	8	12	16	8
t	3	4	4	4	8	8	8	12
Secure (%)	31.66	8.49	20.07	24.83	9.75	12.16	12.75	4.73

also exists a polynomial ϕ'' of degree strictly less than d for which $\phi''(M) \cdot v = 0$. Such a polynomial is a non-trivial divisor of ϕ, which leads to a contradiction. □

Based on this result, we can prove the following proposition.

Proposition 14. *Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix. Assume that the S-box has no (non-trivial) linear structure. If the minimal polynomial ϕ of M has maximum degree and it is irreducible, then there is no infinitely long invariant subspace trail with active/inactive S-boxes.*

Proof. Due to the previous proposition and since $\deg(\phi) = t$, *for each* $v \in \mathbb{F}^t \setminus 0$ the vectors

$$v, M \cdot v, M^2 \cdot v, \dots, M^{t-1} \cdot v$$

are linearly independent. Hence, there is no non-trivial subspace of $\mathbb{F}^t$ that is M-invariant. Indeed, if $\mathcal{S}$ is a M-invariant subspace, then $v, M \cdot v, M^2 \cdot v, \dots, M^{t-1} \cdot v$ must be in $\mathcal{S}$ for each $v \in \mathcal{S} \setminus \{0\}$. Since $v, M \cdot v, M^2 \cdot v, \dots, M^{t-1} \cdot v$ are linearly independent and since $\mathcal{S}$ is a subspace, it follows that $\langle v, M \cdot v, M^2 \cdot v, \dots, M^{t-1} \cdot v \rangle \subseteq \mathcal{S}$, that is, $\dim(\mathcal{S}) = t$, which implies that $\mathcal{S}$ is a trivial subspace. Hence, there is no non-trivial subspace $\mathcal{S}$ in $\mathbb{F}^t$ that generates an infinitely long invariant subspace trail both for the case of active and for the case of inactive S-boxes (under the assumption that the S-box has no non-trivial linear structure).

□

Note that this result does not imply security against infinitely long *iterative* subspace trails with active S-boxes. Indeed, as shown in the example given in Eq. (10), there are matrices for which there exists an infinitely long iterative subspace trail with active S-boxes but no infinitely long invariant subspace trails. In order to guarantee security against all infinitely long subspace trails (under the assumption that the S-box has no non-trivial linear structure), we propose the following result.

Theorem 8. *Let $l \geq 1$. Given a P-SPN scheme with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix. Assume that the S-box has no (non-trivial) linear structure. If the minimal polynomials of $M, M^2, \dots, M^l$ are of maximum degree and if they are all irreducible, then there is no infinitely long invariant subspace trail with active/inactive S-boxes and no infinitely long iterative subspace trail with active S-boxes of period less than or equal to l.*

The proof is a simple generalization of the previous results, by keeping in mind that an iterative subspace trail of period $l \geq 2$ is a l-round invariant subspace trail.

Discussion. As last point, one may ask how many matrices satisfy the required property just given. Assume that an irreducible polynomial $\phi(x) \in \mathbb{F}[x]$ of degree t is given. Working with matrices over $\mathbb{F}^{t\times t}$, it is always possible to associate a companion matrix C to such a minimal polynomial, as given in Definition 9 (note that the characteristic polynomial and the minimal one are equivalent in this case). It follows that all matrices M *similar* to C (i.e., all matrices M of the form $A^{-1} \cdot C \cdot A$ for an invertible matrix A) satisfy Proposition 14 by construction.

For this reason, here we focus on the case of MDS matrices. We practically evaluated the percentage of Cauchy MDS matrices which satisfy the condition given in Proposition 14. The results are shown in Table 5. For each of the tests, we set the sample size to 10 000. We can see that there are major differences between prime fields and binary extension fields. It is possible to observe that, while increasing the field size and the number of cells leads to a lower probability of the matrix to be vulnerable, it also leads to a lower probability of the matrix to satisfy the condition given in Proposition 14. In any case, we recall that the condition just given is only a *sufficient* condition, that is, a matrix does not have to satisfy it in order to guarantee security against the attacks studied in this paper.

8.2 Open Problems

As already mentioned, several problems are still open for future research. They are summarized in the following.

- In the whole paper, we work independently of the details of the S-box. However, in some cases, the S-box has some linear structure that can be exploited in order to improve the results presented here. As a future open problem, one could extend the result given in this paper for the case of active S-boxes to the case in which there exist non-trivial $\mathcal{U}, \mathcal{V}$ s.t. for each u there exists a certain v s.t. $S(\mathcal{U} + u) = \mathcal{V} + v$.
- It could make sense to analyze how the key schedule influences the possibility to set up a weak-key infinitely long subspace trail. What is a possible countermeasure that allows to prevent this case? Does the analysis in [10] also apply to P-SPN schemes?
- Here, we only considered the case of linear layers defined as invertible matrices over $\mathbb{F}^{t\times t}$. It could be interesting to extend our results to the case in which the entries of the matrix are linearized polynomials (i.e., polynomials of the form $P(x) = \bigoplus_{i=0}^{d} \rho_i \cdot x^{2^i}$ for $d \geq 1$, which can be computed efficiently over a binary field).

Acknowledgements. We thank the anonymous reviewers for their valuable comments. In particular, we thank them for the hint of using the Frobenius normal form and primary decomposition theorem in order to present the results proposed in the paper, and for the suggestion regarding the condition on the linear layer given in Section 8.1 for preventing infinitely long subspace trails. Further, we thank Nathan Keller for interesting discussions regarding the topic. Lorenzo Grassi is supported by the European Research Council under the ERC advanced grant agreement under grant ERC-2017-ADG Nr. 788980 ESCADA.

References

[1] Abdelraheem, M.A., Ågren, M., Beelen, P., Leander, G.: On the Distribution of Linear Biases: Three Instructive Examples. In: Advances in Cryptology - CRYPTO 2012. LNCS, vol. 7417, pp. 50–67. Springer (2012)

[2] Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A., Schofnegger, M.: Feistel structures for mpc, and more. In: Computer Security - ESORICS 2019. LNCS, vol. 11736, pp. 151–171 (2019)

[3] Albrecht, M.R., Grassi, L., Rechberger, C., Roy, A., Tiessen, T.: MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity. In: Advances in Cryptology – ASIACRYPT 2016. LNCS, vol. 10031, pp. 191–219 (2016)

[4] Albrecht, M.R., Rechberger, C., Schneider, T., Tiessen, T., Zohner, M.: Ciphers for MPC and FHE. In: Advances in Cryptology – EUROCRYPT 2015. LNCS, vol. 9056, pp. 430–454 (2015)

[5] Aly, A., Ashur, T., Ben-Sasson, E., Dhooghe, S., Szepieniec, A.: Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols. Cryptology ePrint Archive, Report 2019/426 (2019), https://eprint.iacr.org/2019/426

[6] Ashur, T., Dhooghe, S.: MARVELlous: a STARK-Friendly Family of Cryptographic Primitives. Cryptology ePrint Archive, Report 2018/1098 (2018)

[7] Avanzi, R.: The QARMA Block Cipher Family. Almost MDS Matrices Over Rings With Zero Divisors, Nearly Symmetric Even-Mansour Constructions With Non-Involutory Central Rounds, and Search Heuristics for Low-Latency S-Boxes. IACR Trans. Symmetric Cryptol. **2017**(1), 4–44 (2017)

[8] Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., Regazzoni, F.: Midori: A Block Cipher for Low Energy. In: Advances in Cryptology – ASIACRYPT 2015. LNCS, vol. 9453, pp. 411–436 (2015)

[9] Bar-On, A., Dinur, I., Dunkelman, O., Lallemand, V., Keller, N., Tsaban, B.: Cryptanalysis of SP Networks with Partial Non-Linear Layers. In: Advances in Cryptology – EUROCRYPT 2015. LNCS, vol. 9056, pp. 315–342 (2015)

[10] Beierle, C., Canteaut, A., Leander, G., Rotella, Y.: Proving Resistance Against Invariant Attacks: How to Choose the Round Constants. In: Advances in Cryptology – CRYPTO 2017. LNCS, vol. 10402, pp. 647–678 (2017)

[11] Beyne, T.: Block Cipher Invariants as Eigenvectors of Correlation Matrices. In: Advances in Cryptology - ASIACRYPT 2018. LNCS, vol. 11272, pp. 3–31 (2018)

[12] Beyne, T., Canteaut, A., Dinur, I., Eichlseder, M., Leander, G., Leurent, G., Naya-Plasencia, M., Perrin, L., Sasaki, Y., Todo, Y., Wiemer, F.: Out of Oddity - New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems. In: Advances in Cryptology - CRYPTO 2020. LNCS, vol. 12172, pp. 299–328 (2020)

[13] Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: Advances in Cryptology – EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23 (1999)

[14] Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology **4**(1), 3–72 (1991)

[15] Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer (1993)

[16] Blondeau, C., Leander, G., Nyberg, K.: Differential-Linear Cryptanalysis Revisited. Journal of Cryptology **30**(3), 859–888 (2017)

[17] Canteaut, A., Carpov, S., Fontaine, C., Lepoint, T., Naya-Plasencia, M., Paillier, P., Sirdey, R.: Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression. J. Cryptology **31**(3), 885–916 (2018)

[18] Daemen, J., Govaerts, R., Vandewalle, J.: Correlation Matrices. In: Fast Software Encryption – FSE'94. LNCS, vol. 1008, pp. 275–285 (1994)

[19] Daemen, J., Rijmen, V.: AES and the Wide Trail Design Strategy. In: EUROCRYPT 2002. LNCS, vol. 2332, pp. 108–109 (2002)

[20] Dinur, I., Kales, D., Promitzer, A., Ramacher, S., Rechberger, C.: Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC. In: Advances in Cryptology - EUROCRYPT 2019. LNCS, vol. 11476, pp. 343–372 (2019)

[21] Dinur, I., Liu, Y., Meier, W., Wang, Q.: Optimized Interpolation Attacks on LowMC. In: Advances in Cryptology – ASIACRYPT 2015. LNCS, vol. 9453, pp. 535–560 (2015)

[22] Dobraunig, C., Eichlseder, M., Grassi, L., Lallemand, V., Leander, G., List, E., Mendel, F., Rechberger, C.: Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit. In: Advances in Cryptology – CRYPTO 2018. LNCS, vol. 10991, pp. 662–692 (2018)

[23] Gérard, B., Grosso, V., Naya-Plasencia, M., Standaert, F.X.: Block Ciphers That Are Easier to Mask: How Far Can We Go? In: CHES 2013. LNCS, vol. 8086, pp. 383–399 (2013)

[24] Grassi, L., Khovratovich, D., Roy, A., Rechberger, C., Schofnegger, M.: Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. Cryptology ePrint Archive, Report 2019/458 (2019), https://eprint.iacr.org/2019/458.pdf – accepted at USENIX 2021

[25] Grassi, L., Leander, G., Rechberger, C., Tezcan, C., Wiemer, F.: Weak-Key Distinguishers for AES. Cryptology ePrint Archive, Report 2019/852 (2019), https://eprint.iacr.org/2019/852 – accepted at SAC 2020

[26] Grassi, L., Lüftenegger, R., Rechberger, C., Rotaru, D., Schofnegger, M.: On a generalization of substitution-permutation networks: The HADES design strategy. In: EUROCRYPT (2). LNCS, vol. 12106, pp. 674–704. Springer (2020)

[27] Grassi, L., Rechberger, C., Rønjom, S.: Subspace Trail Cryptanalysis and its Applications to AES. IACR Trans. Symmetric Cryptol. **2016**(2), 192–225 (2016)

[28] Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round AES. In: Advances in Cryptology – EUROCRYPT 2017. LNCS, vol. 10211, pp. 289–317 (2017)

[29] Grassi, L., Rechberger, C., Rotaru, D., Scholl, P., Smart, N.P.: MPC-Friendly Symmetric Key Primitives. In: ACM SIGSAC Conference on Computer and Communications Security – 2016. pp. 430–443. ACM (2016)

[30] Grosso, V., Leurent, G., Standaert, F., Varici, K.: LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations. In: Fast Software Encryption - FSE 2014. LNCS, vol. 8540, pp. 18–37 (2014)

[31] Hogben, L.: Handbook of Linear Algebra. CRC Press, 2nd edn. (2016)

[32] Kaiser, K.: Advanced Linear Algebra. https://www.math.uh.edu/~klaus/Advanced%20Linear%20Algebra_rev.pdf (2008)

[33] Kales, D., Perrin, L., Promitzer, A., Ramacher, S., Rechberger, C.: Improvements to the Linear Layer of LowMC: A Faster Picnic. Cryptology ePrint Archive, Report 2017/1148 (2017)

[34] Keller, N., Rosemarin, A.: Mind the Middle Layer: The HADES Design Strategy Revisited. Cryptology ePrint Archive, Report 2020/179 (2020), https://eprint.iacr.org/2020/179

[35] Knudsen, L.R.: Truncated and Higher Order Differentials. In: Fast Software Encryption – FSE 1994. LNCS, vol. 1008, pp. 196–211 (1994)

[36] Leander, G., Abdelraheem, M.A., AlKhzaimi, H., Zenner, E.: A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In: Advances in Cryptology - CRYPTO 2011. LNCS, vol. 6841, pp. 206–221 (2011)

[37] Leander, G., Minaud, B., Rønjom, S.: A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In: Advances in Cryptology – EUROCRYPT 2015. LNCS, vol. 9056, pp. 254–283 (2015)

[38] Leander, G., Tezcan, C., Wiemer, F.: Searching for Subspace Trails and Truncated Differentials. IACR Trans. Symmetric Cryptol. **2018**(1), 74–100 (2018)

[39] Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Advances in Cryptology – EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397 (1993)

[40] Méaux, P., Journault, A., Standaert, F., Carlet, C.: Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. In: Advances in Cryptology - EUROCRYPT 2016. LNCS, vol. 9665, pp. 311–343 (2016)

[41] Peyrin, T., Wang, H.: The MALICIOUS Framework: Embedding Backdoors into Tweakable Block Ciphers. In: Advances in Cryptology - CRYPTO 2020. LNCS, vol. 12172, pp. 249–278 (2020)

[42] Piret, G., Roche, T., Carlet, C.: PICARO - A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance. In: Applied Cryptography and Network Security - ACNS 2012. LNCS, vol. 7341, pp. 311–328 (2012)

[43] Storjohann, A.: An $O(n^3)$ algorithm for the frobenius normal form. In: ISSAC. pp. 101–105. ACM (1998)

[44] Todo, Y., Leander, G., Sasaki, Y.: Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64. In: Advances in Cryptology - ASIACRYPT 2016. LNCS, vol. 10032, pp. 3–33 (2016)

[45] Wang, Y., Wu, W., Guo, Z., Yu, X.: Differential Cryptanalysis and Linear Distinguisher of Full-Round Zorro. In: ACNS 2014. LNCS, vol. 8479, pp. 308–323 (2014)

[46] Youssef, A.M., Mister, S., Tavares, S.E.: On the Design of Linear Transformations for Substitution Permutation Encryption Networks. In: Selected Areas in Cryptography - SAC 1996. pp. 40–48 (1997)

A Related Work

In order to discuss the results in [1] and [11], and the relation between them and the ones presented in this paper, we first briefly recall the definition of *correlation matrices* [18].

Definition 13. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a vectorial Boolean function. The correlation matrix $C^F \in \mathbb{R}^{2^m \times 2^n}$ of F is the representation of the transition matrix of F with respect to the character basis of the algebra $\mathbb{C}[\mathbb{F}_2^n]$ and $\mathbb{C}[\mathbb{F}_2^m]$. The coordinates of C^F are

$$C^F_{u,v} = \frac{1}{2^n} \cdot \sum_{x \in \mathbb{F}_2^n} (-1)^{u^T \cdot F(x) + v^T \cdot x}.$$

Using these notions, we recall the results presented in the literature.

Proposition 15 (Theorem 5 of [1])**.** *Consider an invertible vectorial Boolean function F, a subspace $\mathcal{U}$, the orthogonal subspace $\mathcal{U}^\perp$, and a vector d. Let $C^F_{u,v}$ be the correlation matrix of F, and let $\omega = (\omega_u)_{u \in U^\perp}$, where $\omega_u = (-1)^{d^T \cdot u}$. Then $C^F \cdot \omega^T = \omega^T$ if and only if $F(\mathcal{U} + d) = \mathcal{U} + d$.*

This result has been generalized by Beyne in [11], who defines a "block cipher invariant" in the following way.

Definition 14 (Definition 2 of [11])**.** A vector $v \in \mathbb{C}^{2^n}$ is an invariant for a block cipher $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ if and only if it is an eigenvector of the correlation matrix C^{E_k}. If v is a multiple of $(1, 0, \ldots, 0)^T$, it will be called a trivial invariant.

For the case of invariant subspace trails, the same approach – *opportunely modified* – can potentially be exploited in order to find the results proposed here. In particular, using the properties of C^F just presented, it follows that in the case of a round function $R_k(\cdot) = k \oplus R(\cdot) = k + M \circ \mathfrak{S}(\cdot)$, where $\mathfrak{S}(\cdot) \equiv [S(\cdot) \,||\, \cdots \,||\, S(\cdot) \,||\, I(\cdot) \,||\, \cdots \,||\, I(\cdot)]$ and where $M(\cdot) = M \cdot (\cdot)$, it holds that

$$C^{R_k} = C^k C^R = C^k C^M \cdot C^{\mathfrak{S}} = C^k [C^M] \big([C^S]^{\otimes s} \otimes [C^I]^{\otimes (t-s)} \big),$$

where $C^M_{u,v} = \delta(u + M^T \cdot v)$, $C^I_{u,v} = \delta(u + v)$, and where C^k is a diagonal matrix. In the case studied here, it is not hard to see that if no S-box is active, the eigenvalues and eigenvectors of $C^M_{u,v}$ are strictly related to the eigenvalues and eigenvectors of M, leading to the previous result.

Differences in Our Work. Here we highlight the main differences in our work.

1. Both [1] and [11] focus on invariant subspaces only. As a consequence, one has to take care of the effect of the key (namely, of C^k) on the eigenvectors of C^R (namely, of the part of the round that is independent of the key).

2. We do not require that the subspace is invariant (namely, we do not restrict ourselves to the case $R(\mathcal{U} + v) = \mathcal{U} + w$). At the same time, an r-round iterative subspace trail can be seen as an invariant subspace trail for r rounds of the cipher. Hence, the previous result can be adapted in order to include this case.

3. In our case, we look for infinitely long iterative subspace trails in P-SPN schemes which are independent of the secret key and of the key schedule. Again, this is not possible for an SPN cipher due to the full non-linear layer.

B 2-Round Iterative Subspace Trail – Details

In this section, we present all the details of the concrete example of an iterative subspace trail that is not invariant given in Section 4.2.2.

The starting point is given by the circulant matrix $M = \text{circ}(a, b, c, d)$ with elements $a, b, c, d \in \mathbb{F}_p$, which is invertible if and only if its determinant is different from zero:

$$-a^4 + b^4 - 4ab^2c + 2a^2c^2 - c^4 + 4a^2bd + 4bc^2d - 2b^2d^2 - 4acd^2 + d^4 \neq 0 \mod p.$$

Depending on a, b, c, d, such a matrix can have either 2 or 4 eigenvalues and eigenvectors, while M^2 has always 4 eigenvalues and eigenvectors. In particular, the eigenvalues and eigenvectors of M are given by

$$\begin{aligned}
\lambda_0 = a+b+c+d :& \quad (1,1,1,1)^T\,,\\
\lambda_1 = -\sqrt{a^2+b^2-2ac+c^2-2bd+d^2} :& \quad (b-d, -a+c+\lambda_1, d-b, a-c-\lambda_1)^T\,,\\
\lambda_2 = \sqrt{a^2+b^2-2ac+c^2-2bd+d^2} :& \quad (b-d, -a+c+\lambda_2, d-b, a-c-\lambda_2)^T\,,\\
\lambda_3 = a-b+c-d :& \quad (1,-1,1,-1)^T\,,
\end{aligned}$$

while the eigenvalues and eigenvectors of M^2 are given by

$$\begin{aligned}
&\Lambda_0 = (\lambda_0)^2 = a^2+2a(b+c+d)+b^2+2b(c+d)+c^2+2cd+d^2 : \quad (1,1,1,1)^T\,,\\
&\Lambda_1 = (\lambda_1)^2 = a^2+b^2-2ac+c^2-2bd+d^2 : \quad (1,0,-1,0)^T\,,\\
&\Lambda_2 = (\lambda_2)^2 = a^2+b^2-2ac+c^2-2bd+d^2 : \quad (0,1,0,-1)^T\,,\\
&\Lambda_3 = (\lambda_3)^2 = a^2-2a(b-c+d)+b^2-2b(c-d)+c^2-2cd+d^2 : \quad (1,-1,1,-1)^T\,.
\end{aligned}$$

Let $M_{t\times t} \in \mathbb{F}^{t\times t}$ be the matrix defined as

$$M_{5\times 5} = \begin{pmatrix} x & y_0 & y_1 & y_0 & y_1\\ z_0 & a & b & c & d\\ z_1 & b & c & d & a\\ z_2 & c & d & a & b\\ z_3 & d & a & b & c \end{pmatrix},$$

where

(1) the coefficients are chosen in order to provide invertibility and "full diffusion" (at word level after a finite number of rounds) for cryptographic purposes, and

(2) a, b, c, d are chosen such that the corresponding matrix has only 2 eigenvalues, namely

$$\forall x \in \mathbb{F}_p : \quad a^2+b^2-2\cdot a\cdot c+c^2-2\cdot b\cdot d+d^2 \neq x^2 \mod p,$$

(remember that $x \mapsto x^2$ is not a permutation over $\mathbb{F}_p$ for a prime $p \geq 3$ – see e.g. Hermite's criterion). For example, a choice of the form $a=c$ and $b=d$ is not allowed, since the matrix would then have 4 eigenvalues.

Note that

$$\textit{(1)} \quad \underbrace{\begin{pmatrix} a & b & c & d\\ b & c & d & a\\ c & d & a & b\\ d & a & b & c\end{pmatrix}}_{\equiv \text{circ}(a,b,c,d)} \cdot \begin{pmatrix}0\\1\\0\\-1\end{pmatrix} = \begin{pmatrix} b-d\\ c-a\\ -(b-d)\\ -(c-a)\end{pmatrix},$$

$$\textit{(2)} \quad \begin{pmatrix} a & b & c & d\\ b & c & d & a\\ c & d & a & b\\ d & a & b & c\end{pmatrix}^2 \cdot \begin{pmatrix}0\\1\\0\\-1\end{pmatrix} = (a^2+b^2-2ac+c^2-2bd+d^2)\cdot \begin{pmatrix}0\\1\\0\\-1\end{pmatrix}, \text{ and}$$

$$\textit{(3)} \quad \begin{pmatrix} x & y & x & y\end{pmatrix} \cdot \begin{pmatrix}0\\1\\0\\-1\end{pmatrix} = \begin{pmatrix}0\end{pmatrix}.$$

Working in $\mathbb{F}^5$ and due to these considerations, the subspace $\mathcal{S} = \left\langle (0,0,1,0,-1)^T \right\rangle$ is a 2-round iterative subspace trail, since

(1) $M \cdot \mathcal{S} = \left\langle (0, b-d, c-a, d-b, a-c)^T \right\rangle$, and

(2) $M^2 \cdot \mathcal{S} = \mathcal{S}$.

Finally, note that M^2 is not necessarily equal to a multiple of the identity. For example, note that $(M^2_{5\times5})_{1,5} \neq 0$, where $\left(M^2_{5\times5}\right)_{1,5} = xy_0 + y_0 a + y_1 b + y_0 c + y_1 d$ is different from 0 by appropriately choosing the entries.

Other Examples. Note that many other examples can be constructed in a similar way. For example, the matrix $M_{8\times8}$ defined by

$$M_{8\times8} = \begin{pmatrix} \text{circ}(s,z,s,z) & \text{circ}(a,b,c,d) \\ \text{circ}(a,b,c,d) & \text{circ}(u,v,u,v) \end{pmatrix},$$

where a, b, c, d are chosen such that the corresponding circulant matrix has only 2 eigenvalues, allows for a 2-round iterative subspace trail defined by

$$\mathcal{S} = \left\langle (0,1,0,-1,0,0,0,0)^T \right\rangle.$$

Indeed,

(1) $M_{8\times8} \cdot \left\langle (0,1,0,-1,0,0,0,0)^T \right\rangle = \left\langle (0,0,0,0,b-d,c-a,d-b,a-c)^T \right\rangle$, and

(2) $(M_{8\times8})^2 \cdot \left\langle (0,1,0,-1,0,0,0,0)^T \right\rangle = \left\langle (0,1,0,-1,0,0,0,0)^T \right\rangle$.

C Truncated and Impossible Differentials

So far, we discussed the possibility to set up truncated differentials with probability 1. However, this does not guarantee security against all other generalizations, precisely truncated differentials with probability smaller than 1 and impossible differentials. Here we briefly focus on this case. However, we point out that we do not discuss the minimum number of rounds necessary to provide security against these attacks, since they strongly depend on the details of the linear layer.

As we are going to show, in the case in which the details of the S-box are not taken into account, (the "basic" variants of) truncated and/or of impossible differential distinguishers which are independent of the secret key can be set up for (at most) $2R$ rounds, where $R \geq 2\left\lfloor \frac{t-s}{s} \right\rfloor$ is the maximum number of rounds for which it is possible to set up a truncated differential with probability 1.

Remark. We stress that the details of the construction (e.g., the S-box, the linear layer, the key schedule) can potentially be used to improve the previous attacks. That is, $2R$ rounds refer only to the "basic" variants of such attacks, and this number must be considered only as a lower bound in order to provide security.

C.1 Subspace Trails and Truncated Differentials

Proposition 16. *Given a partial SPN scheme over $\mathbb{F}^t$ with $s \leq \lceil t/2 \rceil$ S-boxes, it is always possible to set up a subspace trail with probability 1 on at least $2 \cdot \left\lfloor \frac{t-s}{s} \right\rfloor$ rounds, defined by*

$$\left\{ \underbrace{\mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, M \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, \ldots, M^{\left\lfloor \frac{t-s}{s} \right\rfloor - 1} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}}_{\textit{no active S-boxes}}, \mathcal{A}^{(1)}, \ldots, \mathcal{A}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)} \right\}, \qquad (12)$$

where $\mathcal{S}^{(\cdot)}$ is defined as in Eq. (4), where $\mathcal{A}^{(i)} := \left\langle M(e_1), \ldots, M(e_s), M \cdot \mathcal{A}^{(i-1)} \right\rangle$ for each $i \geq 1$, and where $\mathcal{A}^{(0)} := M^{\left\lfloor \frac{t-s}{s} \right\rfloor - 1} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}$.

As done before and w.l.o.g., in the following we omit the round key and constant additions (since they only change the coset and we deal with differences).

Proof. The subspace trail defined over the first $\left\lfloor \frac{t-s}{s} \right\rfloor$ rounds is already analyzed in Section 3.1. Such a subspace trail cannot be extended for more rounds without activating any S-box since

$$M^{\left\lfloor \frac{t-s}{s} \right\rfloor -1} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)} \not\subseteq \langle e_{s+1}, \dots, e_t \rangle.$$

Hence, at least one S-box is active after $\left\lfloor \frac{t-s}{s} \right\rfloor$ rounds. It follows that the only way to extend the trail is by increasing the dimension of such a subspace, that is,

$$R\left(M^{\left\lfloor \frac{t-s}{s} \right\rfloor -1} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}\right) \subseteq \mathcal{A}^{(1)} = \langle M^{\left\lfloor \frac{t-s}{s} \right\rfloor} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, M(e_1), \dots, M(e_s) \rangle.$$

Indeed, the only thing one can do is to consider the biggest subspace for which

$$\text{S-box}\left(M^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}\right) \subseteq \langle \underbrace{e_1, e_2, \dots, e_s}_{\text{Due to S-boxes}}, \underbrace{M^{\left\lfloor \frac{t-s}{s} \right\rfloor} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}}_{\text{Due to identity part}} \rangle.$$

In this way, we lose information about the output of the S-box layer (while nothing changes for the part of the identity layer), but we can extend the subspace trail. Working in the same way, it follows that

$$R\left(\mathcal{A}^{(1)}\right) \subseteq \mathcal{A}^{(2)} = \langle M \cdot \mathcal{A}^{(1)}, M(e_1), \dots, M(e_s) \rangle,$$

and, more generally,

$$R\left(\mathcal{A}^{(r)}\right) \subseteq \mathcal{A}^{(r+1)} = \langle M \cdot \mathcal{A}^{(r)}, M(e_1), \dots, M(e_s) \rangle.$$

This operation can be repeated until the dimension of the subspace is smaller than t. Since for a generic scheme the dimension of $\mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}$ is s and the dimension increases by s in each additional round, the dimension remains smaller than t for up to $2 \cdot \left\lfloor \frac{t-s}{s} \right\rfloor$ rounds. □

Truncated Differentials. Due to the relation between subspace trails and truncated differentials [38], it is possible to set up a truncated differential distinguisher on at least $2 \cdot \left\lfloor \frac{t-s}{s} \right\rfloor$ rounds with probability 1.

C.2 Truncated Differentials with Probability Smaller than 1

Here we exploit the relation between truncated differentials and subspace trails [27, 38] and the results just given in order to analyze the minimum number of rounds to prevent these attacks. We recall the following proposition from [27].

Proposition 17. *Let* $\left\{\mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, \dots, M^{\left\lfloor \frac{t-s}{s} \right\rfloor -1} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, \mathcal{A}^{(1)}, \dots, \mathcal{A}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}\right\}$ *be a subspace trail of prob. 1 defined as in Eq. (12). For simplicity, let* $\mathfrak{r} = 2 \cdot \lfloor (t-s)/s \rfloor$ *and let*

$$\{\mathcal{V}^0, \mathcal{V}^1, \dots, \mathcal{V}^{\lfloor (t-s)/s \rfloor -1}, \mathcal{V}^{\lfloor (t-s)/s \rfloor}, \dots, \mathcal{V}^{2 \cdot \lfloor (t-s)/s \rfloor -2}\} :=$$
$$:= \left\{\mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, M \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, \dots, M^{\left\lfloor \frac{t-s}{s} \right\rfloor -1} \cdot \mathcal{S}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}, \mathcal{A}^{(1)}, \dots, \mathcal{A}^{\left(\left\lfloor \frac{t-s}{s} \right\rfloor\right)}\right\}.$$

If there exist $0 \leq v < u \leq w < \mathfrak{r}$ *s.t.*

$$\frac{\dim(\mathcal{V}^v \cap \mathcal{V}^u)}{\dim(\mathcal{V}^u)} > \frac{\dim(\mathcal{V}^w)}{t}$$

(equivalently, s.t. given a text $x \in \mathbb{F}^t$ $P\big(x \in \mathcal{V}^v \mid x \in \mathcal{V}^u\big) > P(x \in \mathcal{V}^w)$*, where* $P(\cdot)$ *denotes the probability), then it is always possible to set up a truncated differential distinguisher for* $w + u - v$ *rounds with prob.* $|\mathbb{F}|^{-\dim(\mathcal{V}^u) + \dim(\mathcal{V}^v \cap \mathcal{V}^u)}$.

The result follows from the fact that for each pair (x, y) of plaintexts, where $x \neq y$,

$$\mathrm{P}\big(E_k(x)-E_k(y) \in \mathcal{V}^w \mid x-y \in \mathcal{V}^0\big)= \mathrm{P}\big(E_k(x)-E_k(y) \in \mathcal{V}^v \mid x-y \in \mathcal{V}^u\big)= \frac{|\mathbb{F}|^{\dim(\mathcal{V}^v\cap\mathcal{V}^u)}}{|\mathbb{F}|^{\dim(\mathcal{V}^u)}}$$

independently of the secret key k, due to the fact that

$$\forall a, b: \quad \exists c, d \text{ s.t. } R^u(\mathcal{V}^0 + a) \subseteq \mathcal{V}^u + b \text{ and } R^{w-v}(\mathcal{V}^v + b) \subseteq \mathcal{V}^w + d,$$

where $R^i(\cdot)$ denotes the i-round encryption function. For comparison, in the case of a random permutation $\Pi(\cdot)$,

$$\mathrm{P}\big(\Pi(x) - \Pi(y) \in \mathcal{V}^w \mid x - y \in \mathcal{V}^0\big)= \frac{|\mathbb{F}|^{\dim(\mathcal{V}^w)}}{|\mathbb{F}|^t}.$$

We finally recall that for each subspace $\mathcal{X}, \mathcal{Y}$,

$$\dim(\mathcal{X} \cap \mathcal{Y}) = \dim(\mathcal{X}) + \dim(\mathcal{Y}) - \dim(\mathcal{X} \cup \mathcal{Y}),$$

where $\dim(\mathcal{X} \cup \mathcal{Y})$ can be easily computed by using a Gram–Schmidt process on $\mathcal{X} \cup \mathcal{Y}$.

C.3 Impossible Differentials

Impossible differential and truncated impossible differential distinguishers/attacks [13] exploit differentials that hold with probability 0.

Proposition 18. *Let $\{\mathcal{V}^0, \ldots, \mathcal{V}^{\mathfrak{r}-1}\}$ be a subspace trail of prob. 1 defined as in Proposition 17. If there exist $0 \leq v < u < \mathfrak{r}$ s.t.*

$$P\big(x \in \mathcal{V}^v \mid x \in \mathcal{V}^u\big)= 0$$

(equivalently, $\dim(\mathcal{V}^v \cap \mathcal{V}^u) = 0$), it is always possible to set up an impossible differential distinguisher for $\mathfrak{r} + u - v$ rounds.

The reason of the previous result is analogous to the one given before for truncated differential distinguishers with prob. ≤ 1.

D Infinitely Long Iterative Subspace Trails with Active S-Boxes

In this section, we give the algorithm using the results described in Line 13 for a maximum period of $l = 2t$.

Computational Cost of Algorithm 3. We mainly focus on loop iterations for the indicator of the final cost. First, we fix the maximum period l of the iterative non-invariant subspace trail. Now, Algorithm 2 is run $l - 1$ times. After that, the next loop is iterated $l' - 1$ times for each $l' \in \{2, \ldots, l\}$, leading to a total number of repetitions of at most $\frac{l(l+1)}{2}$. Finally, the last loop is iterated s times. Operation costs inside these iterations are negligible. This leads to the total runtime being an element in $\mathcal{O}\left(ls\left(2^s t + l\right)\right)$, which is not a major issue in the schemes we consider, since in these schemes the number of S-boxes per round (i.e., s) tends to be small.

Computational Cost in Practice. We used the same hardware as for the practical tests in Section 5.2, i.e., an Intel Xeon E5-2699v4 with a maximum clock frequency of 3.60 GHz. Again, we evaluate the performance of Algorithm 3 when using matrices over prime fields and for $n = 16$, $t \in \{4, 12\}$, and $l = 2t$. For $t = 4$, Algorithm 3 takes about 40 milliseconds. For $t = 12$, Algorithm 3 takes about 1 second.

Algorithm 3: Determining the existence of (iterative) infinitely long subspace trails with *active* S-boxes of period at most $l \geq 2$ based on [37] and Theorem 6.

```
Data: P-SPN scheme over $\mathbb{F}^t$ with $s$ S-boxes applied to the first $s$ words (where
      the S-box has no linear structure).
Result: 1 if (iterative) infinitely long iterative subspace trail with active S-boxes
        (of period at most $l \geq 2$) is found, 0 otherwise.
$flag \leftarrow 0$.
$T \leftarrow \emptyset$. // $T$ stores all iterative subspace trails found
for $r \leftarrow 2$ to $l$ do
    foreach $I \subseteq \{1, 2, \ldots, s\}$ (where $I := \{\iota_1, \ldots, \iota_{|I|}\}$ and $I \neq \emptyset$) do
        Apply Algorithm 2 to $M^r$, and let $\mathcal{I}$ be the resulting "invariant" subspace
          trail with active S-boxes in $I$, or let $\mathcal{I} = \emptyset$ if such a trail does not exist.
        // Check for a meaningful iterative subspace trail
        if $\dim(\mathcal{I}) \geq 1$ then
            if $\mathcal{I} = M \cdot \mathcal{I}$ (i.e., the subspace trail is invariant) then
                break (move to next $r$)
            $I^{(1)} \leftarrow \emptyset, I^{(2)} \leftarrow \emptyset, \ldots, I^{(r-1)} \leftarrow \emptyset$.
            for $j \leftarrow 1$ to $r-1$ do
                $\mathcal{I} \leftarrow M \cdot \mathcal{I}$.
                for $i \leftarrow 1$ to $s$ do
                    $\mathcal{E}^{(i)} \leftarrow \langle e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_s, e_{s+1}, \ldots, e_t \rangle$.
                    if $\mathcal{I} \cap \mathcal{E}^{(i)} \neq \mathcal{I}$ (eq., $\mathcal{I} \not\subseteq \mathcal{E}^{(i)}$) then
                        if $\mathcal{I} \cap \langle e_i \rangle = \langle e_i \rangle$ then
                            $I^{(j)} \leftarrow I^{(j)} \cup \{i\}$.
                        else
                            break (move to next $r$)
            $flag \leftarrow 1$.
            $T \leftarrow T \cup \{\mathcal{I}, r, \{I, I^{(1)}, I^{(2)}, \ldots, I^{(r-1)}\}\}$.
    // In the case $flag = 0$ (hence, $T = \emptyset$), no infinitely long
       iterative subspace trail (of period $\leq l$) was found.
    return flag: infinitely long iterative subspace trails $T$ with active S-boxes
      found.
```

E Results Using our Tool and More Examples of Subspace Trails with Active S-Boxes

E.1 Starkad and Poseidon Matrices

In addition to the statistical tests described in Section 5, we also used our tool for the Cauchy matrices using specific starting sequences defined for Starkad and Poseidon [24]. We recall that the matrix M' over $\mathbb{F}_{2^n}$ for Starkad and the matrix M'' over $\mathbb{F}_p$ for Poseidon are defined by

$$M'_{i,j} = \frac{1}{x_i \oplus y_j} \qquad \text{and} \qquad M''_{i,j} = \frac{1}{x_i + y_j}, \tag{13}$$

where $x_i = i$, $y_i = i + t$, and $i \in [0, t-1]$.

Comparison with Related Results. When using our tool for matrices with various sizes (i.e., different values for t), we can observe that some matrices over $\mathbb{F}_{2^n}$ (i.e., the matrices used for Starkad) are vulnerable to the attacks described in this paper. We can also

Table 6: Vulnerable matrices for Algorithm 1 and orders t and field sizes $n = \lceil \log_2(p) \rceil$ when considering the Starkad and Poseidon specifications.

Poseidon Specification (over $\mathbb{F}_p$)								
$\lceil \log_2(p) \rceil$	8	4	6	16	8	12	16	8
t	3	4	4	4	8	8	8	12
Vulnerable	No	No	No	No	No	No	No	No

Starkad Specification (over $\mathbb{F}_{2^n}$)								
n	8	4	6	16	8	12	16	8
t	3	4	4	4	8	8	8	12
Vulnerable	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

observe, however, that matrices over $\mathbb{F}_p$ using the same t values are not vulnerable. The detailed results for some instances are shown in Table 6.

These results are not new in the literature, since similar conclusions have already been shown in [34, 12]. Moreover, in [34] the authors explain how to modify the choice of x_i and y_j in Eq. (13) in order to fix this problem. This solution consists in changing the starting sequences for the Cauchy generation method. For completeness, we also tested our algorithm for the matrices suggested in [34]. As expected, we arrive at the same conclusion, namely, that it is not possible to set up infinitely long subspace trails for the Cauchy matrices proposed in [34] (in the case of inactive S-boxes).

E.2 Zorro Matrix

We also checked the Zorro [23] matrix with our tool. Zorro is a variant of AES where only 4 S-boxes (at the first row) are applied per round. In our setting, Zorro is a P-SPN cipher over $(\mathbb{F}_{2^8})^{16}$ with $s = 4$ where the linear layer is defined by a 16×16 matrix, where

$$\forall x \in (\mathbb{F}_{2^8})^{16} : \qquad M_{\texttt{Zorro}} \cdot x := MC \cdot SR \cdot x,$$

where

$$SR = \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I_2 & 0 & 0 \\ 0 & 0 & I_3 & 0 \\ 0 & 0 & 0 & I_4 \end{pmatrix},$$

where I is the 4×4 identity matrix, 0 is the 4×4 null matrix, and

$$I_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad I_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \qquad I_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

and where

$$MC = \begin{pmatrix} 2 \cdot I & 3 \cdot I & I & I \\ 3 \cdot I & I & I & 2 \cdot I \\ I & I & 2 \cdot I & 3 \cdot I \\ I & 2 \cdot I & 3 \cdot I & I \end{pmatrix},$$

where again I is the 4×4 identity matrix, and where $2 \equiv X \in \mathbb{F}_{2^8}$ and $3 \equiv X + 1 \in \mathbb{F}_{2^8}$.

As expected, using our tool, we found that there exists no infinitely long (iterative or invariant) subspace trail for this matrix, both in the case of inactive S-boxes and in the case of active S-boxes.[17]

E.3 Examples of Infinitely Long Subspace Trails (Active S-Boxes)

E.3.1 A Generalization of Example Eq. (9)

In Section 6.2, we proposed an example of a matrix for which an infinitely long invariant subspace trail with active S-boxes exists. In this example, one entry of the matrix is fixed and equal to zero. Here we show that this is not a necessary condition in order to guarantee that these subspace trails exist.

Indeed, consider again a P-SPN scheme over $\mathbb{F}^4$ with $s = 1$ (i.e., one S-box is applied in each round). Let M be the matrix defined as

$$M = \begin{pmatrix} 1 & (-M_{1,3} \cdot b - M_{1,4} \cdot c)/a & M_{1,3} & M_{1,4} \\ a & (-a - M_{2,3} \cdot b - M_{2,4} \cdot c)/a & M_{2,3} & M_{2,4} \\ b & (-b - M_{3,3} \cdot b - M_{3,4} \cdot c)/a & M_{3,3} & M_{3,4} \\ c & (-c - M_{4,3} \cdot b - M_{4,4} \cdot c)/a & M_{4,3} & M_{4,4} \end{pmatrix},$$

where $a \neq 0$. A proper choice of a, b, c and $M_{\cdot,\cdot}$ provides invertibility and "full diffusion" (at word level after a finite number of rounds) for cryptographic purposes.

Similar to the previous argument, it is possible to show that the subspace

$$\mathcal{I} = \left\langle e_1 = (1,0,0,0)^T, v = (1,a,b,c)^T \right\rangle$$

generates an infinitely long invariant subspace trail with active S-boxes.

E.3.2 Another Example of Infinitely Long Iterative Subspace Trails (Active S-Boxes)

Here we propose another example of an iterative subspace trail with active S-boxes, obtained by combining the previous results proposed in Section 4.2.2 and in Section 6.2. Given a P-SPN scheme over $\mathbb{F}^8$ with $s = 1$, a concrete example of such a matrix is given by

$$M = \begin{pmatrix} M^{(1)} & M^{(2)} \\ M^{(3)} & M^{(4)} \end{pmatrix}$$

s.t. M provides invertibility and "full diffusion" (at word level after a finite number of rounds) for cryptographic purposes, where

- $M^{(1)}$ is the 4×4 matrix defined in Eq. (9),
- $M^{(4)} = \text{circ}(a, b, c, d)$ as in Section 4.2.2 s.t. $\text{circ}(a, b, c, d)$ has only 2 eigenvalues,
- $M^{(2)}$ satisfies $M^{(2)}_{i,1} = M^{(2)}_{i,3}$ and $M^{(2)}_{i,2} = M^{(2)}_{i,4}$ for $i \in \{1, \ldots, 4\}$, and
- $M^{(3)}$ satisfies $M^{(3)}_{i,1} = 0$ and $M^{(3)}_{i,2} + M^{(3)}_{i,3} + M^{(3)}_{i,4} = 0$ for $i \in \{1, \ldots, 4\}$.

It is not hard to prove that the subspace $\mathcal{I}$ defined as

$$\mathcal{I} = \left\langle (1,0,0,0,\ 0,0,0,0)^T, \left(0, M^{(1)}_{2,0}, M^{(1)}_{3,0}, M^{(1)}_{4,0},\ 0,0,0,0\right)^T, (0,0,0,0,\ 0,1,0,-1)^T \right\rangle,$$

generates an infinitely long iterative (non-invariant) subspace trail with active S-boxes.

[17] We recall that the statistical attacks [45] on Zorro exploit the existence of differentials with probability higher than what expected by the designers, and not the existence of infinitely long subspace trails.