IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2021, No. 2, pp. 314–352. DOI:10.46586/tosc.v2021.i2.314-352

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, Netherlands
[2] Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology, Graz, Austria l.grassi@cs.ru.nl,firstname.lastname@iaik.tugraz.at

Abstract. Designing cryptographic permutations and block ciphers using a substitution-permutation network (SPN) approach where the nonlinear part does not cover the entire state has recently gained attention due to favorable implementation characteristics in various scenarios.
For word-oriented partial SPN (P-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 that allow us to either set up or 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 to prevent the analyzed attacks. On the practical side, we present a tool that can determine whether a given linear layer is vulnerable based on these results. Furthermore, 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 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

1 Introduction

Modern cryptography developed many techniques that go well beyond solving traditional confidentiality and authenticity problems in two-party communications. This includes practical applications of secure multi-party computation (MPC), (fully) homomorphic encryption (FHE), and zero-knowledge (ZK) proofs using symmetric primitives. Designs of primitives in symmetric cryptography for these applications are usually led by heuristics such as simplifying their arithmetic representations or linear operations being more efficient than nonlinear ones in these scenarios. The latter example is also used in the context of masking, a widespread countermeasure against side-channel attacks in which all the computations are performed on shared secrets.

Driven by all these application areas, many new symmetric primitives have recently been proposed. They include on one hand masking-friendly designs like NOEKEON [DPAR00], PICARO [PRC12], `Zorro` [GGNPS13], LS-designs [GLSV14], and candidates from the currently ongoing effort of choosing a next "lightweight" generation of primitives for e.g. authenticated encryption [BCDM20, DEMS19]. On the other hand, there is an increasing num-

Received: 2020-09-01 Revised: 2021-03-01 Accepted: 2021-05-01 Published: 2021-06-11

ber of MPC-/FHE-/ZK-friendly proposals, including LowMC [ARS+15], FLIP [MJSC16], Kreyvium [CCF+18], Rasta [DEG+18], and Dasta [HL20], MiMC [AGR+16, GRR+16b], GMiMC [AGP+19], HadesMiMC [GLR+20b], Ciminion [DGGK19], Jarvis and Friday [AD18], *Vision* and *Rescue* [AAB+20], and Poseidon [GKR+21].

1.1 Choosing the Linear Layer in Partial SPN Schemes

Some of the recalled designs (e.g., LowMC, `Zorro`, HadesMiMC 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 an input block is transformed into an output block by applying several alternating *rounds* of substitution boxes and affine permutations to provide confusion and diffusion. For a t-word SPN scheme over a fixed finite field, the substitution layer usually consists of t parallel (independent) nonlinear functions, called S-boxes. In many cases, the permutation layer is 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), however, part of the substitution layer is replaced by an identity mapping, leading to practical advantages for applications in which nonlinear operations are more expensive than linear operations. This approach was proposed and applied to AES with `Zorro` in [GGNPS13]: reducing 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 in LowMC [ARS+15]. LowMC is a family of block ciphers that combines an incomplete S-box layer with a strong linear layer to provide security and be competitive in applications like MPC, FHE, or ZK.

Many strategies proposed in the literature to guarantee security for SPN schemes are no longer applicable to P-SPN schemes and have to be replaced by more ad-hoc approaches. This includes the well-known *wide trail strategy* [DR02], which is one of the main techniques for achieving security against various statistical attacks, as the differential [BS91, BS93] and linear [Mat93] ones. Instead of choosing larger S-boxes with strong properties, the wide trail strategy aims to design the linear round transformations so that the minimum number of active S-boxes over multiple rounds is increased. This strategy is directly applicable in the case in which the nonlinear layer is (almost) full. In the case in which the nonlinear layer covers less than half of the state, a dedicated strategy is instead required and tools such as mixed integer linear programming (MILP) or SAT solvers can be used in order to find a good estimation of the minimum number of active S-boxes over multiple rounds.[1] In the case of `Zorro`, the heuristic argument proposed by the designers turned out to be insufficient, as iterative differential and linear characteristics were later found and used to break the full construction [WWGY14, BDD+15]. Similarly, the authors of LowMC chose the number of rounds to guarantee that no differential or linear characteristic can cover the entire function 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 [DLMW15].

A crucial difference between `Zorro` and LowMC regards the fact that `Zorro` uses the same linear layer in all rounds, whereas LowMC uses different pseudo-randomly generated 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 [ARS+15]), it has some drawbacks. First, the computation time or memory may become a problem, even when considering the optimizations proposed in [KPP+17, DKP+19]. Secondly, the security analysis against other attacks may become harder, since the linear layer is different in each round. Further, a poor (but valid with

[1] For completeness, we mention that these tools are actually often used/required also in the case in which the nonlinear layer is full.

respect to the specification) choice of the linear layers can significantly reduce the security, as shown concretely in [DLMW15]. Finally, the possibility to have different matrices at every round can be exploited in order to insert a backdoor, as recently shown in [PW20] in the case of a tweakable version of LowMC.

1.2 Our Contribution and Related Work

Automated characteristic search tools and dedicated key-recovery algorithms for SP networks with partial nonlinear layers have been presented in [BDD+15], where the authors propose generic techniques for differential and linear cryptanalysis. As a main result, this tool can be used to understand how many rounds a *given* scheme requires to be secure. However, focusing on the matrix that defines the fixed linear layer in a P-SPN scheme like `Zorro`, it is not clear which properties this matrix must satisfy to prevent cryptanalytic attacks in general.

Our Goal. While we cannot hope to tackle this question in its generality, we aim at a relevant subset of undesirable properties that can lead to attacks: infinitely long truncated differentials with probability 1 [Knu94], or equivalently *infinitely long subspace trails* [GRR16a, GRR17], i.e., the existence of a nontrivial subspace $\mathcal{U} \subseteq \mathbb{F}_q^t$ of inputs (where $q = 2^n$ or $q = p^n$ for a prime $p \geq 3$ and $n \in \mathbb{N}$) that is mapped into a proper (affine) subspace of the state space over any number of rounds.

Impact of Subspace Trails on Hades-Like Schemes. While such a subspace trail on its own represents a distinguisher (i.e., its existence can be exploited to distinguish the analyzed P-SPN scheme from a pseudo-random permutation), it can also be the starting point for an attack. As a concrete example, a preimage attack on the hash function Poseidon based on the existence of such trails has recently been shown in [BCD+20, Sect. 6.2]. The attacked hash function is based on the Hades design strategy [GLR+20b], which uses external rounds with full S-box layers and middle rounds with partial S-box layers. The linear layer is defined as the multiplication with a fixed MDS matrix, where no other properties were originally required on such a matrix. Thus, 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. This weakness was exploited for the particular matrices used in [GKR+19, GKR+21], where attacks on the corresponding hash functions have been found [BCD+20, KR21].

Infinitely Long Subspace Trails: Necessary & Sufficient Conditions for P-SPN Schemes. We present sufficient and necessary conditions that the matrix defining the linear layer must satisfy to guarantee that no infinitely long (nontrivial) subspace trails exist. Specifically, we analyze

(1) the case *without* active S-boxes in which the input of the S-box is constant, or equivalently, the input difference is equal to zero (see Section 3 and Section 4), and

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

In both cases, we work independently of the round keys and round constants, and we show how to construct an infinitely long subspace trail if it exists. We note that the first case is independent of the details of the S-box. In the second case, we distinguish between S-boxes with nontrivial linear structures and S-boxes without them. If the S-boxes do not have any nontrivial linear structures (which is often the case), the only possible infinitely long subspace trails with/without active S-boxes are the ones studied in this paper.

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 in [AÅBL12], and later on generalized in [Bey18]. In more detail, the results in [AÅBL12] were found by analyzing the invariant subspace trails of PRINTCIPHER (which was presented one year before in [LAAZ11]), while the result in [Bey18] was found as a generalization and improvement of the nonlinear invariant subspace attack on Midori-64 [TLS16]. However, all these results focus only on SPN schemes and invariant subspaces. Consequently, this analysis heavily depends 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. For example, if the subkeys are defined as the sum of the master key and a round constant, the existence of such an invariant subspace can be prevented by carefully choosing the round constants, as shown in [BCLR17].

More generally, the infinitely long subspace trails (if existent) are always related to the invariant subspaces of the matrix M defining the linear layer, namely the subspaces $\mathcal{X}$ that remain invariant when applying the matrix multiplication: $M \cdot \mathcal{X} = \mathcal{X}$. These subspaces can be found via the *primary decomposition theorem*, which allows splitting the full space $\mathbb{F}_q^t$ 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).

Besides nontrivial infinitely long invariant subspace trails, our analysis also covers iterative subspace trails. 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 $l \geq 2$ (where $M^l \neq \mu \cdot M$ for each $\mu \in \mathbb{F}_q$). In the 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 with active and without active S-boxes, we present rigorous *necessary and sufficient conditions which guarantee that no infinitely long (invariant or iterative) subspace trail exists*. As a final result, we can 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 can detect the vulnerabilities described in this paper (invariant and iterative trails), both in the case with and without active S-boxes and for binary and prime fields. We make our implementation available online.[2]

The tool is split into three different algorithms to cover all our results. The vulnerability of a single matrix can be evaluated quickly. To better understand 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.

2 Preliminaries

Notation. We denote the finite fields we are working with by $\mathbb{F}_q$, where $q = 2^n$ or $q = p^n$ for a prime $p \geq 3$ and $n \in \mathbb{N}$. For brevity, and where there is no difference regarding the results, we abuse the notation $\mathbb{F}$ instead of $\mathbb{F}_q$. We denote subspaces with

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

calligraphic letters (e.g., $\mathcal{S}$). Further, we use the superscript notation together with parentheses to differentiate subspaces with similar properties (e.g., $\mathcal{S}^{(i)}$). Given a subspace $\mathcal{S} \subseteq \mathbb{F}^t$, we denote by $\mathcal{S}^c \subseteq \mathbb{F}^t$ a complementary subspace such that $\mathcal{S} \oplus \mathcal{S}^c = \mathbb{F}^t$. We recall that two cosets $\mathcal{S} + a$ and $\mathcal{S} + b$ are equal if and only if $a - b \in \mathcal{S} \subseteq \mathbb{F}^t$. We use the symbol $\oplus$ together with two spaces to denote the direct sum of two spaces. Given $v, w \in \mathbb{F}^t$, the span $\langle v, w \rangle \subseteq \mathbb{F}^t$ is always defined with respect to the space $\mathbb{F}$, that is, $\langle v, w \rangle = \{\alpha \cdot v + \beta \cdot w \mid \alpha, \beta \in \mathbb{F}\}$. We denote by $\{e_1, \ldots, e_t\}$ the unit vectors of $\mathbb{F}_q^t$ (i.e., e_i has a single 1 in the i-th word). 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 $M_{i,j}$. Given an arbitrary subspace $\mathcal{X} \subseteq \mathbb{F}^t$ and a matrix M, let $M \cdot \mathcal{X} := \{M \cdot x \mid x \in \mathcal{X}\}$.

2.1 Partial SPN Schemes

In this paper, we will focus on P-SPN block ciphers and permutations over $(\mathbb{F}_q^t, +, \cdot)$.[3] All our results are independent of the round keys and constants. For this reason, in the following we do not clearly distinguish between block ciphers and unkeyed permutations, and we just refer to them using the term *schemes*.

Partial SPN (P-SPN) Schemes. We denote the application of r rounds of a t-word P-SPN scheme by $E^r : \mathbb{F}^t \to \mathbb{F}^t$. For every input $x = (x_1, \ldots, x_t) \in \mathbb{F}^t$, the output is defined by $E^r(x) = (R_r \circ \cdots \circ R_1)(x + c^{(0)})$, where $R_i : \mathbb{F}^t \to \mathbb{F}^t$ is defined as $R_i(x) = R(x) + c^{(i)}$ and $c^{(i)}$ is a publicly known round constant or a secret round key for $i \in \{0, \ldots, r\}$.

Let $1 \leq s < \lceil t/2 \rceil$ be the number of S-boxes per round.[4] We denote by R the composition of the S-box layer and of 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 nonlinear permutation, and hence $t - s$ input words are unaffected by the S-box layer, which is the only difference to classical SPN schemes. We also assume that the s S-boxes are applied to the first s words (note that given any P-SPN scheme with the S-boxes in fixed positions, it is always possible to find an equivalent representation such that the S-boxes are applied to the first s words).

The linear layer $M(\cdot)$ is defined by the multiplication with an invertible matrix $M \in \mathbb{F}^{t \times t}$, that is, $M(x) = M \cdot x$. In the following, we assume that the matrix M ensures *full diffusion after a finite number of rounds*, in the sense that there exists an $r \in \mathbb{N}$ such that every word of the internal state after the application of r rounds depends on every input word $x_1, \ldots, x_t$. For example, the smallest integer r that satisfies the previous condition for an MDS matrix is 1, for the linear layer in AES it is 2, while it does not exist for a diagonal matrix. We refer to [BJK+16a, BJK+16b, App. D] for a more detailed analysis about this concept.

Before going on, we point out that all word-wise (aligned) P-SPN schemes can be written in the above way.

Hades-Like Schemes. The recently proposed HADES strategy [GLR+20b] 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.

[3] In the case in which $q = 2^n$, the field corresponds to $(\mathbb{F}_{2^n}^t, \oplus, \cdot)$, where $\oplus$ corresponds to the `XOR` operation. 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 of two elements in $\mathbb{F}_q$.

[4] Note that if $s \geq \lceil t/2 \rceil$, then at least one S-box is active every two rounds in the case in which the linear layer is instantiated with an MDS matrix (namely, a matrix with maximum branch number).

2.2 Invariant Subspaces and Subspace Trails

Subspace Trails. Subspace trails were first defined in [GRR16a], and they are strictly related to truncated differential attacks, as shown in [LTW18].

Definition 1 (*Subspace Trail*)**.** Let $(\mathcal{U}_1, \dots, \mathcal{U}_{r+1})$ denote a collection of $r+1$ nontrivial subspaces with $\dim(\mathcal{U}_i) \leq \dim(\mathcal{U}_{i+1}) < t$. If for each $i \in \{1, \dots, r\}$ and for each $a_i \in \mathbb{F}^t$ 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 $(\mathcal{U}_1, \dots, \mathcal{U}_{r+1})$ is a *subspace trail* of length r for the function $F(\cdot) = R_r \circ \cdots \circ R_1(\cdot)$. If the relations hold with equality, the subspace trail is called a *constant-dimensional subspace trail*.

In the entire paper, we sometimes refer to a subspace trail $(\mathcal{U}_1, \dots, \mathcal{U}_{r+1})$ as a subspace trail "generated" by $\mathcal{U}_1$. Before going on, we mention that the link between truncated differential trails and subspace trails is recalled in Appendix A.

Invariant Subspace Trails. We use the term "invariant subspace trail" for referring to a subspace trail in which the subspace is invariant (that is, $\mathcal{U}_i = \mathcal{U}_j$ for each $i, j = 1, \dots, r$).

Definition 2 (*Invariant Subspace Trail*)**.** Let $\mathcal{U} \subset \mathbb{F}^t$ be a subspace. $\mathcal{U}$ generates an r-round invariant subspace trail for the function $F(\cdot) = R_r \circ \cdots \circ R_1(\cdot)$ if for each $i \in \{1, \dots, r\}$ and for each $a_i \in \mathbb{F}^t$ there exists $a_{i+1} \in \mathcal{U}_{i+1}^c$ such that

$$R_i(\mathcal{U} + a_i) = \mathcal{U} + a_{i+1}.$$

We point out that this is not the original definition introduced in [LAAZ11] and reconsidered e.g. in [LMR15]. In these cases, the authors consider SPN schemes, and the existence of an invariant subspace is related to the existence of weak keys. In particular, given a weak key k (with $k = \left(k^{(0)}, \dots, k^{(r)}\right)$, where $k^{(j)}$ is the j-th round key), a (nontrivial) subspace $\mathcal{I} \subset \mathbb{F}^t$ generates an invariant subspace trail of length r for the round function $R^{(k)}(\cdot) = R(\cdot) + k$ if for each $i \in \{1, \dots, r\}$ there exist $a_0, a_1, \dots, a_r \in \mathbb{F}^t$ such that $R^{(k^{(i)})}(\mathcal{I} + a_i) = R(\mathcal{I} + a_i) + k^{(i)} = \mathcal{I} + a_{i+1}$ for each $i \in \{0, 1, \dots, r-1\}$. In our case, this restriction is not mandatory anymore, and we are free to work independently of the value of the secret key.

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

Definition 3 (*Iterative Subspace Trail*)**.** Let $(\mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_l)$ be a constant-dimensional subspace trail for l rounds with $\dim(\mathcal{V}_i) < t$. 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 arbitrary number of times, i.e., if

$$(\mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_l, \mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_l, \dots, \mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_l)$$

is a 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 $(\mathcal{V}_1, \dots, \mathcal{V}_l)$ be an infinitely long iterative subspace trail of period l. If $\dim(\langle \mathcal{V}_1, \dots, \mathcal{V}_l \rangle) < t$, then $\langle \mathcal{V}_1, \dots, \mathcal{V}_l \rangle$ 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 each coset of $\mathcal{V}_l$ is mapped into a coset of $\mathcal{V}_1$). □

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

2.3 Decomposition Theorem & Frobenius Normal Form

In this section, we recall several notions from linear algebra useful for presenting our results, starting with the concept of eigenvalues and eigenspaces.

Definition 4. Given an invertible matrix $M \in \mathbb{F}^{t \times t}$, the subspace $\mathcal{P} = \langle \rho_1, \ldots, \rho_d \rangle \subseteq \mathbb{F}^t$ (with $\mathcal{P} \neq \{0\}$) is the (right) eigenspace of M for the eigenvalue $\lambda \in \mathbb{F} \setminus \{0\}$ if the condition $M \cdot \rho_i = \lambda \cdot \rho_i$ is satisfied $\forall i \in \{1, \ldots, d\}$.

Definition 5. $M \in \mathbb{F}^{t \times t}$ is a diagonalizable matrix if and only if there exists an (invertible) matrix $P \in \mathbb{F}^{t \times t}$ and there exist $\lambda_1, \ldots, \lambda_t \in \mathbb{F}^t$ such that $P^{-1} \cdot M \cdot P = D = \mathrm{diag}(\lambda_1, \ldots, \lambda_t)$ is a diagonal matrix.

Definition 6. A field $\mathbb{F}$ is *algebraically closed* if every nonconstant polynomial in $\mathbb{F}[x]$ has a root in $\mathbb{F}$.

Definition 7. Let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix. The characteristic polynomial $\psi \in \mathbb{F}[x]$ is defined as $\psi(x) = \det(x \cdot I - M)$. The minimal polynomial $\phi \in \mathbb{F}[x]$ is the monic polynomial of minimal degree such that

(1) $\phi(M) \cdot v = 0^t = (0, 0, \ldots, 0)^T \in \mathbb{F}^t$ for each $v \in \mathbb{F}^t$, and

(2) for each polynomial $p \in \mathbb{F}[x]$ that is annihilating (in the sense that $p(M) \cdot v = 0^t$ for each $v \in \mathbb{F}^t$), ϕ divides p.

Proposition 2 ([Kai08, Theorem 1])**.** *Let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix with the minimal polynomial ϕ. There exists (at least) one vector $v \in \mathbb{F}^t$ such that*

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

are linearly independent.

By definition, $\det(M) = (-1)^t \cdot \psi(0)$. Moreover,

(1) the minimal polynomial divides the characteristic polynomial (which implies that $\deg(\phi) \leq \deg(\psi) = t$), and

(2) an eigenvalue of the matrix is a root of both the minimal and of the characteristic polynomial, and vice-versa (i.e., each root is an eigenvalue).

Definition 8. 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 $M \cdot \mathcal{V} = \mathcal{V}$.

Definition 9. 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 *directly indecomposable* if there are *no* nontrivial subspaces $\mathcal{V}_1, \mathcal{V}_2 \subseteq \mathcal{V}$ such that $\mathcal{V} = \mathcal{V}_1 \oplus \mathcal{V}_2$.
- $\mathcal{V}$ is said to be *cyclic* if $\exists v \in \mathcal{V}$ such that $\mathcal{V} = \langle v, M \cdot v, M^2 \cdot v, \ldots, M^l \cdot v, \ldots \rangle \equiv \langle v \rangle_M$.

As is well-known, not all matrices are diagonalizable. When working over a field $\mathbb{F}$, there always exists an invertible matrix $Q \in \mathbb{F}^{t\times t}$ such that $F := Q^{-1} \cdot M \cdot Q$ is in the *Frobenius normal form*. The Frobenius normal form can be exploited to easily compute the characteristic and the minimal polynomial of a given matrix. It can also be used to split the full space $\mathbb{F}^t$ into independent subspaces that are invariant through the matrix M.

Definition 10. 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 $Q \in \mathbb{F}^{t\times t}$ such that

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

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 $p_i(x) = x^{t_i} + \sum_{j=0}^{t_i-1} c_{j,i} \cdot x^j$ such that

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

(2) p_l corresponds to the minimal polynomial ϕ of M and $\psi(x) = \prod_{i=0}^{l} p_i(x)$ is the characteristic polynomial of M.

Note that given a companion matrix C_i over $\mathbb{F}^{t_i}$, we have that $\langle e_1\rangle_{C_i}$ generates the full subspace $\mathbb{F}^{t_i}$, since $p_i(e_1) = e_2, p_i(e_2) = e_3, \dots, p_i(e_{t_i-2}) = e_{t_i-1}, p_i(e_{t_i-1}) = e_{t_i}$ are linearly independent, while $p_i(e_{t_i}) = -c_{0,i} \cdot e_1 - c_{1,i} \cdot e_2 + \dots - c_{t_i-1,i} \cdot e^{t_i}$.

Theorem 1 (Primary Decomposition Theorem [Hog16, Sect. 6.4] - [Kai08, Theorem 3])**.** *Let $M \in \mathbb{F}^{t\times t}$ be an invertible matrix. Let $\phi \in \mathbb{F}[x]$ be its minimal polynomial such that*

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

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

$$\mathbb{F}^t = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \dots \oplus \mathcal{A}_m, \tag{2}$$

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

$$\mathcal{A}_j := \ker([p_j(M)]^{\alpha_j}) := \left\{ x \in \mathbb{F}^t \;\middle|\; [p_j(M)]^{\alpha_j} \cdot x = \underbrace{0 \;||\; 0 \;||\; \dots \;||\; 0}_{\equiv 0^t} \right\},$$

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

1. *$\mathcal{A}_i$ are M-invariant for each i, and*
2. *the minimal polynomial of a linear operator M_i induced on $\mathcal{A}_i$ by M is $(p_i(\cdot))^{\alpha_i}$.*

We emphasize that the previous decomposition does not imply that there are no nontrivial 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 dimension one 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 (Without Active S-Boxes)

Focusing on P-SPN schemes which use the same linear layer in each round (e.g., `Zorro` [GGNPS13]), here we study the properties that the matrix that defines the linear layer must satisfy in order to prevent infinitely long invariant subspace trails without active S-boxes.

3.1 Preliminary Results

Due to the fact that the nonlinear layer is only partial in P-SPN schemes, parts of the state go through the S-box layer unchanged. In particular, if the nonlinear 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 $\max\left\{1, \left\lfloor \frac{t-s}{s} \right\rfloor\right\}$ rounds. Note that $\left\lfloor \frac{t-s}{s} \right\rfloor \geq 1$ if and only if $s < \lceil t/2 \rceil$. Indeed, if the matrix that defines the linear layer has maximum branch number and if $s \geq \lceil t/2 \rceil$, then at least one S-box is active every two rounds (however, since $s < t$, then it is always possible to choose the initial subspace such that no S-box is active in the first round).

By choosing texts in the same coset of $\mathcal{S} = \langle v_1, \ldots, v_{\dim(\mathcal{S})} \rangle$ such that

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

for each $j \in \{1, \ldots, \dim(\mathcal{S})\}$ and where $M^0 = I$ is the identity matrix, no S-box is active in the first $\max\left\{1, \left\lfloor \frac{t-s}{s} \right\rfloor\right\}$ 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 $\mathcal{S}^{(i)} \subseteq \mathbb{F}^t$ be defined as

$$\mathcal{S}^{(i)} = \begin{cases} \mathbb{F}^t & \text{if } i = 0, \\ \left\{ v \in \mathbb{F}^t \;\middle|\; (M^j \cdot v)[1, \ldots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s, 0 \leq j < i \right\} & \text{otherwise.} \end{cases} \tag{3}$$

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. For each $i \geq 1$,*

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

where $t - i \cdot s \leq \dim\left(\mathcal{S}^{(i)}\right) \leq t$.

Proof. Let $x \in \mathcal{S}^{(1)}$. By definition, $x \in \mathcal{S}^{(2)}$ if and only if

$$x \in \mathcal{S}^{(1)} \cap \{y \in \mathbb{F}^t \mid (M \cdot y)[1, \ldots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s\},$$

or equivalently, if $x \in \left\{ v \in \mathbb{F}^t \;\middle|\; (M^j \cdot v)[1, \ldots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s, j \in \{0, 1\} \right\}$. Since

$$\begin{aligned} &\{y \in \mathbb{F}^t \mid (M \cdot y)[1, \ldots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s\} \\ &= \{(M^{-1} \cdot z) \in \mathbb{F}^t \mid z[1, \ldots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s\} \\ &= M^{-1} \cdot \{z \in \mathbb{F}^t \mid z[1, \ldots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s\} \\ &= M^{-1} \cdot \mathcal{S}^{(1)}, \end{aligned}$$

it follows that $\mathcal{S}^{(2)} = \mathcal{S}^{(1)} \cap M^{-1} \cdot \mathcal{S}^{(1)}$. Working recursively, $x \in \mathcal{S}^{(i+1)}$ if and only if $x \in \left\{ v \in \mathbb{F}^t \mid (M^j \cdot v)[1, \ldots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s, 0 \leq j \leq i \right\}$, that is, if $x \in \mathcal{S}^{(i)} \cap \{y \in \mathcal{S}^{(i)} \mid (M \cdot y)[1, \ldots, s] = 0 \,||\, \cdots \,||\, 0 \in \mathbb{F}^s\}$. It follows that $\mathcal{S}^{(i+1)} = \mathcal{S}^{(i)} \cap M^{-1} \cdot \mathcal{S}^{(i)}$. □

Moreover, the following result holds.

Lemma 2. *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 $\mathfrak{R} \geq \left\lfloor \frac{t-s}{s} \right\rfloor$ be the (positive) integer such that $\dim\left(\mathcal{S}^{(\mathfrak{R})}\right) \geq 1$ and $\dim\left(\mathcal{S}^{(\mathfrak{R}+1)}\right) = 0$ (where $\mathfrak{R} = \infty$ if $\dim\left(\mathcal{S}^{(r)}\right) \geq 1$ for each $r \geq 1$). 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 generated by $\mathcal{S}^{(r)}$ without active S-boxes.

Proof. $\left(\mathcal{S}^{(r)}, M \cdot \mathcal{S}^{(r)}, M^2 \cdot \mathcal{S}^{(r)}, \ldots, M^{r-1} \cdot \mathcal{S}^{(r)}\right)$ is a subspace trail if for each $i \in \{0, 1, \ldots, r-1\}$ and for each $a \in \mathbb{F}^t$, there exists $b \in \mathbb{F}^t$ such that $R(M^i \cdot \mathcal{S}^{(r)} + a) = M^{i+1} \cdot \mathcal{S}^{(r)} + b$. By definition of the round function $R(x) = c + M \circ S(x)$:

- The S-box layer only changes the coset. Indeed, the first s words of $M^i \cdot \mathcal{S}^{(r)} + a$ are constant, due to the definition of $\mathcal{S}^{(r)}$ and due to the fact that the S-box layer is composed of s nonlinear functions and $t - s$ identity functions. Hence, $S(M^i \cdot \mathcal{S}^{(r)} + a) = M^i \cdot \mathcal{S}^{(r)} + a'$ for a certain $a' \in \mathbb{F}^t$.
- Since the linear layer is a linear operation, $M \cdot (M^i \cdot \mathcal{S}^{(r)} + a') = M^{i+1} \cdot \mathcal{S}^{(r)} + a''$.
- Finally, the last key or constant addition only changes the coset. □

This well-known result (see e.g. [ARS+15, Sect. 5.1] or [GGNPS13, Sect. 4.1]) does not require any assumption on 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 [AÅBL12, Bey18], invariant subspace trails can be set up by exploiting the eigenspaces of the matrix M that defines the linear layer.

Proposition 3. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes per round defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix defining the linear layer. Let $\lambda_1, \ldots, \lambda_\tau \in \mathbb{F}$ be its eigenvalues and let $\mathcal{P}_1, \ldots, \mathcal{P}_\tau \subseteq \mathbb{F}^t$ 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 $\mathcal{I} \subseteq \mathbb{F}^t$ generates a (nontrivial) infinitely long invariant subspace trail without active S-boxes.

Proof. To prove the previous result, we have to show that for each $a \in \mathbb{F}^t$ there exists $b \in \mathbb{F}^t$ such that $M \circ S(\mathcal{I} + a) = \mathcal{I} + b$. 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. □

Examples. Consider a P-SPN scheme over $\mathbb{F}_p^4$ with $s = 1$ for a prime $p \geq 101$. 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 (e.g., such a 4×4 matrix is MDS matrix for each $p \geq 101$). As a second example, if

$$M = \mathrm{circ}(2,3,1,1) = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 3 & 1 & 1 & 2 \\ 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \end{pmatrix},$$

the only eigenspace 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 without active S-boxes even if they have eigenspaces.

3.3 A Necessary and Sufficient Condition for the Existence of Infinitely Long Invariant Subspace Trails (Without Active S-boxes)

As shown in Section 2.3, a subspace does not have to be an eigenspace of a matrix M in order to be M-invariant. In particular, as we have seen in Theorem 1, the space $\mathbb{F}^t$ can be rewritten as a direct sum decomposition $\mathbb{F}^t = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \cdots \oplus \mathcal{A}_m$, where – among other properties – all subspaces $\mathcal{A}_i$ are M-invariant. Here we generalize the previous result by replacing the eigenspaces of the matrix with the subspaces $\mathcal{A}_i$, which lead us to a necessary and sufficient condition.

Theorem 2. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix that defines the linear layer. A subspace $\mathcal{I}$, where $1 \leq \dim(\mathcal{I}) < t$, generates an infinitely long invariant subspace trail without 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., given $x, y \in \mathbb{F}^t$, $\mathrm{Prob}(R(x) - R(y) \in \mathcal{I} \mid x - y \in \mathcal{I}) = 1$. We use this approach in the entire paper.

The fact that a subspace $\mathcal{I} \subseteq \mathcal{S}^{(1)}$ such that $\mathcal{I} = M \cdot \mathcal{I}$ generates an infinitely long invariant subspace trail without 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 $\mathcal{I}$ without 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 $\mathcal{I} = M \cdot \mathcal{I}$. □

Theorem 3. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix that defines the linear layer. Let $\{\mathcal{A}_1, \ldots, \mathcal{A}_m\}$ be the primary decomposition of $\mathbb{F}^t$ with respect to the matrix M, as defined in Theorem 1, i.e., a collection of M-invariant independent subspaces in $\mathbb{F}^t$ such that $\mathbb{F}^t = \bigoplus_i \mathcal{A}_i$. Let $\{\mathcal{X}_1, \ldots, \mathcal{X}_m\}$ be a collection of subspaces defined as*

$$\mathcal{X}_i := \mathcal{A}_i \cap \langle e_{s+1}, \ldots, e_t \rangle. \tag{4}$$

A subspace $\mathcal{I}$, where $1 \leq \dim(\mathcal{I}) < t$, generates an infinitely long invariant subspace trail without active S-boxes if and only if

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

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

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

Proof. Proving that $\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_m \rangle$ generates an infinitely long invariant subspace trail without active S-boxes is trivial. Indeed, by definition of $\mathcal{P}_i$, no S-box is active (since $\mathcal{P}_i \subseteq \mathcal{X}_i \subseteq \langle e_{s+1}, \dots, e_t \rangle$ for $i \in \{1, \dots, m\}$). 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 without active 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 $\langle e_{s+1}, \dots, e_t \rangle$, since no S-box is active by definition of $\mathcal{I}$. Indeed, if there exists a nontrivial $\mathcal{P}_i$ such that $\mathcal{P}_i \cap \langle e_1, \dots, e_s \rangle \neq \{0\}$, then eventually at least one S-box is active (remember that we are working with differences and that $\mathcal{I}$ generates an infinitely long subspace trail), which contradicts the assumption that no S-box is active. Secondly, note that $\mathcal{P}_i \subseteq \mathcal{A}_i$ is M-invariant. Indeed, if $x \in \mathcal{P}_i$, then $M \cdot x$ belongs to $\mathcal{A}_i$ (since $\mathcal{A}_i$ is M-invariant) and to $\mathcal{I}$ (since it generates an infinitely long subspace trail), which implies that $M \cdot x \in (\mathcal{A}_i \cap \mathcal{I}) = \mathcal{P}_i$. Moreover, $\mathcal{I} = \langle \mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_m \rangle$ since $\mathcal{A}_i \cap \mathcal{A}_j = \{0\}$ for $i \neq j$, and since $\mathbb{F}^t = \bigoplus_i \mathcal{A}_i$.

Finally, $\mathcal{P}_i \subseteq \mathcal{X}_i \cap (M \cdot \mathcal{X}_i)$ 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 4. *Under the assumptions of the previous theorem, let $\mathcal{X}_i^{(0)} := \mathcal{A}_i \cap \langle e_{s+1}, \dots, e_t \rangle$. For $j \geq 1$, we define*

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

Let $l_i \geq 0$ be the smallest (finite) integer such that $\mathcal{X}_i^{(l_i)} = \mathcal{X}_i^{(l_i+1)}$. The biggest M-invariant subspace $\mathcal{P}_i$ of $\mathcal{X}_i$ that satisfies Theorem 3 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 $\dim\left(\mathcal{X}_i^{(j-1)} \cap (M \cdot \mathcal{X}_i^{(j-1)})\right) = \dim(\mathcal{X}_i^{(j-1)})$ if and only if $\mathcal{X}_i^{(j-1)} = \left(M \cdot \mathcal{X}_i^{(j-1)}\right)$, which implies that $\mathcal{X}_i^{(j)} = \mathcal{X}_i^{(j-1)}$. By construction, this is the biggest M-invariant subspace of $\mathcal{A}_i \cap \langle e_{s+1}, \dots, e_t \rangle$.

Finally, note that the index l_i such that $\mathcal{X}_i^{(j)} = \mathcal{X}_i^{(j+1)}$ 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 such that $\mathcal{X}_i^{(j)} = \mathcal{X}_i^{(j+1)} \neq \{0\}$ 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 without active S-boxes presented in Proposition 3 satisfies Theorem 3. The two results are equivalent if the matrix is diagonalizable.*

Proof. The invariant subspace considered in Proposition 3 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 3 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 [GKR+19, GKR+21] (recalled in Section 4.1) for $t = 24$ and $\mathbb{F}_{2^n}$, where $n = 63$. As shown in [KR21, Page 20], the subspace $\mathcal{S}^{(5)}$ defined as in Eq. (3) 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 Without Active S-Boxes

The previous results can be generalized to obtain a necessary and sufficient condition regarding the existence of infinitely long *iterative* subspace trails without active S-boxes.

Proposition 5. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix that defines the linear layer. A subspace $\mathcal{I}$, where $1 \leq \dim(\mathcal{I}) < t$, generates an infinitely long iterative (non-invariant) subspace trail of period $l \geq 2$ without 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, $\mathcal{I} \subseteq \mathcal{S}^{(l)} \cap \left(M^l \cdot \mathcal{S}^{(l)}\right)$.*[5]

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

Proposition 6. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix that defines the linear layer. Let $\{\mathcal{A}_1^{(l)}, \mathcal{A}_2^{(l)}, \ldots, \mathcal{A}_m^{(l)}\}$ be the primary decomposition of $\mathbb{F}^t$ with respect to the matrix M^l, as defined in Theorem 1, that is, a collection of M^l-invariant independent subspaces in $\mathbb{F}^t$ for which $\mathbb{F}^t = \bigoplus_i \mathcal{A}_i^{(l)}$. 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 without 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. □

[5] 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 infinitely long invariant subspace trail, but at the same time there exists an infinitely long iterative subspace trail without active S-boxes. As we are going to show, this is not possible.

Proposition 7. *Consider a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1). An infinitely long iterative subspace trail without active S-boxes can only exist if there exists an infinitely long invariant subspace trail without active S-boxes.*

Proof. As shown in Proposition 1, let $(\mathcal{V}_1, \dots, \mathcal{V}_l)$ be an infinitely long *iterative* subspace trail of period l (without active S-boxes). If $\dim(\langle \mathcal{V}_1, \dots, \mathcal{V}_l \rangle) < t$, then $\langle \mathcal{V}_1, \dots, \mathcal{V}_l \rangle$ generates an infinitely long *invariant* subspace trail. Hence, if $\dim(\langle \mathcal{V}_1, \dots, \mathcal{V}_l \rangle) = t$, it would be possible that an iterative subspace trail without active S-boxes exists and at the same time no invariant subspace trail exists. However, note that $\dim(\langle \mathcal{V}_1, \dots, \mathcal{V}_l \rangle) = t$ can *never* occur in the case without active S-boxes. Indeed, since $\mathcal{V}_i \subseteq \langle e_{s+1}, \dots, e_t \rangle$ for each $i \in \{1, \dots, l\}$ (to guarantee that no S-box is active), it follows that $\langle \mathcal{V}_1, \dots, \mathcal{V}_l \rangle \subseteq \langle e_{s+1}, \dots, e_t \rangle$ can never generate the full space $\mathbb{F}^t$ (indeed, $\langle \mathcal{V}_1, \dots, \mathcal{V}_l \rangle \cap \langle e_1, \dots, e_s \rangle = \{0\}$). □

This does not mean that iterative subspace trails without active S-boxes are useless. Indeed, let $(\mathcal{V}_1, \dots, \mathcal{V}_l)$ be an infinitely long iterative subspace trail of period l without active S-boxes. If $\dim(\mathcal{V}_i) < \dim(\langle \mathcal{V}_1, \dots, \mathcal{V}_l \rangle)$ (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

As a first concrete example, we consider the case of a linear layer defined via a matrix with low multiplicative order.

Definition 12. Let $M \in \mathbb{F}^{t \times t}$ be an invertible matrix. M has a multiplicative order equal to $l \geq 1$ if and only if l is the smallest (positive) integer for which there exists $\mu \in \mathbb{F} \setminus \{0\}$ such that $M^l = \mu \cdot I$, where $I \in \mathbb{F}^{t \times t}$ is the identity matrix.

Proposition 8. *Given a P-SPN scheme over $\mathbb{F}^t$ defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix defining the linear layer. If the multiplicative order of M is l such that $2 \leq l \leq \mathfrak{R}$ (that is, $M^l = \mu \cdot I$ for a certain $\mu \in \mathbb{F} \setminus \{0\}$), where $\mathfrak{R} \geq \left\lfloor \frac{t-s}{s} \right\rfloor$ is defined as in Lemma 2, 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 $\left(\mathcal{S}^{(l)}, M \cdot \mathcal{S}^{(l)}, \dots, M^{l-1} \cdot \mathcal{S}^{(l)}\right)$ is an iterative subspace trail without 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 [GKR+21] – An Example from the Literature. An example has recently been pointed out in [KR21] and [BCD+20]. In these papers, the authors focus on the Cauchy matrix $M \in (\mathbb{F}_{2^n})^{t \times t}$ proposed in [GKR+21] and defined as

$$M_{i,j} = \frac{1}{x_i + x_j + r}, \tag{5}$$

where $x_i = i - 1$ for $i \in \{1, \dots, t\}$ 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$^\pi$ [GKR+21]. In [YMT97, Sect. 3.2] and in [KR21, BCD+20], 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.[6] Hence, the previous result applies perfectly to this case. For the concrete definition of such a subspace we refer to [KR21, Sect. 5.2].

4.2 Linear Layers with Low-Degree Minimal Polynomials

As we have just seen, a matrix M has a low multiplicative order if there exists a small l such that $M^l = \mu \cdot I$, 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

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

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

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 the invertible matrix that defines the linear layer. Let ϕ be the minimal polynomial of M, and let l be its degree. Assume l is "low", namely l satisfies $2 \leq l \leq \mathfrak{R}$ (where $\mathfrak{R} \geq \left\lfloor \frac{t-s}{s} \right\rfloor$ is defined as in Lemma 2). Moreover, let $1 \leq h \leq l$ be a divisor of l (and let $l' \geq 1$ such that $l = l' \cdot h$). Assume that the minimal polynomial is of the form*

$$\phi(x) = x^l + \sum_{i=1}^{l'-1} \alpha_{i \cdot h} \cdot x^{i \cdot h} + \alpha_0, \tag{6}$$

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. (3). If $1 \leq \dim(\mathcal{I}) < t$, $\mathcal{I}$ generates an infinitely long iterative subspace trail of period h (invariant if $h = 1$) without active S-boxes.

Note that the special case $h = l$ corresponds to the one presented in Proposition 8.

Proof. The proof is similar to the one already presented in Proposition 8, 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. (5) 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 9, we see that $l = 6$, $h = 2$, $l' = 3$. An iterative subspace trail can thus be constructed, as also shown in [KR21].

[6] In [BCD+20], 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.

4.2.2 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. (6), that is, $\phi(x) = \sum_{i=0}^{l'} \alpha_{i\cdot h} \cdot x^{i\cdot h}$, and assume $h \geq 2$. 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, then 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 the finite field $\mathbb{F}$ is not algebraically closed, given a zero $\hat{y}$ of ϕ' as before, it is possible that there is no $\hat{x}$ that satisfies $(\hat{x})^h = \hat{y}$, which is related to the existence of 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. Here we exploit these facts in order to present a more generic example of an iterative subspace trail.

Lemma 3. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be the invertible matrix that defines the linear layer. Let $\lambda_1^{(l)}, \ldots, \lambda_\tau^{(l)} \in \mathbb{F}^t$ be the eigenvalues of M^l for some $l \geq 1$, and let $\mathcal{P}_1^{(l)}, \ldots, \mathcal{P}_\tau^{(l)} \subseteq \mathbb{F}^t$ be their corresponding eigenspaces (where $\tau \leq t$). The subspace $\mathcal{I}$ defined as $\mathcal{I} := \left\langle \mathcal{S}^{(l)} \cap \mathcal{P}_1^{(l)}, \mathcal{S}^{(l)} \cap \mathcal{P}_2^{(l)}, \ldots, \mathcal{S}^{(l)} \cap \mathcal{P}_\tau^{(l)} \right\rangle$ 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 8. In particular, it is sufficient to note that no S-box is active due to the definition of $\mathcal{S}^{(l)}$ (see Eq. (3)), 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, or more formally, the condition stated in Lemma 3 implies the condition stated in Proposition 8. Indeed, let $l \geq 2$ be the smallest integer such that $M^l = \mu \cdot I$. Then $e_1, \ldots, e_t$ are all eigenvectors of M^l with eigenvalue μ. Given $\mathcal{S}^{(l)}$ constructed as in Eq. (3) such that no S-box is active in the first l rounds, then $\mathcal{S}^{(l)}$ is an invariant subspace of M^l, since $\langle e_1, \ldots, e_t \rangle$ is an eigenspace of M^l corresponding to the eigenvalue μ. It follows that $\left(\mathcal{S}^{(l)}, M \cdot \mathcal{S}^{(l)}, M^2 \cdot \mathcal{S}^{(l)}, \ldots, M^{l-1} \cdot \mathcal{S}^{(l)}\right)$ is an infinitely long iterative (constant-dimensional) subspace trail.

We remark that the two conditions are not equivalent (that is, the condition stated in Proposition 8 does in general not imply the condition stated in Lemma 3), as shown in the following concrete example.

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

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

and

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

if $a^2+b^2-2ac+c^2-2bd+d^2$ is a quadratic residue modulo p,[7] while the eigenvalues and eigenvectors of M^2 are given by

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

Since $x \mapsto x^2$ is not a permutation over $\mathbb{F}_p$ for any prime $p \geq 3$ (see Hermite's criterion), it is possible that there exist a,b,c,d, such that $a^2+b^2-2ac+c^2-2bd+d^2 = (a-c)^2+(b-d)^2$ is a quadratic non-residue. As a concrete example, by taking $a-c=b-d$, then $(a-c)^2+(b-d)^2 = 2\cdot(a-c)^2$ is not a quadratic residue modulo p if $L_p(2)=-1$ (where $L_p:\mathbb{F}_p \to \{-1,0,1\}$ is the Legendre symbol), which happens if $p = 3,5 \mod 8$ (we refer to [Nag51] for more details). Hence, while M^2 has always four eigenvalues, it is possible that M has only two eigenvalues for certain values of $a,b,c,d \in \mathbb{F}_p$.[8]

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 $s=1$, an example of such a matrix is

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

for particular values of $a,b,c,d,x,y,w,z_j \in \mathbb{F}_p$ such that *(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 $\mathrm{circ}(a,b,c,d)$ 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 $\mu \in \mathbb{F}_p$. Finally, note that M^2 is not necessarily equal to a multiple of the identity. For example, note that $(M^2)_{1,5} \neq 0$, where $\left(M^2\right)_{1,5} = xy_0+y_0a+y_1b+y_0c+y_1d$ is different from 0 by appropriately choosing the entries.

5 Practical Tests (Without Active S-Boxes)

In this section, we first present an algorithm which can be used to find vulnerabilities and to detect weak matrices (with respect to 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 4. 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 nonlinear layer, i.e., $\mathcal{X}_i^{(0)} = \mathcal{A}_i \cap \langle e_{s+1},\ldots,e_t\rangle$. Now we apply Proposition 4 to each of these subspaces $\mathcal{X}_i^{(0)}$, which means reducing the dimensions

[7] By definition, $x \in \mathbb{F}_p$ is a quadratic residue modulo p if $y \in \mathbb{F}_p$ such that $x = y^2$, while it is a quadratic non-residue otherwise.

[8] 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 4.

Data: P-SPN scheme over $\mathbb{F}^t$ with s S-boxes applied to the first s words.
Result: 1 if an invariant infinitely long subspace trail without active S-boxes 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
    $\mathcal{A}_i \leftarrow (M \cdot \mathcal{A}_i \cap \mathcal{A}_i)$.
$\mathcal{I} \leftarrow \langle \mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m \rangle$.
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 without active S-boxes found.*

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 with respect to 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 7 for more details.

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 [Sto98]. 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 $\mathcal{O}(t^3 + t^2) = \mathcal{O}(t^3)$.

Computational Cost in Practice. In our practical runtime tests, we focus on prime fields $\mathbb{F}_p$ for $p \geq 3$ and we use `Sage`. 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).

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.[9] As the source for randomness we use `Sage`'s random engine in both cases (and for choosing

[9] We recall that $M \in \mathbb{F}^{t \times t}$ is a Cauchy matrix if there exists $\{x_i, y_i\}_{i=1}^t$ such that $M_{i,j} = \frac{1}{x_i + y_j}$, 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 1: Percentage of vulnerable matrices for Algorithm 1 and orders t, when considering prime fields $\mathbb{F}_p$.

$\lceil \log_2(p) \rceil$	8	4	6	16	8	12	16	8
t	3	4	4	4	8	8	8	12
Vulnerable (%) *(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

Table 2: Percentage of vulnerable matrices for Algorithm 1 and orders t, when considering binary fields $\mathbb{F}_{2^n}$.

n	8	4	6	16	8	12	16	8
t	3	4	4	4	8	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

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 $\mathbb{F}_{2^n}$ and $\mathbb{F}_p$ with $n \in \{4, 6, 8, 12, 16\}$ and $\lceil \log_2(p) \rceil \in \{4, 6, 8, 12, 16\}$, respectively. Moreover, we tested our algorithm on the concrete matrices used to instantiate Starkad and Poseidon. We present these results in Appendix C.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 used different values for p for each specified range. We can immediately see that the size 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 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.

Assumption on the S-Box. From now on, we only work with S-boxes that do not have any nontrivial linear structures. That is, for an S-box S over $\mathbb{F}$, we assume that it is not possible to find nontrivial subspaces $\mathcal{U}, \mathcal{V} \subset \mathbb{F}$ (that is, $\mathcal{U}, \mathcal{V} \neq \{0\}, \mathbb{F}$) such that *for each*

$u \in \mathbb{F}$ there exists $v \in \mathbb{F}$ such that $S(\mathcal{U} + u) = \mathcal{V} + v$. If the S-box has no nontrivial 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 [LTW18]. 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.

This choice is made both in order to simplify the presentation and since many of the S-boxes used in the literature satisfy this assumption. Note that given an infinitely long subspace trail with probability 1, the following facts hold.

- If the S-box does not have any nontrivial linear structure, then each S-box can either be fully active or fully passive (equivalently, each input of the S-boxes either takes all possible values or is constant).
- If the S-box has a nontrivial linear structure, then it is possible that the input of the S-boxes can take values only in a specific nontrivial affine subspace.

It follows that the infinitely long subspace trails analyzed in the following can be constructed for all possible S-boxes. However, if the S-box has a nontrivial linear structure, then other infinitely long subspace trails may exist as well.

6.1 Preliminary Results: Subspace Trails & 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 10. *Given a partial SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $\mathfrak{R} \geq \left\lfloor \frac{t-s}{s} \right\rfloor$ be the (positive) integer defined as in Lemma 2 (namely, $\dim\left(\mathcal{S}^{(\mathfrak{R})}\right) \geq 1$ and $\dim\left(\mathcal{S}^{(\mathfrak{R}+1)}\right) = 0$). Let $\mathfrak{R} < \infty$ be a finite number. There exists a subspace trail with probability 1 on at least $\mathfrak{R} + \left\lfloor \frac{t-s}{s} \right\rfloor$ rounds, defined by*

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

where $\mathcal{S}^{(i)}$ is defined as in Eq. (3) and where $\mathcal{A}^{(i)} := \left\langle M(e_1), \dots, M(e_s), M \cdot \mathcal{A}^{(i-1)} \right\rangle$ for $i \geq 1$ (where $\mathcal{A}^{(0)} := M^{\mathfrak{R}-1} \cdot \mathcal{S}^{(\mathfrak{R})}$).

As for Lemma 2, this well-known result (whose proof can be found in Appendix A) only depends on the number of S-boxes, and no assumption on the matrix M is made. Like in 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 13. Let $s \in \{1, \dots, t-1\}$ be an integer. Let $\mathcal{V} \subseteq \mathbb{F}^t$ be a subspace and let $I \subseteq \{1, \dots, s\}$. We say that the subspace $\mathcal{V}$ is *I-compatible* if and only if

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

2. $\langle e_{\iota_1}, \ldots, e_{\iota_{|I|}} \rangle \subseteq \mathcal{V}$.

If there exists $I \subseteq \{1, \ldots, s\}$ such that $\mathcal{V}$ is I-compatible, then I is unique, in the sense that $\mathcal{V}$ cannot be J-compatible for any $J \neq I$. At the same time, note that it is possible that there is no I such that $\mathcal{V}$ 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 such that the subspace $\mathcal{V}$ is I-compatible.

Proposition 11. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix defining the linear layer. Let $\lambda_1, \ldots, \lambda_\tau \in \mathbb{F}$ be the eigenvalues of M, and let $\mathcal{P}_1, \ldots, \mathcal{P}_\tau \subseteq F^t$ 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*

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

where $\mathcal{P}'_h$ is a subspace[10] 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 13 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 13 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. Let $\omega \in \{0, 1\}$. Given a P-SPN scheme with $s = 1$, consider the following 4×4 matrix M defined over a field $\mathbb{F}_p$ for $p \geq 3$:

$$M = \begin{pmatrix} \omega & ((1-\omega) - M_{1,3} \cdot b - M_{1,4} \cdot c)/a & M_{1,3} & M_{1,4} \\ a & (-a \cdot \omega - M_{2,3} \cdot b - M_{2,4} \cdot c)/a & M_{2,3} & M_{2,4} \\ b & (-b \cdot \omega - M_{3,3} \cdot b - M_{3,4} \cdot c)/a & M_{3,3} & M_{3,4} \\ c & (-c \cdot \omega - M_{4,3} \cdot b - M_{4,4} \cdot c)/a & M_{4,3} & M_{4,4} \end{pmatrix}, \tag{7}$$

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

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

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.

Lastly, we remark that matrices of the form Eq. (7) 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 [BBI+15] and QARMA[Ava17].

[10] 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 eigenspaces 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 and without active S-boxes.

Theorem 4. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be the invertible matrix that defines the linear layer. Assume that the S-box has no (nontrivial) linear structure. Let $I \subseteq \{1,\dots,s\}$ 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 $I = \{i_1, i_2, \dots, i_{|I|}\}$).

Our approach is based on the strategy proposed for Theorem 3 and Proposition 11. 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 11. 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., $\langle e_{i_1}, e_{i_2}, \dots, e_{i_{|I|}}\rangle \subseteq \mathcal{I}$ and $\mathcal{I} \subseteq \langle e_{i_1}, e_{i_2}, \dots, e_{i_{|I|}}, e_{s+1}, \dots, e_t\rangle$), 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 $x \in \mathcal{I}$ such that $M \cdot x \notin \mathcal{I}$, then $\mathcal{I}$ would not be M-invariant. Moreover, since the subspace trail is M-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[11] 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 $I \subseteq \{1,\dots,s\}$ such that $\mathcal{I}$ is I-compatible. □

As expected, the result presented in Proposition 11 satisfies the previous theorem. This is due to the fact that the subspace $\mathcal{I}$ defined in Proposition 11 is related to the eigenspaces of M, which satisfy the condition $\mathcal{I} = M \cdot \mathcal{I}$. We formulate the following corollary.

Corollary 2. *The infinitely long subspace trail with active S-boxes presented in Proposition 11 satisfies Theorem 4.*

A generalization of Proposition 11 (by replacing the eigenspaces with the generic invariant subspaces of M) is given in the following Theorem.

Theorem 5. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be the invertible matrix that defines the linear layer. Assume that the S-box has no (nontrivial) linear structure. Let $\{\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m\}$ be the primary decomposition of $\mathbb{F}^t$ with respect to 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 $I = \{i_1, \dots, i_{|I|}\} \subseteq \{1, 2, \dots, s\}$ (that is, where

[11] 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

1. *for each $i \in \{1, \ldots, m\}$: $\mathcal{P}_i \subseteq \left(\mathcal{A}_i \cap \langle e_{i_1}, e_{i_2}, \ldots, e_{i_{|I|}}, e_{s+1}, \ldots, e_t \rangle\right)$ is an M-invariant subspace, and*
2. *$\mathcal{I}$ 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 nontrivial 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 without active 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 3. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix that defines the linear layer. Let $\{\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m\}$ be the primary decomposition of $\mathbb{F}^t$ with respect to the matrix M. If there exists $I \subseteq \{1, \ldots, s\}$ and a subspace $\mathcal{A}_i$ such that $\mathcal{A}_i$ 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 without active 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 $p \geq 101$. 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 without active S-boxes exists.

6.4 Infinitely Long Iterative Subspace Trails with Active S-Boxes

Here 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 over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be the invertible matrix that defines the linear layer. Assume that the S-box has no (nontrivial) linear structure. Let $l \geq 1$ be the period of the iterative subspace trail. For each $j \in \{1,2,\ldots,l\}$, let $I_j \subseteq \{1,\ldots,s\}$ 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 $j \in \{0,1,\ldots,l-1\}$;

(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 $\{\mathcal{I}, M\cdot\mathcal{I}, M^2\cdot\mathcal{I}, \ldots, M^{l-1}\cdot\mathcal{I}\}$. Since we assume that the S-box has no (nontrivial) linear structure, such a trail has active S-boxes if and only if the first condition (namely, for each $j \in \{1,2,\ldots,l\}$ there exists I_j such that $M^{j-1}\cdot\mathcal{I}$ 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 over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t\times t}$ be the invertible matrix that defines the linear layer. Assume that the S-box has no (nontrivial) linear structure. Let $l \geq 2$, and let $\{\mathcal{A}_1^{(l)}, \mathcal{A}_2^{(l)}, \ldots, \mathcal{A}_m^{(l)}\}$ be the primary decomposition of $\mathbb{F}^t$ with respect to 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 $I_j = \{i_{1,j}, \ldots, i_{|I_j|,j}\} \subseteq \{1,\ldots,s\}$ in the j-th round (where j is taken modulo l) if and only if

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

where

1. *for each $i \in \{1,\ldots,m\}$: $\mathcal{P}_i \subseteq \left(\mathcal{A}_i^{(l)} \cap \langle e_{i_1,0}, e_{i_2,0}, \ldots, e_{i_{|I_0|,0}}, e_{s+1}, \ldots, e_t\rangle\right)$ is an M^l-invariant subspace, and*

2. *for each $j \in \{0,1,\ldots,l-1\}$: $(M^j\cdot\mathcal{I})$ is I_j-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. (7). The subspace $\mathcal{I} = \langle e_1 = (1,0,0,0)^T \rangle$ generates an infinitely long iterative subspace trail with active S-boxes (of period 2) of the form

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

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 $M = \mathrm{circ}(0,1,1,1)$. Clearly, both $\langle (0,1,1,0)^T \rangle$ and $\langle (0,1,0,1)^T \rangle$ are invariant subspace trails without active S-boxes. As shown before, $\langle (1,0,0,0)^T, (0,1,1,1)^T \rangle$ is an invariant subspace trail with active S-boxes, while $\langle (1,0,0,0)^T \rangle$ 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., $\mathcal{I} = \langle (1,0,0,0)^T, (0,1,1,0)^T, (0,1,0,1)^T \rangle$.

About Iterative Subspace Trails with Active S-Boxes

Due to the results presented in Proposition 7, one may ask if there exist nontrivial 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 without active S-boxes or invariant subspace trails with active S-boxes. For this purpose, 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

$$M = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -2 & 1 \\ 1 & -4 & 2 \end{pmatrix}. \tag{8}$$

The (nontrivial) 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 or without active 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.

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 an (invariant) infinitely long invariant subspace trail with *active* S-boxes is found, 0 otherwise.

foreach $I_s \subseteq \{1, 2, \dots, s\}$ *such that* $|I_s| \geq 1$ *(where* $I_s := \{\iota_1, \dots, \iota_{|I_s|}\}$*)* **do**
  $\mathcal{I} \leftarrow \langle e_{\iota_1}, \dots, e_{\iota_{|I_s|}} \rangle$.
  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*** $\mathcal{I} \cap \langle e_{\iota_1}, \dots, e_{\iota_{|I_s|}}, e_{s+1}, \dots, e_t \rangle \neq \mathcal{I}$ **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.*

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 [LMR15] for the detection of invariant subspace trails and the one proposed in [GLR+20a] for the detection of weak-key subspace trails.

Let us focus on the algorithm proposed in [LMR15]. 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 scheme, 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 [LMR15, Lemma 1] serves as the basis for our algorithms. After 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 an invariant subspace. If this is not the case, they keep increasing the dimension of the subspace until full dimension is reached.

7.2 Algorithms for Detecting "Weak" Matrices

7.2.1 Infinitely Long Invariant Subspace Trails with Active S-Boxes

Our main algorithm is based on the idea proposed in [LMR15] 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 $I_s = \{\iota_1, \dots, \iota_{|I_s|}\}$.

Table 3: Percentage of vulnerable matrices using Algorithm 1, Algorithm 2, Algorithm 3 over prime fields $\mathbb{F}_p^t$. We denote by "Sx" and "Vx" the security and vulnerability w.r.t. 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

2. Now, as in the approach described in [LMR15], we keep increasing the dimension of the subspace until it stabilizes. For this purpose, we keep including $M^j \cdot e_i$ to the space 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 a $j_i \geq 1$ s.t. $M^{j_i+h} \cdot e_i \in \mathcal{I}$ for $h \geq 1$,

$$\mathcal{I} = \left\langle e_{\iota_1}, M \cdot e_{\iota_1}, \ldots, M^j \cdot e_{\iota_1}, \ldots, e_{\iota_{|I|}}, M \cdot e_{\iota_{|I|}}, \ldots, M^j \cdot e_{\iota_{|I|}} \right\rangle \tag{9}$$

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 [LMR15], this quickly becomes too expensive due to the large number of unit vectors in the nonlinear 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 of time – an advantage that is not related to our algorithm, but to the setting we consider.

Table 4: Percentage of vulnerable matrices using Algorithm 1, Algorithm 2, Algorithm 3 over binary fields $\mathbb{F}_{2^n}^t$. We denote by "Sx" and "Vx" the security and vulnerability w.r.t. 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

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, together with `Sage`. 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.

7.2.2 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 in Appendix B.

7.3 Percentage of "Weak" Linear Layers

As in the case of Algorithm 1, we estimate the percentage of "weak" linear layers w.r.t. Algorithm 2 and Algorithm 3. We refer to Section 5.2 for a description about the matrices we used for our tests. Our sample size is 100 000, we focus on the case $s = 1$, and we used different values for p for each specified range. To get a better understanding of the results provided by our algorithms, we made the following distinctions:

(1) matrices which are vulnerable with respect to Algorithm 2,
(2) matrices which are vulnerable with respect to Algorithm 2 and secure with respect to Algorithm 1,
(3) matrices which are vulnerable with respect to Algorithm 3 and secure with respect to Algorithm 2,
(4) matrices which are vulnerable with respect to Algorithm 3 and secure with respect to Algorithm 1 and Algorithm 2.

Table 3 and Table 4 show the results for matrices over $\mathbb{F}_p$ and $\mathbb{F}_{2^n}$ respectively. We can immediately observe 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 with respect to Algorithm 3, but not vulnerable with respect to the other two algorithms (see also Section 6.4). Indeed, for our sample size, the percentage for these matrices is close to zero.

8 Security Against Infinitely Long Subspace Trails

Until now, we presented necessary and sufficient conditions that a (highly nontrivial) linear layer must satisfy in order to prevent the existence of infinitely long subspace trails. Here, we present a sufficient condition on the matrix that defines the linear layer of the P-SPN scheme that – if satisfied – ensures that no infinitely long (invariant/iterative) subspace trail (with/without active S-boxes) exists. Finally, we list some open problems that could be interesting for future research.

8.1 Sufficient Condition for Preventing Infinitely Long Subspace Trails

As a final result, we propose a sufficient condition on the matrix M defining the linear layer of the P-SPN scheme that – if satisfied – ensures that no infinitely long (invariant/iterative) subspace trail (with/without active 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.

In order to reach this goal, we first prove the following result:

Proposition 12. *Let ϕ be the minimal polynomial of an invertible matrix $M \in \mathbb{F}^{t\times t}$. Assume that ϕ is irreducible and let $v \in \mathbb{F}^t \setminus \{0\}$. For each monic polynomial $\phi' \in \mathbb{F}[x]$ such that $\phi'(M) \cdot v = 0$ and $\deg(\phi') \leq \deg(\phi)$, it follows that $\phi' = \phi$.*

Before proving the result, we mention that if ϕ' is a multiple of ϕ, then $\deg(\phi') > \deg(\phi)$ and $\phi'(M) \cdot w = 0$ for each $w \in \mathbb{F}^t$.

Proof. Let $v \in \mathbb{F}^t \setminus \{0\}$ such that $\phi'(M) \cdot v = 0$ for a certain polynomial ϕ' for which $\deg(\phi') < \deg(\phi)$. In such a case, $\{v, M \cdot v, \dots, M^{\deg(\phi)-1} \cdot v\}$ are not linearly independent. In particular, the subspace $\mathcal{V} = \langle v, M \cdot v, \dots, M^{\deg(\phi')-1} \cdot v \rangle$ is a proper M-invariant subspace of $\mathbb{F}^t$. Due to [Kai08, Prop. 2], we have that $\phi\big|_{\mathcal{V}} = \phi'$ divides ϕ. However, this is not possible, since ϕ is irreducible. It follows that each monic polynomial $\phi' \in \mathbb{F}[x]$ such that $\phi'(M) \cdot v = 0$ and $\deg(\phi') \leq \deg(\phi)$ has the same degree as ϕ.

Next, we have to prove that $\phi' = \phi$. As before, let $v \in \mathbb{F}^t \setminus \{0\}$ such that $\phi'(M) \cdot v = 0$ 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 $\{v, M \cdot v, \dots, M^d \cdot v\}$ 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 $\{v, M \cdot v, \dots, M^{d-1} \cdot v\}$ that is equal to zero.[12] Thus, there also exists a polynomial ϕ'' of degree strictly less than d for which $\phi''(M) \cdot v = 0$. Such a polynomial is a nontrivial divisor of ϕ, which leads to a contradiction. □

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

Proposition 13. *Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix that defines the linear layer. Assume that the S-box has no (nontrivial) linear structure. If the minimal polynomial ϕ of M has maximum degree t and is irreducible, there is no infinitely long invariant subspace trail with/without active S-boxes.*

Proof. Due to Proposition 12 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 nontrivial subspace of $\mathbb{F}^t$ that is M-invariant. Indeed, if $\mathcal{S}$ is an 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 nontrivial subspace $\mathcal{S}$ in $\mathbb{F}^t$ that generates an infinitely long invariant subspace trail both in the case with and without active S-boxes (under the assumption that the S-box has no nontrivial 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. (8), 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 nontrivial linear structure), we propose the following result.

Theorem 8. *Let $l \geq 1$. Given a P-SPN scheme over $\mathbb{F}^t$ with s S-boxes defined as in Eq. (1), let $M \in \mathbb{F}^{t \times t}$ be the invertible matrix that defines the linear layer. Assume that the S-box has no (nontrivial) linear structure. If all the minimal polynomials of $M, M^2, \dots, M^l$ are of maximum degree t and irreducible, then there is no infinitely long subspace trail with/without 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 an l-round invariant subspace trail.

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

Table 5: Percentages of Cauchy MDS matrices fulfilling the requirement in Proposition 13.

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 (%)	≥ 33.75	≥ 18.93	≥ 24.96	≥ 25.42	≥ 12.22	≥ 12.34	≥ 12.78	≥ 8.73

Discussion. Lastly, one may ask how many matrices satisfy the required property just given. Assume an irreducible polynomial $\phi \in \mathbb{F}[x]$ of degree t. Working with matrices over $\mathbb{F}_q^{t \times t}$, it is always possible to associate a companion matrix C to such a minimal polynomial, as given in Definition 10 (the characteristic polynomial and the minimal polynomial are equal in this case). Hence, 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 13 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 13. The results are shown in Table 5. For each of the tests, we set the sample size to 10 000. It is possible to observe that increasing the state size leads to a lower probability of the matrix to satisfy the condition given in Proposition 13. 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 provide 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.

- The goal of this work is to guarantee that the choice of the matrix M prevents *infinitely long* subspace trails. As a next step, given a matrix for which no infinitely long subspace trail exists, one may ask how many rounds are needed in order to activate at least one S-box. In our practical tests regarding this issue, and when focusing on $s = 1$, we observed that $t + \varepsilon$ rounds for $\varepsilon \in \{0, 1\}$ are in general sufficient with high probability. We leave the open problem to find an upper bound on the number of rounds needed for reaching this goal that depends both on *(1)* the details of the matrix defining the scheme and *(2)* the number of S-boxes per round.

- If the analyzed S-box has a nontrivial linear structure (namely, there exist nontrivial linear structures $\mathcal{U}, \mathcal{V}$ such that for each u there exists a certain v such that $S(\mathcal{U}+u) = \mathcal{V} + v$), then it is potentially possible to extend the result given in this paper for the case of active S-boxes in order to include this case as well.

- Here, we only considered the case of linear layers defined as invertible matrices over $\mathbb{F}_q^{t \times t}$. In the binary case (i.e., $q = 2^n$), it could be interesting to extend our results to the case in which the linear layer M is defined as

$$(M(x))[i] = \sum_{j=1}^{t} L_{i,j}(x[j]), \quad \text{where} \quad L_{i,j}(z) = \sum_{h=0}^{n-1} \lambda_h^{(i,j)} \cdot z^{2^h}$$

are linearized polynomials (which can be efficiently computed over a binary field) and where $z \in \mathbb{F}$.

Acknowledgments

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. The authors also thank Christof Beierle for shepherding this final version of the paper. 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

[AAB+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols. *IACR Trans. Symmetric Cryptol.*, 2020(3):1–45, 2020.

[AÅBL12] Mohamed Ahmed Abdelraheem, Martin Ågren, Peter Beelen, and Gregor Leander. On the Distribution of Linear Biases: Three Instructive Examples. In *CRYPTO 2012*, volume 7417 of *LNCS*, pages 50–67, 2012.

[AD18] Tomer Ashur and Siemen Dhooghe. MARVELlous: a STARK-Friendly Family of Cryptographic Primitives. Cryptology ePrint Archive, Report 2018/1098, 2018.

[AGP+19] Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger. Feistel Structures for MPC, and More. In *Computer Security - ESORICS 2019*, volume 11736 of *LNCS*, pages 151–171, 2019.

[AGR+16] Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity. In *ASIACRYPT 2016*, volume 10031 of *LNCS*, pages 191–219, 2016.

[ARS+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. Ciphers for MPC and FHE. In *EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 430–454, 2015.

[Ava17] Roberto Avanzi. 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.

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A Block Cipher for Low Energy. In *ASIACRYPT 2015*, volume 9453 of *LNCS*, pages 411–436, 2015.

[BCD+20] Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, and Friedrich Wiemer. Out of Oddity - New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems. In *CRYPTO 2020*, volume 12172 of *LNCS*, pages 299–328, 2020.

[BCDM20] Tim Beyne, Yu Long Chen, Christoph Dobraunig, and Bart Mennink. Dumbo, Jumbo, and Delirium: Parallel Authenticated Encryption for the Lightweight Circus. *IACR Trans. Symmetric Cryptol.*, 2020(S1):5–30, 2020.

[BCLR17] Christof Beierle, Anne Canteaut, Gregor Leander, and Yann Rotella. Proving Resistance Against Invariant Attacks: How to Choose the Round Constants. In *CRYPTO 2017*, volume 10402 of *LNCS*, pages 647–678, 2017.

[BDD+15] Achiya Bar-On, Itai Dinur, Orr Dunkelman, Virginie Lallemand, Nathan Keller, and Boaz Tsaban. Cryptanalysis of SP Networks with Partial Non-Linear Layers. In *EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 315–342, 2015.

[Bey18] Tim Beyne. Block Cipher Invariants as Eigenvectors of Correlation Matrices. In *ASIACRYPT 2018*, volume 11272 of *LNCS*, pages 3–31, 2018.

[BJK+16a] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In *Advances in Cryptology - CRYPTO 2016*, volume 9815 of *LNCS*, pages 123–153, 2016.

[BJK+16b] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS. Cryptology ePrint Archive, Report 2016/660, 2016. https://eprint.iacr.org/2016/660.

[BLN17] Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential-Linear Cryptanalysis Revisited. *Journal of Cryptology*, 30(3):859–888, 2017.

[BS91] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[BS93] Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer, 1993.

[CCF+18] Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression. *J. Cryptology*, 31(3):885–916, 2018.

[DEG+18] Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Eik List, Florian Mendel, and Christian Rechberger. Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit. In *CRYPTO 2018*, volume 10991 of *LNCS*, pages 662–692, 2018.

[DEMS19] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. ASCON v1.2. NIST Lightweight Cryptography Finalist (2021), CAESAR Finalist, 2019.

[DGGK19] Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters. Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields. In *EUROCRYPT 2021*, LNCS, 2019.

[DKP+19] Itai Dinur, Daniel Kales, Angela Promitzer, Sebastian Ramacher, and Christian Rechberger. Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC. In *EUROCRYPT 2019*, volume 11476 of *LNCS*, pages 343–372, 2019.

[DLMW15] Itai Dinur, Yunwen Liu, Willi Meier, and Qingju Wang. Optimized Interpolation Attacks on LowMC. In *ASIACRYPT 2015*, volume 9453 of *LNCS*, pages 535–560, 2015.

[DPAR00] Joan Daemen, Michaël Peeters, Gilles Van Assche, and Vincent Rijmen. Nessie Proposal: NOEKEON, 2000.

[DR02] Joan Daemen and Vincent Rijmen. AES and the Wide Trail Design Strategy. In *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 108–109, 2002.

[GGNPS13] B. Gérard, Vincent Grosso, M. Naya-Plasencia, and François-Xavier Standaert. Block Ciphers That Are Easier to Mask: How Far Can We Go? In *Cryptographic Hardware and Embedded Systems - CHES 2013*, volume 8086 of *LNCS*, pages 383–399, 2013.

[GKR+19] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. Cryptology ePrint Archive, Report 2019/458, 2019.

[GKR+21] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 2021.

[GLR+20a] Lorenzo Grassi, Gregor Leander, Christian Rechberger, Cihangir Tezcan, and Friedrich Wiemer. Weak-Key Distinguishers for AES. In *SAC*, LNCS. Springer, 2020.

[GLR+20b] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy. In *EUROCRYPT*, volume 12106 of *LNCS*, pages 674–704, 2020.

[GLSV14] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici. LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations. In *Fast Software Encryption - FSE 2014*, volume 8540 of *LNCS*, pages 18–37, 2014.

[GRR16a] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace Trail Cryptanalysis and its Applications to AES. *IACR Trans. Symmetric Cryptol.*, 2016(2):192–225, 2016.

[GRR+16b] Lorenzo Grassi, Christian Rechberger, Dragos Rotaru, Peter Scholl, and Nigel P. Smart. MPC-Friendly Symmetric Key Primitives. In *ACM SIGSAC Conference on Computer and Communications Security – 2016*, pages 430–443. ACM, 2016.

[GRR17] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. A new structural-differential property of 5-round AES. In *EUROCRYPT 2017*, volume 10211 of *LNCS*, pages 289–317, 2017.

[HL20] Phil Hebborn and Gregor Leander. Dasta - Alternative Linear Layer for Rasta. *IACR Trans. Symmetric Cryptol.*, 2020(3):46–86, 2020.

[Hog16] Leslie Hogben. *Handbook of Linear Algebra*. CRC Press, 2nd edition, 2016.

[Kai08] Klaus Kaiser. Advanced Linear Algebra. https://www.math.uh.edu/~klaus/Advanced%20Linear%20Algebra_rev.pdf, 2008.

[Knu94] Lars R. Knudsen. Truncated and Higher Order Differentials. In *Fast Software Encryption – FSE 1994*, volume 1008 of *LNCS*, pages 196–211, 1994.

[KPP+17] Daniel Kales, Léo Perrin, Angela Promitzer, Sebastian Ramacher, and Christian Rechberger. Improvements to the Linear Layer of LowMC: A Faster Picnic. Cryptology ePrint Archive, Report 2017/1148, 2017.

[KR21] Nathan Keller and Asaf Rosemarin. Mind the Middle Layer: The HADES Design Strategy Revisited. In *EUROCRYPT 2021*, LNCS. Springer, 2021.

[LAAZ11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In *CRYPTO 2011*, volume 6841 of *LNCS*, pages 206–221, 2011.

[LMR15] Gregor Leander, Brice Minaud, and Sondre Rønjom. A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In *EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 254–283, 2015.

[LTW18] Gregor Leander, Cihangir Tezcan, and Friedrich Wiemer. Searching for Subspace Trails and Truncated Differentials. *IACR Trans. Symmetric Cryptol.*, 2018(1):74–100, 2018.

[Mat93] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In *EUROCRYPT 1993*, volume 765 of *LNCS*, pages 386–397, 1993.

[MJSC16] Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. In *EUROCRYPT 2016*, volume 9665 of *LNCS*, pages 311–343, 2016.

[Nag51] T. Nagell. Euler's Criterion and Legendre's Symbol. Introduction to Number Theory, 1951.

[PRC12] Gilles Piret, Thomas Roche, and Claude Carlet. PICARO - A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance. In *Applied Cryptography and Network Security - ACNS 2012*, volume 7341 of *LNCS*, pages 311–328, 2012.

[PW20] Thomas Peyrin and Haoyang Wang. The MALICIOUS Framework: Embedding Backdoors into Tweakable Block Ciphers. In *CRYPTO 2020*, volume 12172 of *LNCS*, pages 249–278, 2020.

[Sto98] Arne Storjohann. An $O(n^3)$ algorithm for the frobenius normal form. In *ISSAC*, pages 101–105. ACM, 1998.

[TLS16] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64. In *ASIACRYPT 2016*, volume 10032 of *LNCS*, pages 3–33, 2016.

[WWGY14] Yanfeng Wang, Wenling Wu, Zhiyuan Guo, and Xiaoli Yu. Differential Cryptanalysis and Linear Distinguisher of Full-Round Zorro. In *ACNS 2014*, volume 8479 of *LNCS*, pages 308–323, 2014.

[YMT97] A. M. Youssef, S. Mister, and S. E. Tavares. On the Design of Linear Transformations for Substitution Permutation Encryption Networks. In *Selected Areas in Cryptography - SAC 1996*, pages 40–48, 1997.

A Truncated Differentials and Subspace Trails

Differential attacks [BS91] exploit the fact that pairs of inputs with certain differences yield other differences in the corresponding outputs 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 [Knu94], in which the attacker can predict only part of the difference between pairs of texts. Using the subspace terminology, given pairs of inputs that belong to the same coset of a subspace $\mathcal{X}$, one considers the probability that the corresponding outputs belong to the same coset of a subspace $\mathcal{Y}$ to set up an attack (see e.g. [BLN17] for details). In particular, note that two texts $x, y \in \mathbb{F}^t$ are in the same coset of a given subspace (i.e., there exists $v \in \mathbb{F}^t$ such that $x, y \in \mathcal{V} + v$) if and only if their difference belongs to such a subspace (i.e., $x - y \in \mathcal{V}$). The relation between truncated differential trails and subspace trails has been studied in details in [LTW18, BLN17].

Proof of Proposition 10

As done before, in the following we omit the round keys and the constant additions (we recall that they only change the cosets, while here we deal with differences).

The subspace trail defined over the first $\mathfrak{R}$ rounds is already analyzed in Section 3.1. By definition of $\mathfrak{R}$, at least one S-box is active after $\mathfrak{R}$ rounds. It follows that the only way to extend the trail is by increasing the dimension of such a subspace, that is,

$$R\left(M^{\mathfrak{R}-1} \cdot \mathcal{S}^{(\mathfrak{R})}\right) \subseteq \mathcal{A}^{(1)} = \left\langle M^{\mathfrak{R}} \cdot \mathcal{S}^{(\mathfrak{R})}, M(e_1), \ldots, M(e_s) \right\rangle.$$

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

$$\text{S-box}\left(M^{(\mathfrak{R})} \cdot \mathcal{S}^{(\mathfrak{R})}\right) \subseteq \Big\langle \underbrace{e_1, e_2, \ldots, e_s}_{\text{Due to S-boxes}}, \quad \underbrace{M^{\mathfrak{R}} \cdot \mathcal{S}^{(\mathfrak{R})}}_{\text{Due to identity part}} \quad \Big\rangle.$$

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

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

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

Remark. Due to the relation between subspace trails and truncated differentials [LTW18] mentioned before, it is possible to set up a truncated differential distinguisher on at least $\mathfrak{R} + \left\lfloor \frac{t-s}{s} \right\rfloor$ rounds with probability 1. 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, $\mathfrak{R} + \left\lfloor \frac{t-s}{s} \right\rfloor$ 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. Hence, 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.

B Infinitely Long Iterative Subspace Trails with Active S-Boxes

In this section, we give the algorithm using the results described in Section 7.2.2 for a maximum period of $l = 2t$.

Algorithm 3: Determining the existence of (iterative) infinitely long subspace trails with *active* S-boxes of period at most $l \geq 2$ based on [LMR15] 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.*

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 $\mathcal{O}(ls\,(2^s t + l))$, 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.

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

C.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 [GKR+21]. 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

$$M'_{i,j} = \frac{1}{x_i \oplus y_j} \qquad \text{and} \qquad M''_{i,j} = \frac{1}{x_i + y_j}, \tag{10}$$

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

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

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 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 [KR21, BCD+20]. Moreover, in [KR21] the authors explain how to modify the choice of x_i and y_j in Eq. (10) 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 [KR21]. As expected, we arrive at the same conclusion, namely, that it is not possible to set up infinitely long subspace trails without active S-boxes for the Cauchy matrices proposed in [KR21].

C.2 Zorro Matrix

We also evaluated the Zorro [GGNPS13] 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 scheme 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, neither with nor without active S-boxes.[13]

[13] We recall that the statistical attacks on Zorro [WWGY14] exploit the existence of differentials with a probability higher than what was expected by the designers, and not the existence of infinitely long subspace trails.