A new look in the representation of AES like S-box

Pablo Freyre Arrozarena, Adrián Alfonso Peñate,

Alejandro Freyre Echevarría, Ramses Rodríguez Aulet

***Abstract*— Substitution box plays an essential role in block ciphers as their main non-linear component in the round function, providing confusion. In this paper, it will be proven how the action of any substitution box on every fixed element can be represented through an affine transformation using an invertible matrix in a finite field. Furthermore, a particular way to represent the action of permutations on every element through a modular addition is given. An analysis of the AES substitution box is conducted based on the theoretical results obtained.**

***Tóm tắt*— S-box đóng một vai trò thiết yếu trong mật mã khối, được dùng để thực hiện các phép thay thế phi tuyến, gây ra sự hỗn loạn. Trong bài báo này, nhóm tác giả sẽ chứng minh cách hoạt động của bất kỳ S-box nào trên mọi phần tử cố định có thể được biểu diễn thông qua phép biến đổi Affine, bằng cách sử dụng ma trận khả nghịch trong một trường hữu hạn. Hơn nữa, một cách cụ thể để biểu diễn hành động của các hoán vị trên mọi phần tử thông qua một phép cộng mô-đun được đưa ra. Phân tích hộp thay thế AES được tiến hành từ các kết quả lý thuyết thu được.**

Keywords— S-box; permutations; invertible matrices; modular addition; symmetric group.

Từ khóa— S-box; hoán vị; ma trận khả nghịch; mô-đun bổ sung; nhóm đối xứng.

I. INTRODUCTION

Substitution box, or shortly called S-box, are highly non-linear components used in block ciphers to ensure confusion, playing a vital role against cryptanalytic attacks [1-3]. The security of modern block ciphers strongly depends on the choice of its S-box.

There are several ways to represent S-box: as look-up table, *i.e.*, the complete relationship between inputs and outputs, as truth table by means of their coordinate Boolean functions or, as univariate polynomial over a finite field [4]. All these ways of representation can fully describe the behavior of any S-box around all its input and output values. However, in block ciphers, S-box acts independently on a single element at a time.

In this paper, we introduce a way to represent the action of any invertible S-box S on a given element x through an affine transformation:

$$S(x) = xM^{\lambda_x} \oplus \delta_x M^{\gamma_x}$$

where M is a matrix with primitive characteristic polynomial on a finite field and $\lambda_x, \gamma_x, \delta_x$ are determined by x. We also provide a new way to represent the action of any permutation Π on a given element x through a modular addition:

$$\Pi(x) = x + \theta_x \mod n$$

where θ_x is determined by x. The rest of this paper is organized as follows. Section II presents the notations, definitions and basic mathematical preliminaries. In Section III we introduce new ways to represent S-box acting on a given element and related results. Section IV presents some of the consequences of the new way to represent the action of an S-box in SPN-based block ciphers, as well as the obtained decompositions of one DES [5] and one AES [6, 7]. Finally, we will summarize the conclusions of the paper in Section V.

II. NOTATIONS, DEFINITIONS AND BASIC MATHEMATICAL PRELIMINARIES

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. Let V_n be the n-dimensional vector space over $\mathbb{F}_2$. Let $\mathbb{Z}_{2^n}$ be the set of integers modulo 2^n. Then, for a fixed base of V_n there is a bijective relationship between V_n, $\mathbb{F}_{2^n}$ and $\mathbb{Z}_{2^n}$.

This manuscript is received on May 23, 2022. It is commented on August 15, 2022 and is accepted on December 01, 2022 by the first reviewer. It is commented on December 20, 2022 and is accepted on December 27, 2022 by the second reviewer.

A. S-box and their representations

An $n \times m$ S-box S is defined as a mapping between the *n*-bit vector space V_n and the *m*-bit vector space V_m, *i.e.* $S: V_n \to V_m$ [4, 6].

When $n = m$ transformation *S* is particularly called an *n*-bit S-box. Furthermore, if *S* is an invertible transformation, it is called an *n*-bit permutation. A list specifying each output value for every input value of *S* is known as the look-up table of *S*.

An S-box $S: V_n \to V_m$ can be determined by means of the m Boolean functions $f_1, \dots, f_m$ from V_n into V_2 as their coordinate functions in the way:

$$S(x) = \big(f_1(x), \dots, f_m(x)\big) \quad \forall\, x \in V_n$$

Hence, an S-box *S* can be fully represented by its truth table like a matrix with 2^n rows and m columns containing the output value of each of its coordinate functions for all input values.

Another way to represent an S-box *S* is by means of an univariate polynomial in $\mathbb{F}_{2^n}[x]$ as:

$$S(x) = \sum_{i=0}^{2^n-1} a_i x^i \qquad a_i \in \mathbb{F}_{2^n}$$

B. Groups acting on sets

Let *G* be a group acting on a set Ω [8-10]. Then, we denote by x^g the action of $g \in G$ on $x \in \Omega$.

Given $x \in \Omega$ the subset defined as $x^G = \{x^g : g \in G\}$ is known as the orbit of Ω containing *x*. If $x^G = \Omega$ then *G* acts transitively on Ω, *i.e.*, for any two elements $x_1, x_2 \in \Omega$ there exists $g \in G$ such that $x_2 = x_1^g$.

The subgroup of *G* defined as $G_x = \{g \in G : x^g = x\}$ is known as the stabilizer of $x \in \Omega$ and $G_{x_1,\dots,x_k} = \{g \in G : x_1^g = x_1, \dots, x_k^g = x_k\}$ is known as the stabilizer of $x_1, \dots, x_k \in \Omega$.

A base for *G* is any subset $B = \{\beta_1, \dots, \beta_p\}$ in Ω such that $e = G_{\beta_1,\dots,\beta_p}$ where e denotes the identity. If *G* acts faithfully on Ω, *i.e.*, there are no group elements g such that $x^g = x$ for all $x \in \Omega$ except for $g = e$, each base for *G* has $n - 1$ elements of Ω.

Given a fixed base $B = \{\beta_1, \dots, \beta_p\}$ for *G* the chain of stabilizers can be defined as:

$$e = G_{p+1} \subseteq G_p \subseteq \cdots \subseteq G_2 \subseteq G_1 = G$$

where $G_i = G_{\beta_1,\dots,\beta_{i-1}}$ and there exist the basic orbits in Ω defined as $\Delta_i = \beta_i^{G_i}$ for $1 \le i \le p$. The Schreier structure for a base *B* is then defined as the array $L = (L_{\beta_1}, \dots, L_{\beta_p})$ such that:

$$L_{\beta_i} = \begin{bmatrix} \beta_i & \alpha_1 & \dots & \alpha_{s_i} \\ e & g_i^{(1)} & \dots & g_i^{(s_i)} \end{bmatrix}$$

where $\Delta_i = \{\beta_i, \alpha_1, \dots, \alpha_{s_i}\}$ is a basic orbit, $g_i^{(1)}, \dots g_i^{(s_i)} \in G_i$ and $\beta_i^{g_i^{(1)} g_i^{(2)} \cdots g_i^{(s_i)}} = \alpha_j$ for $1 \le i \le p$ and $1 \le j \le s_i$.

The determination of the basic orbits yields a right transversal of G_{i+1} in G_i

$$T_i = \left\{ \prod_{j=0}^{l} g_i^{(j)} : g_i^{(0)} = e, l = 0,1,2, \dots s_i \right\}$$

containing the right cosets of G_{i+1} in G_i. Thus, every element $g \in G$ can be uniquely determined as $g = t_{n-1} \cdots t_1$ where $t_i \in T_i$ for all $1 \le i \le p$.

C. The permutation group

A permutation Π of *n* elements on a set Ω, *i.e.*, an invertible transformation from Ω into Ω is commonly represented as a two-dimensional array in the way:

$$\begin{pmatrix} 0 & \cdots & n-1 \\ \Pi_0 & \cdots & \Pi_{n-1} \end{pmatrix}$$

where $\Pi_i = \Pi(i)$ for all $0 \le i \le n-1$.

Permutation Π is called a *k*-cycle or cycle of length *k* if and only if [11]:

1. $\Pi^k(i) = i$ for some $0 \le i \le n-1$.
2. $\Pi(j) = j$ for each $0 \le j \le n-1$ such that $\Pi^r(i) \ne j$ for all $0 \le r \le k$.

In this case, there is another way to represent Π as $[i, \Pi(i), \Pi^2(i), \dots, \Pi^{k-1}(i)]$. Moreover, every permutation of *n* elements can be represented as a composition of disjoint cycles.

The set of all permutations of *n* elements on Ω is a group for the composition of permutations known as symmetric group and denoted by S_n. This way, the set S_{2^k} denotes the group of the aforementioned *k*-bit permutations.

S_n acts transitively and faithfully on every set Ω and the action of $\Pi \in S_n$ on $x \in \Omega$ is defined by $x^{\Pi} = \Pi(x)$. Hence, any permutation Π can be uniquely determined by its action on a base and every base for S_n contains $n-1$ elements of Ω.

III. New representation of S-box

In this Section, some results related with the representation of invertible S-box acting on the sets $\Omega = V_n$ and $\Omega = \mathbb{Z}_n$ will be proven.

Theorem 1. *The action of any permutation* $\Pi \in S_{2^n}$ *on every value* $x \in V_n$ *can be represented as*

$$\Pi(x) = xM^{\lambda_x} \oplus \delta_x M^{\gamma_x}$$

where $\delta_x \in V_n$, $\lambda_x, \gamma_x \in \mathbb{Z}_{2^n-1}$ *and M is a matrix with primitive characteristic polynomial in* $\mathbb{F}_2[\xi]$ *of degree n.*

Proof of Theorem 1. Let M be a matrix with primitive characteristic polynomial in $\mathbb{F}_2[\xi]$. Let β_2 be the vector representation of any primitive element on $\mathbb{F}_{2^n}$. From the different elements in V_n

$$\beta_1 = 0, \beta_2, \beta_3 = \beta_2 M, \dots, \beta_{2^n} = \beta_{2^n-1} M$$

a base $B = \{\beta_1, \dots, \beta_{2^n-1}\}$ for S_{2^n} can be chosen. Let $L = (L_{\beta_1}, \dots, L_{\beta_{2^n-1}})$ be the Schreier structure for *B* defined as:

$$\begin{array}{rcl} L_{\beta_1} & = & \begin{bmatrix} \beta_1 & \beta_2 & \dots & \beta_{2^n} \\ I_{2^n} & g_1 & \dots & g_1 \end{bmatrix} \\ L_{\beta_2} & = & \begin{bmatrix} \beta_2 & \beta_3 & \dots & \beta_{2^n} \\ I_{2^n} & g_2 & \dots & g_2 \end{bmatrix} \\ \vdots & \vdots & \vdots & \\ L_{\beta_{2^n-1}} & = & \begin{bmatrix} \beta_{2^n-1} & \beta_{2^n} \\ I_{2^n} & g_{2^n-1} \end{bmatrix} \end{array}$$

where

$$\begin{array}{rcl} g_1 & = & [\beta_1, \beta_2, \dots, \beta_{2^n-1}, \beta_{2^n}] \\ g_2 & = & [\beta_2, \dots, \beta_{2^n-1}, \beta_{2^n}] \\ \vdots & \vdots & \vdots \\ g_{2^n-1} & = & [\beta_{2^n-1}, \beta_{2^n}] \end{array}$$

and I_{2^n} denotes the identity permutation in S_{2^n}.

Thus, for all $2 \le i \le 2^n - 1$ and every elements $x, y \in \beta_i, \dots, \beta_{2^n}$ there exist unique $0 \le k_i \le 2^n - i$ and $\lambda_i \in \mathbb{Z}_{2^n-1}$ such that:

$$y = g_i^{k_i}(x) = xM^{\lambda_i}$$

This way, right transversals T_i are formed with linear transformations in the vector space V_n and right transversal T_1 is formed with help of the transformations:

$$\begin{array}{rcl} \beta_2 & = & \beta_2 \oplus \beta_1 \\ \beta_1 & = & \beta_{2^n} \oplus \beta_{2^n} \end{array}$$

Moreover, the action of any $\Pi \in S_{2^n}$ on every $x \in \{\beta_1, \dots, \beta_{2^n}\}$ is determined by an equation of the form:

$$\begin{array}{rcl} \Pi(x) & = & g_1^{k_1}\left(\cdots\left(g_i^{k_i}(x)\right)\cdots\right) \\ \vdots & = & xM^{\lambda_x} \oplus \delta_x M^{\gamma_x} \end{array}$$

where $\delta_x \in \{\beta_1, \beta_2, \beta_{2^n}, \beta_{2^n} \oplus \beta_2\}$ and $\lambda_x, \gamma_x \in \mathbb{Z}_{2^n-1}$. ■

From the previous Proof we remark that, a random selection of elements $0 \le k_i \le 2^n - i$ for all $1 \le i \le 2^n - 1$ allows to construct a random *n*-bit permutation $\Pi \in S_{2^n}$. Moreover, statement of Theorem 1 is equally true for the action of any permutation $\Pi \in S_{p^n}$ on every input value of the *n*-dimensional vector space over $\mathbb{F}_p$, where *p* is a prime number.

Example 1. Let $\Pi \in S_{16}$ be the permutation

$$\Pi = [F, 1, 8, E, 6, B, 3, 4, 9, 7, 2, D, C, 0, 5, A]$$

found in one of the S-box of the American standard DES [5] which can be represented in k-cycle form as:

$$\Pi = [0, F, A, 2, 8, 9, 7, 4, 6, 3, E, 5, B, D]$$

and let $p(\xi) = 1 \oplus \xi \oplus \xi^4$ be a primitive polynomial in $\mathbb{F}_2[\xi]$ whose companion matrix is:

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

We assume little-endian order to represent each element of the space V_4 in hexadecimal notation. Then, base B defined in Proof of Theorem 1 is

$$B = \{0,1, C, 6,3, D, A, 5, E, 7, F, B, 9,8,4\}$$

and the different permutations in the Schreier structure for B are

$$\begin{array}{ccc} g_1 & = & [0,1,\mathrm{C},6,3,\mathrm{D},\mathrm{A},5,\mathrm{E},7,\mathrm{F},\mathrm{B},9,8,4,2] \\ g_2 & = & [1,\mathrm{C},6,3,\mathrm{D},\mathrm{A},5,\mathrm{E},7,\mathrm{F},\mathrm{B},9,8,4,2] \\ \vdots & \vdots & \vdots \\ g_{15} & = & [4,2] \end{array}$$

Hence, the following relationships hold.

$$\begin{aligned} \Pi(0) &= 0M^9 \oplus 1M^9 \\ \Pi(1) &= 1M^{14} \oplus 3M^0 \\ \Pi(\mathrm{C}) &= CM^{14} \oplus 3M^1 \\ \Pi(6) &= 6M^0 \oplus 3M^3 \\ \Pi(3) &= 3M^3 \oplus 3M^7 \\ \Pi(\mathrm{D}) &= DM^{10} \oplus 2M^0 \\ \Pi(\mathrm{A}) &= AM^9 \\ \Pi(5) &= 5M^4 \\ \Pi(\mathrm{E}) &= EM^{13} \oplus 3M^6 \\ \Pi(7) &= 7M^5 \\ \Pi(\mathrm{F}) &= FM^{10} \oplus 3M^5 \\ \Pi(\mathrm{B}) &= BM^8 \oplus 3M^4 \\ \Pi(9) &= 9M^{11} \oplus 3M^8 \\ \Pi(8) &= 8M^{14} \\ \Pi(4) &= 4M^3 \oplus 3M^2 \\ \Pi(2) &= 2M^{13} \end{aligned}$$

Corollary 1. *For all permutation* $\Pi \in S_{2^n}$ *such that* $\Pi(0) = 0$ *its action on every value* $x \in V_n$ *can be uniquely represented as*

$$\Pi(x) = xM^{\lambda_x}$$

Proof of Corollary 1. By Theorem 1, for all $x \in V_n$ we have

$$\begin{array}{rcl} \Pi(x) & = & g_1^0\left(g_2^{k_2}\left(\cdots\left(g_i^{k_i}(\beta_i)\right)\cdots\right)\right) \\ \vdots & = & xM^{\lambda_i}\cdots M^{\lambda_2}M^0 \\ \vdots & = & xM^{\lambda_i+\cdots+\lambda_2+0 \bmod 2^n-1} \end{array}$$ ■

Proposition 1. *Let* $\Pi \in S_{2^n}$ *be a permutation such that* $\Pi(0) = 0$ *and let* $k > 0$*. Then, for every* $x \in V_n$

$$\Pi^{k+1}(x) = xM^{\left(\lambda_x+\lambda_{\Pi(x)}+\cdots+\lambda_{\Pi^k(x)}\right) \bmod 2^n-1}$$

Proof of Proposition 1. By Corollary 1

$$\begin{array}{rcl} \Pi(\mathrm{x}) & = & xM^{\lambda_x} \\ \Pi^2(\mathrm{x}) & = & \Pi(x)M^{\lambda_{\Pi(x)}} \\ & \vdots & \\ \Pi^{\mathrm{k}+1}(\mathrm{x}) & = & \Pi^{\mathrm{k}}(x)M^{\lambda_{\Pi^{\mathrm{k}}(x)}} \end{array}$$

Then

$$\Pi^{\mathrm{k}+1}(\mathrm{x}) = \mathrm{x}\mathrm{M}^{\lambda_{\mathrm{x}}}\mathrm{M}^{\lambda_{\Pi(\mathrm{x})}}\cdots\mathrm{M}^{\lambda_{\Pi^{\mathrm{k}}(\mathrm{x})}}$$ ■

Proposition 2. *Let* $\Pi \in S_{2^n}$ *be a permutation such that* $\Pi(0) = 0$*. Then, for every* $x \in V_n$ *such that* $x = x_1 \oplus x_2$

$$\Pi(x) = \Pi(x_1)M^{\lambda_1} \oplus \Pi(x_2)M^{\lambda_2}$$

where

$$\lambda_1 = \left(\lambda_x - \lambda_{x_1}\right) \bmod 2^n - 1$$

$$\lambda_2 = \left(\lambda_x - \lambda_{x_2}\right) \bmod 2^n - 1$$

Proof of Proposition 2. By Corollary 1

$$\begin{array}{rcl} \Pi(x) & = & (x_1 \oplus x_2)M^{\lambda_x} \\ & = & x_1M^{\lambda_{x_1}}M^{\lambda_x}M^{-\lambda_{x_1}} \oplus x_1M^{\lambda_{x_2}}M^{\lambda_x}M^{-\lambda_{x_2}} \\ & = & \Pi(x_1)M^{\lambda_1} \oplus \Pi(x_2)M^{\lambda_2} \end{array}$$ ■

Proposition 3. *Let* $\Pi \in S_{2^n}$ *be a permutation such that* $\Pi(0) = 0$ *and let* $k > 0$*. The for every* $x \in V_n$, $\alpha \in \mathbb{F}_{2^n}$

$$\Pi(\alpha x) = \alpha\Pi(x)M^{(\lambda_{\alpha x}-\lambda_x) \bmod 2^n-1}$$

Proof of Proposition 3. By Corollary 1

$$\begin{array}{rcl} \Pi(\alpha x) & = & (\alpha x)M^{\lambda_{\alpha x}} \\ & = & \alpha xM^{\lambda_x}M^{\lambda_{\alpha x}}M^{-\lambda_x} \\ & = & \alpha\Pi(x)M^{(\lambda_{\alpha x}-\lambda_x) \bmod 2^n-1} \end{array}$$ ■

From Propositions 2 and 3 it is clear that, for all $x_1, x_2 \in V_n$ and for all $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}$ such that $x = \alpha_1x_1 \oplus \alpha_2x_2$

$$\begin{array}{rcl} \Pi(x) & = & \Pi(\alpha_1x_1)M^{(\lambda_x-\lambda_{\alpha_1x_1}) \bmod 2^n-1} \\ & & \oplus \Pi(\alpha_2x_2)M^{(\lambda_x-\lambda_{\alpha_2x_2}) \bmod 2^n-1} \\ \Pi(x) & = & \alpha_1\Pi(x_1)M^{(\lambda_{\alpha_1x_1}-\lambda_{x_1}) \bmod 2^n-1}M^{(\lambda_x-\lambda_{\alpha_1x_1}) \bmod 2^n-1} \\ & & \oplus \alpha_2\Pi(x_2)M^{(\lambda_{\alpha_2x_2}-\lambda_{x_2}) \bmod 2^n-1}M^{(\lambda_x-\lambda_{\alpha_2x_2}) \bmod 2^n-1} \\ \Pi(x) & = & \alpha_1\Pi(x_1)M^{(\lambda_x-\lambda_{x_1}) \bmod 2^n-1} \\ & & \oplus \alpha_2\Pi(x_2)M^{(\lambda_x-\lambda_{x_2}) \bmod 2^n-1} \end{array}$$

Theorem 2. *The action of any permutation* $\Pi \in S_n$ *on every value* $x \in \mathbb{Z}_n$ *can be represented as*

$$\Pi(x) = (x + \theta_x) \bmod n$$

where $\theta_x \in \mathbb{Z}_n$.

Proof of Theorem 2. $B = \{0,1,\dots,n-2\}$ is a base for S_n. Let $L = (L_1,\dots,L_{n-1})$ be the Schreier structure for *B* defined as:

$$\begin{array}{rcc} L_1 & = & \begin{bmatrix} 0 & 1 & \dots & n-1 \\ I_n & g_1 & \dots & g_1 \end{bmatrix} \\ L_2 & = & \begin{bmatrix} 1 & 2 & \dots & n-1 \\ I_n & g_2 & \dots & g_2 \end{bmatrix} \\ \vdots & \vdots & \vdots & \\ L_{n-1} & = & \begin{bmatrix} n-2 & n-1 \\ I_n & g_{n-1} \end{bmatrix} \end{array}$$

where

$$\begin{array}{rcc} g_1 & = & [0,1,\dots,n-2,n-1] \\ g_2 & = & [1,\dots,n-2,n-1] \\ \vdots & \vdots & \vdots \\ g_{n-1} & = & [n-2,n-1] \end{array}$$

and I_n denotes the identity permutation in S_n.

Thus, right transversals $T_1,\dots,T_n$ are formed by modular additions in $\mathbb{Z}_n$ and this way the action of any permutation $\Pi \in S_n$ on every element $0 \le i \le n-1$ is determined by an equation of the form:

$$\Pi(i) = (i + \theta_i) \bmod n \quad \blacksquare$$

Example 2. Let $\Pi \in S_{16}$ be the permutation from Example 1. The base defined in the proof of Theorem 2 is:

$$B = \{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E\}$$

and the permutations in the Schreier structure for B are

$$\begin{array}{rcc} g_1 & = & [0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F] \\ g_2 & = & [1,2,3,4,5,6,7,8,9,A,B,C,D,E,F] \\ \vdots & \vdots & \vdots \\ g_{15} & = & [E,F] \end{array}$$

Hence, the following relationships hold.

$$\begin{array}{rcl} \Pi(0) & = & (0+F) \bmod 16 \\ \Pi(1) & = & (1+0) \bmod 16 \\ \Pi(2) & = & (2+6) \bmod 16 \\ \Pi(3) & = & (3+B) \bmod 16 \\ \Pi(4) & = & (4+2) \bmod 16 \\ \Pi(5) & = & (5+6) \bmod 16 \\ \Pi(6) & = & (6+D) \bmod 16 \\ \Pi(7) & = & (7+D) \bmod 16 \\ \Pi(8) & = & (8+1) \bmod 16 \\ \Pi(9) & = & (9+E) \bmod 16 \\ \Pi(A) & = & (A+8) \bmod 16 \\ \Pi(B) & = & (B+2) \bmod 16 \\ \Pi(C) & = & (C+0) \bmod 16 \\ \Pi(D) & = & (D+3) \bmod 16 \\ \Pi(E) & = & (E+7) \bmod 16 \\ \Pi(F) & = & (F+B) \bmod 16 \end{array}$$

Proposition 4. *Let* $\Pi \in S_{2^n}$ *be a permutation. Then, for every* $x \in \mathbb{Z}_n$ such that $x = (x_1 + x_2) \bmod n$

$$\Pi(x) = \left(\Pi(x_1) + \Pi(x_2) - \theta_{x_1} - \theta_{x_2} + \theta_x\right) \bmod n$$

Proof of Proposition 4. By Theorem 2

$$\begin{array}{rcl} \Pi(x) & = & (x + \theta_x) \bmod n \\ & = & (x_1 + x_2 + \theta_x) \bmod n \\ & = & \left(\left(\Pi(x_1) - \theta_{x_1}\right) + \left(\Pi(x_1) - \theta_{x_1}\right) + \theta_x\right) \bmod n \end{array} \quad \blacksquare$$

IV. An approach to block ciphers

Let $S \in S_{2^n}$ be an invertible *n*-bit S-box such that $S(0) \neq 0$. Then, there exists always another *n*-bit permutation $S' \in S_{2^n}$ defined as $S'(x) = S(x) \oplus S(0)$ for all $x \in V_n$ for which $S'(0) = 0$. For instance, from the 8-bit S-box S_{RD} of AES can be defined the 8-bit S-box $S'(x) = S_{\mathrm{RD}}(x) \oplus 0\mathrm{x}63$. From now on assume that *n*-bit permutations establish the *n*-bit vector zero.

A. The linear representation of the round

Let $f: V_n^m \times V_n^m \to V_n^m$ be the round function of a XSL based block cipher, defined by the Exclusive OR μ, the **S**ubstitution layer ρ and the Linear layer σ, in such a way that

$$f(x,k) = \sigma(\rho(\mu(x,k))) = L\big(S(x_1 \oplus k_1), \dots, S(x_m \oplus k_m)\big)$$

where $x = (x_1, \dots, x_m)$ and $k = (k_1, \dots, k_m)$ denote the state and the round key respectively, S is an n-bit permutation and L is an invertible linear function. Some ways to realize L are: an index permutation like Present [12], an invertible $m \times m$ matrix over $\mathbb{F}_{2^n}$ like Shark [13] or some blend of linear functions like AES. Then, in virtue of Corollary 1:

$$f(x,k) = L\left((x_1 \oplus k_1)M^{\lambda_1}, \dots, (x_m \oplus k_m)M^{\lambda_m}\right)$$
$$= L\big(x_1 M^{\lambda_1}, \dots, x_m M^{\lambda_m}\big) \oplus L\big(k_1 M^{\lambda_1}, \dots, k_m M^{\lambda_m}\big)$$

where M is a matrix with primitive characteristic polynomial in $\mathbb{F}_{2^n}[\xi]$ and $\lambda_i = \lambda_{x_i \oplus k_i}$ for all $1 \le i \le m$.

B. An example case for one of DES S-box

Recall from S-box Π of Example 1. By the result of Theorem 1 it can be shown that the following relationship exists between $x \in V_4$ and $\lambda_x \in \mathbb{Z}_{15}$.

x	λ_x	δ_x	γ_x
0	9	1	9
1	14	3	0
C	14	3	1
6	0	3	3
3	3	3	7
D	10	2	0
A	9	0	0
5	4	0	0

x	λ_x	δ_x	γ_x
E	13	3	6
7	5	0	0
F	10	3	5
B	8	3	4
9	11	3	8
8	14	0	0
4	3	3	2
2	13	0	0

Notice that the frequency of repetition for distinct values of λ_x is different. Furthermore, the values of λ_x in the set {1,2,4,6,7,12} does not appear in the obtained decomposition.

In addition, the analysis of the distribution of δ_x and γ_x reveals that $\gamma_x = 0$ if $\delta_x = 0$ and $\delta_x = 3$ is associated to all possible values of γ_x while $\delta_x = 1$ and $\delta_x = 2$ are associated to $\gamma_x = 9$ and $\gamma_x = 0$ respectively, as shown below:

TABLE 1. THE VALUE OF δ_x, λ_x AND FREQUENCY

$\boldsymbol{\delta_x}$	0	2	1	3
$\boldsymbol{\gamma_x}$	0	0	1	{0,1,2,3,4,5,6,7,8}
Frequency	5	1	1	1

Let now analyze the action of Π over a fixed element when a given sub-key k is operating with text. The value of $\Pi(x \oplus k)$ can be decomposed as:

$$\Pi(x) = (x \oplus k)M^{\lambda_{x\oplus k}} \oplus \delta_{x\oplus k}M^{\gamma_{x\oplus k}} = xM^{\lambda_{x\oplus k}} \oplus kM^{\lambda_{x\oplus k}} \oplus \delta_{x\oplus k}M^{\gamma_{x\oplus k}}$$

where for both, x and k, the result of $xM^{\lambda_{x\oplus k}}$ (resp. $kM^{\lambda_{x\oplus k}}$) is conditioned by the frequency of the value of $\lambda_{x\oplus k}$, and the values of $\delta_{x\oplus k}$ and $\gamma_{x\oplus k}$ appear according the distribution described above for the result of the operation $x \oplus k$, *e.g.* if $x = 1, k = D$ then $x \oplus k = C$ and therefore $\delta_{x\oplus k} = 3$ and $\gamma_{x\oplus k} = 1$.

C. Application to AES SubBytes

The S-box used in the *SubBytes* step of AES was chosen to be a high nonlinear bijective mapping in S_{256} through the application of the function $g: a \to a^{-1}$ which describe the finite field inversion in $\mathbb{F}_{2^8}$ and a linear invertible affine transformation f which have no impact in the nonlinear characteristics of g and improve the complexity of its algebraic expression. The affine transformation f can be described as a polynomial multiplication, followed by a bitwise addition ($\oplus$) with a constant [6].

From the results of Theorem 1 we decompose the S-box of AES using the primitive polynomial of degree 8

$$p(\xi) = 1 \oplus \xi \oplus \xi^5 \oplus \xi^6 \oplus \xi^8 \in \mathbb{F}_{2^8}[\xi]$$

obtaining that

$\boldsymbol{\delta_x}$	$\boldsymbol{\gamma_x}$	$\boldsymbol{x}$
1	2	0x00
2	0	0x52
3	0	0x09
3	1	0xc7
0	0	$\forall\, x \notin$ {0x00,0x09,0x52,0xc7}

The obtained decomposition show that 252 out of 256 possible input values of the S-box can be represented as:

$$\Pi_{AES}(x) = xM^{\lambda_x}$$

Next we present the frequency distribution of parameter λ_x obtained for AES S-box.

TABLE 2. THE FREQUENCY DISTRIBUTION OF PARAMETER λ_x OBTAINED FOR AES S-BOX

Freq.	Value of λ_x
0	0; 8; 14; 15; 17; 20; 23; 27; 29; 36; 39; 41; 44; 45; 46; 47; 48; 49; 52; 59; 63; 66; 68; 71; 77; 79; 90; 91; 95; 98; 99; 100; 102; 103; 105; 106; 109; 113; 116; 121; 124; 129; 130; 132; 135; 136; 139; 142; 149; 151; 154; 155; 156; 157; 159; 161; 162; 165; 166; 169; 171; 173; 175; 176; 177; 178; 180; 182; 185; 190; 196; 198; 201; 204; 206; 208; 209; 210; 212; 218; 231; 237; 242; 244; 246; 247; 253; 254; 255
1	2; 4; 5; 7; 9; 11; 12; 13; 16; 18; 21; 22; 25; 26; 30; 31; 33; 34; 37; 38; 51; 54; 55; 70; 72; 76; 78; 80; 81; 82; 85; 87; 88; 92; 93; 101; 108; 111; 112; 114; 115; 117; 120; 123; 125; 127; 128; 131; 141; 143; 145; 146; 150; 152; 153; 158; 160; 163; 164; 167; 168; 170; 174; 179; 183; 184; 186; 192; 193; 194; 197; 200; 202; 205; 211; 213; 214; 215; 216; 217; 219; 220; 221; 222; 224; 225; 226; 229; 230; 232; 233; 235; 236; 239; 240; 241; 243; 245; 249
2	1; 3; 6; 19; 24; 32; 40; 42; 43; 50; 53; 56; 60; 61; 62; 64; 67; 69; 73; 74; 75; 83; 84; 86; 89; 94; 96; 97; 104; 110; 118; 119; 126; 133; 134; 137; 140; 144; 148; 172; 181; 188; 191; 195; 199; 227; 238; 248; 250; 252
3	10; 28; 35; 57; 58; 107; 122; 138; 147; 187; 207; 223; 228; 234; 251
4	65; 189; 203

The above distribution shows that 89 possible values of λ_x do not appear in the decomposition, 99 appear once, 50 appear twice, while 15 and 3 will appear three and four times, respectively.

The implications of the decomposition obtained in this subsection towards the security of AES algorithm as well as the study of the comparison between the decomposition obtained through different primitive polynomials and/or distinct bases are topics for further research in this area.

V. CONCLUSIONS

In this paper, we introduce a particular way to represent the action of any invertible S-box in S_{2^n} on every fixed element of V_n through an affine transformation. Also, we provide another way to represent the action of any permutation on every fixed element of $\mathbb{Z}_n$ as a modular addition. Finally, we apply the theoretical results introduced in this paper to obtain a decomposition of one S-box from the S-box of DES and the S-box of AES.

REFERENCES

[1] Matsui, M. (1993, May). Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of Cryptographic Techniques* (pp. 386-397). Springer, Berlin, Heidelberg.

[2] Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, *4*(1), 3-72.

[3] Armknecht, F. (2004, February). Improving fast algebraic attacks. In *International Workshop on Fast Software Encryption* (pp. 65-82). Springer, Berlin, Heidelberg.

[4] Canteaut, A. (2016). Lecture notes on cryptographic Boolean functions. *Inria, Paris, France*, *3*.

[5] Standard, D. E. (1999). Data encryption standard. *Federal Information Processing Standards Publication*, *112*.

[6] Daemen, J., & Rijmen, V. (2002). *The design of Rijndael* (Vol. 2). New York: Springer-Verlag.

[7] Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J., & Roback, E. (2001). Report on the development of the Advanced Encryption Standard (AES). *Journal of research of the National Institute of Standards and Technology*, *106*(3), 511.

[8] Holt, D. F., Eick, B., & O'Brien, E. A. (2005). *Handbook of computational group theory*. Chapman and Hall/CRC.

[9] Cannon, J. (1983). A computational toolkit for finite permutation groups. In *Proceedings of the Rutgers Group Theory Year* (Vol. 1984, pp. 1-18).

[10] Sims, C. C. (1998). Computational group theory. *Rutgers University*.

[11] Kostrikin, A. (1980). Introducción al Álgebra Ed. *Mir Moscú*.

[12] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C. (2007, September). PRESENT: An ultra-lightweight block cipher. In *International workshop on cryptographic hardware and embedded systems* (pp. 450-466). Springer, Berlin, Heidelberg.

[13] Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A., & Win, E. D. (1996, February). The cipher SHARK. In *International Workshop on Fast Software Encryption* (pp. 99-111). Springer, Berlin, Heidelberg.

ABOUT THE AUTHORS

Pablo Freyre Arrozarena
Workplace: Institute of Cryptography, University of Havana.
Email: pfreyre@matcom.uh.cu

Education: Graduated of Mathematics in 1988; receive his Doctor's degree in 1998.

Recent research interests: Symmetric cryptography; Post-quantum cryptography.

Adrián Alfonso Peñate
Workplace: Institute of Cryptography, University of Havana.
Email: aap910816@gmail.com

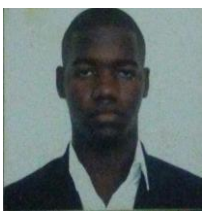
Education: Graduated from Mathematics in 2014; received his Master's degree in 2018.

Recent research interests: Symmetric cryptography; Post-quantum cryptography.

Alejandro Freyre Echevarría
Workplace: Institute of Cryptography, University of Havana.
Email: freyreealejandro@gmail.com

Education: Graduated from Computer Science in 2020; in process to receive his Master's degree.

Recent research interests: Symmetric cryptography; Post-quantum cryptography.



Ramses Rodríguez Aulet
Workplace: Institute of Cryptography, University of Havana.
Email: ramsesrusia@yahoo.com

Education: Graduated from Mathematics in 2017; received his Master's degree in 2020.

Recent research interests: Symmetric cryptography; Post-quantum cryptography.