Journal of Algebra and Its Applications
(2023) 2350233 (18 pages)

DOI: 10.1142/S021949882350233X

On the primitivity of the AES-128 key-schedule

Riccardo Aragona* and Roberto Civino†
DISIM, Università degli Studi dell'Aquila
via Vetoio, 67100 Coppito (AQ), Italy
DISIM, Università degli Studi dell'Aquila
via Vetoio, 67100 Coppito (AQ), Italy
**riccardo.aragona@univaq.it*
†*roberto.civino@univaq.it*

Francesca Dalla Volta
Dipartimento di Matematica e Applicazioni
Università degli studi di Milano - Bicocca
Piazza dell'Ateneo Nuovo, 1, 20126 Milano (MI), Italy
francesca.dallavolta@unimib.it

Please check that title, author's names, affiliations & keywords are correct.

Received 21 March 2022
Revised 16 June 2022
Accepted 21 June 2022
Published

Communicated by

AQ: Please provide communicated by details

The key-scheduling algorithm in the AES is the component responsible for selecting from the master key the sequence of round keys to be xor-ed to the partially encrypted state at each iteration. We consider here the group Γ generated by the action of the AES-128 key-scheduling operation, and we prove that the smallest group containing Γ and all the translations of the message space is primitive. As a consequence, we obtain that no linear partition of the message space can be invariant under its action.

Keywords: Primitive groups; cryptography; group generated by the round functions; AES; key schedule; invariant partitions.

Mathematics Subject Classification: 20B15, 20B35, 94A60

1. Introduction

The encryption functions of the AES are the composition of a sequence of round transformations made by a confusion and a diffusion layer followed by a key addition with the so-called round key, derived by the user master key by means of the public key-scheduling algorithm. While the confusion-diffusion step has been designed to provide long-term resistance against known and possibly future attack, the key-schedule has been chosen also without neglecting the application of the

Please indicate corresponding author.

cipher in resource-constrained devices. The necessary efforts to keep the encryption lighter [16] made *de facto* the confusion-diffusion step almost completely in charge of the security. Although some recent improvements in the AES cryptanalysis are based on structural properties of the SPN design (e.g. [26, 9, 15]), unsurprisingly, also the key-schedule has been targeted in various attacks in recent years [7, 23, 8]. In general, key-scheduling algorithms appear to be the component on which there is the least consensus on general design criteria and arguably the components for which attacks are less standardized.

Despite two decades of cryptanalysis, only recently Leurent and Pernot showed the existence of an invariant subspace for four rounds of the AES-128 key-schedule [22]. Such a finding allowed the authors to provide an alternative representation of the key-schedule as four independent actions on each of the 4-byte-word components of the round key. Although related only to the key-schedule, the result is then used to obtain global improvements in already known differential attacks, showing how the subspace analysis of the key-schedule may highlight some subspace structures that interact with similar structures in the main round function inducing security flaws.

Initially, the more general idea of finding subspaces which are invariant under the encryption functions, for some or possibly all the keys, has been notably exploited by Leander *et al.* to cryptanalyze PRINTcipher [20]. The above-mentioned strategy makes use of the fact that an entire subspace of the message space (or of the key space) is not moved by the encryption functions. Subspace trail cryptanalysis [19], a generalization of invariant subspace cryptanalysis, has been also used to attack reduced-round AES [18].

The imprimitivity attack, introduced by Paterson against an intentionally flawed but apparently secure DES-like block cipher [25], is conceptually similar to invariant subspaces attacks, except it exploits the existence of a full *partition* of the message space that is preserved by the encryption. In particular, in this attack scenario, the cryptanalyst usually takes advantage of an entire *linear partition* of the message space, i.e. a partition made by the cosets of a proper and non-trivial subspace, which is invariant. While it is hard in general to prove the non-existence of invariant subspaces (see [6] for an analysis of the security impact provided by the choice of the round constants), the non-existence of invariant linear partitions after one round can be more easily established using group-theoretical arguments, i.e. proving that a given group containing the encryption functions acts primitively on the message space.

Non-existence results for invariant partitions in standardized constructions have been proved in the last years [29, 27, 28, 4], and more general results determining conditions which imply the non-existence of invariant linear partitions obtained by primitivity arguments can be found in the literature [14, 5].

In this work, we prove a *primitivity* result on the AES-128 key-schedule (see Theorem 3.1 and Corollary 3.4), i.e. we show that no linear partition can be invariant after one round, when each possible vector is considered as round counter.

The strategy used here is the following: the action of the key-schedule is modeled by means of a formal operator defining a group which is proved to be primitive using Goursat's lemma (cf. Theorem 4.1). In particular, we prove that the group generated by the action of the AES-128 key-schedule is primitive provided that a suitable considerably smaller group generated by some AES-128 components is primitive, a result which can be established using known facts [14, 5]. As a consequence, our result can be generalized to each substitution-permutation network whose round components are suitable for generating a primitive group [14] and whose 4-branch AES-like key-schedule is built accordingly. To our knowledge, with respect to invariant partitions, the study carried out in this paper is the first example of group-theoretical investigation of the sole key-schedule, which is in general excluded from primitivity arguments, except for some recent partial results [3, 11].

Related works. In this paper, we use the strategy of a *primitivity reduction* via Goursat's lemma. We show indeed that the primitivity of a complex structure, such as the 4-branch key-schedule transformations of AES, is inherited from the primitivity of the group generated by simpler SPN-like functions, i.e. those acting on the last group of bytes. Similar arguments have been used to prove that the primitivity of other more complex structures (e.g. Feistel networks, Lai-Massey constructions) reduces to the primitivity of their inner SPN-like components [2, 1].

AQ: Please provide section number.

This paper is arranged as follows. In Sec. 2, we introduce the notation and the preliminary results, and present an algebraic representation of the AES-128 key-schedule and the related permutation group. In Sec. 3, we present our primitivity reduction in Theorem 3.1 and show its application to AES in Corollary 3.4. The technical proof of Theorem 3.1 with the use of Goursat's lemma is shown in Sec. 4. Finally, in Sec. 5, we draw our conclusions.

2. Preliminaries and Model

In this section, we introduce some notation and preliminary results, starting by briefly recalling the definition of the AES-128 key-schedule. The reader is invited to refer to Daemen and Rijmen for a detailed description including comments on design choices [16].

The AES-128 key-schedule is an invertible function of $\mathrm{Sym}(\mathbb{F}_2^{128})$ which, using the cipher's components, transforms the previous round key into the next one, starting from the master key, proceeding as shown in Fig. 1, where

— $\lambda : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$ denotes the linear operation `RotWord`,
— $\gamma : \mathbb{F}_2^{8} \to \mathbb{F}_2^{8}$ represents the AES S-Box `SubBytes`,
— $rc_i \in \mathbb{F}_2^{8}$ is a round constant different in each round.

In particular, round-key bits are gathered into four groups, each consisting of 4 bytes. The bytes of the last group are first shifted left by one position and then transformed by the cipher's S-Box. Finally, a round-dependent counter is xor-ed to

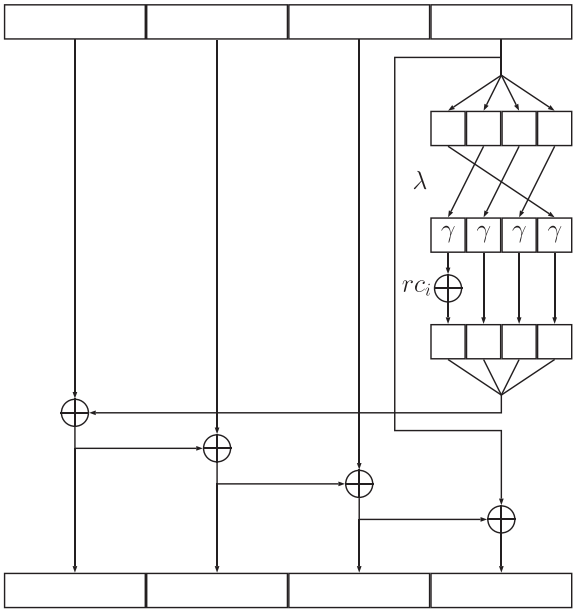

Fig. 1. The ith transformation of the AES-128 key-schedule.

the first byte of the last block. The output of this transformation is then xor-ed to the remaining three blocks of bytes, as shown in Fig. 1.

Notation. In the following, n is a non-negative integer and $V \stackrel{\text{def}}{=} \mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$. If H is a subspace of V we write $H \leq V$, and the same notation is used to denote subgroups. We denote by $\mathbb{0} : V \to V$ the null function on V. Moreover, $\mathrm{Sym}(V)$ denotes the symmetric group acting on V and $\mathbb{1}$ its identity. If $f \in \mathrm{Sym}(V)$ and $x \in V$ we write xf to denote the functional evaluation $f(x)$. The group of the translations on V, i.e. the group of the maps $\sigma_v : V \to V$, such that $x \mapsto x + v$, is denoted by T_n. We also denote by $\mathrm{AGL}(V)$ the group of all affine permutations of V and by $\mathrm{GL}(V)$ the group of the linear ones. In particular, in the case under investigation, we mean by n the size of each group of 4 bytes, i.e. $n = 32$ bits. Under this assumption, the key-scheduling transformation will be acting on V^4 as an element of the symmetric group $\mathrm{Sym}(V^4)$, whose corresponding group of translations is denoted by T_{4n}, where the translation $\sigma_{(v_1,v_2,v_3,v_4)}$ acts on $(x_1, x_2, x_3, x_4) \in V^4$ as

$$(x_1, x_2, x_3, x_4) \mapsto (v_1 + x_1, v_2 + x_2, v_3 + x_3, v_4 + x_4).$$

It is worth noting here that the addition with the round counter in the AES-128 key-schedule acts exactly as a particular translation of T_{4n}.

For sake of clarity, we will use different notations for elements of V, V^2 and V^4. In particular, we will denote an element of V^4 by superscripting an arrow on the symbol, i.e. $\vec{v} \in V^4$, an element of V^2 using symbols in bold, i.e. $\vec{v} = (\boldsymbol{v_1}, \boldsymbol{v_2})$, in

such a way

$$\vec{v} = (\boldsymbol{v_1}, \boldsymbol{v_2}) = (v_1, v_2, v_3, v_4) \in V^4,$$

where $\boldsymbol{v_i} \in V^2$ and $v_j \in V$ for $1 \leq i \leq 2$ and $1 \leq j \leq 4$.

Let us now introduce the elements of group theory used throughout this paper.

Groups. Let G be a group acting on a set M. For each $g \in G$ and $v \in M$ we denote the action of g on v as vg. The group G is said to be *transitive* on M if for each $v, w \in M$ there exists $g \in G$ such that $vg = w$. A partition $\mathcal{B}$ of M is *trivial* if $\mathcal{B} = \{M\}$ or $\mathcal{B} = \{\{v\} \mid v \in M\}$, and G*-invariant* if for any $B \in \mathcal{B}$ and $g \in G$ it holds $Bg \in \mathcal{B}$. Any non-trivial and G-invariant partition $\mathcal{B}$ of M is called a *block system* for G. In particular any $B \in \mathcal{B}$ is called an *imprimitivity block*. The group G is *primitive* in its action on M (or G *acts primitively* on M) if G is transitive and there exists no block system. Otherwise, the group G is *imprimitive* in its action on M (or G *acts imprimitively* on M). We recall here some well-known results that will be useful in the remainder of this paper [12].

Lemma 2.1. *If $T \leq G$ is transitive, then a block system for G is also a block system for T.*

In the case under consideration in this paper, the block system will be a *linear partition*.

Lemma 2.2. *Let M be a finite vector space over $\mathbb{F}_2$ and T its translation group. Then T is transitive and imprimitive on M. A block system $\mathcal{U}$ for T is composed by the cosets of a non-trivial and proper subgroup $U < (M, +)$, i.e.*

$$\mathcal{U} = \{U + v \,|\, v \in M\}.$$

The key-schedule representation. Let us now introduce the representation of the AES-128 key-schedule that allows us to provide an easy description of the subgroup of $\mathrm{Sym}(V^4)$ which is the subject of this work. Let us start by defining the transformation acting on the last group of four bytes, as in Fig 1.

Definition 2.3. Let $\rho_{\mathrm{AES}} \in \mathrm{Sym}(V)$ be the composition of λ and the parallel application of 4 copies of γ, i.e.

$$\rho_{\mathrm{AES}} \stackrel{\mathrm{def}}{=} \lambda\gamma' \in \mathrm{Sym}(V),$$

where $\gamma' : \mathbb{F}_2^{32} \mapsto \mathbb{F}_2^{32}$, $(v_1, v_2, v_3, v_4) \mapsto (v_1\gamma, v_2\gamma, v_3\gamma, v_4\gamma)$, with $v_i \in \mathbb{F}_2^8$.

The function previously defined, up to the xor with the round counter in the first byte, represents the transformation acting on the last group of bytes in the AES-128 key-schedule. The following definition is instead a more general description of the full transformation.

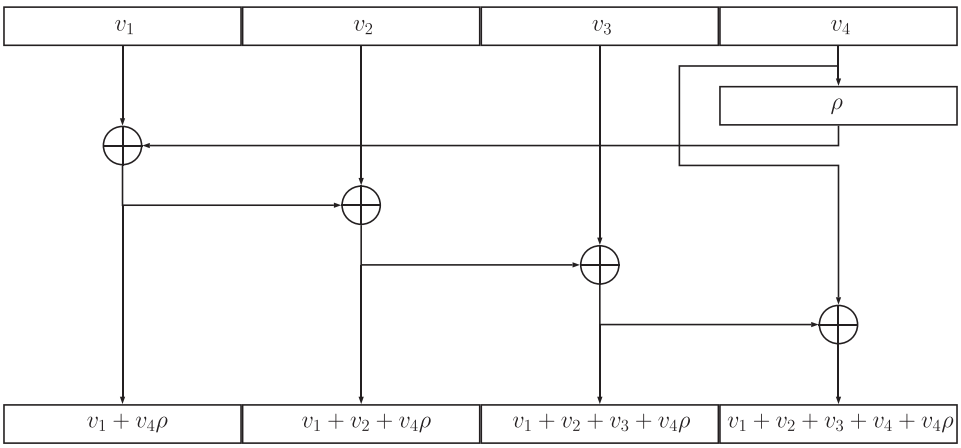

Fig. 2. The key-schedule operator induced by ρ.

Definition 2.4. Given $\rho \in \mathrm{Sym}(V)$, let us define the *AES-like key-schedule operator induced by* ρ as the formal matrix

$$\overline{\rho} \stackrel{\text{def}}{=} \begin{pmatrix} \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ \mathbb{0} & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ \mathbb{0} & \mathbb{0} & \mathbb{1} & \mathbb{1} \\ \rho & \rho & \rho & \mathbb{1}+\rho \end{pmatrix},$$

acting on V^4 as

$$(v_1, v_2, v_3, v_4) \mapsto (v_1 + v_4\rho, v_1 + v_2 + v_4\rho, v_1 + v_2 + v_3 + v_4\rho, v_1 + v_2 + v_3 + v_4 + v_4\rho),$$

as also displayed in Fig. 2. The operator $\overline{\rho}$ has the following inverse acting as

$$(v_1, v_2, v_3, v_4)\overline{\rho}^{-1} = (v_1 + (v_3 + v_4)\rho, v_1 + v_2, v_2 + v_3, v_3 + v_4).$$

It is not hard to notice, when considering ρ_{AES}, that the map

$$\overline{\rho_{\mathrm{AES}}}\sigma_{(\overline{rc_i},\overline{rc_i},\overline{rc_i},\overline{rc_i})},$$

correspond to the ith round-key transformation in the AES-128 key-schedule, where $\overline{rc_i} = (rc_i, 0, 0, 0) \in \mathbb{F}_2^{32}$. Keeping in mind that our focus is to study group-theoretical properties of the subgroup $\Gamma < \mathrm{Sym}(V^4)$ generated by the elements of the type of $\overline{\rho_{\mathrm{AES}}}\sigma_{(\overline{rc_i},\overline{rc_i},\overline{rc_i},\overline{rc_i})}$, for each admissible value of $rc_i \in \mathbb{F}_2^8$, and establish its primitivity by using Lemma 2.2, it is important to notice that Γ does not contain the whole translation group T_{128}. For this reason, Γ needs to be extended by assuming a more general action of the round counter.

Definition 2.5. Let us define the group

$$\Gamma_{\mathrm{AES}} \stackrel{\mathrm{def}}{=} \left\langle \overline{\rho_{\mathrm{AES}}}\sigma_{(x,y,z,t)} \mid (x,y,z,t) \in V^4 \right\rangle .$$

It is easily noticed that

— Γ_{AES}, which contains Γ, is the smallest subgroup of the symmetric group containing both T_{128} and the transformation of the AES-128 key-schedule, when the correct round counter is chosen;
— $\Gamma_{\mathrm{AES}} = \langle \overline{\rho_{\mathrm{AES}}}, T_{128} \rangle$.

In the remainder we prove that Γ_{AES} is primitive. This guarantees that no nontrivial and proper subgroup $U < V^4$ can generate a partition, as in Lemma 2.2, which is invariant under the transformations of Γ_{AES}.

3. The Primitivity of Γ_{AES}

In this section, we prove our main result, i.e. the primitivity of Γ_{AES} (cf. Corollary 3.4), as a consequence of a more general result (cf. Theorem 3.1) in which we show that the primitivity of $\langle \overline{\rho}, T_{4n} \rangle$ *reduces* to the primitivity of $\langle \rho, T_n \rangle$, when $\overline{\rho}$ is the key-schedule operator induced by ρ (cf. Definition 2.4) and provided that ρ is bijective and not affine. The proof of the primitivity reduction is rather technical and makes use of repeated applications of Goursat's lemma (see Sec. 4) so, for the sake of readability, is shown in a separate section.

We can anticipate our main contribution which is stated as follows:

Theorem 3.1 (Primitivity reduction). *Let $\rho \in \mathrm{Sym}(V) \setminus \mathrm{AGL}(V)$. If $\langle \rho, T_n \rangle$ is primitive on V, then $\langle \overline{\rho}, T_{4n} \rangle$ is primitive on V^4.*

Proof. See Sec. 4. □

According to the previous fact, the primitivity of the AES-128 key-schedule can be deduced by the primitivity of the group generated by ρ_{AES} and T_{32}, i.e. by the composition of the linear transformation `RotWord` and the parallel application of 4 copies of the S-Box `SubBytes` and by the translations on the space of 4-byte words. As already mentioned, the primitivity of the latter can be obtained, as shown below, from already established results.

Let us prove that $\rho = \rho_{\mathrm{AES}}$ satisfies the hypothesis of Theorem 3.1, i.e. that $\langle \rho_{\mathrm{AES}}, T_{32} \rangle$ generates a primitive group. To do so, we need the following definitions and a general result of primitivity for substitution-permutation networks [5].

Let us write $n = s \cdot b$, for some $s, b > 1$, and let us decompose V as a direct sum of subspaces accordingly, i.e. $V = \bigoplus_{i=1}^{b} V_i$, where $\dim(V_i) = s$. Each V_i, spanned by the canonical vectors $e_{s(i-1)+1}, \ldots, e_{s(i-1)+s}$, is called a *brick*. Recall that, in the case of ρ_{AES}, we have $n = 32$, $s = 8$ and $b = 4$.

Given $f : \mathbb{F}_2^s \to \mathbb{F}_2^s$, for each $a \in \mathbb{F}_2^s$, $a \neq 0$, we denote by

$$\partial_a(f) : \mathbb{F}_2^s \to \mathbb{F}_2^s, \quad x \mapsto xf + (x+a)f,$$

the *derivative of f in the direction a*. Recall that when $f \in \mathrm{Sym}(\mathbb{F}_2^s)$ is δ-*differentially uniform*, for some $2 \leq \delta \leq 2^s$, then $|\mathrm{Im}(\partial_a(f))| \geq 2^s/\delta$ for each $a \neq 0$. Moreover, if $0f = 0$, we say that f is δ-*anti-invariant* if for any two subspaces $W_1, W_2 \leq \mathbb{F}_2^s$ such that $W_1 f = W_2$, then either $\dim(W_1) = \dim(W_2) < s - \delta$ or $W_1 = W_2 = \mathbb{F}_2^s$.

The next theorem is stated using the notation introduced above in this section.

Theorem 3.2 ([5]). *Let $f \in \mathrm{Sym}(\mathbb{F}_2^s)$ such that 0f=0, let $F \in \mathrm{Sym}(V)$ be the function acting as f on each s-dimensional brick V_i of V and let $\Lambda \in \mathrm{GL}(V)$. If no non-trivial and proper direct sum of bricks of V is invariant under Λ and for some $2 \leq \delta \leq s-1$ the function f is*

— *2^δ-differentially uniform,*
— *$(\delta-1)$-anti-invariant,*

then $\langle F\Lambda, T_n \rangle$ is primitive.

We are now ready to prove the primitivity of $\langle \rho_{\mathrm{AES}}, T_{32} \rangle$ as a consequence of Theorem 3.2.

Theorem 3.3. *The group $\langle \rho_{\mathrm{AES}}, T_{32} \rangle < \mathrm{Sym}(\mathbb{F}_2^{32})$ is primitive.*

Proof. Let $\lambda \in \mathrm{GL}(V)$ and $\gamma' \in \mathrm{Sym}(V)$, as in Definition 2.3, be, respectively, the `RotWord` transformation and the parallel application of 4 copies of γ, the S-Box `SubBytes`. It is well known that γ is, up to affine transformations, the function which sends 0 into 0 and each nonzero element into its multiplicative inverse in $\mathbb{F}_{2^s}$. Such a function is 4-differentially uniform and 1-anti invariant, i.e. satisfies the hypotheses of Theorem 3.2 for $\delta = 2$ [24, 14]. Note that anti-invariance and differential uniformity are invariant under inversion [13] and under affine transformations, i.e. also γ^{-1} satisfies the hypotheses of Theorem 3.2. Moreover, it easily checked that no non-trivial and proper direct sum of bricks of V is invariant under λ, and the same trivially holds also for λ^{-1}. Therefore, from Theorem 3.2, $\langle (\gamma')^{-1}\lambda^{-1}, T_{32} \rangle$ is primitive, and consequently so is $\langle \lambda\gamma', T_{32} \rangle = \langle \rho_{\mathrm{AES}}, T_{32} \rangle$. □

The following final conclusion is derived.

Corollary 3.4. *The group $\langle \overline{\rho_{\mathrm{AES}}}, T_{128} \rangle < \mathrm{Sym}(\mathbb{F}_2^{128})$ generated by the transformations of the AES-128 key-schedule is primitive.*

4. The Primitivity Reduction - Proof of Theorem 3.1

This section is entirely devoted to the proof of Theorem 3.1, which may be skipped entirely from the reader who is not interested in the technical details. Despite its

apparent complexity, the (repeated) use of Goursat's lemma, which is introduced below, represents a reasonable way to describe any generic subspace U which is candidate to be a linear block (and which, *a fortiori*, is necessarily trivial).

In order to prove our result, we need to determine a block system for $V^4 = V^2 \times V^2$, i.e. the set the cosets of a suitable subgroup of $V^2 \times V^2$. This can be accomplished by using the following characterization of subgroups of the direct product of two groups in terms of suitable sections of the direct factors [17].

Theorem 4.1 (Goursat's lemma). *Let G_1 and G_2 be two groups. There exists a bijection between*

(1) *the set of all subgroups of the direct product $G_1 \times G_2$, and*
(2) *the set of all triples $(A/B, C/D, \psi)$ where*

- *A is a subgroup of G_1,*
- *C is a subgroup of G_2,*
- *B is a normal subgroup of A,*
- *D is a normal subgroup of C,*
- *$\psi : A/B \to C/D$ is a group isomorphism.*

Then, each subgroup of $U \leq G_1 \times G_2$ can be uniquely written as

$$U = U_\psi = \{(a, c) \in A \times C \,|\, (a + B)\psi = c + D\}. \tag{1}$$

Note that the isomorphism ψ induces a homomorphism $\varphi : A \to C$ where $a \mapsto a\varphi$ is such that $(a + B)\psi = a\varphi + D$ for any $a \in A$, and such that $B\varphi \leq D$. Such a homomorphism is not necessarily unique.

Corollary 4.2. *In the notation of Theorem* 4.1, *given any homomorphism φ induced by ψ, we have*

$$U_\psi = \{(a, a\varphi + d) \,|\, a \in A, d \in D\}.$$

Proof. Let $(a, c) \in U_\psi$. By definition of φ, $(a + B)\psi = c + D = a\varphi + D$, so $c \in a\varphi + D$, and therefore there exists $d \in D$ such that $c = a\varphi + d$. Conversely, if $a \in A$ and $d \in D$, then $(a + B)\psi = a\varphi + D = a\varphi + d + D$. □

4.1. *Use of Goursat's lemma*

Let U be a subspace of $V^4 = V^2 \times V^2$. From Theorem 4.1 and Corollary 4.2 we have that there exist $A, B, C, D \leq V^2$ and $\psi : A/B \to C/D$ isomorphism inducing an homomorphism $\varphi : A \to C$ such that

$$U = \{(\boldsymbol{a}, \boldsymbol{a}\varphi + \boldsymbol{d}) \mid \boldsymbol{a} \in A, \boldsymbol{d} \in D\}.$$

Without loss of generality, a basis of A can be completed to a basis of $\mathbb{F}_2^{2n}$ and φ can be arbitrarily defined from the basis of the complement A^c of A to a basis of

$(\mathrm{Im}(\varphi))^c$. Finally, φ can be extended by linearity on the whole space $\mathbb{F}_2^{2n}$, providing us with a matrix representation of φ as

$$\begin{pmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{pmatrix},$$

such that for each $(a_1, a_2) \in A \leq \mathbb{F}_2^{2n}$

$$\boldsymbol{a}\varphi = (a_1, a_2)\varphi = (a_1\varphi_{11} + a_2\varphi_{21}, a_1\varphi_{12} + a_2\varphi_{22}) \stackrel{\text{def}}{=} (\boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_2),$$

where for $1 \leq i \leq 2$,

$$\varphi_i = \begin{pmatrix} \varphi_{1i} \\ \varphi_{2i} \end{pmatrix}.$$

Applying again Goursat's lemma on $A, D \leq V^2$, we obtain that

(i) there exist $A', B', C', D' \leq V$ and $\varphi_A : A' \to C'$ an homomorphism such that

$$A = \{(a', a'\varphi_A + d') \,|\, a' \in A', d' \in D'\},$$

(ii) there exist $A'', B'', C'', D'' \leq V$ and $\varphi_D : A'' \to C''$ an homomorphism such that

$$D = \{(a'', a''\varphi_D + d'') \,|\, a'' \in A'', d'' \in D''\}.$$

The previous construction and notation will be used in the remainder of the paper every time a subspace U is considered as a candidate for the linear component of an invariant linear partition. More precisely, we have the following.

Definition 4.3. A subgroup $U \leq V^4$ is a *linear block* for $f \in \mathrm{Sym}(V^4)$ if for each $\vec{v} \in V^4$ there exists $\vec{w} \in V^4$ such that

$$(U + \vec{v})f = U + \vec{w},$$

where we can always choose $\vec{w} = \vec{v}f$.

When a linear block for f is found, by Lemma 2.2 $\langle f, T_{4n}\rangle$ is imprimitive and have the cosets of the linear block as a block system. By virtue of Lemma 2.2, cosets of linear blocks are indeed the only kind of partitions that can be invariant for the groups under considerations, despite the generality of the definition of partition. Note also that if $f \in \mathrm{Sym}(V^4)$ is such that $\vec{0}f = \vec{0}$ and $U < V^4$ is a linear block for f, then U is an invariant subspace for f, i.e. for each $\vec{u} \in U$ there exists $\vec{w} \in U$ such that $\vec{u}f = \vec{w}$. The relation $Uf = U$ can be also expressed, in the notation of this section, as

$$\forall \boldsymbol{a} \in A \forall \boldsymbol{d} \in D\, \exists \boldsymbol{x} \in A \exists \boldsymbol{d} \in D : (\boldsymbol{a}, \boldsymbol{a}\varphi + \boldsymbol{d})f = (\boldsymbol{x}, \boldsymbol{x}\varphi + \boldsymbol{y}). \tag{2}$$

We will use Eq. (2) extensively in the next results when considering functions with linear blocks, sometimes without explicit mention.

4.2. *The proof*

We are now ready to show the steps to prove Theorem 3.1. In the remainder of the paper we will make use of the notation introduced in Sec. 4.1 and we assume, without loss of generality and only for the sake of simplicity, that $0\rho = 0$. This is possible since each possible translation is considered in the group under investigation (cf. Definition 2.5).

The next result is the starting point for the proof of Theorem 3.1: we will show that assuming the existence of a linear block for $\overline{\rho}$, i.e. exploiting an invariant subspace for $\overline{\rho}$, leads to the discovery of a (possibly trivial) invariant subspace for ρ. Note that our main claim follows straightforwardly from Lemma 4.4 when such a subspace is non-trivial. In the reminder of the paper, we will discuss the remaining cases.

Lemma 4.4. *Let $\rho \in \mathrm{Sym}(V)$ and let $U \leq V^4$ be a linear block for $\overline{\rho}$. In the notation of Sec.* 4.1*, we have $D''\rho = D''$.*

Proof. Since U is a linear block for $\overline{\rho}$, taking $\boldsymbol{a} = \mathbf{0}$ in Eq. (2) and considering the description of D as a subgroup of $\mathbb{F}_2^{2n}$ (cf. (ii) in Sec. 4.1), for each $a'' \in A''$ and $d'' \in D''$, we have $(0, 0, a'', a''\varphi_D + d'') \in U$. Moreover, assuming $a'' = 0$ and noticing that U is a linear block for each element of $\langle\overline{\rho}\rangle \leq \mathrm{Sym}(V^4)$, we have $(0, 0, 0, d'')\overline{\rho} = (d''\rho, d''\rho, d''\rho, d'' + d''\rho) \in U$ and $(0, 0, 0, d'')\overline{\rho}^{-3} = (d''\rho, d''\rho, d''\rho, d'') \in U$. Therefore

$$(d''\rho, d''\rho, d''\rho, d'' + d''\rho) + (d''\rho, d''\rho, d''\rho, d'') = (0, 0, 0, d''\rho) \in U. \tag{3}$$

Hence, there exist $\boldsymbol{x} \in A$ and $\boldsymbol{y} \in D$ such that $(0, 0, 0, d''\rho) = (\boldsymbol{x}, \boldsymbol{x}\varphi + \boldsymbol{y})$, and so $\boldsymbol{x} = \mathbf{0}$ and $(0, d''\rho) = \boldsymbol{y} \in D$. From $(0, d''\rho) \in D$ we have that there exist $x'' \in A''$ and $y'' \in D''$ such that $x'' = 0$ and $d''\rho = y'' \in D''$, which leads, since ρ is a permutation, to $D''\rho = D''$, as claimed. □

We will use Lemma 4.4 to prove that if $\langle\overline{\rho}, T_{4n}\rangle$ is imprimitive, then an imprimitivity block for $\langle\rho, T_n\rangle$ can be found. From Lemma 4.4, D'' is a natural first candidate for an imprimitivity block for $\langle\rho, T_n\rangle$. The proof of Theorem 3.1 is organized as follows: assuming that U is an imprimitivity block for $\langle\overline{\rho}, T_{4n}\rangle$, from Lemma 4.4 we have that D'' is a block for ρ. When D'' is nontrivial and proper there is nothing left to prove. In the case $D'' = \mathbb{F}_2^n$ we derive a contradiction and in the case $D'' = \{0\}$ we prove that, instead, C'' is a block for ρ. As before, the proof is completed when C'' is nontrivial and proper and a contradiction is derived when $C'' = \mathbb{F}_2^n$. In the remaining case $C'' = \{0\}$, A' is proved to be a block for ρ, and the extremal possibilities for A' are excluded by way of contradictions. In order to prove what anticipated, the following technical lemma is needed in some of the sub-cases.

Lemma 4.5. *Let $\rho \in \mathrm{Sym}(V)$ and let $U \leq V^4$ be a linear block for $\overline{\rho}$. In the notation of Sec.* 4.1, *if $D = \{\mathbf{0}\}$ we have*

(1) $A = A\varphi$;
(2) *if $(a_1, a_2) \in A$, then $a_1, a_2 \in A'$.*

Proof. Let us address each claim separately. Since U is a linear block for $\overline{\rho}$ such that $D = \{\mathbf{0}\}$, it means that $U = \{(\boldsymbol{a}, \boldsymbol{a}\varphi) \mid \boldsymbol{a} \in A\}$ is a linear block also for $\overline{\rho}^{-1}$ (cf. Definition 2.4 for the inverse of $\overline{\rho}$) and, as in Eq. (2), assuming $\boldsymbol{d} = (0, 0)$ and $\boldsymbol{y} = (0, 0)$, we have that for each $\boldsymbol{a} = (a_1, a_2) \in A$ there exists $\boldsymbol{x} \in A$ such that $(\boldsymbol{a}, \boldsymbol{a}\varphi)\overline{\rho}^{-1} = (\boldsymbol{x}, \boldsymbol{x}\varphi)$. This means that

$$\begin{aligned}(a_1, a_2, \boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_2)\overline{\rho}^{-1} &= (a_1 + (\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\rho, a_1 + a_2, a_2 + \boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\\ &= (\boldsymbol{x}, \boldsymbol{x}\varphi).\end{aligned}$$

Hence $\boldsymbol{x}\varphi = (a_2 + \boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2) = (a_2, \boldsymbol{a}\varphi_1) + (\boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_2) \in A\varphi$. Since $\boldsymbol{x}\varphi$ and $\boldsymbol{a}\varphi$ belong to $A\varphi$, we have $(a_2, \boldsymbol{a}\varphi_1) \in A\varphi$. Similarly, for each $\boldsymbol{a} = (a_1, a_2) \in A$, there exists $\boldsymbol{x} \in A$ such that

$$\begin{aligned}(\boldsymbol{a}, \boldsymbol{a}\varphi)\overline{\rho}^{-2} &= (a_1 + \xi + (a_2 + \boldsymbol{a}\varphi_2)\rho, a_2 + \xi, a_1 + \boldsymbol{a}\varphi_1, a_2 + \boldsymbol{a}\varphi_2)\\ &= (\boldsymbol{x}, \boldsymbol{x}\varphi),\end{aligned}$$

where ξ denotes $(\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\rho$. Hence $(a_1 + \boldsymbol{a}\varphi_1, a_2 + \boldsymbol{a}\varphi_2) = (a_1, a_2) + (\boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_2) \in A\varphi$ and so $(a_1, a_2) \in A\varphi$, which proves $A \leq A\varphi$ and, from $|A| \geq |A\varphi|$, we obtain claim (1). Moreover, since we have already proved that $(a_2, \boldsymbol{a}\varphi_1) \in A\varphi = A$, by the description of A as subgroup of $\mathbb{F}_2^{2n}$ (cf. (i) in Sec. 4.1), there exist $x' \in A'$ and $y' \in D'$ such that $(a_2, \boldsymbol{a}\varphi_1) = (x', x'\varphi_A + y')$, and so $a_2 = x' \in A'$. Similarly, for each $(a_1, a_2) \in A$ we have $a_1 \in A'$, i.e. claim (2) is obtained. □

We now use the previous lemma to show our main result, in which we prove that, in general, the AES-like key-schedule construction generates a primitive permutation group, provided that the key-schedule operator $\overline{\rho}$ is induced by a permutation ρ such that $\langle \rho, T_n \rangle$ is primitive. As already anticipated, the proof is organized in several steps. We will proceed as described in the paragraph after Lemma 4.5.

Proof of Theorem 3.1. Let us assume that $\langle \overline{\rho}, T_{4n} \rangle$ is imprimitive, i.e. that there exists a block system $\mathcal{U}$ for $\langle \overline{\rho}, T_{4n} \rangle$. Then, from Lemma 2.2, the block system is of the type

$$\mathcal{U} = \{U + \vec{v} | \vec{v} \in V^4\},$$

for a nontrivial and proper subspace U of V^4. From Lemma 4.4, we have $D''\rho = D''$ and the previous equation means that the subgroup $D'' \leq V$, when nontrivial and proper, is an imprimitivity block for $\langle \rho, T_n \rangle$. If that is the case, there is nothing left to prove. Let us conclude the proof addressing the extremal cases $D'' = \mathbb{F}_2^n$ and $D'' = \{0\}$ separately.

$\boxed{\mathbf{D''=\mathbb{F}_2^n}}$ Note that from Eq. (3), for each $d'' \in D''$ we have $(0,0,0,d'') \in U$, hence

$$(0,0,0,d'')\overline{\rho} = (d''\rho, d''\rho, d''\rho, d''+d''\rho) \in U$$

and so $(d''\rho, d''\rho, d''\rho, d''\rho) \in U$. Since $D'' = \mathbb{F}_2^n$, also $D''\rho = \mathbb{F}_2^n$, therefore for each $\alpha \in \mathbb{F}_2^n$ we have $v_1 = (\alpha,\alpha,\alpha,\alpha) \in U$ and so $v_2 = v_1\overline{\rho}^{-1} = (\alpha,0,0,0) \in U, v_3 = v_2\overline{\rho}^{-1} = (\alpha,\alpha,0,0) \in U$ and $v_4 = v_3\overline{\rho}^{-1} = (\alpha,0,\alpha,0) \in U$. Therefore we have $v_5 = v_2 + v_3 = (0,\alpha,0,0) \in U, v_3 + v_4 + v_5 = (0,0,\alpha,0) \in U$ and $v_1 + v_4 + v_5 = (0,0,0,\alpha) \in U$. We can conclude that $U = \mathbb{F}_2^{4n} = V^4$, a contradiction.

$\boxed{\mathbf{D''=\{0\}}}$ Let us prove first that, in this case, also $B'' = \{0\}$. Indeed, since $B''\varphi_D \leq D''$ (cf. in general the definition of $U = U_{\psi_D}$ in Eq. (1)) and $D'' = \{0\}$, we have $B''\varphi_D = \{0\}$. If we consider Eq. (2) setting $\boldsymbol{a} = \mathbf{0}$ and $\boldsymbol{d} = (b'', b''\varphi_D) = (b'', 0)$ with $b'' \in B'' \leq A''$, then we have $(0,0,b'',0) \in U$. Moreover, we have that

$$(0,0,b'',0)\overline{\rho} = (0,0,b'',b'') \in U,$$

and so $(0,0,b'',b'') + (0,0,b'',0) = (0,0,0,b'') \in U$, which implies$(0,0)\varphi + (0,b'') = (0,b'') \in D$, and so there exists $x'' \in A''$ such that $(0,b'') = (x'', x''\varphi_D)$, from which $0 = 0\varphi_D = b''$, i.e. $B'' = \{0\}$. This also proves that $\varphi_D : A'' \to C''$ is an isomorphism. Now, setting $\boldsymbol{a} = \mathbf{0}$, we have

$$(0,0,a'',a''\varphi_D)\overline{\rho} = (a''\varphi_D\rho, a''\varphi_D\rho, a''+a''\varphi_D\rho, a''+a''\varphi_D+a''\varphi_D\rho) \in U$$

and

$$(0,0,a'',a''\varphi_D)\overline{\rho}^{-3} = (a''\varphi_D\rho, a''\varphi_D\rho, a''+(a''+a''\varphi_D)\rho, a''+a''\varphi_D) \in U.$$

Therefore, there exist $\boldsymbol{x} \in A$ and $\boldsymbol{y} \in D$ such that

$$\begin{aligned}(0,0,a'',a''\varphi_D)\overline{\rho} + (0,0,a'',a''\varphi_D)\overline{\rho}^{-3} &= (0,0,a''\varphi_D\rho + (a''+a''\varphi_D)\rho, a''\varphi_D\rho)\\ &= (\boldsymbol{x}, \boldsymbol{x}\varphi + \boldsymbol{y})\end{aligned}$$

and so $(a''\varphi_D\rho + (a''+a''\varphi_D)\rho, a''\varphi_D\rho) \in D$. This means that $a''\varphi_D\rho = x''\varphi_D$ for some $x'' \in A''$, i.e. $a''\varphi_D\rho \in A''\varphi_D$, and so $A''\varphi_D\rho = A''\varphi_D$, since ρ is a permutation. Since φ_D is an isomorphism, this proves that $C''\rho = C''$. If C'' is a non-trivial and proper subgroup of V, then we have determined another imprimitivity block for $\langle \rho, T_n \rangle$, so the claim is proved. Let us address the extremal cases $C'' = \mathbb{F}_2^n$ and $C'' = \{0\}$ separately.

$\boxed{\mathbf{C''=\mathbb{F}_2^n}}$ First notice that $A'' = \mathbb{F}_2^n$ and $B'' = \{0\} = D''$ since, as already proved, φ_D is an isomorphism. In other words, φ_D is an automorphism. For each $a'' \in A''$, considering $\boldsymbol{a} = \mathbf{0}$, we have

$$(0,0,a'',a''\varphi_D)\overline{\rho}^{-1} = ((a''+a''\varphi_D)\rho, 0, a'', a''+a''\varphi_D) \in U$$

and so $(a''+a''\varphi_D)\rho \in A'$. If we define $S \stackrel{\text{def}}{=} \{a''+a''\varphi_D \mid a'' \in A''\}$, then we have $S\rho \leq A'$. Suppose that $\bar{a} \in A''$ is a fixed point for φ_D: we have $\bar{a} + \bar{a}\varphi_D = 0$, and so $(0,0,\bar{a},\bar{a}\varphi_D)\overline{\rho}^{-1} = (0,0,\bar{a},0)$, which implies that $\bar{a}\varphi_D = 0$, i.e. $\bar{a} = 0$ since φ_D

is an isomorphism. Hence we proved that $\nVdash + \varphi_D$ is injective, and so $S = \mathbb{F}_2^n$, since $A'' = \mathbb{F}_2^n$. Therefore $A' = \mathbb{F}_2^n$, since $\mathbb{F}_2^n = S\rho \leq A' \leq \mathbb{F}_2^n$.

We claim now that also D' is equal to $\mathbb{F}_2^n$. Indeed, if

$$\begin{aligned} U \ni v_1 &\stackrel{\text{def}}{=} (0,0,a'',a''\varphi_D) + (0,0,a'',a''\varphi_D)\overline{\rho} \\ &= (a''\varphi_D\rho, a''\varphi_D\rho, a''\varphi_D\rho, a'' + a''\varphi_D\rho), \end{aligned}$$

then for each $a'' \in A''$ we have

$$v_1\overline{\rho}^{-1} + v_1\overline{\rho}^{-3} = (0, a''\rho, a''\varphi_D\rho + a''\rho, 0) \in U,$$

so $(0, a''\rho) \in A$, which means $a''\rho \in D'$, that is equivalent to saying that $A''\rho \leq D'$. Since $A'' = \mathbb{F}_2^n$ and ρ is bijective we obtain $D' = \mathbb{F}_2^n$.

Therefore we have $A' = D' = \mathbb{F}_2^n$, and so $B' = C' = \mathbb{F}_2^n$, since by hypothesis $A'/B' \cong C'/D'$. This proves that $A = \mathbb{F}_2^{2n}$.

Notice now that $A \leq A\varphi + D \leq C$. Indeed, for each $\boldsymbol{a} = (a_1, a_2) \in A$, considering $\boldsymbol{d} = \boldsymbol{0}$, there exist $\boldsymbol{x} \in A$ and $\boldsymbol{y} \in D$ such that

$$\begin{aligned} (\boldsymbol{a}, \boldsymbol{a}\varphi)\overline{\rho}^{-2} &= \\ &= (a_1 + \xi + (a_2 + \boldsymbol{a}\varphi_2)\rho, a_2 + \xi, a_1 + \boldsymbol{a}\varphi_1, a_2 + \boldsymbol{a}\varphi_2) \\ &= (\boldsymbol{x}, \boldsymbol{x}\varphi + \boldsymbol{y}), \end{aligned}$$

where ξ denotes $(\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\rho$. Hence

$$(a_1 + \boldsymbol{a}\varphi_1, a_2 + \boldsymbol{a}\varphi_2) = (a_1, a_2) + (\boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_2) = \boldsymbol{x}\varphi + \boldsymbol{y} \in A\varphi + D$$

and so $(a_1, a_2) \in A\varphi + D$, which proves $A \leq A\varphi + D$. From $\mathbb{F}_2^{2n} = A \leq A\varphi + D \leq C \leq \mathbb{F}_2^{2n}$ we obtain $C = \mathbb{F}_2^{2n}$. Therefore $D \cong \mathbb{F}_2^n$, since $D'' = \{0\}$ and φ_D is an automorphism, and, from $A/B \cong C/D$, we also have $B \cong \mathbb{F}_2^n$.

We now claim that $B = D$. Indeed, let us consider Eq. (2) with $\boldsymbol{b} = (b_1, b_2) \in B \leq A$. Since $B\varphi \leq D$, we can also choose $\boldsymbol{d} \in D$ such that $\boldsymbol{d} = \boldsymbol{b}\varphi$. Then

$$\begin{aligned} U \ni v_1 &\stackrel{\text{def}}{=} (b_1, b_2, 0, 0)\overline{\rho} = (b_1, b_1 + b_2, b_1 + b_2, b_1 + b_2), \\ U \ni v_2 &\stackrel{\text{def}}{=} (b_1, b_2, 0, 0)\overline{\rho}^{-1} = (b_1, b_1 + b_2, b_2, 0) \end{aligned}$$

and therefore $v_1 + v_2 = (0, 0, b_1, b_1 + b_2) \in U$, from which we derive, since $D'' = \{0\}$, that

$$b_1\varphi_D = b_1 + b_2 \tag{4}$$

and $b_1 \in A'' = A''\varphi_D$ and $b_1 + b_2 \in A''\varphi_D$. So also $b_2 \in A''\varphi_D$. This proves that $B \leq D$, and so $B = D$. Let us now show that this leads to a contradiction.

Again from Eq. (2), this time with $\boldsymbol{a} = 0$ and with $\boldsymbol{d}$ being the same element $(b_1, b_2) \in B = D$, we obtain

$$U \ni v_3 \stackrel{\text{def}}{=} (0, 0, b_1, b_2)\overline{\rho}^{-1} = ((b_1 + b_2)\rho, 0, b_1, b_1 + b_2)$$

and so $v_1 + v_2 + v_3 = v_4 \stackrel{\text{def}}{=} ((b_1 + b_2)\rho, 0, 0, 0) \in U$. Manipulating v_4 as in the case $D'' = \mathbb{F}_2^n$ we prove that $(0, 0, 0, (b_1 + b_2)\rho) \in U$, which means $(b_1 + b_2)\rho = 0\varphi_D = 0$,

i.e. $b_1 = b_2$. Then, from Eq. (4) and since φ_D is an isomorphism, we have $b_1 = b_2 = 0$, a contradiction.

$\boxed{\mathbf{C'' = \{0\}}}$ Since φ_D is an isomorphism, we have $C'' = D'' = B'' = A'' = \{0\}$, and so $D = \{\mathbf{0}\}$. Let us now prove that $B = \{\mathbf{0}\}$. Since $B\varphi \leq D = \{\mathbf{0}\}$, then $B\varphi = \{\mathbf{0}\}$. If $(b_1, b_2) \in B$, then $(b_1, b_2)\varphi = (0, 0)$, and so $(b_1, b_2, 0, 0) \in U$. Similarly to the previous case, we obtain $(0, 0, b_1, b_1 + b_2) \in U$, i.e. there exists $\boldsymbol{x} \in A$ such that $(0, 0, b_1, b_1 + b_2) = (\boldsymbol{x}, \boldsymbol{x}\varphi)$, so we have $(b_1, b_1 + b_2) = (0, 0)$, which implies $(b_1, b_2) = \mathbf{0}$. This proves that $B = \{\mathbf{0}\}$ and that $\varphi : A \to C$ is an isomorphism. From (1) of Lemma 4.5, we have that φ is an automorphism of A. Moreover, for each $\boldsymbol{a} = (a_1, a_2) \in A$, we have $(a_1, a_2)\varphi = (\boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_2) \in A\varphi = A$, and by (2) of Lemma 4.5 we obtain $\boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_2 \in A'$, and so $\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2 \in A'$. Consequently,

$$\mathrm{Im}(\varphi_1 + \varphi_2) = \{\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2 | \boldsymbol{a} \in A\} \leq A'.$$

Note that $\varphi_1 + \varphi_2$ is surjective, since $\varphi = (\varphi_1, \varphi_2)$ is an invertible matrix, and so $\mathrm{Im}(\varphi_1 + \varphi_2) = A'$.

Now, for each $\boldsymbol{a} = (a_1, a_2) \in A$, there exists $\boldsymbol{x} \in A$ such that

$$\begin{aligned}(\boldsymbol{a}, \boldsymbol{a}\varphi)\overline{\rho}^{-2} &= (a_1 + \xi + (a_2 + \boldsymbol{a}\varphi_2)\rho, a_2 + \xi, a_1 + \boldsymbol{a}\varphi_1, a_2 + \boldsymbol{a}\varphi_2)\\ &= (\boldsymbol{x}, \boldsymbol{x}\varphi),\end{aligned}$$

thus we obtain

$$(a_1 + \xi + (a_2 + \boldsymbol{a}\varphi_2)\rho, a_2 + \xi)\varphi = (a_1, a_2) + (a_1, a_2)\varphi \in A\varphi = A,$$

where ξ denotes here the element $(\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\rho$.

Hence

$$\begin{aligned}((\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\rho + (a_2 + \boldsymbol{a}\varphi_2)\rho, (\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\rho) = (a_1, a_2)\varphi^{-1} &\in A\varphi\\ &= A. \qquad (5)\end{aligned}$$

Therefore, from (2) of Lemma 4.5, for each $\boldsymbol{a} \in A$ we have $(\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\rho) \in A'$, and so we obtain $A'\rho = A'$, since

$$\mathrm{Im}(\varphi_1 + \varphi_2) = \{\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2 | \boldsymbol{a} \in A\} = A'$$

and ρ is a permutation. As before, the proof is completed when A' is a non-trivial and proper subgroup of V, since it represents an imprimitivity block for $\langle \rho, T_n \rangle$. Otherwise, the following two cases remain to be discussed.

$\boxed{\mathbf{A' = \mathbb{F}_2^n}}$ Let us denote by

$$\theta \stackrel{\text{def}}{=} \varphi^{-1} = \begin{pmatrix} \theta_{11} & \theta_{12} \\ \theta_{21} & \theta_{22} \end{pmatrix}$$

and let us denote by

$$\theta_1 \stackrel{\text{def}}{=} \begin{pmatrix} \theta_{11} \\ \theta_{21} \end{pmatrix} \text{ and } \theta_2 \stackrel{\text{def}}{=} \begin{pmatrix} \theta_{12} \\ \theta_{22} \end{pmatrix}.$$

Note that from Eq. (5), we have

$$(\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\rho = \boldsymbol{a}\theta_2,$$

which implies that ρ is linear on $\{\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2 \mid \boldsymbol{a} \in A\} = A' = \mathbb{F}_2^n$, a contradiction.

$\boxed{\mathbf{A' = \{0\}}}$ First note that $A'\varphi_A = \{0\}$, so for each $d' \in D'$, considering $a'' = 0$, there exists $y' \in D'$ such that

$$\begin{aligned}(0, d', \bar{\boldsymbol{d}}\varphi_1, \bar{\boldsymbol{d}}\varphi_2)\overline{\rho}^{-1} &= ((\bar{\boldsymbol{d}}\varphi_1 + \bar{\boldsymbol{d}}\varphi_2)\rho, d', d' + \bar{\boldsymbol{d}}\varphi_1, \bar{\boldsymbol{d}}\varphi_1 + \bar{\boldsymbol{d}}\varphi_2) \\ &= (0, y', \bar{\boldsymbol{y}}\varphi_1, \bar{\boldsymbol{y}}\varphi_2),\end{aligned}$$

where $\bar{\boldsymbol{d}} = (0, d')$ and $\bar{\boldsymbol{y}} = (0, y')$. Therefore $(\bar{\boldsymbol{d}}\varphi_1 + \bar{\boldsymbol{d}}\varphi_2)\rho = 0$, and so $\bar{\boldsymbol{d}}\varphi_1 + \bar{\boldsymbol{d}}\varphi_2 = 0$. This means that we have $(0, d', d' + \bar{\boldsymbol{d}}\varphi_1, 0) \in U$ which, since also $(0, d', \bar{\boldsymbol{d}}\varphi_1, \bar{\boldsymbol{d}}\varphi_2) \in U$, implies that $(0, 0, d', \bar{\boldsymbol{d}}\varphi_2) \in U$. We obtain $D' \leq A'' = \{0\}$ and thus $D' = \{0\}$. Since $A'/B' \cong C'/D'$ and $A' = D' = \{0\}$, we also have $C' = B' = \{0\}$, and so $A = \{\mathbf{0}\}$. Finally, since $D = \{\mathbf{0}\}$ and $A/B \cong C/D$, we also have $C = B = \{\mathbf{0}\}$, and so U is trivial, a contradiction. □

Remark 1. Note that in Theorem 3.1 we have obtained our claim by reaching the contradiction that D'' (or C'' or A'') is an invariant subspace for ρ. We should actually prove that D'' generates an invariant partition. However, computations are nearly identical and identically tedious and therefore are not included in this presentation. The intrigued reader may find the same results rewriting the proof of Theorem 3.1 obtaining that $(D'' + v) \mapsto D'' + w$ for some $w \in \mathbb{F}_2^n$.

5. Conclusions

In this work, we have considered the group $\Gamma_{\text{AES}} = \langle \overline{\rho_{\text{AES}}}, T_{128} \rangle$ generated by the AES-128 key-schedule transformations and we have proved that no partition of $V^4 = \mathbb{F}_2^{128}$ can be invariant under its action. However, the slow global diffusion of the operator does not suffice to make the key-schedule transformation free from invariant linear partitions when the composition of more rounds is considered. In particular, since λ^2 and λ^4 admit proper and nontrivial invariant subspaces which are a direct sum of bricks of V, we can conclude that group generated by i consecutive key-schedule transformations $\langle \overline{\rho_{\text{AES}}}^{\,i}, T_{128} \rangle$ is

— primitive if $i = 1$ (this work) and
— imprimitive if $i \in \{0, 2 \bmod 4\}$ (see e.g. [14, Proposition 5.1] or [10] and [22]).

It comes then with no surprise that $\overline{\rho_{\mathrm{AES}}}^4$ admits invariant subspaces, like those found by Leurent and Pernot [22], using an algorithm of Leander *et al.* [21]. One example is $U < V^4$, where

$$U \stackrel{\text{def}}{=} \{(a, b, c, d, 0, b, 0, d, a, 0, 0, d, 0, 0, 0, d) \mid a, b, c, d \in \mathbb{F}_2^8\}.$$

Although the results of this work are not straightforwardly generalized using the same methods to the case $i = 3$, we find it easy to believe that also $\langle \overline{\rho_{\mathrm{AES}}}^3, T_{128} \rangle$ act primitively on V^4. Moreover, there is no reason to believe that the same result is not valid for the 192-bit and 256-bit versions of AES key-schedule. However, the increasing complexity of the strategy used here does not seem to be suitable for addressing the problem, which might require a different methodology.

Acknowledgments

All the authors are members of INdAM-GNSAGA (Italy). This work was partially supported by the Centre of EXcellence on Connected, Geo-Localized and Cybersecure Vehicles (EX-Emerge), funded by Italian Government under CIPE resolution no. 70/2017 (Aug. 7, 2017).

References

[1] R. Aragona and R. Civino, On invariant subspaces in the Lai–Massey scheme and a primitivity reduction, *Mediterranean J. Math.* **18**(4) (2021) 1–14.
[2] R. Aragona, M. Calderini, R. Civino, M. Sala and I. Zappatore, Wave-shaped round functions and primitive groups, *Adv. Math. Commun.* **13**(1) (2019) 67–88.
[3] R. Aragona, M. Calderini and R. Civino, Some group-theoretical results on Feistel networks in a long-key scenario, *Adv. Math. Commun.* **14**(4) (2020) 727–743.
[4] R. Aragona, A. Caranti and M. Sala, The group generated by the round functions of a GOST-like cipher, *Ann. Mat. Pura Appl.* **196**(1) (2017) 1–17.
[5] R. Aragona, M. Calderini, A. Tortora and M. Tota, Primitivity of PRESENT and other lightweight ciphers, *J. Algebra Appl.* **17**(6) (2018) 1850115.
[6] C. Beierle, A. Canteaut, G. Leander and Y. Rotella, Proving resistance against invariant attacks: How to choose the round constants, in *Advances in Cryptology—CRYPTO 2017. Part II*, Lecture Notes in Computer Science, Vol. 10402 (Springer, Cham, 2017), pp. 647–678.
[7] A. Biryukov and D. Khovratovich, Related-key cryptanalysis of the full AES-192 and AES-256, in *Advances in Cryptology—ASIACRYPT 2009*, Lecture Notes in Computer Science, Vol. 5912 (Springer, Berlin, 2009), pp. 1–18.
[8] C. Boura, V. Lallemand, M. Naya-Plasencia and V. Suder, Making the impossible possible, *J. Crypt.* **31**(1) (2018) 101–133.
[9] N. G. Bardeh and S. Rønjom, The exchange attack: How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts, in *Advances in Cryptology—ASIACRYPT 2019. Part III*, Lecture Notes in Computer Science, Vol. 11923 (Springer, Cham, 2019), pp. 247–370.
[10] M. Calderini, A note on some algebraic trapdoors for block ciphers, *Adv. Math. Commun.* **12**(3) (2018) 515–524.
[11] M. Calderini, Primitivity of the group of a cipher involving the action of the key-schedule, *J. Algebra Appl.* (2020).

AQ: Please update ref. 11.

[12] Peter J. Cameron. *Permutation groups*, London Mathematical Society Student Texts, Vol. 45 (Cambridge University Press, Cambridge, 1999).
[13] C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* **15**(2) (1998) 125–156.
[14] A. Caranti, F. D. Volta and M. Sala, On some block ciphers and imprimitive groups, *Appl. Algebra Engrg. Comm. Comput.* **20**(5–6) (2009) 339–350.
[15] O. Dunkelman, N. Keller, E. Ronen and A. Shamir, The retracing boomerang attack, in *Advances in Cryptology—EUROCRYPT 2020. Part I*, Lecture Notes in Computer Science, Vol. 12105 (Springer, Cham, 2020), pp. 280–309.
[16] J. Daemen and V. Rijmen, *The design of Rijndael. Information Security and Cryptography* (Springer-Verlag, Berlin, 2002).
[17] E. Goursat, Sur les substitutions orthogonales et les divisions régulières de l'espace, *Ann. Sci. École Norm. Sup.* 6 (1889) 9–102.
[18] L. Grassi, C. Rechberger and S. Rønjom, A new structural-differential property of 5-round AES, in *Advances in Cryptology—EUROCRYPT 2017. Part II*, Lecture Notes in Computer Science, Vol. 10211 (Springer, Cham, 2017), pp. 289–317.
[19] L. Grassi, C. Rechberger and S. Rønjom, Subspace trail cryptanalysis and its applications to AES, *IACR Trans. Sym. Crypt.* **2016**(2) (2017) 192–225.
[20] G. Leander, M. A. Abdelraheem, H. AlKhzaimi and E. Zenner, A cryptanalysis of PRINTcipher: the invariant subspace attack, in *Advances in Cryptology—CRYPTO 2011*, Lecture Notes in Computer Science, Vol. 6841 (Springer, Heidelberg, 2011), pp. 206–221.
[21] G. Leander, B. Minaud and S. Rønjom, A generic approach to invariant subspace attacks: Cryptanalysis of Robin, iSCREAM and Zorro, in *Advances in Cryptology—EUROCRYPT 2015. Part I*, Lecture Notes in Computer Science, Vol. 9056 (Springer, Heidelberg, 2015), pp. 254–283.
[22] G. Leurent and C. Pernot, New representations of the AES key schedule, in *Advances in Cryptology—EUROCRYPT 2021. Part I*, Lecture Notes in Computer Science, Vol. 12696 (Springer, Cham, 2021), pp. 54–84.
[23] H. Mala, M. Dakhilalian, V. Rijmen and M. Modarres-Hashemi, Improved impossible differential cryptanalysis of 7-round AES-128, in *Progress in Cryptology—INDOCRYPT 2010*, Lecture Notes in Computer Science, Vol. 5498 (Springer, Berlin, 2010), pp. 282–291.
[24] K. Nyberg, Differentially uniform mappings for cryptography, in *Advances in Cryptology—EUROCRYPT 1993*, Lecture Notes in Computer Science, Vol. 765 (Springer, Berlin, 1993), pp. 55–64.
[25] K. G. Paterson, Imprimitive permutation groups and trapdoors in iterated block ciphers, in *Fast Software Encryption*, Lecture Notes in Computer Science, Vol. 1636 (Springer, Berlin, 1999), pp. 201–214.
[26] S. Rønjom, N. Ghaedi Bardeh and T. Helleseth, Yoyo tricks with AES, in *Advances in Cryptology—ASIACRYPT 2017. Part I*, Lecture Notes in Computer Science, Vol. 10624 (Springer, Cham, 2017), pp. 217–243.
[27] R. Sparr and R. Wernsdorf, Group theoretic properties of Rijndael-like ciphers, *Discrete Appl. Math.* **156**(16) (2008) 3139–3149.
[28] R. Sparr and R. Wernsdorf, The round functions of KASUMI generate the alternating group, *J. Math. Cryptol.* **9**(1) (2015) 23–32.
[29] R. Wernsdorf, The one-round functions of the DES generate the alternating group, in *Advances in Cryptology—EUROCRYPT 1992*, Lecture Notes in Computer Science, Vol. 658 (Springer, Berlin, 1993), pp. 99–112.