Brno University of Technology

University of L'Aquila

Double-Degree Master’s Programme - InterMaths
Applied and Interdisciplinary Mathematics

Master of Science **Mathematical Engineering** **Brno University of Technology (BUT)**	**Master of Science** **Mathematical Engineering** **University of L'Aquila (UAQ)**

Master's Thesis

Group Theoretical Properties of The Group Generated By The Action of The AES-128 Key Schedule

Supervisor
Dr. Riccardo Aragona

Riccardo Aragona

Candidate
Patrick Appah

Patrick Appah

Student ID (UAQ): 279726
Student ID (BUT): 253522

Academic Year 2022/2023

BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF MECHANICAL ENGINEERING

FAKULTA STROJNÍHO INŽENÝRSTVÍ

INSTITUTE OF MATHEMATICS

ÚSTAV MATEMATIKY

GROUP THEORETICAL PROPERTIES OF THE GROUP GENERATED BY THE ACTION OF THE AES-128 KEY SCHEDULE

GROUP THEORETICAL PROPERTIES OF THE GROUP GENERATED BY THE ACTION OF THE AES-128 KEY SCHEDULE

MASTER'S THESIS

DIPLOMOVÁ PRÁCE

AUTHOR
AUTOR PRÁCE
Patrick Appah

SUPERVISOR
VEDOUCÍ PRÁCE
Dr. Riccardo Aragona

BRNO 2023

BRNO UNIVERSITY OF TECHNOLOGY

Faculty of Mechanical Engineering

MASTER'S THESIS

Brno, 2023

Patrick Appah

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF MECHANICAL ENGINEERING

Assignment Master's Thesis

Institut:	Institute of Mathematics
Student:	**Patrick Appah**
Degree programm:	Applied and Interdisciplinary Mathematics
Branch:	no specialisation
Supervisor:	**Dr. Riccardo Aragona**
Academic year:	2022/23

As provided for by the Act No. 111/98 Coll. on higher education institutions and the BUT Study and Examination Regulations, the director of the Institute hereby assigns the following topic of Master's Thesis:

Group theoretical properties of the group generated by the action of the AES–128 key schedule

Brief Description:

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 G 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.

Master's Thesis goals:

After a description of both the mathematical and cryptographic background, the results regarding the group generated by the action of the AES–128 key schedule will be presented.

Recommended bibliography:

ARAGONA, R., CIVINO, R. and DALLA VOLTA, F. On the Primitivity of the AES-128 key-schedule. J. Algebra Appl., Online Ready (2022), 2350233.

ARAGONA, R. and CIVINO, R. On invariant subspaces in the Lai–Massey scheme and aprimitivity reduction. Mediterranean J. Math. 18(4) (2021) 1–14.

DAEMEN, J. and RIJMEN, V. The design of Rijndael. Information Security and Cryptography. Berlin: Springer-Verlag, 2002.

LEURENT, G. and PERNOT, C. 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.

Deadline for submission Master's Thesis is given by the Schedule of the Academic year 2022/23

In Brno,

L. S.

doc. Mgr. Petr Vašík, Ph.D. Director of the Institute	doc. Ing. Jiří Hlinka, Ph.D. FME dean

Abstract

The AES key scheduling algorithm selects the round keys which are xor-ed with the partially encrypted state in each iteration. In this work, we examine the group Γ that arises from the AES-128 key scheduling operation. We show that the smallest group Γ_{AES} containing Γ and all translations of the message space is primitive. This implies that we cannot have a linear partition of the message space that is invariant under the action of Γ_{AES}.

Keywords

Primitive groups, cryptography, group generated by the round functions, AES, key schedule, invariant partitions.

Appah, Patrick: *Group Theoretical Properties of The Group Generated By The Action of The AES-128 Key Schedule*, Brno University of Technology, Faculty of Mechanical Engineering, 2023. 48 pp. Supervisor: Dr. Riccardo Aragona.

I declare that I wrote the diploma thesis *Group Theoretical Properties of The Group Generated By The Action of The AES-128 Key Schedule* independently under the guidance of *Dr. Riccardo Aragona* using the literature included in the list of references.

Patrick Appah

I am sincerely grateful to my supervisor, Dr. Riccardo Aragona, for his invaluable guidance and support throughout my Master's thesis. His expertise and mentorship have been instrumental in my success.

I also extend my deepest thanks to my family for their unwavering love and encouragement during this journey.

Lastly, I want to express my appreciation to my colleagues for their collaboration and support. Their contributions have made a significant impact on my research. Thank you all for being a crucial part of my academic and personal growth.

Patrick Appah

Contents

List of Figures

List of Tables

1 Introduction

Many businesses and organizations use the Advanced Encryption Standard (AES), a popular encryption algorithm, to protect their data and communications. The four basic operations of the AES algorithm are SubBytes, ShiftRows, MixColumns, and AddRoundKey. The key schedule generates from the original secret key a sequence of round keys which are xor-ed in each round with the partially encrypted state by the AddRoundKey operation. Important cryptographic properties of the group generated by the AES-128 key schedule can impact the security and effectiveness of the algorithm. In this thesis, we investigate the group theoretical properties of this group and how they are related to the AES security of the algorithm.

1.1 Review of Literature

The results of Biryukov and Khovratovich in [1] underline the significance of the key schedule in the construction of safe block ciphers and offer a standard for assessing the security of block ciphers, including the AES algorithm.

In [2], Boura *et al*. introduce new techniques and complexity analyses for impossible differential cryptanalysis, a block cipher attack.The authors present a novel formula for calculating the temporal complexity of an attack and show how the success of an attack depends on the key schedule of a cipher. Additionally, they demonstrate how to use numerous differentials to strengthen impossible differential attacks and how to combine it with other strategies.

Leurent and Pernot recently made the discovery in [3] that there is an invariant subspace for the first four rounds of the AES-128 key schedule despite the fact that the subject of cryptanalysis on AES-128 dates more than two decades. They were able to represent the key schedule as four distinct actions on each of the round key's four 4-byte-word components as a result of their discovery. Despite the fact that this discovery solely pertains to the key schedule, it has been utilized to strengthen already established differential attacks by revealing subspace structures that interact with related structures in the main round function, creating security vulnerabilities. This emphasizes how critical it is to understand the key schedule in order to comprehend the security of the AES-128 cipher.

In the cryptanalysis of several ciphers, including PRINTcipher and reduced-round AES, approaches like invariant subspace and subspace trail cryptanalysis have been used to take advantage of subspaces that are invariant under encryption functions [4, 5, 6]. The imprimitivity attack, which targets block ciphers similar as DES [7], takes advantage of the fact that the encryption preserves a full partition of the message space, specifically a linear partition created by the cosets of a proper and non-trivial invariant subspace. While it is typically difficult to demonstrate the absence of invariant subspaces, group-theoretical arguments that demonstrate how a specific group containing the encryption functions acts primitively on the message space can be used to demonstrate the absence of invariant linear partitions after one round.

1.2 Organization of The Thesis

The structure of this thesis is as follows: in Section 2, we provide an overview of the algebraic and mathematical concepts that provide a rigorous mathematical basis for our study of the AES-128 key schedule's group theoretical properties. Section 3 provides background on cryptography, including the difference between symmetric and asymmetric encryption, and focuses on symmetric cryptography and block ciphers. It specifically discusses AES and its key schedule. In Section 4, we introduce the notation and initial results, and provide an algebraic representation of the AES-128 key schedule and its corresponding permutation group. The reduction of the primitivity of the

AES-128 key schedule (Theorem 5.1) and its application to AES (Corollary 5.6) are presented in Section 5 as the main results of the thesis. We presents the proof of Theorem 5.1, utilizing Goursat's lemma, in Section 6. The concluding remarks of the thesis are presented in Section 7.

2 Algebraic Background

Modern cryptography relies heavily on algebraic and mathematical structures, especially in the design and analysis of cryptographic algorithms. The Advanced Encryption Standard (AES) is a commonly used symmetric-key encryption algorithm that provides robust security guarantees by combining substitution and permutation operations. The algebraic and mathematical properties of the AES-128 key schedule, which generates the round keys used in the encryption and decryption process, have been widely studied.

In this section, we will provide an overview of the algebraic and mathematical concepts that provide a rigorous mathematical basis for our study of the AES-128 key schedule's group theoretical properties. See [8, 9, 10, 11, 12] as references for the concepts and definitions discussed throughout this section.

Definition 2.1 (Vector Space)**.** A vector space defined over a field F (whose elements are called scalars) is a non-empty set V (whose elements are called vectors) together with two binary operations namely vector addition $(+)$ and scalar multiplication $(\cdot)$.

- $(+) : (\mathbf{u},\mathbf{v}) \in V \times V \longrightarrow \mathbf{u} + \mathbf{v} \in V$
- $(\cdot) : (\alpha, \mathbf{u}) \in K \times V \longrightarrow \alpha \cdot \mathbf{u} \in V$

To have a vector space, the operations of vector addition and scalar multiplication are subject to the following vector axioms for every $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in V$, and α and $\beta \in F$.

1. $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$
2. $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$
3. There exists the zero vector $\mathbf{0} \in V$, such that $\mathbf{v} + \mathbf{0} = \mathbf{v} \ \forall \mathbf{v} \in V$
4. For every $\mathbf{v} \in V$, there exists its additive inverse $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
5. $\alpha(\beta\mathbf{v}) = \alpha\beta(\mathbf{v})$
6. $1\mathbf{v} = \mathbf{v}$, where 1 is the multiplicative identity in F
7. $\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}$
8. $(\alpha + \beta)\mathbf{v} = \alpha\mathbf{v} + \beta\mathbf{v}$

An example of a vector space is $GF(2)^n$, a vector space over a Galois field $\mathbb{F}_2$, and of size 2^n, whose elements are binary vectors of length $n \in \mathbb{N}$, and the operations of vector addition and scalar multiplication are performed in the binary field $\mathbb{F}_2$ (integer modulo 2).

Definition 2.2 (Groups)**.** A group is a pair $(G, \circ)$ consisting of a non-empty set G and an operation, here donated by $\circ$, defined on its elements.

$\circ : (a, b) \in G \times G \longrightarrow a \circ b \in G$

For the pair $(G, \circ)$ to qualify as group, the operation $\circ$ must fulfill the following conditions.

- closed: $\forall\, a, b \in G : a \circ\ b \in G$
- Associativity: $\forall\, a, b, c \in G : (a \circ\ b) \circ\ c = a \circ\ (b \circ\ c)$
- Neutral element: $\exists\, \mathrm{e} \in G, \forall\, a \in G : a \circ\ \mathrm{e} = \mathrm{e} \circ a = a$
- Inverse elements: $\forall\, a \in G, \exists\, b \in G : a \circ\ b = b \circ a = \mathrm{e}$

A group is said to be finite if the cardinality of G, denoted as $|G|$, is finite.

Definition 2.3 (Subgroup)**.** A subset H of a group G is a subgroup if and only if H is a group with respect to the group operation of G. That is, H is closed under the group operation and the identity element of G is present in H, and every element in H has its inverse in G, which is also an element of H.

Definition 2.4. (Cosets) Let $(\mathrm{G}, \circ)$ be a group and H be a subgroup of G. For every $x \in G$, the subsets

$$x \circ H = \{g \in G \mid g = x \circ h \quad \text{for some}\, h \in H\}$$

and

$$H \circ x = \{g \in G \mid g = h \circ x \quad \text{for some}\, h \in H\}$$

of G are called the left coset and right coset of H respectively.

Typically, $x \circ H \neq H \circ x$. We say that H is a normal subgroup when this equality holds.

Observe that G is the disjoint union of all the cosets (left and right) of H.

$$G = \bigcup_{x \in G} x \circ H.$$

$$G = \bigcup_{x \in G} H \circ x.$$

Definition 2.5 (Symmetric group)**.** Let X denote a non-empty set. A bijective mapping $\sigma : X \longrightarrow X$ will be called a permutation of X. The group whose elements are all the bijections from X to itself, and whose group operation is the composition of functions is called a symmetric group of X.

Notably, the symmetric group acting on $\mathbb{F}_2^n$ is the set of all bijective functions that map every binary vector in $\mathbb{F}_2^n$ to a unique vector in $\mathbb{F}_2^n$ that form a group under the operation of composition of these bijective functions.

Definition 2.6 (Translation group on $\mathbb{F}_2^n$)**.** A group of transformations that translate the elements of $\mathbb{F}_2^n$ by a fixed binary vector in $\mathbb{F}_2^n$ is referred to as the translation group on $\mathbb{F}_2^n$.

More precisely, given any binary vector x and a fixed vector v both in $\mathbb{F}_2^n$, we have the transformation $T_v : x \in \mathbb{F}_2^n \longrightarrow x + v \ \in \mathbb{F}_2^n$ is a translation of $\mathbb{F}_2^n$.
The set of all such transformations T_v, with v ranging over all binary vectors $\in \mathbb{F}_2^n$, form a group under the operation of function composition, and is called translation group of $\mathbb{F}_2^n$.

Definition 2.7 (Group of affine permutations of $\mathbb{F}_2^n$)**.** An affine permutation of $\mathbb{F}_2^n$ is a bijective map $\Sigma : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ represented as $T(x) = Ax + b$. A is a non-singular $n \times n$ matrix over $\mathbb{F}_2$, b is a fixed vector in $\mathbb{F}_2^n$, and x an arbitrary vector in $\mathbb{F}_2^n$.
The set of such transformations Σ, with A ranging over all non-singular $n \times n$ matrices over the field $\mathbb{F}_2$ and b over all vectors $\in \mathbb{F}_2^n$, that form a group under the operation of function composition, is referred to as the group of affine permutations of $\mathbb{F}_2^n$, which essentially is a subgroup of $\mathrm{Sym}(\mathbb{F}_2^n)$.

Definition 2.8 (Group of linear permutations of $\mathbb{F}_2^n$)**.** We say that a permutation f of $\mathbb{F}_2^n$ is linear if $f(x + y) = f(x) + f(y)$ for every x, y in $\mathbb{F}_2^n$. While every vector in $\mathbb{F}_2^n$ can be uniquely mapped to another vector in $\mathbb{F}_2^n$, the operations of vector addition and multiplication by scalars over $\mathbb{F}_2$ are preserved. The set of all such permutations forming a group under function composition is called the general linear group of $\mathbb{F}_2^n$. In particular there will be a non-singular matrix A over F_2 such that $f(x) = Ax$. So this group is a subgroup of the affine group of $\mathbb{F}_2^n$, hence a subgroup of $\mathrm{Sym}(\mathbb{F}_2^n)$.

Definition 2.9 (Group homomorphism)**.** Let $(G, *)$ and $(H, \diamond)$ be two groups. A function $f : G \longrightarrow H$ such that $f(x * y) = f(x) \diamond f(y)$ is called a group homomorphism.

Definition 2.10 (Group isomorphism)**.** An isomorphism is a homomorphism that is injective and surjective. In other words, an isomorphism is bijective homomorphism.

Definition 2.11 (Group automorphism)**.** Let G be a group. An isomorphism from G onto itself is called an automorphism of G.

Definition 2.12 (Partition of a set)**.** A partition $\mathcal{P}$ of a set X is the collection of non-empty subsets of X such that every subset of X is in exactly one of the elements in $\mathcal{P}$. In particular, $X = \cup_{Y \in \mathcal{P}} Y$ and $Y_1 \cap Y_2 = \emptyset$ if $Y_1 \neq Y_2$. $\mathcal{P}$ is said to be a trivial partition of X if $\mathcal{P} = \{X\}$ or $P = \{\{x\} \mid x \in X\}$.

Definition 2.13 (Transitive group)**.** Let G be a group and let X be a non-empty set. Then G acts on X if there is a function $\cdot : G \times X \longrightarrow X$ that satisfies the following two conditions:

1. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \ \forall \ g_1, g_2 \in G$ and $x \in X$
2. $1_G \cdot x = x$ for all $x \in X$

If G acts on X, then we say that G acts transitively on X if for any two elements $x, y \in X$, there exists a $g \in G$ such that $g \cdot x = y$.

Definition 2.14 (Invariant partition)**.** An invariant partition is a partition of a set that is preserved by a group action. More formally, let G be a group acting on a set X. A partition $\mathcal{P} = \{P_1, P_2, \ldots, P_k\}$ of X is said to be G-invariant or an invariant partition if, for any $g \in G$ and $i \in 1, 2, \ldots, k$, we have $gP_i = \{gp \mid p \in P_i\} = P_j$, for some $j \in \{1, 2, \ldots, k\}$. In other words, the partition remains the same under the action of any element of the group.

For example, consider the group $G = \{1, -1\}$ acting on the set $X = \mathbb{R} \backslash \{0\}$ of real numbers by multiplication. The set X can be partitioned into two subsets, $X_1 = \{x \in X \mid x > 0\}$ and $X_2 = \{x \in X \mid x < 0\}$. This partition is G-invariant, since $gX_1 = X_1$ and $gX_2 = X_2$ if $g = 1$, and $gX_1 = X_2$ and $gX_2 = X_1$ if $g = -1$.

Any non-trivial and G-invariant partition $\mathcal{P}$ of X is called a block system for G. In particular any $X_i \in \mathcal{P}$ 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 X (or G acts imprimitively on X).

Lemma 2.15. *If T is a transitive subgroup of G, then a block system for G is also a block system for T.*

Proof. (See pages 8 and 12 of [13] for idea of proof.) Let G be a group and T be a subgroup of G that is transitive on the set X. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_k\}$ be a block system for G.

We want to show that $\mathcal{P}$ is also a block system for T by showing that if $\mathcal{P}$ is preserved by every element in G, then it is also preserved by every element in T.

If $\mathcal{P}$ is a block system for G, then for any $g \in G$ and any element $x \in X$, if x and $y \in P_i$, for some $i \in \{1, 2, \ldots, k\}$, then gx and $gy \in P_j$, for some $j \in \{1, 2, \ldots, k\}$.

Since T is transitive on X, for any x and $y \in X$, there exists a $t \in T$ such that $tx = y$. Thus, if x and $y \in P_i$, for some $i \in \{1, 2, \ldots, k\}$, then tx and $ty \in P_j$, for some $j \in \{1, 2, \ldots, k\}$, since $\mathcal{P}$ is preserved by every element of G, including t. Therefore, $\mathcal{P}$ is also a block system for T. □

Lemma 2.16. *Let M be a 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 of $(M, +)$, i.e.*

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

Proof. The idea of this proof follows from the notion of transitivity of group action, and block system discussed earlier.

1. Transitivity: Since T is the translation group of M, for any two vectors u and v in M, there exists a translation t in T such that $t(u) = v$. Hence, T acts transitively on M.

2. Imprimitivity: Let U be a non-trivial and proper subgroup of $(M, +)$. Then the cosets of U form a partition of M, and each coset $U + v$ is a translate of U by v. Since the translation group T acts transitively on M, it also acts transitively on the set of cosets of U. T is imprimitive on M since we can also extract an invariant partition $\mathcal{U}$ of M given by the cosets of U under the action of T. i.e. for any $t \in T$ and $v \in M$, $t(U + v) \in \mathcal{U}$.

3. Block System: Since $\mathcal{U}$ is an invariant partition of M under the action of T, it is a block system for T, whose blocks are the cosets $\{U + v \mid v \in M\}$. □

All through this work, the block system will be a linear partition. Given a vector space X over a field F and G, a group of linear transformations of X, an invariant linear partition of X under the action of G can be used to decompose X into a direct sum of G-invariant subspaces.

3 Cryptographic Background

This section will cover the background of cryptography, including an explanation of what it is, a comparison of symmetric versus asymmetric encryption, and a focus on symmetric cryptography. A general review of block ciphers, including iterated block ciphers, will also be given before we delve deeper into the widely used block cipher AES. We will talk specifically on AES in general and its key schedule.

3.1 Brief Background and Overview of Cryptography

Cryptography is essentially the practice of secure communication amidst adversarial behaviour. Cryptography dates as far back as ancient civilizations, where secret messages and codes were used for secure communication. In contemporary times, cryptography has become crucial in securing internet communication, as well as ensuring secure financial transactions and protecting national security. It involves using a set of rules that define how a message is transformed from its original form into a form that appear unintelligible to everyone but the intended recipient. This set of rules is referred to as a *cryptographic algorithm*. The message in its original form is called the *plaintext* whilst the disguised message is called the *cyphertext*. The process of converting a plaintext into a ciphertext is known as *encryption*, whereas that of recovering a plaintext from a ciphertext is known as *decryption*.

With a block diagram, the encryption and decryption process can be described as follows:

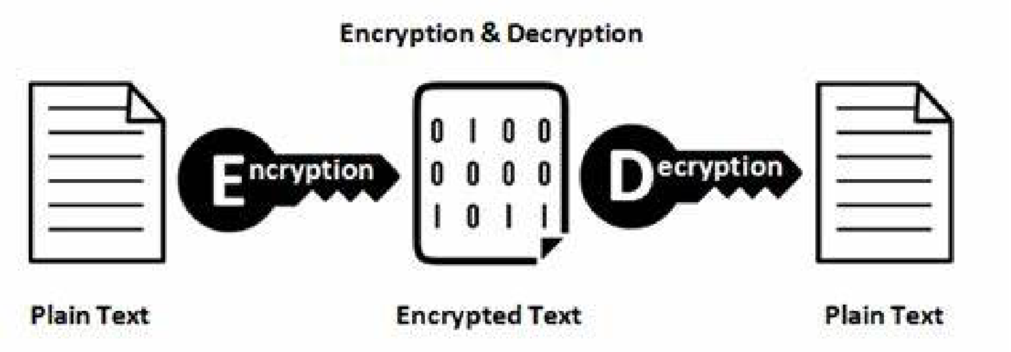

Figure 3.1: Block Diagram Encryption and Decryption process

The most widely used cryptographic algorithms are symmetric (secret key) cryptography, asymmetric (public key) cryptography, and hash functions. We will discuss only symmetric and asymmetric cryptography with a rather much focus on the former. Before we do that, let us introduce the following definition [14].

Definition 3.1 (Cryptosystem)**.** A cryptosystem is a tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where:

- $\mathcal{P}$ is the finite set of possible plaintexts, called plaintext space.
- $\mathcal{C}$ is the finite set of possible ciphertexts, called ciphertext space.
- $\mathcal{K}$ is the finite set of possible keys used for encryption and decryption, called key space.
- $\mathcal{E}$ is the encryption function that maps plaintexts and keys to ciphertexts. Mathematically, it is given by $\mathcal{E}\colon \mathcal{P} \times \mathcal{K} \to \mathcal{C}$.
- $\mathcal{D}$ is the decryption function that maps ciphertexts and keys to plaintexts. Mathematically, it is given by $\mathcal{D}\colon \mathcal{C} \times \mathcal{K} \to \mathcal{P}$.

$\mathcal{E}$ and $\mathcal{P}$ must satisfy the following:

- For any plaintext $p \in \mathcal{P}$ and key $k \in \mathcal{K}$, $\mathcal{D}(\mathcal{E}(p,k),k) = p$.
- For any key $k \in \mathcal{K}$, it should be computationally infeasible to recover the plaintext p from the ciphertext $\mathcal{E}(p,k)$ without knowledge of the key k.

Let us now discuss the asymmetric and symmetric cryptographic algorithms.

3.2 Assymetric Cryptography

In this section we mainly refer to [15]. In asymmetric cryptography, different encryption keys and decryption keys are used. The decryption key is kept secret for its own use and is referred to as a *private key*, whereas the encryption key may be made available to the general public and is referred to as a *public key*. The privacy of the used private key is crucial to the algorithm. This algorithm is also known as the *public-key algorithm*, since the term "public-key" resounds the idea that encryption key can be publicized while the decryption is kept private.

Asymmetric algorithms typically use much longer key sizes compared to the secret key in symmetric algorithms. Due to the mathematical complexity involved in the key generation and encryption/decryption processes, asymmetric algorithms take longer to execute than symmetric algorithms.

An asymmetric algorithm in the encryption and decryption process can be mathematically represented, using the notation introduced in Definition 3.1, as follows:

- Encryption: $\mathcal{E}(p,k_1) = c$
- Decryption: $\mathcal{D}(\mathcal{E}(p,k_1),k_2) = p$,

where k_1 is the public key and k_2 is the the private key. Examples of asymmetric cryptosystems include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC).

With a block diagram, the asymmetric algorithm can be described as follows:

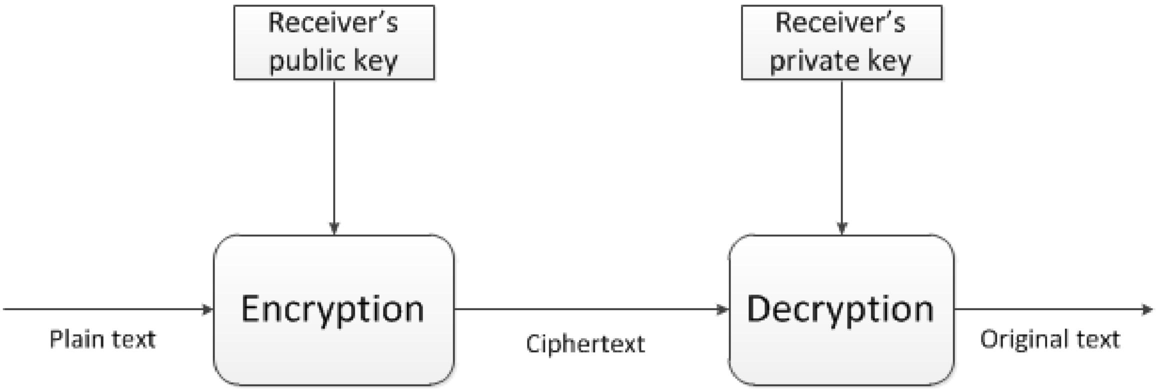

Figure 3.2: Asymmetric Encryption

Let us now introduce symmetric cryptography.

3.3 Symmetric Cryptography

In this section we mainly refer to [16]. Symmetric key cryptographic algorithms are the fundamental blocks upon which any secure systems which demand high sense of secrecy are built. In these kinds of cryptographic algorithms, unlike asymmetric algorithms, the same key is used for both encryption and decryption. Practically, it can thought of a a safe-box where messages can be kept, locked and delivered to the other party. The safe-box can be opened and its content read by the other party if they possess the key to its lock. The security of this algorithm is solely dependent on the private key, known only to the communicating parties involved in the exchange of messages. The fact that the secret key is kept private between the communicating parties, and is not shared with anyone else lends symmetric cryptography the interchangeable name of *private-key cryptography*.

Since symmetric key algorithms are used to encrypt large amounts the data, they have to run at high speeds or at least at the bandwidth of the communication channel so as not to cause a bottleneck. There has been extensive research aimed at increasing the efficiency of symmetric key cryptography without compromising its security.

The symmetric algorithm in the encryption and decryption process can be mathematically represented, using the notation introduced in Definition 3.1, as follows:

- Encryption: $\mathcal{E}(p, k) = c$
- Decryption: $\mathcal{D}(\mathcal{E}(p, k), k) = p$,

where k is the private key used for both encryption and decryption.

With a block diagram, the symmetric algorithm process can be described as follows:

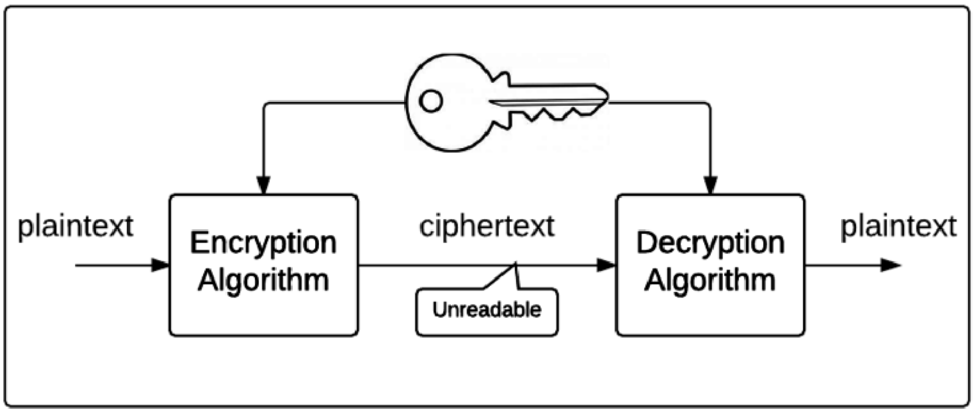

Figure 3.3: Symmetric Encryption

Symmetric key algorithms are mainly divided into two categories: *stream ciphers* and *block ciphers*. In stream ciphers, the plaintext is a binary string, and the ciphertext results from a bit-wise addition modulo 2 of the plaintext with a pseudorandom binary sting called *keystream*. Since this work prioritizes block ciphers, we employ the reader to refer to [17] for far-reaching details about stream ciphers.

3.3.1 Block Ciphers

A block cipher is a type of symmetric encryption algorithm that operates on fixed-length group of bits called *blocks*. The input plaintext is split into fixed-sized blocks, and each block is independently encrypted using a secret key. The final encrypted message is created by combining the resulting ciphertext blocks. Because this work has got to do with the Advanced Encryption Standard (AES), which we will formally introduce later in the work, we note that the plaintext space coincides with the ciphertext space, i.e. $\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$, with n a positive integer. The key space is given by $\mathcal{K} = \mathbb{F}_2^l$, with l a positive integer. (cf. Definition 3.1).

Using the notation of Definition 3.1, let us introduce the definition of an *algebraic* block cipher [18].

Definition 3.2 (Algebraic Block Cipher)**.** Let $\mathcal{E}$ be an encryption function and let $\mathcal{D}$ be a decryption function

$$\mathcal{E}(\mathcal{P},\mathcal{K}),\mathcal{D}(C,\mathcal{K}) : \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^n.$$

For any $k \in \mathbb{F}_2^l$, we denote by $\mathcal{E}_k$ and $\mathcal{D}_k$ the functions

$$\mathcal{E}_k : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n, \quad \mathcal{E}_k(\mathcal{P}) = \mathcal{E}(\mathcal{P},k).$$

$$\mathcal{D}_k : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n, \quad \mathcal{D}_k(C) = \mathcal{D}(C,k).$$

We say that $\mathcal{E}$ is an algebraic block if $\mathcal{E}_k$ is a permutation of $\mathbb{F}_2^n$ and $\mathcal{D} = \mathcal{E}^{-1}$. Each key selects one permutation from the set of $2^n!$ possible permutations.

Modern block ciphers are often *iterated ciphers* that involve sequences of permutations and substitution operations to obtain the needed security. In fact, following Shannon's ideas and proposals from his landmark paper [19], the encryption process starts with a random key and plaintext as input and proceeds through N identical rounds. In each round (with the possible exception of a few, which may somewhat differ) the iterated ciphers perform a non-linear substitution operation on disjoint parts of the input, an undertaking aimed at providing *confusion*. This is followed by a permutation (typically a linear or an affine transformation) on the whole partially encrypted input data, that provides *diffusion*. A cryptosystem reaches confusion if the relationship between the plaintext and ciphertext is extremely obscure. Diffusion refers to the property of spreading the influence of one plaintext symbol over many ciphertext symbols. This implies that even little modifications to the plaintext will have a large impact on the ciphertext. With "iterated" we mean that the encryption function is composition of other permutations of the plaintext space, called *round functions*. The round function is formed by the operations carried out in a round. The round function at the i-th round $(1 \le i \le N)$ takes as input both the output of the $(i-1)$-th round the *round key* $k^{(i)}$, which is constructed starting from the *master key* $k \in \mathcal{K} = \mathbb{F}_2^l$, also called the *cipher key*. The *key schedule* is a public algorithm that constructs $N+1$ round keys $(k^{(0)}, k^{(1)}, \dots, k^{(N)})$.

3.3.2 Substitution Permutation Networks (SPNs)

There are several types of block ciphers, each having its own strengths and weaknesses, and the choice of which cipher to use depends on requirements of the application. Among these types of block ciphers are the two principal types: *Substitution Permutation Networks (SPNs)* and *Feistel ciphers*. The difference between a typical round of these two is that in the latter, the input data of a round is split into two equal halves, and a non-linear function performs substitution and permutation operations on one half of the data at a time. The other half of the data and the output of the non-linear function are then xor-ed, the halves are swapped, and the procedure is repeated for the next round, as opposed to SPNs that use a combination of substitution and permutation operations on the entire input block at once.

Recalling that our work is about AES, we will restrict our reach to only SPNs since the AES uses the SPN framework. We formally define an SPN block cipher as follows.

Definition 3.3. Let $\mathbb{F}_2^n = \underbrace{\mathbb{F}_2^b \times \cdots \times \mathbb{F}_2^b}_{t \text{ times}}$ and let $\mathcal{E} : \mathbb{F}_2^n \times \mathbb{F}_2^l \rightarrow \mathbb{F}_2^n$, with $n = bt$, be an algebraic block cipher with N rounds. Let $k \in \mathbb{F}_2^l$ be the master key and

$$(k^{(0)}, k^{(1)}, \dots, k^{(N)})$$

the $N+1$ round keys produced from k via the key schedule. $\mathcal{E}$ is an SPN block cipher if

$$\mathcal{E}_k(m) = \tau_N \circ \tau_{N-1} \circ \ldots \circ \tau_0(m), \quad m \in \mathbb{F}_2^n$$

where

$$\tau_i = \sigma_{k^{(i)}} \circ \lambda^{(i)} \circ \gamma^{(i)}$$

and

- $\gamma^{(i)}$ is a non-linear substitution;

$$\begin{aligned} \gamma^{(i)} : \mathbb{F}_{2^t}^b &\longrightarrow \mathbb{F}_{2^t}^b \\ \begin{bmatrix} m_1 \\ \vdots \\ m_b \end{bmatrix} &\longmapsto \begin{bmatrix} \gamma_1^{(i)}(m_1) \\ \vdots \\ \gamma_b^{(i)}(m_b) \end{bmatrix}, \end{aligned}$$

  where $\gamma_s^{(i)} : \mathbb{F}_{2^t} \longrightarrow \mathbb{F}_{2^t}$, for $s \in \{1, 2, \ldots, b\}$.

- $\lambda^{(i)} \in \mathrm{AGL}\left(\mathbb{F}_2^n\right) \subset \mathrm{Sym}\left(\mathbb{F}_2^n\right)$, where $\mathrm{AGL}\left(\mathbb{F}_2^n\right)$ is the subgroup of the affine transformations of $\mathbb{F}_2^n$.

- $\sigma_{k^{(i)}}$ is the addition with the round key;

$$\begin{aligned} \sigma_{k^{(i)}} : \mathbb{F}_2^n &\longrightarrow \mathbb{F}_2^n \\ m &\longmapsto m \oplus k^{(i)}, \end{aligned}$$

  where $\oplus$ denotes the bitwise addition modulo 2 (XOR).

3.4 Possible Attacks

The *brute force attack* is one of the most natural strategies an attacker might employ to break a cryptosystem, which is a difficult process. This approach requires the attacker testing every key until they locate the right one, which can take some time. To prevent such assaults, modern cryptosystems are built to make it computationally impossible to guess the right key. Hence, the goal of *cryptanalysis* is to use a cryptosystem's weaknesses to access the contents of encrypted messages.

The *Kerckhoffs' principle*, which presumes that the attacker is privy to cryptosystem being employed, is one of the presumptions made in cryptanalysis. Modern cryptography thus seeks to provide secure cryptosystems without hiding the algorithm that was used.

The attack model in cryptanalysis defines the resources and information at the disposal of an adversary during an attack on a cryptosystem. Depending on the resources and information at the attacker's disposal, the power of the attack can be classified into distinct types, as follows [20]:

- **Ciphertext-only Attack (COA)**: This is the least powerful attack, in which the attacker can only access the encrypted messages and makes assumptions about certain characteristics of the plaintexts. An example of attack under this model is the brute force attack.
- **Known Plaintext Attack (KPA)**: The attacker in a known-plaintext attack has access to some plaintext-ciphertext pairs. This information is used by the attacker to determine the encryption key, which can subsequently be used to decrypt other messages that were encrypted using the same key. A prominent cryptanalysis method that uses this attack model is *linear cryptanalysis*.

- **Chosen Plaintext Attack (CPA)**: In a chosen plaintext attack, the plaintext messages to be encrypted are selected by the attacker, who can then look at the accompanying ciphertexts. The ability to learn the encryption algorithm and determine the key used in the encryption process makes this kind of attack particularly powerful. A prominent cryptanalysis method that uses this attack model is *differential cryptanalysis*.
- **Chosen Ciphertext Attack (CCA)**: In this attack model, the attacker selects a ciphertext and recovers its corresponding plaintext via a decryption algorithm. In other words, the attacker can request that a ciphertext of his choice be decrypted and use the corresponding plaintext to gain insight about the encryption or secret key used. A prominent cryptanalysis method that uses this attack model is differential cryptanalysis on stream ciphers.
- **Related-Key Attack (RKA)**: In this model of attack, the attacker can gain access to the encryption or decryption of a message under related keys, which are keys that are generated from the original key in a specific way. An RKA's objective is to obtain information about the master key by taking advantage of the relationship between the related keys.

While the earlier discussed models of attack do a good job of capturing many realistic scenarios, they are not exhaustive, and advanced cryptanalysis techniques have been created to get around their limitations. In these techniques, an attacker needs a combination of mathematical and puzzle-solving skills, plus luck. There are a few of these more advanced techniques which can be employed [21]:

- **Differential Cryptanalysis**: In differential cryptanalysis one looks at ciphertext pairs, where the corresponding plaintexts have a particular difference. The exclusive-or of such pairs is called a differential and certain differentials have certain probabilities associated with them, depending on what the key is. By analysing the probabilities of the differentials computed in a chosen plaintext attack one can hope to reveal the underlying structure of the key.
- **Linear Cryptanalysis**: Even though a good block cipher should contain non-linear components the idea behind linear cryptanalysis is to approximate the behaviour of the non-linear components with linear functions. Again the goal is to use a probabilistic analysis to determine information about the key.
- **Algebraic Cryptanalysis**: Using a set of algebraic equations to represent the encryption function, algebraic cryptanalysis is a potent method for breaking into cryptographic systems. An attacker can decrypt communications or create new ones by solving these equations in order to obtain the secret encryption key.

Surprisingly these two methods are quite successful against some ciphers. Both DES and AES are designed to resist differential cryptanalysis, whereas AES is designed to also resist linear cryptanalysis.

3.5 ADVANCED ENCRYPTION STANDARD (AES)

3.5.1 AES Selection Process

The Advanced Encryption Standard was chosen in a five-year competition that was organized by NIST (National Institute of Standards and Technology) in 1997 to replace the outdated DES (Data Encryption Standard) encryption algorithm after it had become susceptible to some attacks, thus losing its security potency. In the end, the Rijndael algorithm, created by two Belgian cryptographers Joan Daemen and Vincent Rijmen, was chosen after a thorough review of 15 candidate algorithms from around the world. In the international cryptography community, the AES selection procedure is regarded as a model of openness, transparency, and collaboration [11].

Rijndael was selected by NIST as the Advanced Encryption Standard for a number of reasons, including its high security margin, quick encryption/decryption speed, elegant structure, and suitability for effective software implementations on a wide range of computing platforms. The cryptography world praised Rijndael for its security, performance, and adaptability, and according to NIST, it displayed a strong security margin. Furthermore, compared to the other entries in the AES competition, Rijndael was a lot faster, making it a desirable choice for real-world applications [22].

3.5.2 Structure

The Rijndael block cipher, which is defined by its specification, is a version of the AES. The fundamental distinction between the two is that Rijndael may accept any multiple of 32 bits with a minimum of 128 bits and a maximum of 256 bits, whereas AES can only handle a block length of 128 bits and key lengths of 128, 192, or 256 bits. AES uses one-dimensional arrays of bytes for input and output, with encryption producing ciphertext blocks from plaintext blocks and keys as inputs. Similar to encryption, decryption produces a plaintext block from an input ciphertext block and key. The AES, like every other block cipher, consists of a repetitive round transformation that operates on an intermediate result known as the *state*. The key length determines the number of rounds, which will be indicated by N_r as shown in Table 3.1.

Table 3.1: Key length and number of rounds for AES

Key length	N_r
128 bits	10
192 bits	12
256 bits	14

The state can be represented as by 4×4 matrix of bytes, with each byte representing a different element of the matrix. The plaintext block can be represented by $p_0p_1p_2 \dots p_{15}$, where p_0 represents the first byte and p_{15} represents the last byte of the plaintext block. Likewise, a ciphertext block can be represented by $c_0c_1c_2 \dots c_{15}$. Finally, let the state matrix be represented by

$$S = (s_{i,j})_{0 \le i,j < 4},$$

where $s_{i,j}$ denotes the byte in the $(i+1)^{\text{th}}$ row and $(j+1)^{\text{th}}$ column.

The following equation describes how the plaintext block is mapped into the state matrix during encryption process.

$$s_{i,j} = p_{i+4j}, \quad 0 \le i < 4, 0 \le j < 4.$$

After encryption, each byte of the ciphertext is extracted from the state matrix following the equation;

$$c_h = s_{h \bmod 4, \lfloor h/4 \rfloor}, \quad 0 \le h < 16,$$

where $\lfloor h/4 \rfloor$ denotes the largest integer less than or equal to 4.

The following equation describes how the ciphertext block is mapped into the state matrix during decryption process.

$$s_{i,j} = c_{i+4j}, \quad 0 \le i < 4, 0 \le j < 4.$$

After decryption, each byte of the plaintext is extracted from the state matrix following the equation

$$p_h = s_{h \bmod 4, \lfloor h/4 \rfloor}, \quad 0 \le h < 16.$$

Similarly, the key is mapped onto a rectangular array having four rows. The number of columns of the cipher key we will denote by N_k, and is equal to the length of the key divided by 32.

Let the bytes of keys be represented by $z_0 z_1 z_2 \ldots z_{4N_k-1}$ and the cipher key by

$$K = k_{i,j}, \quad 0 \le i < 4, 0 \le j < N_k.$$

The key bytes are mapped into the cipher key according to:

$$k_{i,j} = z_{i+4j}, \quad 0 \le i < 4, 0 \le j < N_k.$$

The matrix representations of the state key and cipher key for the case $N_k = 4$ are given, respectively, as:

$$\begin{bmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{bmatrix} \qquad \begin{bmatrix} z_0 & z_4 & z_8 & z_{12} \\ z_1 & z_5 & z_9 & z_{13} \\ z_2 & z_6 & z_{10} & z_{14} \\ z_3 & z_7 & z_{11} & z_{15} \end{bmatrix}.$$

3.5.3 Encryption

Adding an initial key to the input state is the first step in the AES encryption process. Next, a series of $N_r - 1$ round transformations are applied, with the final round being unique from the earlier rounds. The current state and a round key, which is created using the key schedule derived from the cipher key, are the only inputs required for each round. The *SubBytes*, *ShiftRows*, *MixColumns*, and *AddRoundKey* stages make up the round transformation. Because it skips the MixColumns step, the final round is atypical.

Table 3.2 shows the steps of the AES encryption process for a 128-bit block size and a 128-bit cipher key.

Table 3.2: AES Encryption Process

Round	Input	Key	Transformation	Output
Initial	Plaintext	Cipher Key	Key Addition	State
Round 1	State	Round Key 1	SubBytes	State’
	State’		ShiftRows	State”
	State”		MixColumns	State”’
	State”’		AddRoundKey	State1
...	...	...	...	...
Round 9	State8	Round Key 9	SubBytes	State8’
	State8’		ShiftRows	State8”
	State8”		MixColumns	State8”’
	State8”’		AddRoundKey	State9
Final	State9	Round Key 10	SubBytes	State9’
	State9’		ShiftRows	State9”
	State9”		AddRoundKey	Ciphertext

SubBytes

The SubBytes step is a non-linear byte substitution that swaps out each byte of the state matrix for a corresponding byte from the *S-Box*, a fixed 256-element lookup table. AES employs two different types of S-Boxes, one for encryption and the other for decryption rounds, each of which is the inverse of the other. The S-Box used in the AES encryption algorithm is designed to have a simple mathematical structure, allowing for a formal argument of the resistance of cipher to differential and linear cryptanalysis. The mathematical operations of AES are based on arithmetic in the finite fields $\mathbb{F}_{2^8}$ and $\mathbb{F}_2$. The elements in the finite field $\mathbb{F}_{2^8}$ are represented as polynomials with coefficients in the field $\mathbb{F}_2$ and a degree strictly less than 8. This means that each element of $\mathbb{F}_{2^8}$ may be expressed as a polynomial with binary coefficients (i.e., 0 or 1), and a degree of no more than seven. Arithmetic in $\mathbb{F}_{2^8}$ in the AES algorithm is performed using polynomial modulo the irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1.$$

Each byte $s = [s_7, \ldots, s_0]$ of the AES state matrix is taken in turn and considered as an element of $\mathbb{F}_{2^8}$. Mathematically, the S-Box can be described in two steps:

1. Compute the multiplicative inverse of s in $\mathbb{F}_{2^8}$ to produce a new byte $x = [x_7, \ldots, x_0]$. However, for the element $[0, \ldots, 0]$, which has no multiplicative inverse, it is mapped to zero using a convention to maintain a one-to-one mapping between the input and output of the S-Box.
2. After obtaining the bitvector x, it is mapped to another bitvector y using the following affine $\mathbb{F}_2$ transformation:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} \leftarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

By first inverting the affine transformation and then taking the multiplicative inverse, the decryption S-Box is obtained.

ShiftRows

In the ShiftRows step, the bytes in each row of the state array are shifted cyclically to the left by a certain number of bytes. The first row is left unaltered, followed by a leftward shift of one byte, two bytes, and finally three bytes in the second, third, and fourth rows respectively. The inverse of the ShiftRows operation is simply the equivalent shift in the opposite direction. The ShiftRows operation helps to diffuse the input data and increase the security of the encryption algorithm. The matrix representation of the operation is given by

$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} \mapsto \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,1} & s_{1,2} & s_{1,3} & s_{1,0} \\ s_{2,2} & s_{2,3} & s_{2,0} & s_{2,1} \\ s_{3,3} & s_{3,0} & s_{3,1} & s_{3,2} \end{bmatrix}.$$

Let $s_{i,j}$ and $s'_{i,j}$ represent the state bytes in position $(i+1, j+1)$ position before and after the ShiftRows operation. Then, mathematically, we have

$$s'_{i,j} = s_{i,j+i \bmod 4}, \qquad 0 \leq i,j < 3.$$

MixColumns

In the state matrix, the MixColumns operation makes sure that the rows *interact* with one another over a number of rounds, and when combined with the ShiftRows operation, it makes sure that each byte of the output state is dependent on each byte of the input state. The columns of the state are considered as polynomials over $\mathbb{F}_{2^8}$ and multiplied modulo x^4+1 with a fixed polynomial $c(x)$. Conditions are placed on the coefficients of $c(x)$ by the requirements for invertibility, diffusion, and performance [11]. The polynomial $c(x)$ is given by

$$c(x) = 03 \cdot x^3 + 01 \cdot x^2 + 01 \cdot x + 02,$$

and is coprime to x^4+1, hence invertible. Let $s'_j(x) = c(x) \cdot s_j(x) \mod x^4+1$, where $s'_j(x), s_j(x) \in \mathbb{F}_{2^8}$ are the polynomials generated by the $(j+1)^{\text{th}}$ columns of the state before and after the MixColumns operation respectively. Since modular multiplication with a fixed polynomial can be written as a matrix multiplication, we have

$$\begin{bmatrix} s'_{0,j} \\ s'_{1,j} \\ s'_{2,j} \\ s'_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 03 \end{bmatrix} \begin{bmatrix} s_{0,j} \\ s_{1,j} \\ s_{2,j} \\ s_{3,j} \end{bmatrix}.$$

The above matrix is invertible in $\mathbb{F}_{2^8}$, making it also possible to construct the inverse of the MixColumns operation using a matrix multiplication like the one above.

AddRoundkey

The key addition is denoted AddRoundKey. In this transformation, the state is modified by combining it with a round key with the bitwise XOR operation, as given by the matrix representation

$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} \oplus \begin{bmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{bmatrix}.$$

In each round h, $0 \leq h \leq N_r$, of the encryption process, a round key whose length coincides with that of the block, is generated from the cipher key using the key schedule. The h^{th} round key is composed of bytes $k_{i,j}^{(h)}$, where i and j represent the position of the byte in the round key. The state of the cipher is represented by bytes $s_{i,j}$, where i and j represent the position of the byte in the state. After the AddRoundKey transformation is performed, the state is updated to $s'_{i,j}$, which is equal to the XOR operation of $s_{i,j}$ and $k_{i,j}^{(h)}$. Mathematically speaking, we have

$$s'{}_{i,j} = s_{i,j} \oplus k_{i,j}^{(h)}, \quad \forall\, i, j \in \{0, 1, 2, 3\}.$$

3.5.4 Key Schedule

In this section we present the general structure of the Key Schedule of AES. Then in Section 4 we give its algebraic representation. The *key expansion* and the round key selection make up the two components of the key schedule. The key expansion specifies how the ExpandedKey is derived from the cipher key. Since the encryption requires one round key for the initial key addition and one for each round, the total amount of bits in ExpandedKey is equal to the block length multiplied by the number of rounds plus 1. During the key expansion the cipher key is expanded into a matrix of bytes, consisting of 4 rows and $4(N_r + 1)$ columns. We will denote by W such matrix. The round key of the h^{th} round, given that $h \in \mathbb{N}$ is such that $0 \leq h \leq N_r$, is given by columns $4h$ to $4h - 3$ of W.

The key expansion function depends on the value of N_k: there is a version for N_k less than or equal to 6, and a version for N_k greater than 6. In both versions of the key expansion, the first N_k columns of W are filled with the cipher key. The subsequent columns are defined recursively in terms of previously defined columns. The recursion uses the bytes of the previous column, the bytes of the column N_k positions earlier, and round constants $RC[t]$, defined by a recursion rule in $\mathbb{F}_{2^8}$, given below.

$$\begin{aligned} RC[1] &= 1, \\ RC[2] &= x, \\ RC[t] &= x \cdot RC[t-1] = x^{t-1}, \quad t > 2. \end{aligned}$$

The behavior of the recursion function is determined by the position of the column in W. Suppose $N_k \leq h \leq 4N_r$ and $W_h \in (\mathbb{F}_{2^8})^4$ is the h^{th} column of W. When $N_k \leq 6$, the following Equation 3.1 holds:

$$W_h = \begin{cases} W_{h-N_k} \oplus W_{h-1} & \text{if } h \neq 0 \mod N_k \\ W_{h-N_k} \oplus F_{h/N_k}(W_{h-1}) & \text{if } h \equiv 0 \mod N_k \end{cases}, \tag{3.1}$$

However, when $N_k > 6$, the following Equation 3.2 applies:

$$W_h = \begin{cases} W_{h-N_k} \oplus F_{h/N_k}\left(W_{h-1}\right) & \text{if } h \equiv 0 \mod N_k \\ W_{h-N_k} \oplus G\left(W_{h-1}\right) & \text{if } h \equiv 4 \bmod N_k \\ W_{h-N_k} \oplus W_{h-1} & \text{otherwise,} \end{cases} \tag{3.2}$$

where

- $\{F_\tau\}_{\tau\in\mathbb{N}}$ is the set of non-linear functions:

$$\begin{aligned} F_\tau : (\mathbb{F}_{2^8})^4 &\longrightarrow (\mathbb{F}_{2^8})^4 \\ \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} &\longmapsto \begin{bmatrix} \gamma(a_2) \oplus RC[\tau] \\ \gamma(a_3) \\ \gamma(a_4) \\ \gamma(a_1) \end{bmatrix} \end{aligned}$$

- G is the non-linear function:

$$\begin{aligned} G : (\mathbb{F}_{2^8})^4 &\longrightarrow (\mathbb{F}_{2^8})^4 \\ \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} &\longmapsto \begin{bmatrix} \gamma(a_1) \\ \gamma(a_2) \\ \gamma(a_3) \\ \gamma(a_4) \end{bmatrix} . \end{aligned}$$

- γ is the AES S-Box.

4 Preliminary Results and Model

To begin, we will provide some notation and initial findings, and we will commence by briefly reminding the definition of the AES-128 key schedule. The reader is encouraged to consult Daemen and Rijmen for a full discussion and comments on design decisions [11].

The AES-128 key schedule is an injective function $\in \mathrm{Sym}(\mathbb{F}_2^{128})$, which starting from the master key, takes as input the previous round key and produces/releases as output the corresponding round key at each round of the encryption process.
Below is the ith transformation of the AES-128 key schedule.

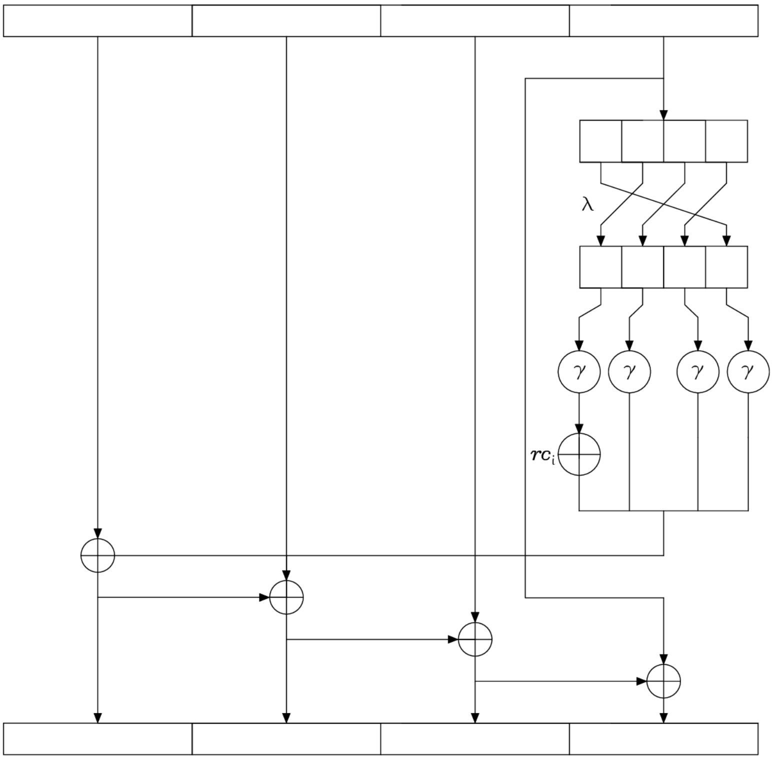

Figure 4.1: The ith transformation of the AES-128 key schedule

Components of Figure 4.1 are given by:

- $\lambda : \mathbb{F}_2^{32} \longrightarrow \mathbb{F}_2^{32}$ is a function that takes as input a 32-bit binary string (i.e., an element of the vector space $\mathbb{F}_2^{32}$) and outputs another 32-bit binary string. It performs a left circular shift on the previous round key (RotWord operation).
- $\gamma : \mathbb{F}_2^{8} \longrightarrow \mathbb{F}_2^{8}$ is a function that takes as input an 8-bit binary string (i.e., an element of the vector space $\mathbb{F}_2^{8}$) and outputs another 8-bit binary string. It represents a byte substitution operation that maps each byte input to a unique byte output.
- $rc_i \in \mathbb{F}_2^8$ is an 8-bit binary string in $\mathbb{F}_2^8$. It is a round constant different in each round.

Observe that the bits of the round key are split into four blocks, with four bytes making up each block. The bytes of the last block are shifted to the left by one position, resulting in the leftmost byte occupying the rightmost position. The newly bitwise arranged block is then transformed by the cipher's S-Box after which a round dependent counter is xor-ed to the first byte of the block.

After the transformation, the resulting output is xor-ed with the other three blocks of bytes, as depicted in Figure 4.1.

Notation

Throughout this work the following notations are used: $n \in \mathbb{Z}^+ \cup \{0\}$ is a non-negative integer and $V = \mathbb{F}_2^n$ is an n-dimensional vector space over the finite field $\mathbb{F}_2$. We write $A \leq V$ if A is a subspace of V, and the same notation is the case if A is a subgroup of V. $\mathbb{0} : V \rightarrow V$ is the null function on V i.e. it maps every element of V to the zero vector of V. $\mathrm{Sym}(V)$ denotes the symmetric group acting on V and $\mathbb{1}$ its identity. We use the notation xf to represent the output of the function f when it is evaluated at the input x, provided that $f \in \mathrm{Sym}(V)$ and $x \in V$. The group of translations on V is denoted by T_n. The group of affine permutations of V is denoted by $\mathrm{AGL}(V)$, while the group of linear permutations is denoted by $\mathrm{GL}(V)$.

Naturally we will think of n as the size of each block of 4 bytes, i.e. $n = 32$ bits. Following from this, $V = \mathbb{F}_2^{32}$, $V^2 = \mathbb{F}_2^{64}$, $V^3 = \mathbb{F}_2^{96}$, and $V^4 = \mathbb{F}_2^{128}$.
It is then easily noticeable that the key scheduling transformation, acting on all four blocks of bytes i.e. V^4 , is an element of $\mathrm{Sym}(V^4)$. The translation group on V^4 will be denoted by T_{4n}, where the translation $\sigma_{(v_1,v_2,v_3,v_4)} \in T_{4n}$ acts on $(x_1, x_2, x_3, x_4) \in V^4$ as

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

Note that the transformation done by the round counter of the AES-128 key schedule is an element of T_{4n}.

To make things easier to understand, we will use different symbols for elements in V, V^2, and V^4. Specifically, we will represent an element in V^4 by adding an arrow above the symbol, like this: $\vec{v} \in V^4$. An element in V^2 will be denoted using bold symbols, like this: $\vec{v} = (\boldsymbol{v}_1, \boldsymbol{v}_2)$, in such a way that we have the following relation:

$$\vec{v} = (\boldsymbol{v}_1, \boldsymbol{v}_2) = (v_1, v_2, v_3, v_4) \in V^4,$$

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

The key-schedule representation

Let us now introduce the representation of the AES-128 key-schedule, given in [23], that allows us to provide an easy description of the subgroup of $\mathrm{Sym}\left(V^4\right)$ which is the subject of this work. Let us start by defining the transformation acting on the last group of four bytes, as in Figure 4.1

Definition 4.1. Let ρ_{AES} represent the transformation of the last block of bytes before the addition with the round counter to the first byte in the block. This transformation is essentially the composition of functions $\lambda \in \mathrm{Sym}(V)$, and $\gamma' \in \mathrm{Sym}(V)$, i.e.

$$\rho_{\text{AES}} \overset{\text{def}}{=} \lambda\gamma'$$

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 $v_i \in \mathbb{F}_2^8$.
NB: $\rho_{\text{AES}} \in \mathrm{Sym}(V)$, (since $\mathrm{Sym}(V)$ is closed under the operation of function composition).

The above transformation captures only the last block of bytes of the AES-128 key schedule. As a result, a more general description of the full transformation is given in the following definition.

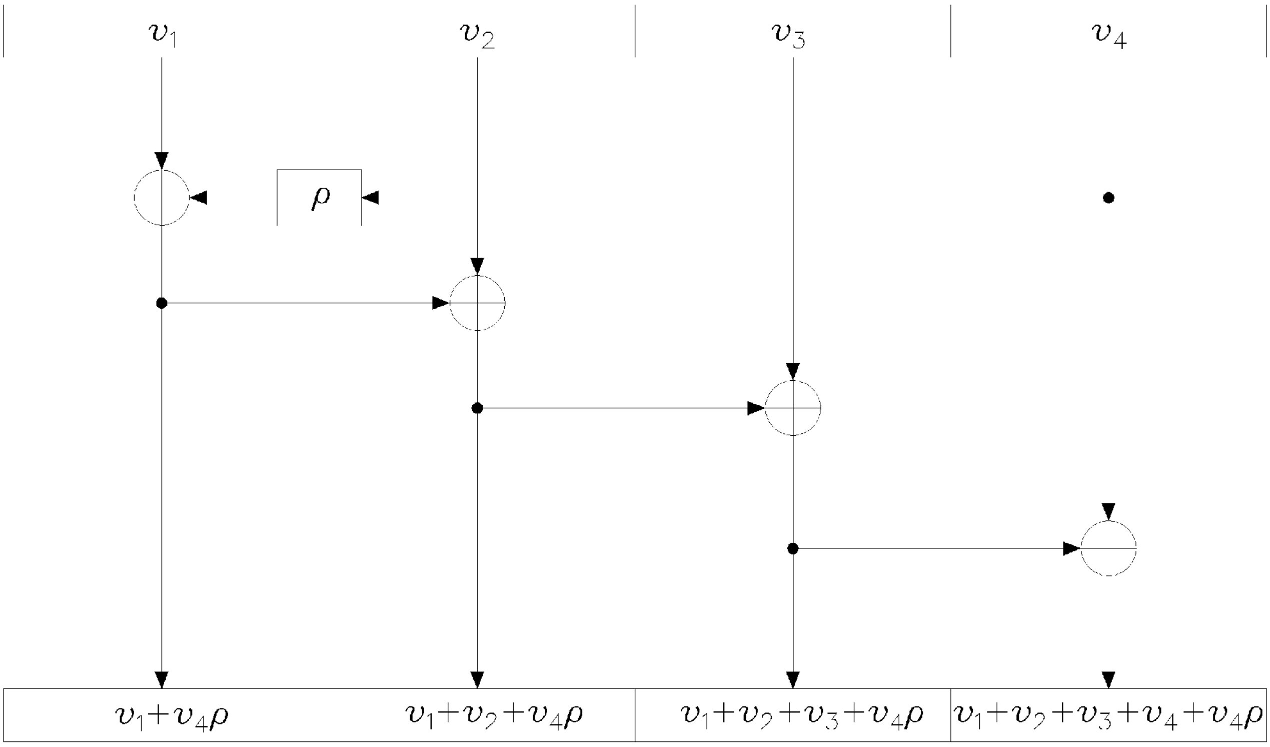

Figure 4.2: The key schedule operator induced by ρ

Definition 4.2. Given $\rho \in \mathrm{Sym}(V)$, we define the operator $\overline{\rho}$ induced by ρ as the formal matrix

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

acting on V^4 as

$$(v_1, v_2, v_3, v_4) \begin{pmatrix} \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ \mathbb{0} & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ \mathbb{0} & \mathbb{0} & \mathbb{1} & \mathbb{1} \\ \rho & \rho & \rho & \mathbb{1}+\rho \end{pmatrix} \mapsto (v_1 + v_4\rho, v_1 + v_2 + v_4\rho, v_1 + v_2 + v_3 + v_4\rho, v_1 + v_2 + v_3 \\ + v_4 + v_4\rho),$$

as corroborated by Figure 4.2. The inverse, $\overline{\rho}^{-1}$ of the operator $\overline{\rho}$ acts on V^4 as

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

Observe that the map $\overline{\rho_{\mathrm{AES}}}\sigma_{(\overline{rc_i}, \overline{rc_i}, \overline{rc_i}, \overline{rc_i})}$ rightly corresponds to and represents the ith round key's transformation of the AES-128 key schedule (4.1), where $\overline{rc_i} = (rc_i, 0, 0, 0) \in \mathbb{F}_2^{32}$. $\sigma_{(\overline{rc_i}, \overline{rc_i}, \overline{rc_i}, \overline{rc_i})}$ acts on

$$(v_1 + v_4\rho_{\mathrm{AES}}, v_1 + v_2 + v_4\rho_{\mathrm{AES}}, v_1 + v_2 + v_3 + v_4\rho_{\mathrm{AES}}, v_1 + v_2 + v_3 + v_4 + v_4\rho_{\mathrm{AES}})$$

as

$$(v_1 + v_4\rho_{\text{AES}}, v_1 + v_2 + v_4\rho_{\text{AES}}, v_1 + v_2 + v_3 + v_4\rho_{\text{AES}}, v_1 + v_2 + v_3 + v_4 + v_4\rho_{\text{AES}}) \mapsto$$

$$\mapsto (v_1 + v_4\rho_{\text{AES}} + \overline{rc_i}\,, v_1 + v_2 + v_4\rho_{\text{AES}} + \overline{rc_i}\,, v_1 + v_2 + v_3 + v_4\rho_{\text{AES}} + \overline{rc_i}\,, v_1 + v_2 + v_3 + v_4 + v_4\rho_{\text{AES}} + \overline{rc_i}\,)\,.$$

Reminding ourselves, the focus of this work is to study the group theoretical properties of the subgroup $\Gamma < \text{Sym}(V^4)$ generated by maps of the type $\overline{\rho_{\text{AES}}}\sigma_{(\overline{rc_i},\overline{rc_i},\overline{rc_i},\overline{rc_i})}$ for each admissible value $rc_i \in \mathbb{F}_2^8$ and show that it is primitive in the spirit of Lemma 2.16. Let us remark that Γ does not contain the whole translation group T_{128}. This is captured in the fact that each $\overline{rc_i}$ can admit only 2^8 elements $\in \mathbb{F}_2^{32}$ as opposed to the 2^{32} elements making up whole vector space $\mathbb{F}_2^{32}$. Due to this, we need to extend Γ by assuming a rather general action of the round counter.

Definition 4.3. We define the group

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

Notice the following facts.

- Γ_{AES}, which contains Γ, is the smallest subgroup of the symmetric group $\text{Sym}(V^4)$ that contains both the whole translation group T_{128} and the transformation of the AES-128 key-schedule, when the correct round counter is chosen.
- $\Gamma_{\text{AES}} = \langle \overline{\rho_{\text{AES}}}, T_{128} \rangle$.

Proof. By definition, $\overline{\rho_{\text{AES}}}\sigma_{(x,y,z,t)}$ is in Γ_{AES} for each (x, y, z, t) in V^4 including $(0, 0, 0, 0)$. Therefore $\overline{\rho_{\text{AES}}}\sigma_{(0,0,0,0)} = \overline{\rho_{\text{AES}}}\,\text{Id} = \overline{\rho_{\text{AES}}}$ is in Γ_{AES} (where Id is the identity permutation). Since Γ_{AES} is a group and $\overline{\rho_{\text{AES}}}$ is in Γ_{AES}, we have that $\overline{\rho_{\text{AES}}}^{-1}$ is also in Γ_{AES} and $\overline{\rho_{\text{AES}}}^{-1}\overline{\rho_{\text{AES}}}\sigma_{(x,y,z,t)} = \sigma_{(x,y,z,t)}$ is in Γ_{AES} for every (x, y, z, t) in V^4. Hence, we have that both $\overline{\rho_{\text{AES}}}$ and $\sigma_{(x,y,z,t)}$ are in Γ_{AES}, and so, $\Gamma_{\text{AES}} = \langle \overline{\rho_{\text{AES}}}, T_{128} \rangle$. □

Left to us is to establish the primitivity of Γ_{AES}, with consequence that no partition which is a block system for Γ_{AES} can be generated from any nontrivial and proper subgroup $U < V^4$.

5 The primitivity of Γ_{AES}

We will prove the primitivity of Γ_{AES} in this section, and while we are at it, we will show that the transitivity of $\langle \overline{\rho}, T_{4n} \rangle$ and nonexistence of a block system for $\langle \overline{\rho}, T_{4n} \rangle$ reduces to the transitivity of $\langle \rho, T_n \rangle$ and nonexistence of a block system for $\langle \rho, T_n \rangle$ when $\overline{\rho}$ as presented in Definition 4.2 is bijective and not affine.

Theorem 5.1 (Primitivity reduction). *Let $\rho \in \text{Sym}(V) \setminus \text{AGL}(V)$. If $\langle \rho, T_n \rangle$ is primitive on V, then $\langle \overline{\rho}, T_{4n} \rangle$ is primitive on V^4.*

Before we delve into the proof, let us first prove that $\rho = \rho_{\text{AES}}$ satisfies the hypothesis of Theorem 5.1 (i.e. the group $\langle \rho_{\text{AES}}, T_{32} \rangle$ is primitive). To do so, the following definitions and the general notion of primitivity of substitution-permutation networks (SPNs) serve useful for us.

Let us write n as the product of two positive integers s and b such that s and b are both greater than 1, i.e., $n = s \cdot b$. We decompose the vector space V into a direct sum of b subspaces, denoted as $V_1, V_2, \dots, V_b$, where each subspace V_i has dimension s. These subspaces are referred to as "bricks". The subspace V_i is spanned by the canonical basis vectors $e_{s(i-1)+1}, e_{s(i-1)+2}, \dots, e_{s(i-1)+s}$, where $e_1, e_2, \dots, e_n$ are the canonical basis vectors of V. For ρ_{AES}, $n = 32$, $s = 8$ and $b = 4$.

Let us recall some useful notions from boolean functions [24].

Given the vector space $\mathbb{F}_2^s$, we refer to a function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$, $n, m \in \mathbb{Z}^+$ as a vectorial boolean function or $(n - m)$ function. In what follows in this work, we consider $m = n$. Given $f : \mathbb{F}_2^s \longrightarrow \mathbb{F}_2^s$, for each nonzero $u \in \mathbb{F}_2^s$, denote by $x\hat{f}_u = xf \oplus (x \oplus u)f$ the derivative of f in the direction of u.

Definition 5.2. We say that f is deferentially δ-uniform if for each nonzero $u \in \mathbb{F}_2^s$, $\left|\text{Im}\left(\hat{f}_u\right)\right| \geq \frac{2^s}{\delta}$.

This means that $\hat{f}_u$ has an image with at least $\frac{2^s}{\delta}$ distinct outputs. In other words, if we flip any nonzero input bit, the resulting output bits are uniformly distributed across all possible s-bit strings with high probability.

Definition 5.3. f is said to be δ-anti-invariant if for any two subspaces W_1 and W_2 of $\mathbb{F}_2^s$ such that $W_1 f = W_2$, either $\dim(W_1) = \dim(W_2) < s - \delta$ or $W_1 = W_2 = \mathbb{F}_2^s$.

Intuitively, this means that if two subspaces of the input space of f have the same output under f, then either they have the same dimension and their dimension is less than $s - \delta$, or they are the entire input space. This is a desirable property for cryptographic functions because it makes it difficult for an attacker to exploit any linear relationships between the input and output of the function.

The notation that was presented earlier in this section is used to express the following theorem.

Theorem 5.4. *[24] Let $f \in \text{Sym}\left(\mathbb{F}_2^s\right)$ such that $0f = 0$, let $F \in \text{Sym}(V)$ be the function acting as f on each s-dimensional brick V_i of V and let $\Lambda \in \text{GL}(V)$. 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

It can be proved that $\langle \rho_{\text{AES}}, T_{32} \rangle$ is primitive as a result of Theorem 5.4.

Theorem 5.5. *The group $\langle \rho_{\text{AES}}, T_{32} \rangle < \text{Sym}\left(\mathbb{F}_2^{32}\right)$ is primitive.*

Proof. [23] As Definition 4.1 has it, Let $\lambda \in \mathrm{GL}(V)$ and $\gamma' \in \mathrm{Sym}(V)$ be the RotWord transformation and the S-Box SubBytes respectively. Essentially, it is widely recognized that the function γ, up to affine transformations, fixes the zero element and sends every non-zero element into its multiplicative inverse in $\mathbb{F}_{2^s}$. Such a function is 4-differentially uniform and 1-anti invariant. This means that it satisfies the premises of Theorem 5.4 for $\delta = 2$. It is worth noting that anti-invariance and differential uniformity remain unchanged under inversion and affine transformations. Thus, γ^{-1} also satisfies the hypotheses of Theorem 5.4. We can easily verify that λ does not leave any non-trivial and proper direct sum of bricks in V invariant. The same applies to λ^{-1}. By Theorem 5.4, we know that $\left\langle (\gamma')^{-1} \lambda^{-1}, T_{32} \right\rangle$ is primitive. Consequently, $\langle \lambda\gamma', T_{32} \rangle = \langle \rho_{\mathrm{AES}}, T_{32} \rangle$ is also primitive.

□

The conclusive statement that follows is obtained.

Corollary 5.6. *The group* $\langle \overline{\rho_{\mathrm{AES}}}, T_{128} \rangle < \mathrm{Sym}\left(\mathbb{F}_2^{128}\right)$ *generated by the transformations of the AES-128 key-schedule is primitive.*

6 The Primitivity Reduction - Proof of Theorem 5.1

This section is completely dedicated to the somewhat technical proof of Theorem 5.1. Notwithstanding its seeming intricacy, the (repeated) application of Goursat's lemma, as presented below, is a reasonable way to characterize any generic subspace U that is a candidate for a linear block.

To demonstrate our outcome, we must identify a block system for V^4, which is equivalent to finding the set of cosets of a suitable subgroup of $V^2 \times V^2$. We can achieve this by utilizing the following characterization of subgroups of the direct product of two groups, which involves identifying appropriate sections of the direct factors [25].

Theorem 6.1 (**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,*
- *$\psi : A/B \longrightarrow C/D$ is a group isomorphism.*

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

$$U = U_\psi = \{(a, c) \in A \times C \mid (a + B)\psi = c + D\}. \tag{6.1}$$

Proof. See page 6 of [26] for an outline of the proof. □

Note that the isomorphism ψ induces a homomorphism $\varphi : A \longrightarrow C$ 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. In fact, if ψ is an isomorphism between A/B and C/D, then we can define a different homomorphism φ' as $a\varphi' = c'$ where $(a + B)\psi = c' + D$. This will also satisfy the required properties, but may be different from φ.

Corollary 6.2. *Following the notation of Theorem 6.1, given any homomorphism φ induced by ψ, we have*

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

Proof. Let $(a, c) \in U_\psi$. By definition of φ, $(a + B)\psi = c + D = a\varphi + D$. From $a\varphi + D = c + D$, we know that c and $a\varphi$ are in the same coset of D. In other words, $c \in a\varphi + D$ which translates to mean that $c = a\varphi + d$ for some $d \in D$, where d is the unique element of D that satisfies $c = a\varphi + d$. Conversely, if $a \in A$ and $d \in D$, then $(a + B)\psi = a\varphi + D = a\varphi + d + D$.

□

6.1 Use of Goursat's Lemma

Given a subspace U of $V^4 = V^2 \times V^2$, and motivated by Theorem 6.1 and Corollary 6.2, we have that there exist $A, B, C, D \leq V^2$ and an isomorphism $\psi : A/B \longrightarrow C/D$ that induces an homomorphism $\varphi : A \longrightarrow C$ such that

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

Without loss of generality, we can extend a basis of A to that of $\mathbb{F}_2^{2n}$ by adding vectors to the original basis of A to obtain a basis for the entire vector space $\mathbb{F}_2^{2n}$, and we can choose any basis of

A^c and any basis of $(\mathrm{Im}(\varphi))^c$, where A^c and $(\mathrm{Im}(\varphi))^c$ are the complements of A in V^2 and $\mathrm{Im}(\varphi)$ respectively, and then extend the function φ to a linear map that maps the basis elements of A^c to the basis elements of $(\mathrm{Im}(\varphi))^c$.

Notice that φ can be arbitrarily defined from the basis of the complement A^c of A to a basis of $(\mathrm{Im}(\varphi))^c$: This means that we have some flexibility in defining how the linear transformation φ maps vectors outside of A to vectors in C as long as we do not interfere with the parts of the space that are already determined by A and φ, i.e. $(\mathrm{Im}(\varphi))^c$. In our case, we define φ to map the basis of A^c to the basis of $(\mathrm{Im}(\varphi))^c$. Note that any vector in A^c can be expressed as a linear combination of the basis vectors of A^c, and since φ is linear, it will preserve this linearity when mapping A^c to $(\mathrm{Im}(\varphi))^c$. Therefore, any mapping from A^c to $(\mathrm{Im}(\varphi))^c$ by φ can be expressed as a linear combination of the basis vectors of $(\mathrm{Im}(\varphi))^c$. Hence, φ maps the entire A^c to $(\mathrm{Im}(\varphi))^c$.

Having extended φ on the whole space $\mathbb{F}_2^{2n}$, the matrix representation theorem (i.e. every linear map between finite-dimensional vector spaces can be represented as a matrix) provides us with a matrix representation of φ as

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

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

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

where for $1 \le i \le 2$

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

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

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

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

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

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

In the rest the work, whenever a subspace U is considered as the linear component of an invariant linear subspace, the above construction and notations will be used, as will be precised in the following.

Definition 6.3. A subgroup $U \le V^4$ is a linear block for $f \in \mathrm{Sym}\left(V^4\right)$ 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 $\vec{w} = \vec{v}f$.

By virtue of Lemma 2.16, when we have found a linear block U for f, then the group $\langle f, T_{4n}\rangle$ is imprimitive where the block system of the group is constructed from the cosets of U. It is also worth noting that if $f \in \mathrm{Sym}\left(V^4\right)$ is such that $\overrightarrow{0}f = \overrightarrow{0}$ and $U < V^4$ is a linear block for f, then U is an invariant subspace for f, i.e. $Uf \subseteq U$. From Definition 6.3 we have that

$$\begin{aligned} (U + \vec{v})f = U + \vec{w} &\implies (U + \vec{v})f = U + \vec{v}f \\ &\implies Uf = U\,, \text{choosing}\, \vec{v} = \vec{0}. \end{aligned}$$

The last equality follows from the fact that f is bijective, i.e. for every $\vec{u} \in U$ there exists a unique $\vec{w} \in U$ such that $\vec{u}f = \vec{w}$. Expressing the relation $Uf = U$ using the notation presented earlier in this section, we have that for every a in A and d in D, there exist x in A and y in D such that

$$(\boldsymbol{a}, \boldsymbol{a}\varphi + \boldsymbol{d})f = (\boldsymbol{x}, \boldsymbol{x}\varphi + \boldsymbol{y}). \tag{6.2}$$

In the forthcoming results, we will make significant use of Equation 6.2 when discussing functions with linear blocks without explicit reminder.

6.2 Main proof of the thesis

This section will present the procedure for proving Theorem 5.1, and the notation established in Section 6.1 will be utilized throughout the remainder of the work. To only make things simpler and no more, we assume without loss of generality that $0\rho = 0$, which is reasonable because every conceivable translation is examined in the group being studied (cf. Definition 4.3).

The proof of Theorem 5.1 begins by assuming the presence of a linear block (which in fact will be an invariant subspace) for $\overline{\rho}$ and using it to find an invariant subspace for ρ. If such a subspace exists, it may be trivial or non-trivial. However, If a non-trivial subspace is found, our main claim follows directly from Lemma 6.6, which we will prove in this section. The rest of the work will focus on the remaining scenarios.

Corollary 6.4. *If $U \leq V^4$ be a linear block for $\overline{\rho} \in \mathrm{Sym}\left(V^4\right)$, then it is also an invariant subspace for $\overline{\rho}$ under our assumption that $0\rho = 0$.*

Proof. See Definition 6.3 for what we mean by $U \leq V^4$ is a linear block for $\overline{\rho} \in \mathrm{Sym}\left(V^4\right)$. Setting $\vec{v} = \vec{0}$, we have $(U + \vec{0})\overline{\rho} = U + \vec{0}\overline{\rho}$, but $\vec{0}\overline{\rho} = (0,0,0,0)\,\overline{\rho} = (0\rho, 0\rho, 0\rho, 0\rho) = \vec{0}$. Therefore, we have the relation $U\overline{\rho} = U$, and consequently, U is an invariant subspace for $\overline{\rho}$. □

Corollary 6.5. *U is a linear block for each element of $\langle\overline{\rho}\rangle \leq \mathrm{Sym}\left(V^4\right)$ if it is a linear block for $\overline{\rho}$.*

Proof. This follows directly from Lemmas 2.15 and 2.16. □

Let us show that U is an invariant subspace for $\overline{\rho}^{-1}$ when the relation $0\rho = 0$ holds.

From Definition 6.3, setting $\vec{v} = 0$, we have $(U+\vec{0})\overline{\rho}^{-1} = U+\vec{0}\overline{\rho}^{-1}$, but $\vec{0}\overline{\rho}^{-1} = (0,0,0,0)\,\overline{\rho}^{-1} = (0\rho, 0, 0, 0) = \vec{0}$. Hence, we have $U\overline{\rho}^{-1} = U$ which concludes our claim that U is an invariant subspace for $\overline{\rho}^{-1}$.

The proof of the following result is taken from [23].

Lemma 6.6. *Let $\rho \in \mathrm{Sym}(V)$ and let $U \leq V^4$ be a linear block for $\overline{\rho}$. In the notation of Section 6.1, we have $D''\rho = D''$.*

Proof. Since U is a linear block for $\overline{\rho}$, setting $\boldsymbol{a} = \mathbf{0}$ in Equation 6.2 and considering the description of D as a subgroup of V^2 (cf. (ii) in Section 6.1), for each $a'' \in A''$ and $d'' \in D''$, we have $(0, 0, a'', a''\varphi_D + d'') \in U$. Also, since U is a linear block for each element of $\langle\overline{\rho}\rangle \leq \mathrm{Sym}\left(V^4\right)$, we have $(0,0,0,d'')\,\overline{\rho} = (d''\rho, d''\rho, d''\rho, d'' + d''\rho) \in U$ and $(0,0,0,d'')\,\overline{\rho}^{-3} = (d''\rho, d''\rho, d''\rho, d'') \in U$ when $a'' = 0$. (Observe that $0\varphi_D = 0$ follows from the linearity of φ). Therefore, we can conclude:

$$(d''\rho, d''\rho, d''\rho, d'' + d''\rho) + (d''\rho, d''\rho, d''\rho, d'') = (0, 0, 0, d''\rho) \in U. \tag{6.3}$$

Hence, there exist $\boldsymbol{x} \in A$ and $\boldsymbol{y} \in D$ such that $(0,0,0,d''\rho) = (\boldsymbol{x}, \boldsymbol{x}\varphi + \boldsymbol{y})$. Consequently, $\boldsymbol{x} = \mathbf{0}$ 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 $(0, d''\rho) = (x'', x''\varphi_D + y'')$. This implies $x'' = 0$ and $d''\rho = y'' \in D''$, which gives us the relation $D''\rho = D''$, as desired, since ρ is a permuation, and therefore a bijective map.

□

Lemma 6.6 is used to show that if $\langle \overline{\rho}, T_{4n}\rangle$ is imprimitive, then it is possible to find an imprimitivity block for $\langle \rho, T_n\rangle$. The first natural candidate for this block is D'', inferring from Lemma 6.6. The proof of Theorem 5.1 proceeds as follows: assuming that U is an imprimitivity block for $\langle \overline{\rho}, T_{4n}\rangle$, we use Lemma 6.6 to show that D'' is a block for ρ. If D'' is nontrivial and proper, then there is nothing more to prove. If $D'' = \mathbb{F}_2^n$, we reach a contradiction, and if $D'' = 0$, we show that C'' is a block for ρ. Like before, the proof is completed when C'' is nontrivial and proper and we reach a contradiction when $C'' = \mathbb{F}_2^n$. In the remaining case when $C'' = \{0\}$, we prove that A' is a block for ρ, and we exclude the extreme possibilities for A' by way of contradictions. We will need the following lemma to prove our anticipated results in some of the above cases. Its proof is given in [23].

Lemma 6.7. *Let $\rho \in \mathrm{Sym}(V)$ and let $U \leq V^4$ be a linear block for $\overline{\rho}$. Following the notation of Section 6.1 , 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. $D = \{\mathbf{0}\}$ means that $U = \{(\boldsymbol{a}, \boldsymbol{a}\varphi) \mid \boldsymbol{a} \in A\}$. Since U is a linear block for $\overline{\rho}$, it is also is a linear block and in fact an invariant subspace for $\overline{\rho}^{-1}$ as shown earlier. It follows from Equation 6.2 that for each $\boldsymbol{a} = (a_1, a_2) \in A$ and $\boldsymbol{d} = (0,0) \in D$, there exist $\boldsymbol{x} \in A$ and $\boldsymbol{y} = (0,0) \in D$ such that $(\boldsymbol{a}, \boldsymbol{a}\varphi)\overline{\rho}^{-1} = (\boldsymbol{x}, \boldsymbol{x}\varphi)$. This means that

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

By comparison, $\boldsymbol{x}\varphi = (a_2 + \boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2) = (a_2, \boldsymbol{a}\varphi_1) + \boldsymbol{a}\varphi \in A\varphi$. By the linearity of φ, $(\boldsymbol{x} + \boldsymbol{a})\varphi = (a_2, \boldsymbol{a}\varphi_1)$. Hence $(a_2, \boldsymbol{a}\varphi_1) \in A\varphi$. In a similar manner, for each $\boldsymbol{a} = (a_1, a_2) \in A$ and $\boldsymbol{d} = (0,0) \in D$, there exist $\boldsymbol{x} \in A$ and $\boldsymbol{y} = (0,0) \in D$ such that

$$(\boldsymbol{a}, \boldsymbol{a}\varphi)\overline{\rho}^{-2} = (a_1 + \zeta + (a_2 + \boldsymbol{a}\varphi_2)\,\rho, a_2 + \zeta, a_1 + \boldsymbol{a}\varphi_1, a_2 + \boldsymbol{a}\varphi_2) = (\boldsymbol{x}, \boldsymbol{x}\varphi),$$

where $\zeta = (\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\,\rho$. We have $\boldsymbol{x}\varphi = (a_1 + \boldsymbol{a}\varphi_1, a_2 + \boldsymbol{a}\varphi_2) = (a_1, a_2) + \boldsymbol{a}\varphi \in A\varphi$. Exploiting the linearity of φ, $(\boldsymbol{x} + \boldsymbol{a})\varphi = (a_1, a_2)$. Therefore $(a_1, a_2) \in A\varphi$. This result proves that $A \leq A\varphi$. Furthermore, considering the fact that $|A| \geq |A\varphi|$, and since we cannot guarantee the bijectivity of φ, we obtain our first claim, namely $A = A\varphi$.

Having proved that $(a_2, \boldsymbol{a}\varphi_1) \in A\varphi = A$, and considering A as a subgroup of V^2 as presented in (i) of Section 6.1, there exist $x' \in A'$ and $y' \in D'$ such that $(a_2, \boldsymbol{a}\varphi_1) = (x', x'\varphi_A + y')$, which implies that $a_2 = x' \in A'$. In like manner, for each $(a_1, a_2) \in A$ we have that $a_1 \in A'$. This result proves our second claim that $a_1, a_2 \in A'$. □

We will now fall on the previous lemma to present our principal result, which essentially is prove that, generally speaking, the construction of the AES-like key-schedule generates a permutation group with no block system, given that the key-schedule operator $\overline{\rho}$ is induced by a permutation ρ such that $\langle \rho, T_n\rangle$ has no block system. As earlier indicated, the proof is structured into multiple steps and we will follow the approach outlined in the paragraph preceding Lemma 6.7.

6.2.1 Proof of Theorem 5.1

Assuming that $\langle \overline{\rho}, T_{4n}\rangle$ is imprimitive, i.e. there exists a block system $\mathcal{U}$ for $\langle \overline{\rho}, T_{4n}\rangle$. Then, from Lemma 2.16, the block system is characterized as being of the type

$$\mathcal{U} = \left\{U + \vec{v} \mid \vec{v} \in V^4\right\},$$

where U is a nontrivial and proper subspace of V^4. We have from Lemma 6.6 that $D''\rho = D''$, which translates to mean that should D'' be a nontrivial and proper of V, then it is an imprimitivity block for $\langle \rho, T_n \rangle$, and there is nothing to prove. We will finalize the proof by tackling apart the extreme cases, $D'' = \mathbb{F}_2^n$ and $D'' = \{0\}$.

$\boxed{\mathrm{D}'' = \mathbb{F}_2^{\mathrm{n}}}$ Recall from Equation 6.3 that for each $d'' \in D''$, $(0,0,0,d'') \in U$. Since U is an invariant subspace for $\overline{\rho}$, it follows that

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

But U is a subspace, and so $(0,0,0,d'') + (d''\rho, d''\rho, d''\rho, d'' + d''\rho) = (d''\rho, d''\rho, d''\rho, d''\rho) \in U$. $D'' = \mathbb{F}_2^n$ implies that $D''\rho = \mathbb{F}_2^n$. Since we have shown that for each $d''\rho \in D''$, $(d''\rho, d''\rho, d''\rho, d''\rho) \in U$, if we claim that $D'' = \mathbb{F}_2^n$, then for each $\alpha \in \mathbb{F}_2^n$, $v_1 = (\alpha,\alpha,\alpha,\alpha) \in U$. Note that $v_2 = v_1\overline{\rho}^{-1} = (\alpha,0,0,0) \in U, v_3 = v_2\overline{\rho}^{-1} = (\alpha,\alpha,0,0) \in U$ and $v_4 = v_3\overline{\rho}^{-1} = (\alpha,0,\alpha,0) \in U$. But $v_5 = v_2 + v_3 = (0,\alpha,0,0) \in U, v_6 = v_3 + v_4 + v_5 = (0,0,\alpha,0) \in U$ and $v_7 = v_1 + v_4 + v_5 = (0,0,0,\alpha) \in U$. If we are considering every possible $\alpha \in \mathbb{F}_2^n$, then v_2, v_5, v_6 and v_7 are all the complementary vector subspaces of U whose direct sum is the entire vector space $U = \mathbb{F}_2^{4n} = V^4$. But this contradicts the fact that U is a proper subspace of $\mathbb{F}_2^{4n} = V^4$.

$\boxed{\mathrm{D}'' = \{\mathbf{0}\}}$ First, Let us prove that $B'' = \{0\}$ holds true in the case under discussion. Recall from the general definition of $U = U_{\psi_D}$ (cf. Equation 6.1) that really, $B''\varphi_D \leq D''$. But D'' implies $B''\varphi_D = \{0\}$. Considering 6.2 and setting $\boldsymbol{a} = \mathbf{0}$ and $\boldsymbol{d} = (b'', b''\varphi_D) = (b'', 0)$ with $b'' \in B'' \leq A''$, it follows that $(0,0,b'',0) \in U$. Additionally, $(0,0,b'',0)\,\overline{\rho} = (0,0,b'',b'') \in U$, hence $(0,0,b'',b'') + (0,0,b'',0) = (0,0,0,b'') \in U$. Consequently, $(0,0)\varphi + (0,b'') = (0,b'') \in D$, and therefore there exists $x'' \in A''$ such that $(0,b'') = (x'', x''\varphi_D)$. This means $0 = 0\varphi_D = b''$, hence $B'' = \{0\}$. Since $\{0\}''\varphi_D = \{0\}$, we have also proved that $\varphi_D : A'' \to C''$ is trivially an isomorphism.

If we assign $\boldsymbol{a} = \mathbf{0}$, we obtain

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

and

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

As a result,

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

for some $\boldsymbol{x} \in A$ and $\boldsymbol{y} \in D$. Observe that $(a''\varphi_D\rho + (a'' + a''\varphi_D)\,\rho, a''\varphi_D\rho) \in D$, with meaning that there exists $x'' \in A''$ such that $a''\varphi_D\rho = x''\varphi_D$. So $a''\varphi_D\rho \in A''\varphi_D$ and since ρ is a permutation, $A''\varphi_D\rho = A''\varphi_D$. Having shown that φ_D is an isomorphism, the last equality gives us that $C''\rho = C''$. If C'' a subgroup of V is nontrivial and proper, then we have found another imprimitivity block for $\langle \rho, T_n \rangle$, thus proving our claim. Let us now tackle the extreme cases $C'' = \mathbb{F}_2^n$ and $C'' = \{0\}$ one after the other.

$\boxed{\mathrm{C}'' = \mathbb{F}_2^n}$ The reader should first notice that under this case, $A'' = \mathbb{F}_2^n$ since we already proved that φ_D is an isomorphism. φ_D transcends being just an isomorphism and it is in fact an automorphism since it is an isomorphism and maps $\mathbb{F}_2^n$ to itself. If we set $\boldsymbol{a} = \mathbf{0}$, we obtain

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

with $(a'' + a''\varphi_D)\,\rho \in A'$. Let $S \overset{\text{def}}{=} \{a'' + a''\varphi_D \mid a'' \in A''\}$, then $S\rho \le A'$. Assume $\bar{a} \in A''$ is invariant under the action of φ_D, i.e. $\bar{a} + \bar{a}\varphi_D = 0$, then $(0, 0, \bar{a}, \bar{a}\varphi_D)\,\overline{\rho}^{-1} = (0, 0, \bar{a}, 0)$. Consequently, there exists $x'' \in A''$ such that $\bar{a} = x''$ and $0 = x''\varphi_D$. This implies that $\bar{a}\varphi_D = 0$ and since φ_D is an isomorphism, $\bar{a} = 0$. We have thus proved that $\mathbb{1} + \varphi_D$ is injective, recalling that if the kernel of a linear map is trivial, then the linear map is injective. As a result, $S = \mathbb{F}_2^n$, since $A'' = \mathbb{F}_2^n$. Since $\rho \in \operatorname{Sym}(\mathbb{F}_2^n)$, we have $\mathbb{F}_2^n = S\rho \le A' \le \mathbb{F}_2^n$, and hence $A' = \mathbb{F}_2^n$.

We will now show that $D' = \mathbb{F}_2^n$. Let

$$v_0 = (0, 0, a'', a''\varphi_D) + (0, 0, a'', a''\varphi_D)\,\overline{\rho} = (a''\varphi_D\rho, a''\varphi_D\rho, a''\varphi_D\rho, a'' + a''\varphi_D\rho) \in U,$$

then for each $a'' \in A''$, we obtain

$$v_0\overline{\rho}^{-1} + v_0\overline{\rho}^{-3} = (0, a''\rho, a''\varphi_D\rho + a''\rho, 0) \in U,$$

with $(0, a''\rho) \in A$ and $a''\rho \in D'$. Equivalently, $A''\rho \le D'$, and since $A'' = \mathbb{F}_2^n$ and $\rho \in \operatorname{Sym}(\mathbb{F}_2^n)$, we have $D' = \mathbb{F}_2^n$, which proves our claim. Therefore, we have $A' = D' = \mathbb{F}_2^n$, and thus $B' = C' = \mathbb{F}_2^n$ since, by hypothesis, $A'/B' \cong C'/D'$ (there exists an isomorphism between the quotient group formed out of the cosets of B' in A' and the quotient group formed out of the cosets of D' in C'). This proves that $A = \mathbb{F}_2^{2n}$.

Let us now show that $A \le A\varphi + D \le C$. See that for each $\boldsymbol{a} = (a_1, a_2) \in A$, and setting $\boldsymbol{d} = \boldsymbol{0}$, there exist $\boldsymbol{x} \in A$ and $\boldsymbol{y} \in D$ such that

$$(\boldsymbol{a}, \boldsymbol{a}\varphi)\overline{\rho}^{-2} == (a_1 + \zeta + (a_2 + \boldsymbol{a}\varphi_2)\,\rho, a_2 + \zeta, a_1 + \boldsymbol{a}\varphi_1, a_2 + \boldsymbol{a}\varphi_2) = (\boldsymbol{x}, \boldsymbol{x}\varphi + \boldsymbol{y}),$$

where $\zeta = (\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\,\rho$. By comparison,

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

Rewriting the second-to-last equation, we have $(a_1, a_2) = (\boldsymbol{x} + \boldsymbol{a})\varphi + \boldsymbol{y}$. This implies that $(a_1, a_2) \in A\varphi + D$, which proves that $A \le A\varphi + D$. Let us now show that $A\varphi + D \le C$. Recall that $A\varphi$ and D are both subspaces of C. Thus, it can be shown that $A\varphi + D = \{\boldsymbol{a}\varphi + \boldsymbol{d} \mid \boldsymbol{a}\varphi \in A\varphi, \boldsymbol{d} \in D\}$ is also a subspace of C, i.e. $A\varphi + D \le C$ in the notation of our work. Furthermore, note that $C \le \mathbb{F}_2^{2n}$. Consequently, from the chain of inclusions $\mathbb{F}_2^{2n} = A \le A\varphi + D \le C \le \mathbb{F}_2^{2n}$, we deduce that $C = \mathbb{F}_2^{2n}$. As a result, we can conclude that $D \cong \mathbb{F}_2^n$, given that $D'' = \{0\}$ and φ_D is an automorphism.

From $A/B \cong C/D$, we can deduce that $B \cong \mathbb{F}_2^n$. Our claim is that $B = D$. Let's consider Equation 6.2 with $\boldsymbol{b} = (b_1, b_2) \in B \le A$. Since we already have the relation $B\varphi \le D$, we can choose $\boldsymbol{d} \in D$ such that $\boldsymbol{d} = \boldsymbol{b}\varphi$. This allows us to derive the following expressions:

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

Thus, we have $v_1 + v_2 = (0, 0, b_1, b_1 + b_2) \in U$. Since $D'' = \{0\}$, we can conclude that:

$$b_1\varphi_D = b_1 + b_2. \tag{6.4}$$

Furthermore, we know that $b_1 \in A'' = A''\varphi_D$ and $b_1 + b_2 \in A''\varphi_D$. Consequently, $b_2 \in A''\varphi_D$ as well. Since $D'' = \{0\}$, we can express D as: $D = \{(a'', a''\varphi_D) \mid a'' \in A''\}$. It is important to observe that $(b_1, b_2) \in D$, which can be equivalently stated as $B \le D$. Therefore, we can conclude that $B = D$.

Let us show that a contradiction arises from this result. From Equation 6.2, setting $\boldsymbol{a} = 0$ and $\boldsymbol{d} = (b_1, b_2) \in B = D$, we obtain

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

Additionally, $v_1 + v_2 + v_3 = v_4 \overset{\text{def}}{=} ((b_1 + b_2)\, \rho, 0, 0, 0) \in U$. Similar to the case when $D'' = \mathbb{F}_2^n$, through a few computations, we can find $(0, 0, 0, (b_1 + b_2)\, \rho) \in U$. This implies that $(b_1 + b_2)\, \rho = 0\varphi_D = 0$, which leads to $b_1 = b_2$. However, based on Equation 6.4 and the isomorphism of φ_D, we have $b_1 = b_2 = 0$, indicating that B is trivial, which is a contradiction.

$\boxed{C'' = \{0\}}$ Based on the fact that φ_D is an isomorphism, we have $C'' = D'' = B'' = A'' = \{0\}$, which implies $D = \{\mathbf{0}\}$.

Next, we will prove that $B = \{\mathbf{0}\}$. From $B\varphi \le D = \{\mathbf{0}\}$, we have $B\varphi = \{\mathbf{0}\}$. If $(b_1, b_2) \in B$, then $(b_1, b_2)\, \varphi = (0, 0) = \boldsymbol{d}$, and thus $(b_1, b_2, 0, 0) \in U$. Similarly to the previous case, we also have $(0, 0, b_1, b_1 + b_2) \in U$, which means there exists $\boldsymbol{x} \in A$ such that $(0, 0, b_1, b_1 + b_2) = (\boldsymbol{x}, \boldsymbol{x}\varphi)$. By comparing the components, we find that $(b_1, b_1 + b_2) = (0, 0)$, which implies $(b_1, b_2) = 0$. This not only proves that $B = \{\mathbf{0}\}$, but it also demonstrates that $\varphi : A \longrightarrow C$ is an automorphism of A (cf. (1) of Lemma 6.7). Furthermore, for each $\boldsymbol{a} = (a_1, a_2) \in A$, we have $(a_1, a_2)\, \varphi = (\boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_2) \in A\varphi = A$. According to (2) of Lemma 6.7, $\boldsymbol{a}\varphi_1, \boldsymbol{a}\varphi_2 \in A'$, and therefore $\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2 \in A'$ since A' is closed under addition. Consequently,

$$\operatorname{Im}(\varphi_1 + \varphi_2) = \{\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2 \mid \boldsymbol{a} \in A\} \le A'.$$

Note that $\varphi_1 + \varphi_2$ is surjective, since $\varphi = (\varphi_1, \varphi_2)$ is an invertible matrix. More precisely, it has maximum rank, that is, the number of rows of (φ_1, φ_2) coincides with the number of rows of $\varphi_1 + \varphi_2$. This means that $\operatorname{Im}(\varphi_1 + \varphi_2) = A'$. Now, for each $\boldsymbol{a} = (a_1, a_2) \in A$, there exists $\boldsymbol{x} \in A$ such that

$$(\boldsymbol{a}, \boldsymbol{a}\varphi)\overline{\rho}^{-2} = (a_1 + \zeta + (a_2 + \boldsymbol{a}\varphi_2)\, \rho, a_2 + \zeta, a_1 + \boldsymbol{a}\varphi_1, a_2 + \boldsymbol{a}\varphi_2) = (\boldsymbol{x}, \boldsymbol{x}\varphi).$$

Thus, we obtain

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

where $\zeta = (\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\, \rho$. We have

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

$$= ((a_1 + \zeta + (a_2 + \boldsymbol{a}\varphi_2)\, \rho, a_2 + \zeta) + (a_1, a_2))\varphi = (a_1, a_2)\,.$$

Hence, substituting back ζ, we get

$$((\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\, \rho + (a_2 + \boldsymbol{a}\varphi_2)\, \rho, (\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\, \rho) = (a_1, a_2)\, \varphi^{-1} \in A\varphi = A. \tag{6.5}$$

We infer from (2) of Lemma 6.7 that for each $\boldsymbol{a} \in A$, $(\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2)\, \rho) \in A'$, from which $A'\rho = A'$, recalling that

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

and ρ permutes A'. As before, we conclude the proof given that A' is a non-trivial and proper subgroup of V, since by that we would have found an imprimitivity block for $\langle \rho, T_n \rangle$. Otherwise, there are two situations that still need to be explored.

$\boxed{\mathrm{A}' = \mathbb{F}_2^{\mathrm{n}}}$ Let us define

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

and denote

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

Examining the right-hand side of Equation 6.5, we obtain $(\boldsymbol{a}\theta_1, \boldsymbol{a}\theta_2)$. By comparing this with the left-hand side of the equation, we arrive at the following expression:

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

which implies that ρ acts linearly on the set $\{\boldsymbol{a}\varphi_1 + \boldsymbol{a}\varphi_2 \mid \boldsymbol{a} \in A\} = A' = \mathbb{F}_2^n$. However, this leads to a contradiction because ρ, being a permutation, is not necessarily linear over the entire space $\mathbb{F}_2^n$.

$\boxed{\mathrm{A}' = \{0\}}$ First, this case implies that $A'\varphi_A = \{0\}$ since φ_A is a homomorphism, hence necessarily a linear map. For each $d' \in D'$, and setting $a'' = 0$, there exists $y' \in D'$ such that

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

where $\overline{\boldsymbol{d}} = (0, d')$ and $\overline{\boldsymbol{y}} = (0, y')$. Hence $(\overline{\boldsymbol{d}}\varphi_1 + \overline{\boldsymbol{d}}\varphi_2)\rho = 0$, from which $\overline{\boldsymbol{d}}\varphi_1 + \overline{\boldsymbol{d}}\varphi_2 = 0$. As a result, by substitution, we have $(0, d', d' + \overline{\boldsymbol{d}}\varphi_1, 0) \in U$. Note that $(0, d', \overline{\boldsymbol{d}}\varphi_1, \overline{\boldsymbol{d}}\varphi_2) + (0, d', d' + \overline{\boldsymbol{d}}\varphi_1, 0) = (0, 0, d', \overline{\boldsymbol{d}}\varphi_2) \in U$, since both summands are in U. This result implies that $d' \in A''$ for every $d' \in D'$, which is equivalent to saying that $D' \leq A'' = \{0\}$. Therefore, we conclude that $D' = \{0\}$. Since there exists an isomorphism between the quotient space A'/B' and the quotient space C'/D', denoted as $A'/B' \cong C'/D'$, and we have $A' = \{0\}$ and $D' = \{0\}$ as trivial, it follows that C' and B' are also trivial, specifically $C' = B' = \{0\}$. In conclusion, we can deduce that $A = \{\mathbf{0}\}$. Finally, considering that D is trivial and A/B is isomorphic to C/D, it follows that both C and B must also be trivial. However, this leads to the contradiction that U is trivial.

Remarks

We proved our claim in Theorem 5.1 via contradiction that if $\langle \overline{\rho}, T_{4n} \rangle$ generates an imprimitive group, it reduces to obtaining that D'' (or C'' or A'') is an invariant subspace for ρ. What we should actually show is that we can construct a block system from D''. Nevertheless, the computations are almost the same and equally tiresome, so they have not been incorporated in this work. However, the reader whose interest we have piqued may find the same results rewriting the proof of Theorem 5.1, obtaining that $(D'' + v)\,\rho \mapsto D'' + w$ for some $w \in \mathbb{F}_2^n$.

7 Conclusions

This study focuses on the group $\Gamma_{\mathrm{AES}} = \langle \overline{\rho_{\mathrm{AES}}}, T_{128} \rangle$, which is generated by the AES-128 key schedule transformations. We have shown that no partition of the vector space $V^4 = \mathbb{F}_2^{128}$ remains invariant under the action of this group. However, when the composition of more rounds is taken into account, the slow global diffusion of the operator is insufficient to free the schedule transformation from invariant linear partitions. Specifically, by examining the subspaces λ^2 and λ^4, it is observed that they possess proper and nontrivial invariant subspaces, which are a direct sum of bricks of V. Consequently, we can conclude that $\left\langle \overline{\rho_{\mathrm{AES}}}^{i}, T_{128} \right\rangle$ is primitive if $i = 1$ (which essentially is this work), and imprimitive if $i \in \{0, 2 \mod 4\}$ (see [27], Proposition 5.1] or [28] and [3]).

Therefore, it should come as no surprise that $\overline{\rho_{\mathrm{AES}}}^{4}$ admits invariant subspaces like those discovered by Leurent and Pernot [3], leveraging an algorithm introduced by Leander *et al.* [29]. One such example is the subspace $U \leq V^4$, defined as follows:

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

References

[1] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full aes-192 and aes-256. In *Advances in Cryptology–ASIACRYPT 2009: 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings 15*, pages 1–18. Springer, 2009.

[2] Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder. Making the impossible possible. *Journal of Cryptology*, 31:101–133, 2018.

[3] Gaëtan Leurent and Clara Pernot. New representations of the aes key schedule. In *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part I*, pages 54–84. Springer, 2021.

[4] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A cryptanalysis of printcipher: the invariant subspace attack. In *Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings 31*, pages 206–221. Springer, 2011.

[5] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace trail cryptanalysis and its applications to aes. *Cryptology ePrint Archive*, 2016.

[6] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. A new structural-differential property of 5-round aes. In *Advances in Cryptology–EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30–May 4, 2017, Proceedings, Part II*, pages 289–317. Springer, 2017.

[7] Kenneth G Paterson. Imprimitive permutation groups and trapdoors in iterated block ciphers. In *FSE*, volume 99, pages 201–214. Springer, 1999.

[8] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[9] Peter J Cameron. *Permutation groups*. Number 45. Cambridge University Press, 1999.

[10] James B Carrell. Groups, matrices, and vector spaces. *A group theoretic approach to linear algebra. Springer, New York*, 2017.

[11] Joan Daemen and Vincent Rijmen. *The design of Rijndael*, volume 2. Springer, 2002.

[12] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[13] John D Dixon and Brian Mortimer. *Permutation groups*, volume 163. Springer Science & Business Media, 1996.

[14] Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, and Gerhard Rosenberger. A course in mathematical cryptography. In *A Course in Mathematical Cryptography*. De Gruyter, 2015.

[15] Dwi Liestyowati. Public key cryptography. In *Journal of Physics: Conference Series*, volume 1477, page 052062. IOP Publishing, 2020.

[16] Sandeep Kumar and Thomas Wollinger. Fundamentals of symmetric cryptography. *Embedded Security in Cars: Securing Current and Future Automotive IT Applications*, pages 125–143, 2006.

[17] Gustavus J. Simmons. *Stream Ciphers*, pages 65–134. 1992.

[18] Anna Rimoldi. *On algebraic and statistical properties of AES-like ciphers*. PhD thesis, University of Trento, 2009.

[19] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[20] Hoda A Alkhzaimi and Lars Ramkilde Knudsen. Cryptanalysis of selected block ciphers. *Kgs. Lyngby: Technical University of Denmark (DTU).(DTU Compute PHD*, (360):35, 2016.

[21] P Nigel Smart. *Cryptography made simple*. Springer, 2016.

[22] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback. Report on the development of the advanced encryption standard (aes). *Journal of research of the National Institute of Standards and Technology*, 106(3):511, 2001.

[23] R. Aragona, R. Civino, and F. Dalla Volta. On the primitivity of the AES-128 key-schedule. *Journal of Algebra and its Applications, 2350233*, 2022.

[24] Riccardo Aragona, Marco Calderini, Antonio Tortora, and Maria Tota. Primitivity of present and other lightweight ciphers. *Journal of Algebra and Its Applications*, 17(06):1850115, 2018.

[25] Edouard Goursat. Sur les substitutions orthogonales et les divisions régulières de l'espace. In *Annales scientifiques de l'École Normale Supérieure*, volume 6, pages 9–102, 1889.

[26] Kristina Kublik. Generalizations of goursat's theorem for groups. *Rose-Hulman Undergraduate Mathematics Journal*, 11(1):2, 2010.

[27] Andrea Caranti, Francesca Dalla Volta, and Massimiliano Sala. On some block ciphers and imprimitive groups. *Applicable algebra in engineering, communication and computing*, 20(5-6):339–350, 2009.

[28] Marco Calderini. A note on some algebraic trapdoors for block ciphers. *arXiv preprint arXiv:1705.08151*, 2017.

[29] Gregor Leander, Brice Minaud, and Sondre Rønjom. A generic approach to invariant subspace attacks: Cryptanalysis of robin, iscream and zorro. In *Advances in Cryptology–EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, pages 254–283. Springer, 2015.