Partition-Based Trapdoor Ciphers

Arnaud Bannier, Nicolas Bodin, and Eric Filiol

ESIEA, $(C+V)^O$ Lab, Laval, France,
{bannier, bodin, filiol}@esiea.fr

Abstract. This paper deals with block ciphers embedding a trapdoor which consists to map a partition of the plaintext space to a partition of the ciphertext space. In a first part, this issue is reduced to the study of the S-boxes of the cipher satisfying a few criteria. Then, differential and linear properties of such S-boxes are assessed and an algorithm to build optimal S-boxes is provided. Finally, these primitives are used to design a small trapdoor cipher resistant to linear and differential cryptanalysis. This trapdoor allows to recover the κ-bit master key with only one plaintext/ciphertext pair and an effort of $2^{\frac{\kappa}{2}}$ encryptions.

Keywords: Substitution-Permutation Network, Trapdoor, Partition, S-box

1 Introduction

1.1 Motivation

Trapdoors are a two-face, key concept in modern cryptography. It is primarily related to the concept of "trapdoor function" – a function that is easy to compute in one direction, yet difficult to compute in the opposite direction without special information, called the "trapdoor". This first "face" relates most of the time to asymmetric cryptography algorithms. It is a necessary condition to get reversibility between the sender/receiver (encryption) or the signer/verifier (digital signature). The trapdoor mechanism is always fully public and detailed. The security and the core principle is based on the existence of a secret information (the private key) which is essentially part of the trapdoor. In other words, the private key can be seen as *the* trapdoor.

The second "face" of the concept of trapdoor relates to the more subtle and perverse concept of "mathematical backdoor" and is a key issue in symmetric cryptography (even if it may be extended to asymmetric cryptography; see for example the case of the DUAL EC_DRBG [15]). In this case, the aim is to insert hidden mathematical weaknesses which enable one who knows them to break the cipher. If possible, these weaknesses should be independent from the secret key. In this context, the existence of a backdoor is a strongly undesirable property.

In the rest of the present section, we will oppose the term of trapdoor (desirable property) to that of backdoor (undesirable property). However, in the

subsequent sections of the paper we will keep the term of trapdoor which has been already used in the very few literature covering this second face of this problem. We suggest however to use the term of backdoor to describe the issue of hidden mathematical weaknesses. This would avoid ambiguity and maybe would favor the research work around a topic which is nowadays mostly addressed by governmental entities in the context of cryptography control and regulations.

Inserting backdoors in encryption algorithms underlies quite systematically the choice of cryptographic standards (DES, AES...). The reason is that the testing, validation and selection process is always conducted by governmental entities (NIST or equivalent) with the technical support of secret entities (NSA or equivalent). So an interesting and critical research area is: "how easy and feasible is it to design and insert backdoor (at the mathematical level) in encryption algorithms?" This paper intends to address one very particular case of this question. It is important to keep in mind that a backdoor may be itself defined in the following two ways.

- As a "natural weakness" known – but non disclosed – only by the tester/validator/final decision-maker (e.g. the NSA). The best historic example is that of the differential cryptanalysis. Following Biham and Shamir's seminal work in 1991, NSA acknowledged that it was aware of that cryptanalysis years ago. Most of experts estimate that it was nearly 20 years ago.
- As an intended design weakness put by the author of the algorithm. To the authors knowledge, there is no known cases for public algorithms yet.

As far as symmetric cryptography is concerned, there are two major families of cipher systems for which the issue of backdoor must be considered differently.

- *Stream ciphers.* Their design complexity is rather low since they mostly rely on algebraic primitives (LFSRs and Boolean functions which have intensely been studied in the open litterature). Until the late 70s, backdoors relied on the fact that quite all algorithms were proprietary and hence secret. It was then easy to hide non primitive polynomials, weak combining Boolean functions... The Hans Buehler case in 1995 [16] shed light on that particular case.
- *Block ciphers.* This class of encryption algorithm is rather recent (end of the 70s for the public part). They exhibit so a huge combinatorial complexity that it is reasonable to think to backdoor. As described in [6, section 5.5] for a κ-bit secret key and a m-bit input/output block cipher there are $((2^m)!)^{2^\kappa}$ possible such block ciphers. For such an algorithm, the number of possible internal states is so huge that we are condemned to have only a local view of the system, that is, the round function or the basic cryptographic primitives. We cannot be sure that there is no degeneration effect at a higher level. This point has been addressed in [6, pp 124] when considering correlation attacks. Therefore, it seems reasonable to think that this combinatorial richness of block cipher may be used to hide a backdoor.

1.2 Previous Work

One of the first trapdoor cipher was created in 1997 by Rijmen and Preneel in [14]. The S-boxes are selected randomly and then modified to be weak to the linear cryptanalysis. They are finally applied to a Feistel cipher such as CAST or LOKI91. But because of the big size of the S-boxes, the linear table of such an S-box cannot be computed. However the knowledge of the trapdoor gives a good linear approximation of the S-boxes which is then used in a linear cryptanalysis. As an example, the authors created a 64-bit block cipher based on CAST cipher, and four 8×32 S-boxes. If the parameters of the trapdoors are known, a probabilistic algorithm allows to recover the key easily. Such a family of trapdoor ciphers leads to recover only a part of the key, and the authors claim that the trapdoor is undetectable. But in [17], Wu and al. discovered a way to recover the trapdoor if the attacker knows its global design but not the parameters. They also showed that there exists no parameter allowing to hide the trapdoor. Nevertheless, it is worthwhile to mention that in practice, if a real cipher containing a trapdoor is given, the presence of the trapdoor will certainly not be revealed. Thereby, we will not focus in this section and in the rest of this article on ways to recover the trapdoor, but still propose strong enough S-boxes to hide this trapdoor if its global design is not revealed.

Our work is mainly a generalization of the ideas presented by Patterson in [13]. In this article, a DES-like trapdoor cipher exploiting a weakness induced by the round functions is presented. The group generated by the round functions acts imprimitively on the message space to allow the design of the trapdoor. In other words, this group preserves a partition of the message space between input and output of the round function. Such a construction leads to the design of a trapdoor cipher composed of 32 rounds and using a 80 bits key. The knowledge of the trapdoor allows to recover the key using 2^{41} operations and 2^{32} plaintexts. Even if the mathematical material to build the trapdoor is given, no general algorithm is detailed to construct such S-boxes. Furthermore, as author says, S-boxes using these principles are incomplete (half of the cipher text bits are independent of half of the plaintext bits). Finally, the security against the differential attack is said *not as high as one might expect*. These three points are corrected or improved in our work, in which we also answer to the author's question in which he wondered whether the structure of trapped S-boxes acting imprimitively on the message space had to be linear.

More recently in [1], the authors created non-surjective S-boxes embedding a parity check to create a trapdoor cipher. The message space is thus divided into cosets and leads to create an attack on this DES-like cipher in less than 2^{23} operations. The security of the whole algorithm, particularly against linear and differential cryptanalysis is not given and the authors admit that their attack is dependent on the first and last permutation of the cipher. Finally, the non-surjective S-boxes may lead to detect easily the trapdoor by simply calculating the image of each input vector. This problem is naturally avoided in a SPN in which S-boxes are bijective by definition.

In a slightly different context, Caranti and al. answer to Patterson's question by the affirmative in [4], by proving that the imprimitivity of the group generated by round functions is actually related to the cosets of a linear subspace. They also give some conditions to create such a primitive group to design a secure cipher that cannot contain such trapdoor, and finally show that AES respects these conditions. They add in [3] an algorithm to verify this last condition simply and show that AES and Serpent S-boxes verify this property.

1.3 Contributions

As detailed in the previous section, we intend to generalize the work of [13] and [7] for Substitution-Permutation Networks (SPN). We study such encryption systems which map a partition of the plaintext space to a partition of the ciphertext space, independently from the round keys. To this end, the next section introduces some notations and definitions. Then, our results are organized as follows.

First, we show in Section 3 that the round function of such an encryption system must necessarily map a partition to another one. Moreover, this partition must be linear (the set of vector space cosets). Then we show that the subtitution layer must necessarily map a linear partition to another one.

Second, we show in Section 4 that at least one S-box must map a linear partition to another one. When combining all these results, we prove that any encryption system which maps a partition to another one, must involve a S-box which itself maps a linear partition to another one. In practical terms, it means that we can restrict the study of the global encryption algorithm to the that of a single S-box.

Then, we study in Section 5 the linear and differential properties of S-boxes which map a linear partition to another one. We obtain several structural theorems as well as lower bounds regarding the linear and differential uniformity of such S-boxes. We also give an algorithm to build this kind of S-boxes which reach these bounds, effectively.

As a practical application, we give in Section 6 an example (a toy cipher) of a trapdoor encryption system, based on our results. We explain how it works and its design rationales. Let us mention the fact that our attack used then to break this system (with the knowledge of the trapdoor) has been suggested by Paterson who never used it practically.

Eventually, the conclusion and future works are presented in Section 7. Furthermore, it should be stressed that almost all the proofs of our results will be given in Appendices.

2 Preliminaries

Let us begin with some notations and conventions.

Notation. Let n and s denote positive integers. For two maps f and g, the composition $g \circ f$ (or simply gf) denotes the evaluation of f followed by g. For

any set E, let $\#E$ denotes its cardinality. If F is a subset of E, F^c denotes its complement.

Let us denote the Galois field of order two by $\mathbb{F}_2$ and $0_n = (0, \ldots, 0)$ the zero vector of $\mathbb{F}_2^n$. All the vector spaces considered in this paper are over the finite field $\mathbb{F}_2$. It is worthwhile to mention that $(\mathbb{F}_2^n)^s$ will be often identified with $\mathbb{F}_2^{ns}$. The concatenation of two vectors x and y is denoted $[x \parallel y]$.

A n-bit S-box is any permutation of $\mathbb{F}_2^n$. If x and y are two elements of $\mathbb{F}_2^n$, then $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$. If $L : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a linear map, define $L^\intercal : \mathbb{F}_2^m \to \mathbb{F}_2^n$ by $\langle L^\intercal(x), y \rangle = \langle x, L(y) \rangle$ for every $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$. In other words, $L^\intercal$ is the transpose of L for the bilinear form $\langle \cdot, \cdot \rangle$.

Since we are concerned with ciphers which associate a partition of the ciphertext space to another partition of the plaintext space, let us introduce the following definition.

Definition 2.1. *Let f be a permutation of E and $\mathcal{A}$, $\mathcal{B}$ be two partitions of E. Let $f(\mathcal{A})$ denote the set $\{f(A) \mid A \in \mathcal{A}\}$. We say that f maps $\mathcal{A}$ to $\mathcal{B}$ if $f(\mathcal{A}) = \mathcal{B}$.*

The two partitions $\{\{x\} \mid x \in E\}$ and $\{E\}$ are called the *trivial partitions* of E. Observe that, for any permutation f of E,

$$f(\{\{x\} \mid x \in E\}) = \{\{x\} \mid x \in E\} \quad \text{and} \quad f(\{E\}) = \{E\} \ .$$

That is, every permutation maps a trivial partition to another one. Moreover it should be highlighted that if f maps $\mathcal{A}$ to $\mathcal{B}$ and if $\mathcal{A}$ is non-trivial, then so is $\mathcal{B}$.

In this paper, we are going to use a special kind of partitions which consists of cosets of a linear subspace. Such partitions have already been introduced by [7, Definition 4.4] and are recalled below.

Definition 2.2 (linear partition). *Let $\mathcal{A}$ be a partition of $\mathbb{F}_2^n$. Let V denote its part containing 0_n. The partition $\mathcal{A}$ is said* linear *if V is a subspace of $\mathbb{F}_2^n$ and if every part of $\mathcal{A}$ is a coset of V in $\mathbb{F}_2^n$, in other words, if*

$$\mathcal{A} = \{x + V \mid x \in \mathbb{F}_2^n\} = \mathbb{F}_2^n \,/\, V \ .$$

We denote $\mathcal{L}(V)$ such a partition.

It turns out that the linear partitions associated to the two trivial subspaces of $\mathbb{F}_2^n$, that is $\{0_n\}$ and $\mathbb{F}_2^n$, correspond with the two trivial partitions of $\mathbb{F}_2^n$. Moreover, if V is a non-trivial subspace of $\mathbb{F}_2^n$, then the linear partition $\mathcal{L}(V)$ is also non-trivial.

The following two propositions are interesting properties of linear partitions which will be used in the rest of the paper.

Proposition 2.3. *Let V_1, V_2, W_1, W_2 be four subspaces of $\mathbb{F}_2^n$ and f be a permutation of $\mathbb{F}_2^n$ which maps $\mathcal{L}(V_1)$ to $\mathcal{L}(W_1)$ and $\mathcal{L}(V_2)$ to $\mathcal{L}(W_2)$. Then f maps $\mathcal{L}(V_1 \cap V_2)$ to $\mathcal{L}(W_1 \cap W_2)$.*

Proposition 2.4. *Let V, W be two subspaces of $\mathbb{F}_2^n$ and f be a permutation of $\mathbb{F}_2^n$ which maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. There exists an automorphism L of $\mathbb{F}_2^n$ such that $L(V) = W$. In particular, V and W are isomorphic.*

3 Substitution-Permutation Networks and Partitions

Substitution-Permutation Networks, or SPN for short, belong to the class of iterated block ciphers. As every iterated block ciphers, the encryption function consists to apply a simple keyed operation called *round function* several times. A different *round key* is used for each iteration of the round function. In practice, these rounds keys are extracted from a master key using an algorithm called *key schedule*. In a SPN, the round function is made of three distinct stages: a *key addition*, a *substitution layer* and a *permutation* or *diffusion layer*. The substitution layer consists of the parallel evaluation of several S-boxes and is the only part of the cipher which is not linear or affine. Then, the diffusion layer is the evaluation of some linear maps (generally one).

Definition 3.1 (SPN). *Let $s, n \geq 1$ be two integers. Let $\sigma_1, \ldots, \sigma_s$ be n-bit S-boxes and $\pi : \mathbb{F}_2^{ns} \to \mathbb{F}_2^{ns}$ be an isomorphism. Define the map*

$$\begin{aligned} \sigma : (\mathbb{F}_2^n)^s &\longrightarrow (\mathbb{F}_2^n)^s \\ (x_1, \ldots, x_s) &\longmapsto (\sigma_1(x_1), \ldots, \sigma_s(x_s)) \ . \end{aligned}$$

For any round key k in $\mathbb{F}_2^{ns}$, let $\alpha_k : \mathbb{F}_2^{ns} \to \mathbb{F}_2^{sn}$ defined by $\alpha_k(x) = x + k$. The maps α_k, σ and π are called the key addition*, the* substitution layer *and the* diffusion layer *respectively.*

The round function F_k associated with the round key k in $\mathbb{F}_2^{ns}$ is defined by $F_k = \pi\sigma\alpha_k$. Let $r \geq 1$ be an integer. The r-round encryption function *associated with the round keys $(k_1, \ldots, k_{r+1})$ in $(\mathbb{F}_2^{ns})^{r+1}$ is defined by*

$$E_{(k_1,\ldots,k_{r+1})} = \alpha_{k_{r+1}} F_{k_r} \ldots F_{k_1} \ .$$

It is worth recalling that we consider a SPN which maps a partition to another one independently from the round keys used. Thus, we consider round keys which are not necessarily derived from a master key by a key schedule. Consequently, the key schedule will be deliberately omitted throughout the article.

Now, we turn our attention to the key addition and to the diffusion layer. The next proposition explains the fundamental property of linear partitions according to the key addition. This result was introduced by Harpes in [7]. Later, Caranti et al. gave a similar result expressed for imprimitive groups in [4]. For convenience, we restate this result with our own notations.

Proposition 3.2. *Let m be a positive integer. Let $\mathcal{A}$ and $\mathcal{B}$ be two partitions of $\mathbb{F}_2^m$. For each k in $\mathbb{F}_2^m$, let α_k denote the permutation of $\mathbb{F}_2^m$ defined by $\alpha_k(x) = x + k$. Then, the permutation α_k maps $\mathcal{A}$ to $\mathcal{B}$ for any k in $\mathbb{F}_2^m$ if and only if $\mathcal{A} = \mathcal{B}$ and $\mathcal{A}$ is a linear partition.*

The, we focus on the diffusion layer in the next proposition.

Proposition 3.3. *Let m be a positive integer. Let L be an automorphism of $\mathbb{F}_2^m$ and V a subspace of $\mathbb{F}_2^m$. Then, $L(\mathcal{L}(V)) = \mathcal{L}(L(V))$. In particular, L maps a linear partition to another one.*

Using the previous two propositions, we can now state our first main result about the structure of SPN which maps a partition of the plaintext space to a partition of the ciphertext space independently of the round keys.

Theorem 3.4. *Let $\mathcal{A}$ and $\mathcal{B}$ be two partitions of $\mathbb{F}_2^{ns}$. Suppose for any $(k+1)$-tuples of round keys $(k_1, \ldots, k_{r+1})$ in $(\mathbb{F}_2^{ns})^{r+1}$ that the encryption function $E_{(k_1,\ldots,k_{r+1})}$ maps $\mathcal{A}$ to $\mathcal{B}$. Define $\mathcal{A}_1 = \mathcal{A}$ and for all $2 \leq i \leq r+1$, $\mathcal{A}_i = (\pi\sigma)^{i-1}(\mathcal{A})$. Then,*

- *$\mathcal{A}_{r+1} = \mathcal{B}$;*
- *for any $1 \leq i < r+1$ and for any k_i in $\mathbb{F}_2^{ns}$, $F_{k_i}(\mathcal{A}_i) = \mathcal{A}_{i+1}$;*
- *for any $1 \leq i \leq r+1$, $\mathcal{A}_i$ is a linear partition.*

The result of this theorem can be restated in the following way. Firstly, the partitions $\mathcal{A}$ and $\mathcal{B}$ must be linear. However, the number of linear partitions is well below the number of any partition. Hence, the apparent and initial combinatorial aspect of our study is reduced to an algebraic one.

Secondly, we only suppose that the encryption function maps $\mathcal{A}$ to $\mathcal{B}$ after r rounds. Nevertheless, Theorem 3.4 ensures that any reduced version of this function also maps the partition $\mathcal{A}$ to another linear partition. In particular, the round function necessarily maps one linear partition to another one. As a consequence, our study of the full cipher is reduced to the study of the round function. Moreover, we have the following result.

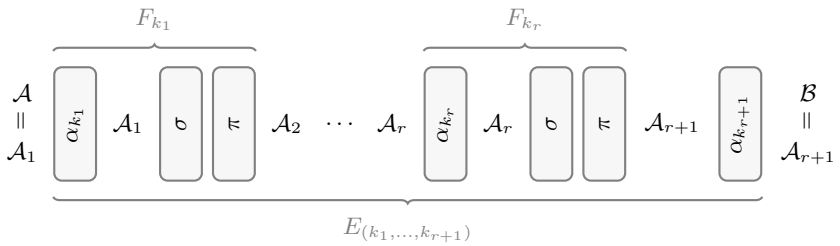

Fig. 1. Representation of Theorem 3.4

Corollary 3.5. *Keep the notations of Theorem 3.4. For all $1 \leq i \leq r+1$, let V_i denote the part of $\mathcal{A}_i$ containing 0. According to Theorem 3.4, $\mathcal{A}_i = \mathcal{L}(V_i)$. Let $1 \leq i \leq r$ be an integer. Then,*

$$\sigma(\mathcal{L}(V_i)) = \mathcal{L}(W_i) \ .$$

where W_i denotes the subspace $\pi^{-1}(V_{i+1})$. In particular, the substitution layer must at least map one linear partition to another one.

Combined with Theorem 3.4, this corollary ensures that if a cipher maps a partition $\mathcal{A}$ to a partition $\mathcal{B}$, then the substitution layer has to map at least one linear partition to another one. Our study is thus reduced to the substitution layer, which is the aim of the following section.

4 Structure of the Substitution Layer

In the remainder of this section, V and W denote two subspaces of $(\mathbb{F}_2^n)^s$. Recall that the substitution layer is itself composed of several cryptographic primitives, the S-boxes. Suppose that the substitution layer σ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. At first sight, this hypothesis implies properties over all the S-boxes and not over each S-box independently of the others. The goal of this section is to highlight properties which only apply to one S-box.

4.1 Truncating a Few S-Boxes

Let E be any non-empty subset of $[\![1, s]\!]$. Let us define the following maps

$$\begin{aligned} T_E : (\mathbb{F}_2^n)^s &\longrightarrow (\mathbb{F}_2^n)^E & \sigma_E : (\mathbb{F}_2^n)^E &\longrightarrow (\mathbb{F}_2^n)^E \\ (x_i)_{1\leq i\leq s} &\longmapsto (x_i)_{i\in E} & (x_i)_{i\in E} &\longmapsto (\sigma_i(x_i))_{i\in E} \ . \end{aligned}$$

If E has cardinality m, then we identify $(\mathbb{F}_2^n)^E$ with $(\mathbb{F}_2^n)^m$. The map T_E allows to shorten a vector of $(\mathbb{F}_2^n)^s$ to keep only the coordinates whose indices belongs to E. Note that T_E is a linear map. The application σ_E is a substitution layer limited to the S-boxes whose indices lies in E. Observe that $\sigma_{[\![1,s]\!]}$ is the substitution layer of the SPN. Moreover, the maps $\sigma_{\{i\}}$ and σ_i are equal for all $1 \leq i \leq s$.

Proposition 4.1 (Truncating a few S-boxes). *Suppose that σ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Let E be a non-empty subset of $[\![1, s]\!]$. Then, the permutation σ_E maps $\mathcal{L}(T_E(V))$ to $\mathcal{L}(T_E(W))$.*

Choosing $E = \{i\}$ in the previous proposition gives that the i-th S-box σ_i maps a linear partition to another one. Therefore, the hypothesis on σ implies one property on each S-box. Nonetheless, these properties can be trivial.

Let $\mathcal{I}$ be a partition of $[\![1, s]\!]$. According to Proposition 4.1, for any part I of $\mathcal{I}$, the limited substitution layer σ_I maps a linear partition to another linear one. However, the converse being false in general, this proposition alone cannot characterize the whole substitution layer. The next subsection intends to obtain the equivalence.

Example 4.2. Consider the subspace $V = \{(x, x) \mid x \in \mathbb{F}_2^3\}$ of $(\mathbb{F}_2^3)^2$. Define the permutations f and g of $\mathbb{F}_2^3$ by the following tables. Here, the elements of $\mathbb{F}_2^3$ are given in hexadecimal. For instance, 3 stands for $(0, 1, 1)$.

x	0	1	2	3	4	5	6	7
$f(x)$	0	4	2	6	1	5	3	7

x	0	1	2	3	4	5	6	7
$g(x)$	2	6	4	1	5	7	0	3

It is easy to verify that f is a linear map whereas g is not.

Firstly, let the 3-bit S-boxes σ_1 and σ_2 be both equal to f. Thus, the substitution layer σ is also a linear map on $(\mathbb{F}_2^3)^2$. According to Proposition 3.3, σ maps $\mathcal{L}(V)$ to $\mathcal{L}(V)$ as $\sigma(V) = V$. However, the previous proposition does not imply anything on the S-boxes σ_1 and σ_2. Indeed, $T_{\{1\}}(V)$ and $T_{\{2\}}(V)$ are both equal to $\mathbb{F}_2^3$, and hence $\mathcal{L}(T_{\{1\}}(V))$ and $\mathcal{L}(T_{\{2\}}(V))$ are trivial partitions.

Secondly, let σ_1 and σ_2 be both equal to g. By contradiction, suppose that σ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$ where W is a subspace of $(\mathbb{F}_2^3)^2$. As $\sigma(V) = V$, we obtain that $V = W$. Then, $\sigma(\mathtt{0},\mathtt{1}) = (\mathtt{2},\mathtt{6})$. Using Lemma A.2 given in Appendix, it follows that $\sigma((\mathtt{0},\mathtt{1}) + V) = (\mathtt{2},\mathtt{6}) + V$. However, $(\mathtt{1},\mathtt{2})$ belongs to $(\mathtt{0},\mathtt{1}) + V$ and $\sigma(\mathtt{1},\mathtt{2}) = (\mathtt{6},\mathtt{4})$ does not lies in $(\mathtt{2},\mathtt{6}) + V$. This is a contradiction. Let $\mathcal{I}$ denote $\{\{1\},\{2\}\}$. As explain above, σ_I maps $\mathcal{L}(T_I(V))$ to $\mathcal{L}(T_I(V))$ but σ does not maps $\mathcal{L}(V)$ to any linear partition. This illustrates that the converse of Proposition 4.1 does not hold.

4.2 Structure of the Subspaces V and W

Let I be a subset of $[\![1, s]\!]$. Let us define

$$\mathrm{Triv}_I = \prod_{i=1}^{s} \mathrm{Triv}_I^{(i)} \quad \text{with} \quad \mathrm{Triv}_I^{(i)} = \begin{cases} \{0_n\} & \text{if } i \in I^c \\ \mathbb{F}_2^n & \text{if } i \in I \ . \end{cases}$$

In other words, $\mathrm{Triv}_I = \{x \in (\mathbb{F}_2^n)^s \mid \forall i \in I^c, x_i = 0_n\}$. We call Triv_I the *trivial product subspace* associated to I. It is indeed easily seen that Triv_I is a subspace of $(\mathbb{F}_2^n)^s$. Note that any trivial product subspaces is the Cartesian product of trivial spaces for each S-box. They are essential in our study because σ always maps $\mathcal{L}(\mathrm{Triv}_I)$ to $\mathcal{L}(\mathrm{Triv}_I)$, no matter the S-boxes σ_i are.

Moreover, we define $V_I = V \cap \mathrm{Triv}_I = \{v \in V \mid \forall i \in I^c, v_i = 0_n\}$ and $W_I = W \cap \mathrm{Triv}_I$. Note that both V_I and W_I are subspaces of $(\mathbb{F}_2^n)^s$ since they are the intersection of two subspaces. It is worthwhile to note that σ maps $\mathcal{L}(V_I)$ to $\mathcal{L}(W_I)$ according to Proposition 2.3.

Finally, let us define the linear map $P_I : (\mathbb{F}_2^n)^s \to \mathrm{Triv}_I$ which maps the vector $(x_1, \ldots, x_s)$ to $(y_1, \ldots, y_s)$ where $y_i = x_i$ if i belongs to I and 0_n otherwise. Observe that P_I is a projection from $(\mathbb{F}_2^n)^s$ onto the subspace Triv_I. Note also that V_I is always a subspace of $P_I(V)$. Moreover, $T_I(V) = T_I(P_I(V))$.

The next lemma gives some relations between the above notations. It will be then especially used in the proof of the main theorem of Subsection 4.4.

Lemma 4.3. *Let $\mathcal{I}$ be a partition of $[\![1, s]\!]$. Then V equals the internal direct sum $\bigoplus_{I\in\mathcal{I}} V_I$ if and only if $V_I = P_I(V)$ for any part I of $\mathcal{I}$. In this case, the decomposition of an element v of V is $v = \sum_{I\in\mathcal{I}} P_I(v)$.*

Lemma 4.4. *Suppose that σ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Let $\mathcal{I}$ be a partition of $[\![1, s]\!]$. Then $V = \bigoplus_{I\in\mathcal{I}} V_I$ if and only if $W = \bigoplus_{I\in\mathcal{I}} W_I$.*

The previous lemma allows to focus only on partitions $\mathcal{I}$ of $[\![1, s]\!]$ such that $V = \bigoplus_{I\in\mathcal{I}} V_I$ instead of partitions satisfying both $V = \bigoplus_{I\in\mathcal{I}} V_I$ and $W = \bigoplus_{I\in\mathcal{I}} W_I$.

Proposition 4.5 (Substitution layer structure). *Let $\mathcal{I}$ be a partition of $[\![1, s]\!]$ such that $V = \bigoplus_{I\in\mathcal{I}} V_I$. The permutation σ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$ if and only if σ_I maps $\mathcal{L}(T_I(V))$ to $\mathcal{L}(T_I(W))$ for any I in $\mathcal{I}$.*

In the case where $V = \bigoplus_{I \in \mathcal{I}} V_I$, this proposition gives the converse of Proposition 4.1. Recall that if $\mathcal{I}$ and $\mathcal{J}$ are two partitions of $[\![1, s]\!]$, then the partition $\mathcal{I}$ is said *finer* than $\mathcal{J}$ if for any I in $\mathcal{I}$, there exists J in $\mathcal{J}$ such that $I \subseteq J$. Thus, the finer the partition $\mathcal{I}$ is, the less S-boxes are involved in the limited substitution layers σ_I, the closer we are to the primitives of the SPN. Fortunately, we have the following lemma.

Lemma 4.6. *The set of the partitions $\mathcal{I}$ of $[\![1, s]\!]$ satisfying $V = \bigoplus_{I \in \mathcal{I}} V_I$ has a least element (or a minimum) denoted $\mathcal{I}_{\min}$.*

Consequently, we consider this minimal partition $\mathcal{I}_{\min}$ is the remainder of this section.

4.3 Linked and Independent S-Boxes

Proposition 4.5 and Lemma 4.6 then suggest the following definition.

Definition 4.7 (Linked and independent S-boxes). *Suppose that σ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Let I be a part of $\mathcal{I}_{\min}$.*

- *If $I = \{i\}$ with i in $[\![1, s]\!]$, the S-box σ_i is said* independent*. Moreover, if $V_{\{i\}} = \{0_{nb}\}$ or $V_{\{i\}} = \mathrm{Triv}_{\{i\}}$, the S-box σ_i is said* inactive*. Otherwise, σ_i is said* active*.*
- *If $\#I \geq 2$, then the S-boxes whose indices lie in I are said* linked together*.*

Actually, if an S-box σ_i is independent with regards to the subspaces V and W, then it can be replaced with any other S-box which maps $\mathcal{L}(T_{\{i\}}(V))$ to $\mathcal{L}(T_{\{i\}}(W))$ and the substitution layer σ still maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Furthermore, if σ_i is inactive, then it can be replaced with any other n-bit S-box. On the contrary, if only one of the linked S-boxes is replaced, then the desired property of the substitution layer may not hold.

Example 4.8. Let us go on with Example 4.2. It is easy to check that $\mathcal{I}_{\min} = \{\{1, 2\}\}$, and thus, the two S-boxes are linked together. If σ_1 denotes the map f and σ_2 the map g, it can be verified that σ does not map $\mathcal{L}(V)$ to $\mathcal{L}(V)$ anymore. Thus, linked S-boxes cannot be replaced independently.

Lemma 4.9. *Let I be a part of $\mathcal{I}_{\min}$ and E be a non-empty proper subset of I.*

- *If V_E is a trivial product subspace, then $V_E = \mathrm{Triv}_{\emptyset} = \{0_{ns}\}$.*
- *If $P_E(V)$ is a trivial product subspace, then $P_E(V) = \mathrm{Triv}_E$.*

The next lemma states an important result about a particular case of linked S-boxes.

Lemma 4.10. *Let E be a non-empty proper subset of I. Suppose that $V_E = V_{I \setminus E} = \{0_{ns}\}$ and $P_E(V) = T_E$. Then, for all i in E, σ_i is an affine map.*

Example 4.11. Let us continue Example 4.8. One can check that Lemma 4.10 applies for both $E = \{1\}$ and $E = \{2\}$. As a consequence, σ_1 and σ_2 must be affine maps.

4.4 Reduction to an S-Box

It is now time to present our main result concerning the substitution layer. The proof is exceptionally put in the body of the paper since it helps to understand the structure of the subspaces V, W and their relations with the S-boxes.

Theorem 4.12. *Let $n > 2$ and s be two positive integers. Let $\sigma_1, \ldots, \sigma_s$ be n-bit S-boxes. Define the permutation σ of $(\mathbb{F}_2^n)^s$ which maps the element $(x_i)_{1 \leq i \leq s}$ to $(\sigma_i(x_i))_{1 \leq i \leq s}$. Let V and W be two subspaces of $(\mathbb{F}_2^n)^s$ such that σ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Suppose that V is not a trivial product subspace. Then, at least one of the S-boxes maps a non-trivial linear partition to another one.*

Proof. Let us prove this result by complete induction on the number s of S-boxes. Suppose that $s = 1$. In this case, $\sigma = \sigma_1$. By hypothesis, V is different from $\{0_n\}$ and $\mathbb{F}_2^n$. Hence, $\mathcal{L}(V)$ is a non-trivial partition and σ_1 maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$.

Let $s \geq 2$ be an integer. Suppose that the result holds for any positive integer strictly lower than s. Firstly, suppose that all the S-boxes are independent. In other words, $\mathcal{I}_{\min} = \{\{i\} \mid i \in [\![1, s]\!]\}$. If each S-box is inactive, then V is a trivial product subspace, a contradiction with our hypothesis. Thus, there exists at least one active S-box σ_i. In this case, $\{0_{ns}\} \subsetneq V_{\{i\}} \subsetneq \mathrm{Triv}_{\{i\}}$. According to Lemma 4.3, the equality $P_{\{i\}}(V) = V_{\{i\}}$ holds. Then, $T_{\{i\}}(V_{\{i\}}) = T_{\{i\}}(P_{\{i\}}(V)) = T_{\{i\}}(V)$ is a non-trivial subspace of $\mathbb{F}_2^n$, so $\mathcal{L}(T_{\{i\}}(V))$ is also non-trivial. Finally, Proposition 4.1 states that σ_i maps $\mathcal{L}(T_{\{i\}}(V))$ to $\mathcal{L}(T_{\{i\}}(W))$, and thus the result holds in this case.

Now, suppose that some S-boxes are linked together. Then, there exists an element I of $\mathcal{I}_{\min}$ such that $\#I \geq 2$. Next, at least one of the following three cases holds.

- Suppose that there exists a non-empty proper subset E of I such that $P_E(V)$ is not a trivial product subspace. Let m denote the cardinality of E. Recall that $T_E(P_E(V)) = T_E(V)$. It follows that $T_E(V)$ is not a trivial product subspace of $(\mathbb{F}_2^n)^m$. According to Proposition 4.1, σ_E maps $\mathcal{L}(T_E(V))$ to $\mathcal{L}(T_E(W))$. Note that E is a non-empty proper subset of I, so of $[\![1, s]\!]$. Hence $m < s$, so the induction hypothesis ensures that at least one of the S-boxes of σ_E maps a non-trivial partition to another one.
- Suppose that there exists a subset E of I such that V_E is not a trivial product subspace. Recall that σ maps $\mathcal{L}(V_E)$ to $\mathcal{L}(W_E)$. Proposition 4.1 ensures that σ_E maps $\mathcal{L}(T_E(V_E))$ to $\mathcal{L}(T_E(W_E))$. It is easily seen that $T_E(V_E)$ is not a trivial product subspace. As before, the result is a consequence of the induction hypothesis.
- Suppose that $P_E(V)$ and V_E are trivial product subspaces for any non-empty proper subset E of I. Let E be a non-empty proper subset of I. Hence, $P_E(V)$, V_E and $V_{I \setminus E}$ are trivial product subspaces. Then, Lemma 4.9 implies that $P_E(V) = \mathrm{Triv}_E$, $V_E = V_{I \setminus E} = \{0_{ns}\}$. According to Lemma 4.10, the S-boxes $\sigma_1, \ldots, \sigma_m$ are affine maps. Combining Proposition 3.3 and 3.2, we obtain that these S-boxes maps any non-trivial linear partition to another linear one.

In any case, the result holds for this integer s. The result follows by induction.

Combining Theorem 3.4 and Corollary 3.5 with Theorem 4.12, we have proven that in a cipher which maps a partition to another one, at least one of the S-boxes must map a linear partition to another linear one.

The following section aims to design such an S-box with the best security against the main known cryptanalysis of block cipher.

5 Relation with Linear and Differential Cryptanalysis

Differential [2] and linear [11] cryptanalysis are considered as the most important attacks against block ciphers [8]. The resistance of a S-box against these cryptanalysis is assessed with its difference distribution table and its linear approximation table respectively.

Let f be a permutation of $\mathbb{F}_2^n$. The difference distribution table and the linear distribution table of f are the two families DT_f and LT_f indexed by $(\mathbb{F}_2^n)^2$ and defined for any (a, b) in $(\mathbb{F}_2^n)^2$ by

$$\begin{aligned}(\mathrm{DT}_f)_{a,b} &= \#\{x \in \mathbb{F}_2^n \mid f(x) + f(x+a) = b\} \\ (\mathrm{LT}_f)_{a,b} &= \#\{x \in \mathbb{F}_2^n \mid \langle a, x\rangle = \langle b, f(x)\rangle\} - 2^{m-1} \ .\end{aligned}$$

Moreover, the permutation f is said *differentially δ-uniform* if $(\mathrm{DT}_f)_{a,b} \leq \delta$ for any (a, b) in $(\mathbb{F}_2^n)^2$ with $a \neq 0$. Similarly, f is *linearly λ-uniform* if $|(\mathrm{LT}_f)_{a,b}| \leq \lambda$ for every (a, b) in $(\mathbb{F}_2^n)^2$ with $a \neq 0$. It is worthwhile to mention that the smaller the differential uniformity is, the more resistant f is against differential cryptanalysis. The same applies for linear cryptanalysis.

Recall that two permutations f and g of $\mathbb{F}_2^n$ are said *equivalent* is there exist two linear maps L_1, L_2 of $\mathbb{F}_2^n$ and two elements v_1, v_2 of $\mathbb{F}_2^n$ such that

$$\forall x \in \mathbb{F}_2^n, \quad g(x) = L_2(f(L_1(x) + v_1)) + v_2 \ .$$

It is well known that equivalent permutations have the same differential uniformity and the same linear uniformity, see for instance [5] and [12]. More precisely, their differential tables are equal up to row and column permutations. This result holds for linear tables up to the sign of the coefficients.

Suppose that f is a permutation of $\mathbb{F}_2^n$ which maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Proposition 2.4 ensures that there exists an automorphism L of $\mathbb{F}_2^n$ such that $L(V) = W$. According to Proposition 3.3, L^{-1} maps $\mathcal{L}(W)$ to $\mathcal{L}(V)$. Then, $L^{-1}f$ is equivalent to f and maps $\mathcal{L}(V)$ to $\mathcal{L}(V)$. Consequently, without loss of generality, we can suppose that $V = W$ in our study of the linear and differential properties of f.

In this section, we consider the following elements. Let V be a subspace of $\mathbb{F}_2^n$ and f be a permutation of $\mathbb{F}_2^n$ which maps $\mathcal{L}(V)$ to $\mathcal{L}(V)$. Recall that $\mathcal{L}(V) = \mathbb{F}_2^n \,/\, V$. Let d denote the dimension of V. To avoid the trivial cases $V = \{0_n\}$ and $V = \mathbb{F}_2^n$, we suppose that $1 \leq d \leq n-1$. Therefore, the subspace V admits a complement space U of dimension $n - d$. Thus, the space $\mathbb{F}_2^n$ can be

written as the direct sum $U \oplus V$ of U and V. In other words, every element x in $\mathbb{F}_2^n$ can be uniquely written as $u + v$ with u and v in U and V respectively. Hence, the linear partition $\mathcal{L}(V)$ equals $\{[u] \mid u \in U\}$ where $[u] = u + V$ denotes the coset u in the quotient space $\mathbb{F}_2^n \,/\, V$.

The following theorem is the structure result of permutations preserving a linear partition. It can be seen as a corollary of the Krasner-Kaloujnine embedding theorem [9]. However, for convenience, a proof of our special case is given in Appendix.

Theorem 5.1. *There exist a unique permutation ρ of U and a unique family of permutations $(\tau_u)_{u \in U}$ of V such that, for all $x = u + v$ in $\mathbb{F}_2^n$,*

$$f(u + v) = \rho(u) + \tau_u(v) \ .$$

Conversely, if ρ is a permutation of U and if $(\tau_u)_{u \in U}$ is a family of permutations of V, then the map g defined by $g(u + v) = \rho(u) + \tau_u(v)$ maps $\mathcal{L}(V)$ to $\mathcal{L}(V)$.

This theorem allows one to design a S-box which maps $\mathcal{L}(V)$ to $\mathcal{L}(V)$ using permutations with smaller domains. Furthermore, these permutations can be chosen arbitrarily.

Example 5.2. Let us consider the permutation f of $\mathbb{F}_2^5$ defined by the following table.

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.A	.B	.C	.D	.E	.F
0.	1F	0D	08	1B	06	15	10	18	14	11	07	04	03	1D	0B	13
1.	1A	19	0E	16	0C	09	1E	00	0F	01	02	17	0A	05	1C	12

For instance, f maps the element 1A to 02, both denoted in hexadecimal. Denote $V = \{00, 07, 1A, 1D\}$ and $U = \{00, 01, 02, 03, 08, 09, 0A, 0B\}$. It is easy to check that V is a subspace of $\mathbb{F}_2^5$ and that U is a complement subspace of V in $\mathbb{F}_2^5$. Therefore, $\mathcal{L}(V) = \mathbb{F}_2^5 \,/\, V = \{[u] \mid u \in U\}$. The different cosets of this quotient space are given in the following table.

	[00]	[01]	[02]	[03]	[08]	[09]	[0A]	[0B]
$u + 00$	00	01	02	03	08	09	0A	0B
$u + 07$	07	06	05	04	0F	0E	0D	0C
$u + 1A$	1A	1B	18	19	12	13	10	11
$u + 1D$	1D	1C	1F	1E	15	14	17	16

We can easily check that the permutation f maps $\mathcal{L}(V)$ to $\mathcal{L}(V)$. Consequently, f induces a permutation of $\mathbb{F}_2^5 \,/\, V$ and thus a permutation ρ of U. As an example, $f(00) = 1F$ belongs to [02], so $f([00]) = [02]$. Therefore, $\rho(00) = 02$. In the same way, we obtain the following permutation of U. For each u in U, define the permutation τ_u of V by $\tau_u(v) = f(u+v)+\rho(u)$. We have the following permutations.

u	00	01	02	03	08	09	0A	0B
$\rho(u)$	02	0A	08	01	09	0B	00	03

	τ_{00}	τ_{01}	τ_{02}	τ_{03}	τ_{08}	τ_{09}	τ_{0A}	τ_{0B}
00	1D	07	00	1A	1D	1A	07	07
07	1A	1A	1D	07	1A	00	1D	00
1A	00	1D	07	00	07	1D	1A	1A
1D	07	00	1A	1D	00	07	00	1D

By construction, we finally have $f(u+v) = \rho(u) + \tau_u(v)$ for any $x = u+v$ in $\mathbb{F}_2^5$.

In the rest of this section, let us fix the permutations ρ and the family $(\tau_u)_{u\in U}$ given by Theorem 5.1.

The goal of this part is to express the linear and differential properties of f according to the ones of the permutations ρ and $(\tau_u)_{u\in U}$. However, these permutations are not defined on $\mathbb{F}_2^n$ but on the subspaces U and V of $\mathbb{F}_2^n$. Thus, the concept of linear or differential table is inexistent for such maps. To solve this problem, we define two isomorphisms between U and $\mathbb{F}_2^{n-d}$ and between V and $\mathbb{F}_2^d$. Then, we consider the maps induced by ρ and $(\tau_u)_{u\in U}$ on these spaces.

Notation. Let $\mathcal{B} = (b_i)_{1\leq i\leq n-d}$ be a basis of U and $\mathcal{C} = (c_i)_{1\leq i\leq d}$ a basis of V. Let us denote

$$\begin{array}{cc} L_U : \mathbb{F}_2^{n-d} \longrightarrow U & L_V : \mathbb{F}_2^d \longrightarrow V \\ (x_1,\ldots,x_{n-d}) \longmapsto \sum_{i=1}^{n-d} x_i b_i & (y_1,\ldots,y_d) \longmapsto \sum_{i=1}^{d} y_i c_i \end{array}$$

It is easily seen that L_U and L_V are both isomorphisms of vector spaces. Define the permutation $\rho' = L_U^{-1}\rho L_U$ of $\mathbb{F}_2^{n-d}$. Finally, for each u in U, let τ'_u denote the permutation $L_V^{-1}\tau_u L_V$ of $\mathbb{F}_2^d$.

Example 5.3. Using the previous example, let us consider the basis $\mathcal{B} = (\mathtt{07}, \mathtt{1A})$ of V and the basis $\mathcal{C} = (\mathtt{01}, \mathtt{02}, \mathtt{08})$ of U. Thus, the isomorphisms $L_U : \mathbb{F}_2^3 \to U$ and $L_V : \mathbb{F}_2^2 \to V$ are given by:

x	0	1	2	3	4	5	6	7
$L_U(x)$	00	01	02	03	08	09	0A	0B

x	0	1	2	3
$L_V(x)$	00	07	1A	1D

The permutation ρ' of $\mathbb{F}_2^3$ and the permutations τ'_u of $\mathbb{F}_2^2$ are given by

u	0	1	2	3	4	5	6	7
$\rho'(u)$	2	6	4	1	5	7	0	3

	τ'_{00}	τ'_{01}	τ'_{02}	τ'_{03}	τ'_{08}	τ'_{09}	τ'_{0A}	τ'_{0B}
0	3	1	0	2	3	2	1	1
1	2	2	3	1	2	0	3	0
2	0	3	1	0	1	3	2	2
3	1	0	2	3	0	1	0	3

5.1 Linear Approximation Table

The next theorem relates the linear table of f to the one of ρ'. The coefficients of the linear approximation table of f taken into account by this result are in practice the greatest. Thus, they determine the linear uniformity of f.

Theorem 5.4. *Let a and b be two elements of $V^\perp$. Denote $a^t = L_U^\intercal(a)$ and $b^t = L_U^\intercal(b)$. Then,*

$$(\mathrm{LT}_f)_{a,b} = 2^d \times (\mathrm{LT}_{\rho'})_{a^t,b^t} \ .$$

Remark 5.5. Let us consider the map $L_U^\intercal : \mathbb{F}_2^n \to \mathbb{F}_2^{n-d}$. Then,

$$\ker(L_U^\intercal) = (\operatorname{Im} L_U)^\perp = U^\perp \ .$$

Observe that $U^\perp \cap V^\perp = (U+V)^\perp = (\mathbb{F}_2^n)^\perp = \{0\}$. Consequently, the restriction $L_U^\intercal : V^\perp \to \mathbb{F}_2^{n-d}$ is one-to-one and thus onto because of the rank-nullity theorem.

Example 5.6. Let us consider the restriction of $L_U^\intercal : \mathbb{F}_2^5 \to \mathbb{F}_2^3$ to $V^\perp$.

a	00	05	0B	0E	13	16	18	1D
$L_U^\intercal(a)$	0	1	7	6	3	2	4	5

The linear approximation tables LT_f of f and $\mathrm{LT}_{\rho'}$ of ρ' are presented in Section E of the appendices. The rows and columns of LT_f have been rearranged in order to highlight Theorem 5.4. As an example, $(\mathrm{LT}_f)_{\mathtt{1D},\mathtt{16}} = 2^3 \times (\mathrm{LT}_{\rho'})_{\mathtt{5},\mathtt{2}} = -8$ because $L_U^\intercal(\mathtt{1D}) = \mathtt{5}$ et $L_U^\intercal(\mathtt{16}) = \mathtt{2}$.

Corollary 5.7. *For the linear cryptanalysis, the permutation f is at least*

- 2^{d+1}*-uniform if* $d < n-1$,
- 2^{n-1}*-uniform if* $d = n-1$.

Note 5.8. We know that any 4-bit S-box is at least 4-uniform for the linear cryptanalysis, see for example [10]. As a consequence, the permutation f is at least 2^{d+2}-uniform si $n - d = 4$.

Example 5.9. In Section E, we can see that the permutation f is 8-uniform for the linear cryptanalysis. Thus, we reach the lower bound given by Corollary 5.7 since the parameters of this example are $n = 5$ et $d = 2$.

5.2 Differential Distribution Table

Unlike to linear cryptanalysis, where only a local view of the table was provided, the results for differential cryptanalysis brings both local and global outlooks.

Theorem 5.10. *Let $a = u_a + v_a$ and $b = u_b + v_b$ be elements of $\mathbb{F}_2^n$. Denote $u'_a = L_U^{-1}(u_a)$ et $u'_b = L_U^{-1}(u_b)$. Then*

$$\sum_{i \in [u_a]} (\mathrm{DT}_f)_{i,b} = \sum_{j \in [u_b]} (\mathrm{DT}_f)_{a,j} = 2^d \times (\mathrm{DT}_{\rho'})_{u'_a,u'_b} \ .$$

Especially, $(\mathrm{DT}_f)_{a,b} \leq 2^d \times (\mathrm{DT}_{\rho'})_{u'_a,u'_b}$.

The previous theorem can restated in the following way. If DT_f is rearranged coset by coset, a trivial operation allows to recover $\mathrm{DT}_{\rho'}$. On the other hand, the next theorem is similar to Theorem 5.4 but for differential cryptanalysis. Again, it generally highlights the coefficients of DT_f involved in the differential uniformity of f.

Theorem 5.11. *Let v_a and v_b be two elements of V. Denote $v'_a = L_V^{-1}(v_a)$ and $v'_b = L_V^{-1}(v_b)$. Then*

$$(\mathrm{DT}_f)_{v_a,v_b} = \sum_{u \in U} (\mathrm{DT}_{\tau'_u})_{v'_a,v'_b} \ .$$

Particularly, the subtable $((\mathrm{DT}_f)_{v_a,v_b})_{v_a,v_b \in V}$ can be expressed according to the differential tables $\mathrm{DT}_{\tau'_u}$ with u in U.

Example 5.12. To illustrate Theorems 5.10 and 5.11, we rearrange the rows and the columns of the differential table of f presented in Section E of the appendices. With this order, we can see the differential table of ρ' by considering the differential table of f coset by coset. In fact, Theorem 5.10 states that the sum of all elements in the same row or column of the subtable $(\mathrm{DT}_f)_{[u_1],[u_2]}$ is equal to the coefficient (x_1, x_2) of $\mathrm{DT}_{\rho'}$ multiplied by 2^2, where $x_i = L_V^{-1}(u_i)$. For instance, if we consider the subtable

$$(\mathrm{DT}_f)_{[09],[03]} = \begin{array}{c|cccc} & 03 & 04 & 19 & 1E \\ \hline 09 & 4 & \cdot & 4 & \cdot \\ 0E & \cdot & 4 & \cdot & 4 \\ 13 & 4 & \cdot & 4 & \cdot \\ 14 & \cdot & 4 & \cdot & 4 \end{array}$$

we can see that the sum of each row or column equals $8 = 2^2 \times (\mathrm{DT}_{\rho'})_{5,3}$ since $L_V(5) = 09$ and $L_V(3) = 03$.

Finally, Theorem 5.11 ensures that the subtable $(\mathrm{DT}_f)_{V,V} = (\mathrm{DT}_f)_{[00],[00]}$ is the sum of the differential tables of the τ_u.

Corollary 5.13. *The permutation f is at least λ-uniform for the differential cryptanalysis where λ denotes the even integer directly greater than $\frac{2^n}{2^d-1}$.*

Example 5.14. In Section E of the appendices, we can see that f is 12-uniform for the differential cryptanalysis. Thus, we reach the lower bound given by Corollary 5.13.

5.3 The Design of a Trapdoor S-Box and Further Observations

We now explain how to design such a trapdoor S-box. To this end, let us express the conditions given by the theorems of this section.

- Theorem 5.4 implies to reduce at most the linear uniformity of ρ' to keep the one of f as small as possible.
- In the same way, Theorem 5.10 implies to reduce at most the differential uniformity of ρ'.
- The same theorem also stresses that the greater the number of non-zero coefficient of $\mathrm{DT}_{\rho'}$ is, the better.
- Finally, Theorem 5.11 teaches us that the sum of the differential distribution tables $\mathrm{DT}_{\tau'_u}$ should be as low as possible.

Now, to design the S-box f, one needs to pick a permutation ρ' of $\mathbb{F}_2^{n-d}$ that is 4-uniform if $n-d$ is even or 2-uniform otherwise for both linear and differential cryptanalysis. Then, one searches for permutations τ'_u of $\mathbb{F}_2^d$ satisfying the last condition. This search can be conduced randomly over every d-bit S-boxes. Finally, construct the S-box f as in Theorem 5.1. If the differential and linear uniformities of f are too far from the lower bounds given by Corollaries 5.7 and 5.13, then start again. In practice, these bounds are reached (or almost reached) after a small number of iterations. According to Theorem 5.4, the smaller the linear uniformity of ρ' is, the smaller the one of f is.

Moreover, we should emphasize that the closer the dimension d of V from n is, the weaker the S-box f is against linear cryptanalysis and the stronger f is against differential cryptanalysis. The lower bounds given by Corollaries 5.7 and 5.13 are represented on Figure 2 for any value of $n \leq 8$.

$n\backslash d$	1	2	3	4	5	6	7
4	4	8	8	.	.	.	.
5	8	8	16	16	.	.	.
6	4	16	16	32	32	.	.
7	4	8	32	32	64	64	.
8	4	8	16	64	64	128	128

$n\backslash d$	1	2	3	4	5	6	7
4	16	6	4	.	.	.	.
5	32	12	6	4	.	.	.
6	64	22	10	6	4	.	.
7	128	44	20	10	6	4	.
8	256	86	38	18	10	6	4

Fig. 2. Lower bounds for the linear (left) and differential (right) uniformities of f.

Finally, it should be highlighted that the linear and differential uniformities of the S-box of Rijndeal [6] are far below the lower bounds given by Corollaries 5.7 and 5.13, no matter the dimension d of the subspace V is. As a consequence, this S-box does not map any linear partition to another linear one.

6 An Illustrative Example of a Trapdoor Cipher

6.1 Description of the Algorithm

In this last part, we use the previous results to design a toy trapdoor cipher. This cipher is a 24-bit Substitution-Permutation Network with 8 rounds (see Definition 3.1). The substitution layer σ consists of four parallel evaluations of the same 6-bit S-box S given in Section F of the appendices. The diffusion layer π is an isomorphism of $(\mathbb{F}_2^6)^4$ also defined in Section F.

The key schedule and the round function are represented in Figure 3. This algorithm derives 8 round keys from a 24-bit master key. Note that the master key is exactly the first round key k_1. The only primitive of the key schedule is an isomorphism L of $(\mathbb{F}_2^6)^2$ described in Section F. Every round of the key schedule follows the same pattern. Suppose that $k_i = (x_1, x_2, x_3, x_4)$ in $(\mathbb{F}_2^3)^4$ is the i-th round key. First, a round constant is added to the current round key. This addition is computed in $(\mathbb{F}_2^6)^4$, so with the exclusive-or operation. The round constant c_i of the i-th round is defined as the binary decomposition

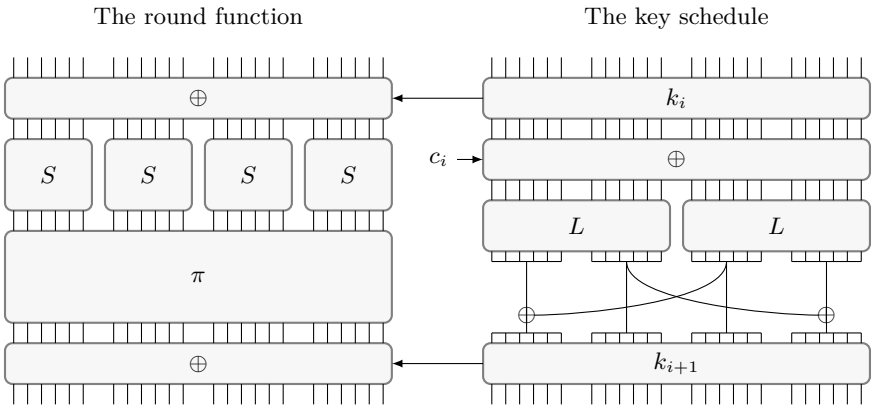

Fig. 3. Representation of the toy trapdoor cipher

of the 4-tuple $(i, 2i, 3i, 4i)$ of integers. For example, in hexadecimal, we have $c_7 = (\texttt{07}, \texttt{0E}, \texttt{15}, \texttt{1C})$. Let $y = (y_1, y_2, y_3, y_4)$ be the result of this operation. Then y is seen as the element $((y_1, y_2), (y_3, y_4))$ and the isomorphism L is evaluated in parallel. In other words, y is mapped to $z = (z_1, z_2, z_3, z_4)$ with $(z_1, z_2) = L(y_1, y_2)$ and $(z_3, z_4) = L(y_3, y_4)$. Finally, the $(i + 1)$-th round key is defined as $(z_1 + z_3, z_2, z_3, z_2 + z_4)$.

Before analyzing our cipher resistance to differential and linear cryptanalysis, we ask the reader to forget for a while that this cipher can obviously be broken very easily with a single plaintext/ciphertext pair through an exhaustive search. The purpose is to compare the known key recovery attacks (linear and differential cryptanalysis) when the attacker is unaware of the trapdoor with attack which exploit the sole knowledge of the trapdoor. While this comparison is a bit artificial here and holds only for illustrative purposes, it totally makes sense for real-life cryptosystems.

6.2 Differential and Linear Cryptanalysis

In [6], Deamen and Rijmen introduced the differential and the linear branch number of a linear transformation. With an exhaustive search, it can be checked that the differential and linear branch numbers of π both are both equal to 4. This implies that any 2-round trail has at least 4 active S-boxes. Thus, a 6-round trail involves at least 12 active S-boxes. Note that the S-box S is differentially 14-uniform and linearly 16-uniform. Therefore, the probability of a 6-round differential trail is lower bounded by $(\frac{14}{64})^{12} \approx 2^{-26.3}$ and the bias of a 6-round linear trail is lower bounded by $(\frac{16}{32})^{12} = 2^{-12}$. Consequently, a differential cryptanalysis of the 6-round version of our cipher would require at least 2^{26} chosen plaintext/ciphertext pairsand a linear cryptanalysis would require 2^{24} known plaintext/ciphertext pairs. Here it does note make sense by definition of

the cipher block size. Since our cipher is a 24-bit SPN, these cryptanalysis are ineffective on the 6-round version, so on the full cipher.

6.3 The Trapdoor

Let us define the following two 3-dimensional subspaces of $\mathbb{F}_2^6$

$$V = \{\texttt{00}, \texttt{0C}, \texttt{17}, \texttt{1B}, \texttt{25}, \texttt{29}, \texttt{32}, \texttt{3E}\} \quad \text{and} \quad W = \{\texttt{00}, \texttt{07}, \texttt{11}, \texttt{16}, \texttt{2B}, \texttt{2C}, \texttt{3A}, \texttt{3D}\} \ .$$

It can be verified that S maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$, π maps $\mathcal{L}(W^4)$ to $\mathcal{L}(V^4)$ and L maps $\mathcal{L}(V^2)$ to $\mathcal{L}(V^2)$. First, we consider the round function. The partition $\mathcal{L}(V^4)$ is left invariant under the key addition. Next, the substitution layer σ maps $\mathcal{L}(V^4)$ to $\mathcal{L}(W^4)$ and the diffusion layer maps $\mathcal{L}(W^4)$ to $\mathcal{L}(V^4)$. Thus, the whole round function maps $\mathcal{L}(V^4)$ to $\mathcal{L}(V^4)$. At this point, the cipher is vulnerable to the basic attack of [13] which uses 2^{12} chosen plaintext/ciphertext pairs and gives then partial information about the unknown plaintext of any ciphertext. Moreover, in contrast to the trapdoor cipher presented in [13], ours has not the drawback of being incomplete, thanks to the more complicated definition of the subspace V.

Now, let us present a key schedule dependent attack suggested in [13] but not realized. Let k_1 and k_1' be two keys in $(\mathbb{F}_2^6)^4$ and suppose that they lie in the same coset of V^4. Since $\mathcal{L}(V^4)$ is equal to the quotient space $(\mathbb{F}_2^6)^4/V^4$ and as the cosets $[k_1]$ and $[k_2]$ are equal, the maps α_{k_1} and $\alpha_{k_1'}$ (representing the two key additions) induce the same permutation of the cosets in $\mathcal{L}(V^4)$.

With a close look to our key schedule, we can see that it also maps $\mathcal{L}(V^4)$ to $\mathcal{L}(V^4)$. In other words, if k_i and k_i' are in the same coset of V^4 in the quotient space $(\mathbb{F}_2^6)^4/V^4$, then so are k_{i+1} and k_{i+1}'. Consequently, if the two first round keys k_1 and k_1' (i.e. the master keys) lies in the same coset, then the two corresponding encryption function induce the same permutations of the cosets of the message space.

Let U denotes the subspace $\{\texttt{00}, \texttt{01}, \texttt{02}, \texttt{03}, \texttt{04}, \texttt{05}, \texttt{06}, \texttt{07}\}$ of $\mathbb{F}_2^6$ which is a complement of V. Then $\mathcal{L}(V) = \{[u] \mid u \in U\}$. We can now present the trapdoor. Suppose that (p, c) is a single known plaintext/ciphertext pair.

- For each k_1 in U^4, test whether the encryption of p with the master key k_1 lies in the same coset of $\mathcal{L}(V^4)$ as c.
- For each candidate k_1, test for each k_1' in $[k_1]$ if the encryption of p with k_1' is equal to c.

Observe that in practice, there is a very small number of candidates. Thus, the overall complexity of this cryptanalysis is roughly 2×2^{12} encryptions compared to 2^{24} for the brute force. Moreover, if there are too many candidates, we can use two known plaintext/ciphertext pairs instead of one.

The main disadvantage of this cipher is that the linear approximation table and the difference distribution table of the S-box S can seem very suspicious. To this end, we define the S-box S' given in Section F. This other S-box is equal to S with probability $\frac{60}{64}$. Now, let E and E' denote the encryption functions

of our cipher using the S-boxes S and S' respectively. Assuming that all the round keys are independent and uniformly distributed (which is false, but works in practice) and that the plaintext p is chosen uniformly, $E(p) = E'(p)$ with probability $(\frac{60}{64})^{32} \approx 12\%$ since the whole 8-round ciphers involve 32 S-boxes. Let us explain the trapdoor of this second cipher which is a chosen plaintext attack.

- Pick roughly $5 \times \frac{100}{12} \approx 40$ plaintexts in the same coset and get the associated ciphertexts.
- Find the coset containing the greatest number of ciphertexts and let (p_i, c_i) be the pairs such that c_i lies in this coset.
- For almost all these pairs, $E(p_i) = c_i$. The key can then be recovered using the previous trapdoor.

7 Conclusion and Future Works

In this paper, we have addressed the following issue: "is it possible to design a mathematical backdoor which would rely mostly on suitable partitionning techniques of the plaintext and ciphertext spaces, independently from the round (sub)keys". We had in mind initially to exploit combinatorial properties of the core primitives. The overall conclusion we get is that if we want to design such a backdoor, the only solution is to stay in the algebraic domain and no specially combinatorial tools or primitive are possible. Let us summarize in detail the main results.

If one wishes to design any encryption system which maps any (plaintext) partition $\mathcal{A}$ to any other (ciphertext) partition $\mathcal{B}$, independently from the round keys (here the knowledge of the pair $(\mathcal{A}, \mathcal{B})$ is precisely the trapdoor) then

- the round function must map a linear partition to another linear one, and
- at leat one S-box must do the same.

This means that the partitions considered for trapdoor are in the algebraic domain and not in the combinatorial one. We are condemned to consider highly structured algebraic objects.

From that, we have been able to design and to propose a trapdoored encryption system which is weak for the cryptanalysis suggested by Paterson [13] and which enables to recover the secret κ-bit key with a single plaintext/ciphertext pair and with computing complexity in $\mathcal{O}(2^{\frac{\kappa}{2}})$.

For the candidates S-boxes enabling to design such a trapdoor (partitionning trapdoor), we have performed a detailed study with respect to their linear and differential properties (tables). We have given lower bounds with respect to their linear and differential uniformities and we have explained how to achieve them totally (linear) or nearly totally (differential). Finally, we have designed an almost optimal trapdoored system with respect to our approach and initial goal.

This study shows that the linear and differential tables we have obtained are highly structured. Thus we have proved that our trapdoor class implies

necessarily a high algebraic structure. In terms of trapdoor detectability, we conjecture that *it is easy to detect and identify our trapdoor from the results presented in this paper.*

As future works, we would primarily address the two following issues. Firstly, what would be the results if we consider non independent round keys? In other words, we would like to consider a key schedule algorithm which therefore would be part of the trapdoor.

Secondly, we want to explore and formalize exhaustively a criterion which would enable either to design better hidden trapdoors or in the contrary to evaluate the presence of a potential hidden backdoor in the same way as linear and differential tables do (refer to Harpes work [7]). The idea with respect to this criterion is the following: let denote $\mathcal{S}$ the set of S-boxes which map any linear partition to any other linear partition. For any S-box f we define the distance with respect to $\mathcal{S}$ as follows

$$\min\{\#\mathrm{Supp}(\tau) \mid \tau \in \mathfrak{S}(\mathbb{F}_2^n), f \circ \tau \in \mathcal{S}\} \ .$$

This represents the minimal number of points we have to modify in the S-box to obtain a S-box which lies in $\mathcal{S}$. In other words, the aim is to have a distance measure to a trapdoored S-box. In the second version of our toy trapdoored system (Section 6) we have indeed deteriorated the S-box (modified a few points). This second version "behaves" similarly to the original version with a probability 0.12. As a consequence, recovering the secret key will require more plaintext/ciphertext pairs.

References

1. Vesela Angelova and Yuri Borissov. Plaintext recovery in des-like cryptosystems based on s-boxes with embedded parity check. *Serdica Journal of Computing*, 7(3):257p–270p, 2013.
2. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, 4(1):3–72, 1991.
3. A 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.
4. A Caranti, F Dalla Volta, Massimiliano Sala, and Francesca Villani. Imprimitive permutations groups generated by the round functions of key-alternating block ciphers and truncated differential cryptanalysis. *arXiv preprint math/0606022*, 2006.
5. Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.
6. Joan Daemen and Vincent Rijmen. *The design of Rijndael*. Springer Verlag, 2002.
7. Carlo Harpes. *Cryptanalysis of iterated block ciphers*. PhD thesis, Diss. Techn. Wiss. ETH Zürich, Nr. 11625, 1996. Ref.: JL Massey; Korref.: U. Maurer, 1996.
8. Lars R Knudsen and Matthew JB Robshaw. *The block cipher companion*. Springer, 2011.

9. Marc Krasner and Léo Kaloujnine. Produit complet des groupes de permutations et problème d'extension de groupes. iii. *Acta Sci. Math.(Szeged)*, 14:69–82, 1951.
10. Gregor Leander and Axel Poschmann. On the classification of 4 bit s-boxes. In *Arithmetic of Finite Fields*, pages 159–176. Springer, 2007.
11. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology—EUROCRYPT'93*, pages 386–397. Springer, 1994.
12. Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology—Eurocrypt'93*, pages 55–64. Springer, 1993.
13. Kenneth G Paterson. Imprimitive permutation groups and trapdoors in iterated block ciphers. In *Fast Software Encryption*, pages 201–214. Springer, 1999.
14. Vincent Rijmen and Bart Preneel. A family of trapdoor ciphers. In *Fast Software Encryption*, pages 139–148. Springer, 1997.
15. Dan Shumow and Niels Ferguson. On the possibility of a back door in the nist sp800-90 dual ec prng. In *Proc. Crypto*, volume 7, 2007.
16. Res Strehle. *Verschlüsselt: der Fall Hans Bühler*. Werd, 1994.
17. Hongjun Wu, Feng Bao, Robert H Deng, and Qin-Zhong Ye. Cryptanalysis of rijmen-preneel trapdoor ciphers. In *Advances in Cryptology—Asiacrypt'98*, pages 126–132. Springer, 1998.

A Proofs for Section 2

Proposition A.1. *Let f be a permutation of E and $\mathcal{A}$, $\mathcal{B}$ be two partitions of E. If for any part A of $\mathcal{A}$, $f(A)$ lies in $\mathcal{B}$, then f maps $\mathcal{A}$ to $\mathcal{B}$.*

Proof. Suppose that for all A in $\mathcal{A}$, $f(A)$ lies in $\mathcal{B}$. By hypothesis, $f(\mathcal{A})$ is included in $\mathcal{B}$. It remains to show that $\mathcal{B}$ is a subset of $f(\mathcal{A})$. Let B be a part of $\mathcal{B}$ and let y be an element of B. Since f is onto, there exists x in E such that $f(x) = y$. Furthermore, there exists a unique part A of $\mathcal{A}$ which contains x as $\mathcal{A}$ is a partition de E. Then, y belongs to $f(A)$ and B. Observe that $f(A)$ and B are two non-disjoint parts of $\mathcal{B}$. Consequently, $f(A) = B$ and B belongs to $f(\mathcal{A})$. The result follows.

Lemma A.2. *Let V, W be two subspaces of $\mathbb{F}_2^n$ and f be a permutation of $\mathbb{F}_2^n$ which maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. For any x in $\mathbb{F}_2^n$, f maps $x + V$ to $f(x) + W$.*

Proof. Let x be an element of $\mathbb{F}_2^n$. By hypothesis, there exists y in $\mathbb{F}_2^n$ such that $f(x + V) = y + W$. Observe that x lies in $x + V$, so $f(x)$ lies in both $y + W$ and $f(x) + W$. Since $y + W$ and $f(x) + W$ are two non-disjoint parts of $\mathcal{L}(W)$, they must be equal. Thus, $f(x + V) = f(x) + W$.

Proof (of Proposition 2.3). Let $x + (V_1 \cap V_2)$ be a part $\mathcal{L}(V_1 \cap V_2)$. Observe that $x + (V_1 \cap V_2) = (x + V_1) \cap (x + V_2)$. Now,

$$f(x + (V_1 \cap V_2)) = f((x + V_1) \cap (x + V_2)) = f(x + V_1) \cap f(x + V_2)$$

as f is one-to-one. Then, Lemma A.2 ensures that $f(x + V_1) = f(x) + W_1$ and $f(x + V_2) = f(x) + W_2$. Next,

$$f(x + (V_1 \cap V_2)) = (f(x) + W_1) \cap (f(x) + W_2) = f(x) + (W_1 \cap W_2) \ .$$

This show that the image of any part of $\mathcal{L}(V_1 \cap V_2)$ under f lies in $\mathcal{L}(W_1 \cap W_2)$. The result is then a consequence of Proposition A.1.

Proof (of Proposition 2.4). By definition, $f(V)$ belongs to $\mathcal{L}(W)$. Thus, there exists an element x of $\mathbb{F}_2^n$ such that $f(V) = x + W$. Consequently, V and W have the same finite cardinality. Hence, V and W have the same dimension denoted by d. Let $(v_i)_{i \leq d}$ and $(w_i)_{i \leq d}$ be two basis of V and W respectively. According to the incomplete basis theorem, there exist two families $(v_i)_{d < i \leq n}$ and $(w_i)_{d < i \leq n}$ such that $\mathcal{B}_V = (v_i)_{i \leq n}$ et $\mathcal{B}_W = (w_i)_{i \leq n}$ are two basis of $\mathbb{F}_2^n$. Denoting by L the linear map which maps v_i to w_i for all $1 \leq i \leq n$, we get an automorphism of $\mathbb{F}_2^n$ satisfying the equality $L(V) = W$.

B Proofs for Section 3

Proof (of Proposition 3.2). Suppose that $\alpha_x(\mathcal{A}) = \mathcal{B}$ for any x in $\mathbb{F}_2^m$. Especially, $\mathcal{A} = \alpha_{0_m}(\mathcal{A}) = \mathcal{B}$ as α_{0_m} is the identity map. Let V denote the part of $\mathcal{A}$

containing 0_m. It is sufficient to show that V is a subgroup of $\mathbb{F}_2^m$ because any subgroup of $\mathbb{F}_2^m$ is also $\mathbb{F}_2$-linear subspace of $\mathbb{F}_2^m$. Let v_1 and v_2 be two elements of V. Since $\alpha_{v_1}(0_n) = v_1$, the intersection $\alpha_{v_1}(V) \cap V$ is non-empty. We know that α_{v_1} maps $\mathcal{A}$ to $\mathcal{A}$, so $\alpha_{v_1}(V)$ lies in $\mathcal{A}$. Thus, $\alpha_{v_1}(V) = V$ since $\mathcal{A}$ is a partition. It follows that $\alpha_{v_1}(v_2) = v_1 + v_2$ is an element of V. Therefore, the subset V of $\mathbb{F}_2^m$ is closed under the operation of addition and because every element of $\mathbb{F}_2^n$ is its own inverse, V is a subgroup of $\mathbb{F}_2^m$. Furthermore, for any x in $\mathbb{F}_2^m$, $\alpha_x(V) = x + V$ must be a part of $\mathcal{A}$. Thus, $\mathcal{A}$ is linear.

Conversely, suppose that $\mathcal{A}$ is linear and that $\mathcal{A} = \mathcal{B}$. Let V denotes the part containing 0_m and let x be an element of $\mathbb{F}_2^m$. Then,

$$\alpha_x(\mathcal{A}) = \alpha_x(\{y + V \mid y \in \mathbb{F}_2^m\}) = \{(x + y) + V \mid y \in \mathbb{F}_2^m\} = \mathcal{A} \ .$$

The result is proven.

Proof (of Proposition 3.3). Since L is an automorphism, we have

$$\begin{aligned} L(\mathcal{L}(V)) &= L(\{x + V \mid x \in \mathbb{F}_2^m\}) = \{L(x + V) \mid x \in \mathbb{F}_2^m\} \\ &= \{L(x) + L(V) \mid x \in \mathbb{F}_2^m\} = \{x + L(V) \mid x \in \mathbb{F}_2^m\} \ . \end{aligned}$$

Moreover, $L(V)$ is a subspace of $\mathbb{F}_2^m$ because L is a linear map. Consequently, $L(\mathcal{L}(V)) = \mathcal{L}(L(V))$.

Proof (of Theorem 3.4). Observe that $\alpha_0 = \mathrm{Id}$, and thus $F_0 = \pi\sigma\alpha_0 = \pi\sigma$. Now, choosing $(k_1, \ldots, k_{r+1}) = (0, \ldots, 0)$ gives

$$\begin{aligned} \mathcal{B} = E_{(k_1,\ldots,k_{r+1})}(\mathcal{A}_1) &= \alpha_{k_{r+1}} F_{k_r} \ldots F_{k_1}(\mathcal{A}_1) = \alpha_0 (F_0)^r (\mathcal{A}_1) \\ &= (\pi\sigma)^r(\mathcal{A}_1) = \mathcal{A}_{r+1} \ . \end{aligned}$$

Let $1 \leq i \leq r$ be an integer. Let k_i be any element of $\mathbb{F}_2^{ns}$. Define $k_j = 0_{ns}$ for all $j \neq i$. By hypothesis, the equality $\alpha_{k_{r+1}} F_{k_r} \ldots F_{k_1}(\mathcal{A}_1) = \mathcal{A}_{r+1}$ holds. Thus, $F_{k_i} \ldots F_{k_1}(\mathcal{A}_1) = (\alpha_{k_{r+1}} F_{k_r} \ldots F_{k_{i+1}})^{-1}(\mathcal{A}_{r-1})$. On one hand,

$$\begin{aligned} F_{k_i} \ldots F_{k_1}(\mathcal{A}_1) &= F_{k_i}(F_{k_{i-1}} \ldots F_{k_1})(\mathcal{A}_1) = F_{k_i}(F_0)^i(\mathcal{A}_1) \\ &= F_{k_i}(\pi\sigma)^i(\mathcal{A}_1) = F_{k_i}(\mathcal{A}_i) \ . \end{aligned}$$

On the other hand,

$$\begin{aligned} (\alpha_{k_{r+1}} F_{k_r} \ldots F_{k_{i+1}})^{-1}(\mathcal{A}_{r+1}) &= (\alpha_0 (F_0)^{r-i-1})^{-1}(\mathcal{A}_{r+1}) \\ &= ((\pi\sigma)^{r-i-1})^{-1}(\mathcal{A}_{r+1}) = \mathcal{A}_{i+1} \ . \end{aligned}$$

Therefore, $F_{k_i}(\mathcal{A}_i) = \mathcal{A}_{i+1}$, or equivalently $\alpha_{k_i}(\mathcal{A}_i) = (\pi\sigma)^{-1}(\mathcal{A}_{i+1})$. Since this equality holds for every k_i, Proposition 3.2 states that $\mathcal{A}_i$ is a linear partition.

It remains to show that $\mathcal{A}_{r+1}$ is linear. Let k_{r+1} be an element of $\mathbb{F}_2^{ns}$. Define $k_i = 0$ for any $1 \leq i \leq r$. Then,

$$\mathcal{A}_{r+1} = \alpha_{k_{r+1}} F_{k_r} \ldots F_{k_1}(\mathcal{A}_1) = \alpha_{k_{r+1}}(F_0)^r(\mathcal{A}_1) = \alpha_{k_{r+1}}(\mathcal{A}_{r+1}) \ .$$

Again, Proposition 3.2 implies that $\mathcal{A}_{r+1}$ is linear and the result is proven.

Proof (of Corollary 3.5). By definition, $\pi\sigma(\mathcal{A}_i) = \mathcal{A}_{i+1}$. This equality can be restated as $\pi\sigma(\mathcal{L}(V_i)) = \mathcal{L}(V_{i+1})$, or equivalently $\sigma(\mathcal{L}(V_i)) = \pi^{-1}(\mathcal{L}(V_{i+1}))$. As π is an automorphism of $\mathbb{F}_2^{ns}$, then so π^{-1} is. By Proposition 3.3, we have $\pi^{-1}(\mathcal{L}(V_{i+1})) = \mathcal{L}(\pi^{-1}(V_{i+1}))$. The result follows.

C Proofs for Section 4

C.1 Proofs for Subsection 4.1

Proof (of Proposition 4.1). Let $x = (x_i)_{i\in E}$ be an element of $(\mathbb{F}_2^n)^E$. Let y be the element of $(\mathbb{F}_2^n)^s$ defined by $y_i = x_i$ if i belongs to E and $y_i = 0_n$ otherwise. Thus, $T_E(y) = x$. By hypothesis, σ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Hence, Lemma A.2 implies that, $\sigma(y + V) = \sigma(y) + W$. Next,

$$T_E(\sigma(y + V)) = T_E(\sigma(y)) + T_E(W)$$

since T_E is a linear map. Furthermore,

$$\begin{aligned} T_E(\sigma(y + V)) &= T_E\sigma(\{y + v \mid v \in V\}) = \{T_E\sigma(y + v) \mid v \in V\} \\ &= \{\sigma_E(T_E(y + v)) \mid v \in V\} = \sigma_E(\{T_E(y + v) \mid v \in V\}) \\ &= \sigma_E(\{T_E(y) + T_E(v) \mid v \in V\}) = \sigma_E(T_E(y) + T_E(V)) \ . \end{aligned}$$

Therefore, $\sigma_E(x + T_E(V)) = T_E(\sigma(y)) + T_E(W)$. In other words, the image of any part of $\mathcal{L}(T_E(V))$ under σ lies in $\mathcal{L}(T_E(W))$. The result is a consequence of Proposition A.1.

C.2 Proofs for Subsection 4.2

Proof (of Lemma 4.3). Suppose that $V = \bigoplus_{I\in\mathcal{I}} V_I$. Let $v = (v_1, \ldots, v_s)$ be an element of V. By hypothesis, v can be uniquely written as $\sum_{I\in\mathcal{I}} v_I$ where v_I belongs to V_I for every I in $\mathcal{I}$ Let I be a part of $\mathcal{I}$. For every i in I, we have

$$(P_I(v))_i = v_i = \sum_{I'\in\mathcal{I}} (v_{I'})_i = (v_I)_i \ ,$$

since $(v_{I'}) = 0_n$ for all part I' of $\mathcal{I}$ distinct from I. As $P_I(v)_i = 0_n = (v_I)_i$ for every i in I^c, we obtain that $P_I(v) = v_I$. Thus, $P_I(v)$ is included in V_I. The equality follows because the other inclusion always holds.

Conversely, suppose that $V_I = P_I(V)$ for all I in $\mathcal{I}$. Let v be an element of V. Clearly, $v = \sum_{I\in\mathcal{I}} P_I(v)$. By hypothesis, $P_I(v)$ belongs to V_I for any I in $\mathcal{I}$. The uniqueness of this decomposition directly follows from the definition of the V_I. Therefore, $V = \bigoplus_{I\in\mathcal{I}} V_I$.

Proof (of Lemma 4.4). Suppose that $V = \bigoplus_{I\in\mathcal{I}} V_I$. Firstly, let us prove that $W = \sum_{I\in\mathcal{I}} W_I$. Since the W_I are subspaces of W, the inclusion $\sum_{I\in\mathcal{I}} W_I \subseteq W$ clearly holds. Now, let w be an element of W. Define $x = \sigma^{-1}(0_{ns}) = (\sigma_i^{-1}(0_n))_{1\leq i\leq n}$. According to Lemma A.2, we have $\sigma(x+V) = \sigma(x)+W = W$.

Hence, there exists an element v of V satisfying the equality $\sigma(x+v) = w$. Then, Lemma 4.3 ensures that $v = \sum_{I\in\mathcal{I}} P_I(v)$. For any $1 \leq i \leq s$, we have

$$\sigma(x + P_I(v))_i = \sigma_i(x_i + P_I(v)_i) = \begin{cases} 0_n & \text{if } i \in I^c \ , \\ \sigma_i(x_i + v_i) & \text{if } i \in I \ , \end{cases}$$

because $\sigma_i(x_i) = 0_n$. Consequently, $\sigma(x + P_I(v))$ lies in Triv_I and W, so in W_I. Note that

$$w = \sigma(x + v) = \sum_{I\in\mathcal{I}} \sigma(x + P_I(v))$$

since $\mathcal{I}$ is a partition of $[\![1, s]\!]$. The inclusion $W \subseteq \sum_{I\in\mathcal{I}} W_I$ follows. Finally, the definition of the W_I implies that $W = \bigoplus_{I\in\mathcal{I}} W_I$.

Conversely, suppose that $W = \bigoplus_{I\in\mathcal{I}} W_I$. Following the previous reasoning with σ^{-1} instead of σ gives the equality $V = \bigoplus_{I\in\mathcal{I}} V_I$, as desired.

Proof (of Proposition 4.5). The implication is an immediate consequence of Proposition 4.1. Conversely, suppose that σ_I maps $\mathcal{L}(T_I(V))$ to $\mathcal{L}(T_I(W))$ for any I in $\mathcal{I}$. According to Lemma 4.3, for any part I of $\mathcal{I}$, $V_I = P_I(V)$ and thus $T_I(V) = T_I(P_I(V)) = T_I(V_I)$. Then Lemma 4.4 ensure that the same result holds of the subspace W.

Even if it means to change the order of the S-boxes and the coordinates of the spaces V and W, we can assume that every part of $\mathcal{I}$ is an integer interval. Denote $\mathcal{I} = \{I_1, \ldots, I_m\}$ such that $x = [T_{I_1}(x) \parallel \ldots \parallel T_{I_m}(x)]$ for every x in $(\mathbb{F}_2^n)^s$. Let x and v be elements of $(\mathbb{F}_2^n)^s$ and V respectively. By hypothesis, for all $1 \leq i \leq m$, there exists an element w_{I_i} of $T_{I_i}(W_{I_i})$ such that

$$\sigma_{I_i}(T_{I_i}(x) + T_{I_i}(v)) = \sigma_{I_i}(T_{I_i}(x)) + w_{I_i} \ .$$

As $W = \bigoplus_{i=1}^m W_{I_i}$, the vector $w = [w_{I_1} \parallel \ldots \parallel w_{I_m}]$ belongs to W. Observe that $T_{I_i}(w) = w_{I_i}$ for any $1 \leq i \leq m$. Hence,

$$\begin{aligned} \sigma(x + v) &= [\sigma_{I_1}(T_{I_1}(x) + T_{I_1}(v)) \parallel \ldots \parallel \sigma_{I_m}(T_{I_m}(x) + T_{I_m}(v))] \\ &= [\sigma_{I_1}(T_{I_1}(x)) + w_{I_1} \parallel \ldots \parallel \sigma_{I_m}(T_{I_1}(x)) + w_{I_m}] \\ &= [\sigma_{I_1}(T_{I_1}(x)) \parallel \ldots \parallel \sigma_{I_m}(T_{I_1}(x))] + [w_{I_1} \parallel \ldots \parallel w_{I_m}] = \sigma(x) + w \ . \end{aligned}$$

Consequently, $\sigma(x+V) \subseteq \sigma(x)+W$. Furthermore, Proposition 2.4 states that V and W are isomorphic. Thus, $\#\sigma(x+V) = \#(\sigma(x)+W)$ because σ is bijective. The equality $\sigma(x + V) = \sigma(x) + W$ follows. Finally, the result comes from Proposition A.1.

Minimal Partition

Notation (partition intersection). Let $\mathcal{I}$ and $\mathcal{J}$ be two partitions of $[\![1, s]\!]$. We denote by $\mathcal{I} \cap \mathcal{J}$ the set $\{I \cap J \mid I \in \mathcal{I} \text{ et } J \in \mathcal{J}\} \setminus \{\emptyset\}$. Note that $\mathcal{I} \cap \mathcal{J}$ is a partition of $[\![1, s]\!]$ finer than $\mathcal{I}$ and $\mathcal{J}$.

Lemma C.1. *Let $\mathcal{I}$ and $\mathcal{J}$ be two partitions of $[\![1, s]\!]$ such that $V = \bigoplus_{I\in\mathcal{I}} V_I = \bigoplus_{J\in\mathcal{J}} V_J$. Then, $V = \bigoplus_{K\in\mathcal{I}\cap\mathcal{J}} V_K$.*

Proof. Le v be an element of V and K be an element of $\mathcal{I} \cap \mathcal{J}$. According to Lemma 4.3, we have to prove that $P_K(v)$ belongs to V_K. By definition, there exists elements I and J of $\mathcal{I}$ and $\mathcal{J}$ such that $K = I \cap J$. Since $V = \bigoplus_{I'\in\mathcal{I}} V_{I'}$, the same lemma ensures that $P_I(v)$ lies in V_I, hence in V. In the same way, using the equality $V = \bigoplus_{J'\in\mathcal{J}} V_{J'}$, we obtain that $P_J(P_I(v))$ lies in V_J, so in V. The result follows because $P_J(P_I(v)) = P_{I\cap J}(v) = P_K(v)$.

Proof (of Lemma 4.6). Let $\mathcal{P}$ denote the set of the partitions $\mathcal{I}$ of $[\![1, s]\!]$ satisfying $V = \bigoplus_{I\in\mathcal{I}} V_I$. By virtue of Lemma C.1, the set $\mathcal{P}$ is closed under the operation of intersection. Then, it is sufficient to define $\mathcal{I}_{\min}$ as the intersection of all the elements of $\mathcal{P}$.

C.3 Proofs for Subsection 4.3

Generality on Linked S-Boxes

Lemma C.2. *Let I be an element of $\mathcal{I}_{\min}$. Let E be a non-empty proper subset of I. Then $V_E \subsetneq P_E(V)$ and $P_E(V) \neq \{0_{ns}\}$.*

Proof. By construction, V_E is a subset of $P_E(V)$. Let us prove that $V_E \neq P_E(V)$. By contradiction, suppose that $V_E = P_E(V)$. Let v be an element of V. By hypothesis, $P_E(v)$ belongs to V_E. Especially, $P_E(v)$ lies in V, so $v + P_E(v)$ also lies in V. Since $v + P_E(v) = P_{E^c}(v)$, we obtain that $P_{E^c}(v)$ belongs to V_{E^c}. Define $\mathcal{J} = \{E, E^c\}$. Form Lemma 4.3, we have that $V = \bigoplus_{J\in\mathcal{J}} V_J$. Then, $V = \bigoplus_{K\in\mathcal{I}_{\min}\cap\mathcal{J}} V_K$ follows from Lemma C.1. Observe that the partition $\mathcal{I}_{\min} \cap \mathcal{J}$ is strictly finer than $\mathcal{I}_{\min}$ because E is a proper subset of I. This is a contradiction, and therefore $V_E \subsetneq P_E(V)$.

By contradiction, suppose that $P_E(V) = \{0_{ns}\}$. From the previous result, we have that $\{0_{ns}\} \subseteq V_E \subseteq P_E(V) = \{0_{ns}\}$, which is a contradiction. Thus, $P_E(V) \neq \{0_{ns}\}$.

Proof (of Lemma 4.9). By contradiction, suppose that V_E is any trivial product space different from $\{0_{ns}\}$. Hence, there exists a non-empty subset F of E such that $V_E = \mathrm{Triv}_F$. Therefore $\mathrm{Triv}_F \subseteq V$ and so $\mathrm{Triv}_F = V_F$. Next, $\mathrm{Triv}_F = V_F \subseteq P_F(V) = \mathrm{Triv}_F$, and thus $V_F = P_F(V)$. Since F is a non-empty proper subset of P, we have a contradiction with Lemma C.2. Consequently, $V_E = \{0_{bm}\}$.

By contradiction, suppose that $P_E(V)$ is any trivial product space different from Triv_E. There exists a proper subset F of E such that $P_E(V) = \mathrm{Triv}_F$. Thus, for every v in V and every i in $E \setminus F$, $Prj_E(v)_i = 0_n$. As a consequence, $P_{E\setminus F}(V) = \{0_{ns}\}$. This is a contradiction with Lemma C.2 because $E \setminus F$ is a non-empty proper subset of I. The result follows.

Study of a Special Case of Linked S-Boxes Without loss of generality, Proposition 4.5 allows to suppose that $\mathcal{I}_{\min} = \{I\}$ with $I = [\![1, s]\!]$.

Lemma C.3. *Let E be a subset of $[\![1, s]\!]$. Then $\#V = \#T_E(V) \times \#V_{E^c}$.*

Proof. Let m denote $\#E$. Consider the restriction of the linear map T_E to V. Its kernel is

$$\ker(T_E) = \{v \in V \mid T_E(v) = 0_{nm}\} = \{v \in V \mid \forall i \in E, v_i = 0_n\} = V_{E^c} \ .$$

From the first isomorphism theorem, the quotient space V/V_{E^c} is isomorphic to the image $T_E(V)$. Particularly, the equality $\#V/\#V_{E^c} = \#T_E(V)$ holds.

Lemma C.4. *Let $E = [\![1, m]\!]$ with $1 \leq m < s$. Suppose that $V_E = V_{E^c} = \{0_{ns}\}$ and $T_E(V) = (\mathbb{F}_2^n)^m$. There exist two isomorphisms $\varphi : T_E(V) \to T_{E^c}(V)$ and $\psi : T_E(W) \to T_{E^c}(W)$ such that*

$$V = \{[a \parallel \varphi(a)] \mid a \in (\mathbb{F}_2^n)^m\} \quad et \quad W = \{[b \parallel \psi(b)] \mid b \in (\mathbb{F}_2^n)^m\} \ .$$

Proof. Lemma C.3 ensures that $\#V = \#T_E(V) \times \#V_{E^c}$. By hypothesis, $V_{E^c} = \{0_{ns}\}$, so $\#V_{E^c} = 1$. It follows that $\#V = \#T_E(V)$. Therefore, V and $T_E(V)$ have the same dimension d. Let $\mathcal{B} = (b^1, \ldots, b^d)$ be a basis of $T_E(V)$. By definition, there exist elements $c^1, \ldots, c^d$ of V such that $T_E(c^i) = b^i$ for all $1 \leq i \leq d$. That is, $c^i = [b^i \parallel T_{E^c}(c^i)]$. Note that $c^1, \ldots, c^d$ are linearly independent as the b^i are and thus $(b^i)_{1 \leq i \leq d}$ is a basis of V. Define the linear map $\varphi : T_E(V) \to T_{E^c}(V)$ that associates $T_{E^c}(c^i)$ with b^i. Let v be an element of V. Then x can be written as $x = \sum_{i=1}^{d} \lambda_i c^i$ where the λ_i are elements of $\mathbb{F}_2$. Next,

$$v = \sum_{i=1}^{d} \lambda_i c^i = \sum_{i=1}^{d} [\lambda_i T_E(c^i) \parallel \lambda_i T_{E^c}(c^i)] = \Big[\sum_{i=1}^{d} \lambda_i b^i \parallel \varphi(\sum_{i=1}^{d} \lambda_i b^i) \Big] = [a \parallel \varphi(a)]$$

where a denotes the element $\sum_{i=1}^{d} \lambda_i b^i$ of $T_E(V)$. Consequently, every element of V can be written in the desired form. As the converse inclusion is obvious, the equality $V = \{[a \parallel \varphi(a)] \mid a \in (\mathbb{F}_2^n)^m\}$ follows. Hence, the map φ is onto. Applying Lemma C.3 with the subset E^c gives $\#V = \#T_{E^c}(V) \times \#V_E = \#T_{E^c}(V)$, and thus $T_{E^c}(V)$ is also a d-dimensional subspace. Therefore, φ is a isomorphism.

Recall that σ maps $\mathcal{L}(V_E)$ to $\mathcal{L}(W_E)$. Then, Proposition 2.4 states that V_E and W_E are isomorphic, and so $W_E = \{0_{ns}\}$. In the same way, we obtain that $W_{E^c} = \{0_{ns}\}$. Next, Proposition 4.1 implies that σ_E maps $\mathcal{L}(T_E(V))$ to $\mathcal{L}(T_E(W))$. Again, we get that $T_E(W) = (\mathbb{F}_2^n)^m$. The preceding argument gives an isomorphism $\psi : T_E(W) \to T_{E^c}(W)$ such that $W = \{[b \parallel \psi(b)] \mid b \in (\mathbb{F}_2^n)^m\}$.

Lemma C.5. *Let m be a non-negative integer. Let $f : (\mathbb{F}_2^n)^m \to (\mathbb{F}_2^n)^m$ be a map such that there exists $\tau : (\mathbb{F}_2^n)^m \to (\mathbb{F}_2^n)^m$ satisfying*

$$\forall x \in (\mathbb{F}_2^n)^m, \ \exists y \in (\mathbb{F}_2^n)^m, \ \forall z \in (\mathbb{F}_2^n)^m, \ f(x + z) = y + \tau(z) \ .$$

Then f is an affine map.

Proof. By hypothesis, choosing $x = 0$ gives the existence of an element y_0 of $(\mathbb{F}_2^n)^m$ such that $f(z) = y_0 + \tau(z)$ for every z in $(\mathbb{F}_2^n)^m$. Thus,

$$\forall z \in (\mathbb{F}_2^n)^m,\ \tau(z) = f(z) + y_0\ . \tag{1}$$

Let x be an element of $(\mathbb{F}_2^n)^m$. By hypothesis, there exists an element y of $(\mathbb{F}_2^n)^m$ such that $f(x+z) = y + \tau(z)$ for any z in $(\mathbb{F}_2^n)^m$. Especially, choosing $z = x$ gives $f(0) = f(x+x) = y + \tau(x)$, and thus $y = \tau(x) + f(0)$. Let z be an element of $(\mathbb{F}_2^n)^m$. Hence,

$$f(x+z) = y + \tau(z) = \tau(x) + \tau(z) + f(0)\ . \tag{2}$$

Then we can combine equations (1) and (2) to obtain

$$f(x+z) = \big(f(x) + y_0\big) + \big(f(z) + y_0\big) + f(0) = f(x) + f(z) + f(0)\ .$$

Since this equality holds for every x and z in $(\mathbb{F}_2^n)^m$, f is an affine map.

Proof (of Lemma 4.10). Firstly, we have $T_E(V) = (\mathbb{F}_2^n)^m$ since $P_E(V) = T_E$. Even if it means to change the order of the S-boxes and the coordinates of the spaces V and W, we can assume that $E = [\![1, m]\!]$ with $0 < m < s$. According to Lemma C.4, there exist two isomorphisms $\varphi : T_E(V) \to T_{E^c}(V)$ and $\psi : T_E(W) \to T_{E^c}(W)$ such that

$$V = \{[a \parallel \varphi(a)] \mid a \in (\mathbb{F}_2^n)^m\} \quad \text{et} \quad W = \{[b \parallel \psi(b)] \mid b \in (\mathbb{F}_2^n)^m\}\ .$$

Let τ denotes the permutation $\psi^{-1}\sigma_{E^c}\varphi$ of $(\mathbb{F}_2^n)^m$ because $T_E(V) = T_E(W) = (\mathbb{F}_2^n)^m$. Let x be an element of $(\mathbb{F}_2^n)^m$. From Lemma A.2, we have

$$\sigma([x \parallel 0_{b(n-m)}] + V) = y + W\ .$$

with $y = \sigma([x \parallel 0_{b(n-m)}])$. Then, let c denotes the element $T_E(y) + \psi^{-1}T_{E^c}(y)$ of $(\mathbb{F}_2^n)^m$. On one hand,

$$\begin{aligned}\sigma([x \parallel 0_{b(n-m)}] + V) &= \sigma(\{[x \parallel 0_{b(n-m)}] + [a \parallel \varphi(a)] \mid a \in (\mathbb{F}_2^n)^m\}) \\ &= \sigma(\{[x+a \parallel \varphi(a)] \mid a \in (\mathbb{F}_2^n)^m\}) \\ &= \{[\sigma_E(x+a) \parallel \sigma_{E^c}(\varphi(a))] \mid a \in (\mathbb{F}_2^n)^m\}\ .\end{aligned}$$

On the other hand,

$$\begin{aligned}y + W &= \{y + [b \parallel \psi(b)] \mid b \in (\mathbb{F}_2^n)^m\} \\ &= \{[T_E(y) + b \parallel T_{E^c}(y) + \psi(b)] \mid b \in (\mathbb{F}_2^n)^m\}\ .\end{aligned}$$

Let a be an element of $(\mathbb{F}_2^n)^m$. Since $[\sigma_E(x+a) \parallel \sigma_{E^c}(\varphi(a))]$ belongs to $y + W$, there exists an element b of $(\mathbb{F}_2^n)^m$ such that

$$[\sigma_E(x+a) \parallel \sigma_{E^c}(\varphi(a))] = [T_E(y) + b \parallel T_{E^c}(y) + \psi(b)]\ .$$

This is equivalent to the equalities $\sigma_E(x+a) = T_E(y) + b$ and $\sigma_{E^c}(\varphi(a)) = T_{E^c}(y) + \psi(b)$. This last one can be restated as

$$b = \psi^{-1}\sigma_{E^c}\varphi(a) + \psi^{-1}T_{E^c}(y) = \tau(a) + \psi^{-1}T_{E^c}(y) \ .$$

When combined with the first equality it gives

$$\sigma_E(x+a) = T_E(y) + b = T_E(y) + \tau(a) + \psi^{-1}T_{E^c}(y) = \tau(a) + c \ .$$

We have proven that for any x in $(\mathbb{F}_2^n)^m$, there exists c in $(\mathbb{F}_2^n)^m$ such that, for all a in $(\mathbb{F}_2^n)^m$, $\sigma_E(x+a) = \tau(a) + c$. Then, Lemma C.5 states that σ_E is an affine map.

Let i be an element of E. The map $I_i : \mathbb{F}_2^n \to (\mathbb{F}_2^n)^s$, $x \mapsto (\delta_{i,1}x, \ldots, \delta_{i,n}x)$ is clearly linear (where $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise). Observe that $\sigma_i = T_i\sigma_E I_i$. Therefore, σ_i is the composition of several affine maps and thus it is an affine map.

D Proofs for Section 5

Proof (of Theorem 5.1). Let us demonstrate the implication. By hypothesis, f maps $\mathcal{L}(V)$ to $\mathcal{L}(V)$. Thus, f induces a permutation ρ of U defined as follows. Let u be an element of U. Hence, there exists a unique u' in U such as $f([u]) = [u']$. Define then $\rho(u) = u'$. For each element u of U, define the permutation τ_u of V which maps v to $f(u+v) + \rho(u)$. By construction, for any u in U and any v in V the following equalities hold:

$$\tau_u(v) = f(u+v) + \rho(u) \quad \text{and hence} \quad f(u+v) = \rho(u) + \tau_u(v) \ .$$

The existence of the permutations ρ and τ_u is now proven. Now, let show their uniqueness. Suppose that there exist a permutation $\tilde{\rho}$ of U and a family of permutations $(\tilde{\tau}_u)_{u\in U}$ of V satisfying the result. Let (u, v) be an element of $U \times V$. By hypothesis, we have

$$\rho(u) + \tau_u(v) = \tilde{\rho}(u) + \tilde{\tau}_u(v) \ .$$

Because the sum of U and V is direct, it follows that $\rho(u) = \tilde{\rho}(u)$ and $\tau_u(v) = \tilde{\tau}_u(v)$. The uniqueness of ρ and the τ_u follows.

Conversely, let ρ be a permutation of U and $(\tau_u)_{u\in U}$ be a family of permutations of V. Denote g the map from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by $g(u+v) = \rho(u) + \tau_u(v)$. Since $\mathbb{F}_2^n = U \oplus V$ and ρ and the τ_u are permutations of U and V respectively, The map g is a permutation of $\mathbb{F}_2^n$. Let u be an element of U. Therefore,

$$\begin{aligned} g([u]) &= \{g(u+v) \mid v \in V\} = \{\rho(u) + \tau_u(v) \mid v \in V\} \\ &= \{\rho(u) + v \mid v \in V\} = [\rho(u)] \ . \end{aligned}$$

Hence, g maps $\mathcal{L}(V)$ to $\mathcal{L}(V)$.

The following lemma explains how the linear properties of ρ' and the τ'_u are expressed according to the applications ρ and τ_u.

Lemma D.1. *Let W be a m-dimensional subspace of $\mathbb{F}_2^n$ and $L : \mathbb{F}_2^m \to W$ be an isomorphism. Let μ be a permutation of W. Denote μ' the permutation $L^{-1}\mu L$ of $\mathbb{F}_2^m$. Let a and b be elements of W. Finally, Define $a' = L^{-1}(a)$, $b' = L^{-1}(b)$, $a^t = L^\intercal(a)$ and $b^t = L^\intercal(b)$. Then,*

$$\begin{aligned}(\mathrm{DT}_{\mu'})_{a',b'} &= \#\{w \in W \mid \mu(w) + \mu(w+a) = b\} \ , \\ (\mathrm{LT}_{\mu'})_{a^t,b^t} &= \#\{w \in W \mid \langle a, w\rangle = \langle b, \mu(w)\rangle\} - 2^{m-1} \ .\end{aligned}$$

Proof. Let us begin with the linear table of μ'. By definition,

$$\begin{aligned}(\mathrm{LT}_{\mu'})_{a^t,b^t} + 2^{m-1} &= \#\{x \in \mathbb{F}_2^m \mid \langle a^t, x\rangle = \langle b^t, \mu'(x)\rangle\} \\ &= \#\{x \in \mathbb{F}_2^m \mid \langle L^\intercal(a), x\rangle = \langle L^\intercal(b), L^{-1}\mu L(x)\rangle\} \ .\end{aligned}$$

Using the property of the transposed map, it follows

$$(\mathrm{LT}_{\mu'})_{a^t,b^t} + 2^{m-1} = \#\{x \in \mathbb{F}_2^m \mid \langle a, L(x)\rangle = \langle b, \mu(L(x))\rangle\} \ .$$

Let E denote the set of the right side of the previous equality. Then, $\#E = \#L(E)$ because L is a bijection. Consequently,

$$(\mathrm{LT}_{\mu'})_{a^t,b^t} + 2^{m-1} = \#\{w \in W \mid \langle a, w\rangle = \langle b, \mu(w)\rangle\} \ .$$

It remains to prove the result about the differential table of μ'. By definition,

$$\begin{aligned}(\mathrm{DT}_{\mu'})_{a',b'} &= \#\{x \in \mathbb{F}_2^m \mid \mu'(x) + \mu'(x+a') = b'\} \\ &= \#\{x \in \mathbb{F}_2^m \mid L^{-1}\mu L(x) + L^{-1}\mu L(x + L^{-1}(a)) = L^{-1}(b)\} \ .\end{aligned}$$

Because L is one-to-one, $L(x) = L(y)$ if and only if $x = y$. Furthermore, using the linearity of L, it follows that

$$\begin{aligned}(\mathrm{DT}_{\mu'})_{a',b'} &= \#\{x \in \mathbb{F}_2^m \mid L(L^{-1}\mu L(x) + L^{-1}\mu L(x + L^{-1}(a))) = LL^{-1}(b)\} \\ &= \#\{x \in \mathbb{F}_2^m \mid \mu(L(x)) + \mu(L(x) + a) = b\} \ .\end{aligned}$$

Again, considering the image of the last set under L, we obtain

$$(\mathrm{DT}_{\mu'})_{a',b'} = \#\{w \in W \mid \mu(w) + \mu(w+a) = b\} \ .$$

This concludes the proof.

D.1 Proofs for Subsection 5.1

Proof (of Theorem 5.4). By definition,

$$\mathrm{LT}_{a,b} + 2^{n-1} = \#\{x \in \mathbb{F}_2^n \mid \langle a, x\rangle = \langle b, f(x)\rangle\} \ .$$

Let $x = u+v$ be an element of $\mathbb{F}_2^n$. According to Theorem 5.1, the equality $f(u+v) = \rho(u) + \tau_u(v)$ holds. The following equivalences come from the bilinearity of the map $\langle \cdot, \cdot \rangle$,

$$\begin{aligned}\langle a, x\rangle = \langle b, f(x)\rangle &\Leftrightarrow \langle a, u+v\rangle = \langle b, f(u+v)\rangle \\ &\Leftrightarrow \langle a, u\rangle + \langle a, v\rangle = \langle b, \rho(u)\rangle + \langle b, \tau_u(v)\rangle \ .\end{aligned}$$

Then, $\langle a, v\rangle = \langle b, \tau_u(v)\rangle = 0$ because a and b belong to $V^\perp$. We then obtain that

$$\begin{aligned}\mathrm{LT}_{a,b} + 2^{n-1} &= \#\{u+v \in \mathbb{F}_2^n \mid \langle a, u\rangle = \langle b, \rho(u)\rangle\} \\ &= \#V \times \#\{u \in U \mid \langle a, u\rangle = \langle b, \rho(u)\rangle\} \\ &= 2^d \times \#\{u \in U \mid \langle a, u\rangle = \langle b, \rho(u)\rangle\} \ .\end{aligned}$$

Finally, Lemma D.1 implies that

$$\mathrm{LT}_{a,b} = 2^d\big(\#\{u \in U \mid \langle a, u\rangle = \langle b, \rho(u)\rangle\} - 2^{n-d-1}\big) = 2^d \times (\mathrm{LT}_{\rho'})_{a^t,b^t} \ .$$

The desired result is proven.

Proof (of Corollary 5.7). Suppose that $d < n-1$. Observe that there exist necessarily two elements a^t and b^t of $\mathbb{F}_2^{n-d}$ both non-zero such that $|(\mathrm{LT}_{\rho'})_{a^t,b^t}| \geq 2$. Let a and b denote the elements $(L_U^\intercal)^{-1}(a^t)$ and $b = (L_U^\intercal)^{-1}(b^t)$ of $\mathbb{F}_2^n$. Then, Theorem 5.4 implies that $(\mathrm{LT}_f)_{a,b} \geq 2^{d+1}$. Observing moreover that a and b are non-zero, the corollary is proven. The same reasoning applies for $d = n-1$, but this time, $|(\mathrm{LT}_{\rho'})_{a^t,b^t}| \geq 1$.

D.2 Proofs for Subsection 5.2

Lemma D.2. *Let $a = u_a + v_a$ and $b = u_b + v_b$ be two elements of $\mathbb{F}_2^n$. Define $\mathcal{U} = \{u \in U \mid \rho(u) + \rho(u+u_a) = u_b\}$. Then,*

$$(\mathrm{DT}_f)_{a,b} = \sum_{u \in \mathcal{U}} \#\{v \in V \mid \tau_u(v) + \tau_{u+u_a}(v+v_a) = v_b\} \ .$$

Proof. By definition, we have

$$\begin{aligned}&(\mathrm{DT}_f)_{a,b}\#\{x \in \mathbb{F}_2^n \mid f(x) + f(x+a) = b\} \\ &= \#\{u+v \in \mathbb{F}_2^n \mid \rho(u) + \tau_u(v) + \rho(u+u_a) + \tau_{u+u_a}(v+v_a) = u_b + v_b\} \ .\end{aligned}$$

Observe that $\rho(u)+\rho(u+u_a)$ and $\tau_u(v)+\tau_{u+u_a}(v+v_a)$ lie respectively in U and V. Since any element of $\mathbb{F}_2^n$ can be uniquely written as $u+v$, the previous equality holds if and only if $\rho(u)+\rho(u+u_a) = u_b$ and $P(u,v) : \tau_u(v)+\tau_{u+u_a}(v+v_a) = v_b$ are satisfied. Note that the first equality is equivalent to $u \in \mathcal{U}$. Thus,

$$(\mathrm{DT}_f)_{a,b} = \#\{u+v \in \mathbb{F}_2^n \mid u \in \mathcal{U} \text{ et } P(u,v)\} = \sum_{u \in \mathcal{U}} \#\{v \in V \mid P(u,v)\} \ .$$

The result is proven.

Lemma D.3. *Let λ, μ be two permutations of V and v_a, v_b be two elements of $\mathbb{F}_2^n$. Then,*

$$\begin{aligned}&\textstyle\sum_{v_0\in V} \#\{v \in V \mid \mu(v) + \lambda(v + v_a) = v_0\}\\ =&\textstyle\sum_{v_0\in V} \#\{v \in V \mid \mu(v) + \lambda(v + v_0) = v_b\} = \#V\ .\end{aligned}$$

Proof. For each v_0 in V, define $E_{v_0} = \{v \in V \mid \mu(v) + \lambda(v + v_a) = v_0\}$. Firstly, let us prove that $\bigcup_{v_0\in V} E_{v_0} = V$. The inclusion is immediate. It remains to prove that the converse inclusion holds. Let v be an element of V. Then, v belongs to $E_{\mu(v)+\lambda(v+v_a)}$. The sets E_{v_0} are obviously pairwise disjoint, and thus $\#V = \#\bigcup_{v_0\in V} E_{v_0} = \sum_{v_0\in V} \#E_{v_0}$.

For each v_0 in V, define $F_{v_0} = \{v \in V \mid \mu(v) + \lambda(v + v_a) = v_0\}$. It remains to prove that $\bigcup_{v_0\in V} F_{v_0} = V$. As previously, we only have to prove the converse inclusion. Let v in V. Since λ is onto, there exists an element x of V such that $\lambda(x) = \mu(v) + v_b$. Then, v lies in F_{x+v}. Moreover, the sets F_{v_0} are pairwise disjoint as λ is one-to-one. Finally, $\#V = \sum_{v_0\in V} \#F_{v_0}$ as desired.

Proof (of Theorem 5.10). Let $\mathcal{U}$ denotes the set $\{u \in U \mid \rho(u)+\rho(u+u_a) = u_b\}$. According to Lemma D.2, we have

$$\begin{aligned}\sum_{i\in[u_a]} (\mathrm{DT}_f)_{i,b} &= \sum_{v_0\in V} (\mathrm{DT}_f)_{u_a+v_0,b}\\ &= \sum_{v_0\in V} \Big(\sum_{u\in\mathcal{U}} \#\{v \in V \mid \tau_u(v) + \tau_{u+u_a}(v + v_0) = v_b\}\Big)\ .\end{aligned}$$

Since these sums are finite, they can be exchanged. Hence,

$$\sum_{i\in[u_a]} (\mathrm{DT}_f)_{i,b} = \sum_{u\in\mathcal{U}} \Big(\sum_{v_0\in V} \#\{v \in V \mid \tau_u(v) + \tau_{u+u_a}(v + v_0) = v_b\}\Big)\ .$$

In the same way, it can be proven that

$$\sum_{j\in[u_b]} (\mathrm{DT}_f)_{a,j} = \sum_{u\in\mathcal{U}} \Big(\sum_{v_0\in V} \#\{v \in V \mid \tau_u(v) + \tau_{u+u_a}(v + v_a) = v_0\}\Big)\ .$$

By virtue of Lemma D.3, we obtain

$$\sum_{i\in[u_a]} (\mathrm{DT}_f)_{i,b} = \sum_{j\in[u_b]} (\mathrm{DT}_f)_{a,j} = \sum_{u\in\mathcal{U}} \#V = \#\mathcal{U} \times 2^d\ .$$

Finally, Lemma D.1 ensures that $\#\mathcal{U} = (\mathrm{DT}_{\rho'})_{u'_a,u'_b}$. The result follows.

Proof (of Theorem 5.11). Applying Lemma D.2 with $a = 0 + v_a$ and $b = 0 + v_b$, we obtain

$$(\mathrm{DT}_f)_{v_a,v_b} = \sum_{u\in U} \#\{v \in V \mid \tau_u(v) + \tau_u(v + v_a) = v_b\}\ ,$$

since $\mathcal{U} = \{u \in U \mid \rho(u) + \rho(u + 0) = 0\} = U$. Then, the result comes from Lemma D.1.

Proof (of Corollary 5.13). According to Theorem 5.11, the difference distribution subtable $((\mathrm{DT}_f)_{v_a,v_b})_{v_a,v_b\in V}$ of f is the sum of the differential tables of several d-bit S-boxes. Consider the second row of this subtable. Necessarily, its first coefficient is zero. Hence, there are at most $2^d - 1$ non-zero coefficients. Recall that the sum of all the coefficients of the differential table of a d-bit S-box equals 2^d. Consequently, the sum of the coefficient of the second row of the subtable equals $\#U \times 2^d = 2^n$. In the perfect case where this sum is uniformly distributed over all the coefficients, they all equal to $\frac{2^n}{2^d-1}$. The result follows since any coefficient is the sum of even integer, so must also be an even integer.

E Differential Distribution and Linear Approximation Tables of Examples 5.6 and 5.12

In every table given is this section, the dots "·" stand for the integer 0. This helps to emphasize the structures of the tables. The next tables represent the linear approximation tables LT_f of f and $\mathrm{LT}_{\rho'}$ of ρ'. As explained in Example 5.6, that the rows and columns of LT_f does not follow the natural order in $\mathbb{F}_2^6$.

ρ'

	0	1	2	3	4	5	6	7
0	4	.	.	.	.	.	.	.
1	.	2	2	.	.	2	-2	.
2	.	.	-2	-2	-2	2	.	.
3	.	-2	.	-2	2	.	-2	.
4	.	2	.	-2	.	-2	.	-2
5	.	.	-2	2	.	.	-2	-2
6	.	2	-2	.	2	.	.	2
7	.	.	.	.	2	2	2	-2

$V^\intercal$ (columns) / $V^\intercal$ (rows)

	00	05	16	13	18	1D	0E	0B	01	02	03	04	06	07	08	09	0A	0C	0D	0F	10	11	12	14	15	17	19	1A	1B	1C	1E	1F
00	16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
05	·	8	8	·	·	8	-8	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
16	·	·	-8	-8	-8	8	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
13	·	-8	·	-8	8	·	-8	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
18	·	8	·	-8	·	-8	·	-8	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1D	·	·	-8	8	·	·	-8	-8	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
0E	·	8	-8	·	8	·	·	8	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
0B	·	·	·	·	8	8	8	-8	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
01	·	·	·	·	·	·	·	·	6	-6	4	-2	·	-2	-4	-2	2	2	·	2	4	-2	-6	2	·	2	-2	-6	-4	-2	·	-2
02	·	·	·	·	·	·	·	·	-6	4	-6	-2	-2	-4	-2	·	2	·	-6	6	2	·	-2	·	-2	2	-2	-4	-2	2	2	4
03	·	·	·	·	·	·	·	·	4	-6	6	·	-2	-2	2	2	·	-2	-6	4	-2	2	4	-2	-2	·	·	2	2	4	2	6
04	·	·	·	·	·	·	·	·	-2	-2	·	-2	4	-6	·	2	2	-2	-4	-6	·	2	2	-2	4	2	-2	-2	·	6	-4	-6
06	·	·	·	·	·	·	·	·	·	2	2	4	2	-2	-2	2	4	6	-2	·	-6	-6	·	-2	2	4	4	2	-2	·	6	-2
07	·	·	·	·	·	·	·	·	-2	·	2	-6	-2	·	-2	4	6	-4	2	2	-6	-4	2	4	-2	-2	2	·	-2	-2	-6	·
08	·	·	·	·	·	·	·	·	4	2	-2	·	6	6	-6	2	·	-2	2	4	-2	2	4	-2	-2	·	·	-6	2	4	2	-2
09	·	·	·	·	·	·	·	·	2	·	-2	-2	2	·	2	-4	2	4	-2	-2	-2	4	6	-4	-6	2	-2	·	-6	-6	-2	·
0A	·	·	·	·	·	·	·	·	-2	-2	·	-2	-4	-6	·	2	-6	-2	4	2	·	2	2	-2	-4	2	6	-2	·	-2	4	-6
0C	·	·	·	·	·	·	·	·	-2	-4	-2	2	-6	4	-6	·	-2	·	-2	2	-2	·	2	·	2	6	-6	4	2	-2	-2	-4
0D	·	·	·	·	·	·	·	·	·	2	2	4	2	-2	-2	-6	4	-2	-2	·	2	2	·	6	-6	4	4	2	6	·	-2	-2
0F	·	·	·	·	·	·	·	·	-2	-6	-4	6	·	-2	4	-2	2	2	·	2	-4	-2	2	2	·	-6	-2	-6	4	-2	·	-2
10	·	·	·	·	·	·	·	·	-4	2	6	·	-2	6	2	2	·	-2	-6	-4	-2	2	-4	-2	-2	·	·	-6	2	-4	2	-2
11	·	·	·	·	·	·	·	·	-2	·	2	2	6	·	6	4	-2	-4	2	2	2	-4	2	4	-2	6	-6	·	-2	-2	2	·
12	·	·	·	·	·	·	·	·	2	-2	-4	-6	·	2	4	2	-2	6	·	-2	-4	2	-2	6	·	6	2	-2	4	2	·	2
14	·	·	·	·	·	·	·	·	2	4	2	-2	-2	-4	-2	·	2	·	2	-2	2	·	6	·	6	2	-2	-4	6	-6	2	4
15	·	·	·	·	·	·	·	·	·	2	2	-4	2	-2	-2	-6	-4	-2	-2	·	-6	2	·	6	2	-4	-4	2	-2	·	6	-2
17	·	·	·	·	·	·	·	·	2	2	·	2	-4	-2	·	6	6	2	4	-2	·	6	-2	2	-4	-2	-6	2	·	2	4	-2
19	·	·	·	·	·	·	·	·	2	2	·	2	4	-2	·	6	-2	2	-4	6	·	6	-2	2	4	-2	2	2	·	-6	-4	-2
1A	·	·	·	·	·	·	·	·	-2	-4	-2	-6	2	4	2	·	6	·	-2	2	6	·	2	·	2	-2	2	4	2	-2	6	-4
1B	·	·	·	·	·	·	·	·	-4	-6	-2	·	6	-2	-6	2	·	-2	2	-4	-2	2	-4	-2	-2	·	·	2	2	-4	2	6
1C	·	·	·	·	·	·	·	·	-6	-2	4	2	·	2	-4	2	-2	6	·	-2	4	2	6	6	·	-2	2	-2	-4	2	·	2
1E	·	·	·	·	·	·	·	·	·	2	2	-4	2	-2	-2	2	-4	6	-2	·	2	-6	·	-2	-6	-4	-4	2	6	·	-2	-2
1F	·	·	·	·	·	·	·	·	-6	·	6	-2	2	·	2	-4	2	4	6	6	-2	4	-2	-4	2	2	-2	·	2	2	-2	·

In the same way, the next tables represent the difference distribution tables DT_f of f and $\mathrm{DT}_{\rho'}$ of ρ' and the $\mathrm{DT}_{\tau'_u}$ of the τ'_u.. As explained in Example 5.12, that the rows and columns of DT_f does not follow the natural order in $\mathbb{F}_2^6$.

ρ'

	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	.	2	2	2	2	.	.
2	.	.	.	.	2	2	2	2
3	.	.	2	2	.	.	2	2
4	.	2	2	.	2	.	.	2
5	.	2	.	2	.	2	.	2
6	.	2	2	.	.	2	2	.
7	.	2	.	2	2	.	2	.

τ'_{00}

	0	1	2	3
0	4	.	.	.
1	.	4	.	.
2	.	.	.	4
3	.	.	4	.

τ'_{01}

	0	1	2	3
0	4	.	.	.
1	.	.	.	4
2	.	.	4	.
3	.	4	.	.

τ'_{02}

	0	1	2	3
0	4	.	.	.
1	.	.	.	4
2	.	4	.	.
3	.	.	4	.

τ'_{03}

	0	1	2	3
0	4	.	.	.
1	.	.	.	4
2	.	.	4	.
3	.	4	.	.

τ'_{08}

	0	1	2	3
0	4	.	.	.
1	.	4	.	.
2	.	.	4	.
3	.	.	.	4

τ'_{09}

	0	1	2	3
0	4	.	.	.
1	.	.	4	.
2	.	4	.	.
3	.	.	.	4

τ'_{0A}

	0	1	2	3
0	4	.	.	.
1	.	.	4	.
2	.	.	.	4
3	.	4	.	.

τ'_{0B}

	0	1	2	3
0	4	.	.	.
1	.	4	.	.
2	.	.	.	4
3	.	.	4	.

		[00]				[01]				[02]				[03]				[08]				[09]				[0A]				[0B]			
		00	07	1A	1D	01	06	1B	1C	02	05	18	1F	03	04	19	1E	08	0F	12	15	09	0E	13	14	0A	0D	10	17	0B	0C	11	16
[00]	00	32	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
	07	·	12	8	12	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
	1A	·	8	12	12	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
	1D	·	12	12	8	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
[01]	01	·	·	·	·	·	·	·	·	·	4	4	·	4	·	·	4	2	2	2	2	·	4	4	·	·	·	·	·	·	·	·	·
	06	·	·	·	·	·	·	·	·	4	·	·	4	·	4	4	·	2	2	2	2	·	4	4	·	·	·	·	·	·	·	·	·
	1B	·	·	·	·	·	·	·	·	4	·	·	4	4	·	·	4	2	2	2	2	4	·	·	4	·	·	·	·	·	·	·	·
	1C	·	·	·	·	·	·	·	·	·	4	4	·	·	4	4	·	2	2	2	2	4	·	·	4	·	·	·	·	·	·	·	·
[02]	02	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	·	4	·	4	·	·	·	8
	05	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	4	·	4	·	8	·	·	·
	18	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	4	·	4	·	·	8	·	·
	1F	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	·	4	·	4	·	·	8	·
[03]	03	·	·	·	·	·	·	·	·	·	4	4	·	2	2	2	2	·	·	·	·	·	·	·	·	·	·	4	4	·	4	·	4
	04	·	·	·	·	·	·	·	·	·	4	4	·	2	2	2	2	·	·	·	·	·	·	·	·	·	·	4	4	·	4	·	4
	19	·	·	·	·	·	·	·	·	4	·	·	4	2	2	2	2	·	·	·	·	·	·	·	·	4	4	·	·	4	·	4	·
	1E	·	·	·	·	·	·	·	·	4	·	·	4	2	2	2	2	·	·	·	·	·	·	·	·	4	4	·	·	4	·	4	·
[08]	08	·	·	·	·	2	2	2	2	2	2	2	2	·	·	·	·	2	2	2	2	·	·	·	·	·	·	·	·	4	4	·	·
	0F	·	·	·	·	2	2	2	2	2	2	2	2	·	·	·	·	2	2	2	2	·	·	·	·	·	·	·	·	4	4	·	·
	12	·	·	·	·	2	2	2	2	2	2	2	2	·	·	·	·	2	2	2	2	·	·	·	·	·	·	·	·	·	·	4	4
	15	·	·	·	·	2	2	2	2	2	2	2	2	·	·	·	·	2	2	2	2	·	·	·	·	·	·	·	·	·	·	4	4
[09]	09	·	·	·	·	·	·	4	4	·	·	·	·	4	·	4	·	·	·	·	·	2	2	2	2	·	·	·	·	·	4	·	4
	0E	·	·	·	·	4	4	·	·	·	·	·	·	·	4	·	4	·	·	·	·	2	2	2	2	·	·	·	·	4	·	4	·
	13	·	·	·	·	4	4	·	·	·	·	·	·	4	·	4	·	·	·	·	·	2	2	2	2	·	·	·	·	4	·	4	·
	14	·	·	·	·	·	·	4	4	·	·	·	·	·	4	·	4	·	·	·	·	2	2	2	2	·	·	·	·	·	4	·	4
[0A]	0A	·	·	·	·	2	2	2	2	·	4	4	·	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	·	·	·	·
	0D	·	·	·	·	2	2	2	2	4	·	·	4	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	·	·	·	·
	10	·	·	·	·	2	2	2	2	·	4	4	·	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	·	·	·	·
	17	·	·	·	·	2	2	2	2	4	·	·	4	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	·	·	·	·
[0B]	0B	·	·	·	·	·	·	8	·	·	·	·	·	·	·	4	4	·	4	·	4	·	·	·	·	4	4	·	·	·	·	·	·
	0C	·	·	·	·	·	·	·	8	·	·	·	·	4	4	·	·	4	·	4	·	·	·	·	·	·	·	4	4	·	·	·	·
	11	·	·	·	·	·	8	·	·	·	·	·	·	·	·	4	4	·	4	·	4	·	·	·	·	·	·	4	4	·	·	·	·
	16	·	·	·	·	8	·	·	·	·	·	·	·	4	4	·	·	4	·	4	·	·	·	·	·	4	4	·	·	·	·	·	·

F Primitives of the Toy Trapdoor Cipher of Section 6

The permutation S of $\mathbb{F}_2^6$ is given by the following table.

S	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.A	.B	.C	.D	.E	.F
0.	38	21	24	3C	25	20	2C	28	0E	0C	11	12	3F	0C	0F	3B
1.	3E	16	1A	34	10	23	37	02	2A	35	0A	2E	2F	3A	27	18
2.	31	33	03	3C	30	05	2C	1E	1B	29	17	08	0B	09	04	07
3.	32	06	13	1C	2B	39	1F	36	00	15	22	1C	19	01	14	26

For instance, $S(25) = 05$. The permutation S' of $\mathbb{F}_2^6$ is then defined in a similar way.

S'	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.A	.B	.C	.D	.E	.F
0.	38	21	24	3C	25	20	2C	28	0E	0C	11	12	3F	0C	1C	3B
1.	3E	16	1A	34	10	23	37	02	2A	35	0A	2E	2F	3A	27	18
2.	31	33	03	3C	30	05	2C	1E	1B	29	17	08	0B	09	04	07
3.	32	06	15	13	2B	39	1F	36	00	0F	22	1C	19	01	14	26

Observe that $S(x) \neq S'(x)$ if x lies in $\{0E, 32, 33, 39\}$ and that $S(x) = S'(x)$ for any other element x of $\mathbb{F}_2^6$.

The diffusion layer π is an isomorphism of $(\mathbb{F}_2^6)^4$. Because of the linearity of this map, π is define only a a basis of $(\mathbb{F}_2^6)^4$. The following table gives the images under π of the elements of the standard basis of $(\mathbb{F}_2^6)^4$.

x	$\mapsto$	$\pi(x)$	x	$\mapsto$	$\pi(x)$
(00, 00, 00, 01)	$\mapsto$	(3B, 3D, 30, 26)	(00, 01, 00, 00)	$\mapsto$	(08, 33, 18, 2D)
(00, 00, 00, 02)	$\mapsto$	(2E, 05, 16, 01)	(00, 02, 00, 00)	$\mapsto$	(39, 14, 1F, 2F)
(00, 00, 00, 04)	$\mapsto$	(19, 11, 3D, 3C)	(00, 04, 00, 00)	$\mapsto$	(0F, 02, 2E, 19)
(00, 00, 00, 08)	$\mapsto$	(01, 01, 38, 04)	(00, 08, 00, 00)	$\mapsto$	(20, 04, 0D, 03)
(00, 00, 00, 10)	$\mapsto$	(05, 0F, 02, 2A)	(00, 10, 00, 00)	$\mapsto$	(2D, 28, 03, 1F)
(00, 00, 00, 20)	$\mapsto$	(31, 1C, 12, 0A)	(00, 20, 00, 00)	$\mapsto$	(23, 34, 06, 16)
(00, 00, 01, 00)	$\mapsto$	(2D, 04, 0E, 1A)	(01, 00, 00, 00)	$\mapsto$	(0A, 10, 24, 09)
(00, 00, 02, 00)	$\mapsto$	(09, 1D, 16, 12)	(02, 00, 00, 00)	$\mapsto$	(0B, 1D, 19, 04)
(00, 00, 04, 00)	$\mapsto$	(1A, 30, 3D, 04)	(04, 00, 00, 00)	$\mapsto$	(28, 16, 2A, 16)
(00, 00, 08, 00)	$\mapsto$	(3D, 14, 21, 26)	(08, 00, 00, 00)	$\mapsto$	(05, 3A, 04, 15)
(00, 00, 10, 00)	$\mapsto$	(04, 1F, 15, 0D)	(10, 00, 00, 00)	$\mapsto$	(1D, 39, 16, 3B)
(00, 00, 20, 00)	$\mapsto$	(3C, 01, 0B, 10)	(20, 00, 00, 00)	$\mapsto$	(21, 09, 10, 14)

For example,

$$\begin{aligned}\pi(00, 00, 00, 03) &= \pi(00, 00, 00, 01) + \pi(00, 00, 00, 02) \\ &= (3B, 3D, 30, 26) + (2E, 05, 16, 01) = (15, 38, 26, 27)\ .\end{aligned}$$

In the same way, we define the isomorphism L of $(\mathbb{F}_2^6)^2$.

x	$\mapsto$	$L(x)$	x	$\mapsto$	$L(x)$	x	$\mapsto$	$L(x)$	x	$\mapsto$	$L(x)$
(00, 01)	$\mapsto$	(15, 08)	(00, 08)	$\mapsto$	(0B, 26)	(01, 00)	$\mapsto$	(19, 2B)	(08, 00)	$\mapsto$	(07, 08)
(00, 02)	$\mapsto$	(0A, 09)	(00, 10)	$\mapsto$	(31, 15)	(02, 00)	$\mapsto$	(13, 31)	(10, 00)	$\mapsto$	(1A, 2C)
(00, 04)	$\mapsto$	(1C, 31)	(00, 20)	$\mapsto$	(12, 07)	(04, 00)	$\mapsto$	(0B, 13)	(20, 00)	$\mapsto$	(20, 11)