ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

A generalization of Linear Cryptanalysis

Diploma Thesis

Thomas Baignères

2003

Diploma Professor: Prof. Serge Vaudenay EPF Lausanne

LASEC

To Valérie

Contents

Introduction

Acknowledgments

I would like to seize the opportunity to thank Professor Serge Vaudenay, not only for giving me the opportunity to carry on my Diploma Thesis on such an exciting subject, but also for all the projects I had the opportunity to realize in his laboratory and for its course on Cryptography. These are the reasons why I want to dedicate my studies to this area of science.

I also would like to thank Prof. Willi Meier for his acceptance to attend my presentation.

Thank you to Gildas Avoine and to Jean Monnerat for very interesting talks and for all your help.

I can't think of any occasion when Pascal Junod didn't find any time to help me during my work in the laboratory. For this, I want to express my gratitude to him.

A special thank you goes to Mathias for helping me to always keep faith in my work. This is the reason of many of my successes and I owe it to him.

I want to thank my parents for their unconditional support during all those (long) years of study and for giving me the chance to have the life anyone could dream of.

Last but not least, I would like to thank Valérie. You gave a new meaning to my life.

Introduction

1 First glance at linear cryptanalysis

> *Cryptanalysis* is the study of mathematical techniques for attempting to defeat cryptographic techniques, and, more generally, information security services.[1]

This diploma work will consider a specific type of cryptanalysis, called *linear cryptanalysis*. Nowadays, the techniques provided by this theory are systematically taken into consideration when designing specific types of ciphers, called block cipher.

> A *block cipher* is an encryption scheme which breaks up the plaintext messages to be transmitted into strings (called *blocks*) of a fixed length t over an alphabet $\mathcal{A}$, and encrypts one block at a time.[1]

Block ciphers are part of a bigger family of encryption scheme, known as symmetric-key encryption schemes, which use the exact same key to encrypt and to decrypt blocks of text input. The most important block cipher of the last century is with no doubt the Data Encryption Standard (DES), which was defined in the mid 1970s, with the scope to become the US standard. After the National Security Agency (NSA) confirmed its ability to protect non-classified information, DES was published as a Federal Standard by the National Institute of Standards and Technology (NIST) [Nat77]. Since then, this cipher has been a base for the study of block ciphers security.

1.1 The basic attack

Linear cryptanalysis and Differential cryptanalysis are known to be the two major attacks against block ciphers. Every single modern block cipher design takes the results of these two theories into account. Linear cryptanalysis is an original idea proposed by Mitsuru Matsui, based on previous work [TCG91, GC90, MY92] made against another block cipher called FEAL [SM87, Miy89, Miy90]. It was first presented in 1993 at Eurocrypt. Its paper, called *Linear cryptanalysis method for DES Cipher* ([Mat93]) proposes a new type of statistical attack. One of the main progress

[1] As defined in the *Handbook of Applied Cryptography* [MVV97]

compared to the differential cryptanalysis of Biham and Shamir ([BS90]) is to be a known-plaintext attack[1], whether differential cryptanalysis is a chosen-plaintext attack[2]. In its paper, Matsui carries out a first attack against DES, which we describe briefly here, using notations of Figure 1.

- Considering a n rounds DES, the idea is to find a linear expression approximating the behavior of $n-1$ rounds, depending on plaintext, ciphertext and key bits. Using Matsui's convention, we consider that $\mathsf{A}[i]$ represents the i-th bit of a bloc A, and that $\mathsf{A}[i,j,\ldots,k] = \mathsf{A}[i] \oplus \mathsf{A}[j] \oplus \ldots \oplus \mathsf{A}[k]$. We are thus looking for equation of the type:

  $$\mathsf{P}[i_1, i_2, \ldots, i_a] \oplus \mathsf{C}[j_1, j_2, \ldots, j_b] = \mathsf{K}[k_1, k_2, \ldots, k_c] \ ,$$

  where $i_1, i_2, \ldots, i_a$, $j_1, j_2, \ldots, j_b$ and $k_1, k_2, \ldots, k_c$ denote plaintext bits, ciphertext bits and key bits respectively. In the best case (from the point of view of the cryptanalysis), this equation will hold (or at the contrary will be false) with a probability p far from $\frac{1}{2}$. One can measure the effectiveness of such an approximation using the magnitude of $\left|p - \frac{1}{2}\right|$. In order to obtain such an expression on $n-1$ rounds, the cryptanalyst first searches for a linear approximation of substitution boxes, the only non-linear components of DES, and then computes an approximation of one round of the cipher. Next, while using the *piling-up lemma*, it is possible to build an expression approximating $n-1$ rounds of a cipher given the approximations of every single round.

  Lemma 1. ***Piling-up lemma***[3] *Let X_i $(1 \le i \le n)$ be independent random variables whose values are 0 with probability p_i or 1 with probability $1 - p_i$. Then the probability that $X_1 \oplus X_2 \oplus \ldots \oplus X_n = 0$ is*

  $$\frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \left(p_i - \frac{1}{2}\right) \ .$$

- Once such an expression is computed, the missing round is added in order to obtain an expression like the following one:

  $$\mathcal{L} : \mathsf{P}[i_1, i_2, \ldots, i_a] \oplus \mathsf{C}[j_1, j_2, \ldots, j_b] \oplus F_8(\mathsf{C}, \mathsf{K}^{(8)})[l_1, l_2, \ldots, l_d] = \mathsf{K}[k_1, k_2, \ldots, k_c] \ .$$

  In this case, Matsui proceeds to an attack on a 8 rounds DES. He thus finds an approximation on the first 7 rounds and finally adds the last one. It is clear that the approximation will involve only a limited number of bits of the last round key $\mathsf{K}^{(8)}$. These bits (plus the parity bit) are those that linear cryptanalysis will try to recover.

[1] In a known-plaintext attack, the cryptanalyst has access to the ciphertext of several messages, and to the plaintext of those messages.

[2] In a chosen-plaintext attack, the cryptanalyst not only has access to the ciphertext and associated plaintext for several messages, but he also chooses the plaintext that gets encrypted

[3] As in [Mat93]

- In order to carry out the attack, the cryptanalyst guesses the value of the bits of $\mathsf{K}^{(8)}$ involved in the approximation, denoted $k^{(8)}$, and use this value to check if the linear approximation holds or not. For every possible $k^{(8)}$, a counter evaluates the number of times the expression holds, using every plaintext/ciphertext pairs at disposal. To conclude the attack, the cryptanalyst supposes that the counter that displays the largest (or the smallest) value corresponds to the right round key bits. This supposition, called *Wrong-key randomization hypothesis*, says that when the guessed value $k^{(8)}$ is wrong, the linear expression has no more particular reason to hold with a probability $p \neq \frac{1}{2}$.

  Assumption 1. ***Wrong-key randomization hypothesis***[4] *For any linear expression $\mathcal{L}$ operating on n rounds for which*

  $$\left|\mathbf{Pr}\left[\mathcal{L} = 0 \mid \mathsf{K}^{(1)} = k^{(1)}, \ldots, \mathsf{K}^{(n)} = k^{(n)}\right] - \frac{1}{2}\right|$$

  is large for virtually all values $k^{(1)}, \ldots, k^{(n)}$ of the round keys, the following is true: for virtually all possible full keys $(k^{(1)}, \ldots, k^{(n)})$ and for all estimates $\hat{k}$ of the last round key,

  $$\frac{\left|\mathbf{Pr}\left[\mathcal{L} = 0 \mid \mathsf{K} = k_r\right] - \frac{1}{2}\right|}{\left|\mathbf{Pr}\left[\mathcal{L} = 0 \mid \mathsf{K} = \hat{k}\right] - \frac{1}{2}\right|} \gg 1 \quad \forall \hat{k} \neq k_r$$

  where k_r is the right key.

1.2 Improvements

In a second paper [Mat94a] published at Crypto '94, Matsui proposes some improvements to linear cryptanalysis. He introduces a new linear expression on the central $n - 2$ rounds of DES and proposes a way to classify round keys candidates during the attack. He manages to recover 26 round key bits, using 2^{43} plaintext/ciphertext couples, with a probability of success of 85%. The remaining 30 bits are recovered with an exhaustive search. The attack improvement is due to the final ranking of the round key candidates. However, Matsui proposes no proof on the optimality of its method. In a paper [JV03] published at FSE '03, Pascal Junod and Serge Vaudenay propose an optimal way to classify the round key candidates. The use of *Hypothesis tests* and of the Neyman-Pearson lemma allow them to build an optimal distinguisher, which is a solution to the problem of candidates classification. They manage to achieve a rate of success of 85% when approximatively $2^{42.5}$ plaintext/ciphertext couples are at disposal.

[4] As it appears in [Jun01], first appeared in [HKM95]

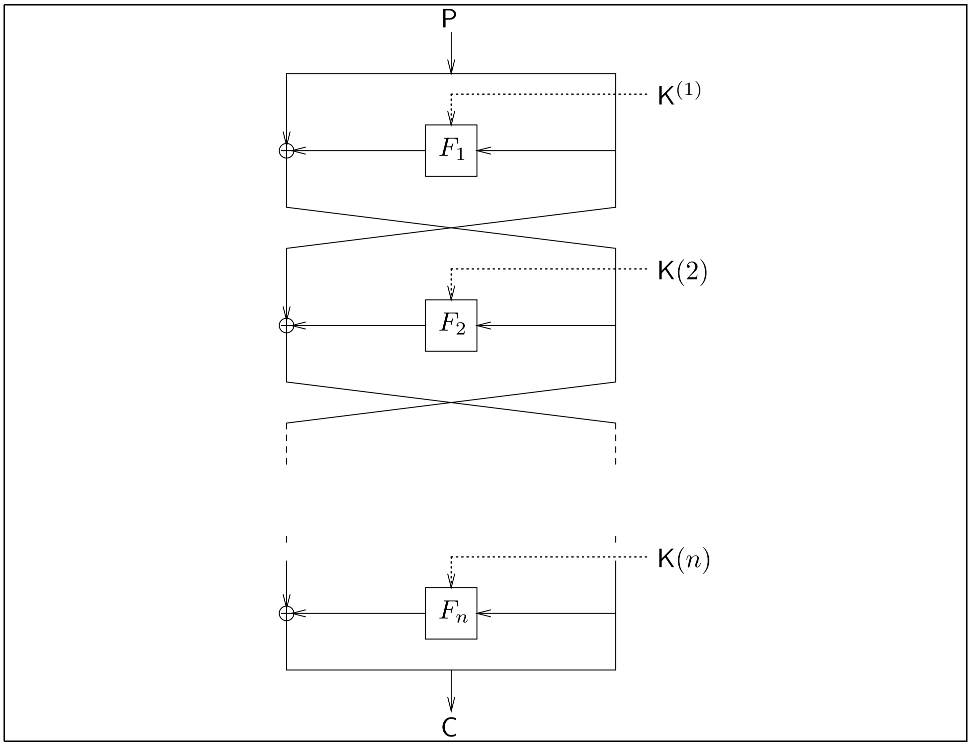


Figure 1: Notations on a n rounds Feistel scheme

2 Generalizing linear cryptanalysis

2.1 Previous work

Since the introduction of linear cryptanalysis by Matsui, some generalizations have been proposed. Carlos Harpes, Gerhard G. Kramer and James L. Massey, in a paper [HKM95] published at Eurocrypt '95, propose for example to generalize Matsui's linear expression with threefold sums. A threefold sum on one round of a cipher is the sum of three terms: a binary function of the round input, a binary function of the round output and a binary function of the round key. These functions are not necessarily simple bits xor anymore. One of the main problems solved in this paper concern the generalization of the piling-up lemma to their theory. Despite the fact that binary function allow more control over the computation of the correlation of plaintext bits, ciphertext bits and key bits, threefold sums still compare one bit of text to one bit of key.

Another work by Matthew G. Parker [Par03] considers linear approximations over spaces of dimension four instead of two. Although no method to obtain linear approximations on several rounds of the cipher given linear expressions on the individual rounds is given (which would be a generalization of the piling-up lemma), significantly higher biases on several S-boxes are found.

Carlo Harpes also proposed some significant modifications on linear cryptanalysis [HM97]. The basic idea is to use *partition-pair*, i.e. a partition of the set of inputs of the first round of the cipher (the input partition), and a partition the set of inputs of the last round of the cipher (the output partition). More precisely, Harpes defines a partition $\mathcal{A}$ of a input (or output) set $\mathcal{X}$ to be a set of non-empty blocks $A_0, \ldots, A_{a-1}$ such that $\mathcal{A} = \{A_0, \ldots, A_{a-1}\}$. The basic attack is based on the property that, taking plaintexts in a fixed block of the input partition, the random variable representing the input of the last round is not uniformly distributed over all possible output blocks and this, for almost all keys.

2.2 Our proposition

We will thus try to generalize linear cryptanalysis by generalizing linear expression used to approximate some rounds of the cipher during the attack. Linear expressions will be replaced by transition matrices[5]. We describe here the content of each chapter of this work:

- In chapter I we realize a study on distinguishers, useful for the final classification of round key candidates. We study two types of distinguishers. The first should be able to make the distinction between two probability distributions of a single random variable. The second one makes the distinction between two distributions of a couple of random variables, defined by a transition matrix. In both cases we will recall some previous results (description of the distinguisher, Neyman-Pearson lemma, computation of the best advantage) before we introduce some new results (given a certain error probability, we provide an estimate of the necessary number of questions of the distinguisher to a generator implementing one of the two distributions before it can take a decision). In the second case, the obtained results will allow us to generalize the measure $\left|p - \frac{1}{2}\right|$ of a linear expression expression efficiency, in order to compute the effectiveness of a transition matrix.

- In chapter II, we provide a toolbox gathering all necessary tools for generalized linear cryptanalysis. We introduce a linear function on finite fields, called the trace, which will allow us to define a certain type of transition matrices (and of bias matrices). Some properties of these matrices are introduced. This chapter also introduces a generalization of the piling-up lemma which should be applicable to our theory. It will allow to find a good approximation (i.e. a good transition matrix) on several rounds of a cipher, given the approximations of each single round (i.e. the transition matrices of each single round).

- In chapter III, we apply the theory to a simple cipher. Two cases are considered, whether to transition matrices used are 2×2 (we will see that this is

[5] This terminology seems to appear in [MG00] for the first time in the world of cryptography.

equivalent to linear cryptanalysis) or 4×4.

- In the last chapter, we summarize some of the main results obtained during this work, give starting points for further researches and conclude.

Chapter I

A study on distinguishers

1 Notation and convention

Random variables $X, Y, \ldots$ are denoted by capital letters, while realizations $x \in \mathcal{X}, y \in \mathcal{Y}, \ldots$ of random variables are denoted by small letters. The fact for a random variable X to follow a distribution D is denoted $X \leftarrow \mathsf{D}$, whilst its probability function is denoted by $\mathbf{Pr}_{X \leftarrow \mathsf{D}}[X = x]$ or $\mathbf{Pr}_{\mathsf{D}}[x]$. The fact that a sequence of iid random variables $X_1, \ldots, X_n$ is such that every random variable X_i of that sequence follows a distribution D will be denoted $\mathbf{X}^n \leftarrow \mathsf{D}^n$. Similarly, a sequence of realizations $x_1, x_2, \ldots, x_n$ will be denoted $\mathbf{x}^n$.

We call support of a distribution D the set $\mathsf{Supp}_{\mathsf{D}}$ of all $x \in \mathcal{X}$ s.t. $\mathbf{Pr}_{\mathsf{D}}[x] \neq 0$.

2 Distinguishability of two distributions of probabilities

2.1 The Problem

We consider a sequence of n iid random variables $X_1, X_2, \ldots, X_n$ following a distribution $\hat{\mathsf{D}}$, taking values in a set $\mathcal{Z}$. We wonder whether $\hat{\mathsf{D}} = \mathsf{D}_0$ or $\hat{\mathsf{D}} = \mathsf{D}_1$ (where D_1 is referred to an "ideal distribution").

2.2 Recall on distinguishers

A distinguisher is an algorithm which gets a realization of the sequence from a Source and which ultimately outputs 0 or 1. In our case, we can query the Source and receive a realization of the random variable X in return. This variable follows either the distribution D_0 or D_1 (see Figure I.1).
A distinguisher is usually limited to n queries to the Oracle. Its capacity to distinguish a distribution from another is given by its *Advantage*, which is a distance between the probabilities that the distinguisher outputs 0 given $\hat{\mathsf{D}} = \mathsf{D}_0$ or $\hat{\mathsf{D}} = \mathsf{D}_1$.

Parameters: a complexity n, an acceptance region $\mathcal{A}$
Input: a random Source $\mathcal{S}$ which generates realizations of a random variable X following a distribution $\hat{\mathsf{D}}$

```
for $i = 1, \ldots, n$ do
    Receive $x_i \in \mathcal{Z}$ from the Source
end for
if $(x_1, x_2, \ldots, x_n) \in \mathcal{A}$
    Output 0
else
    Output 1
end if
```

Algorithm 1: Modeling of a distinguisher limited to n questions

We consider the distinguisher described by Algorithm 1. We see that this distinguisher depends on a certain set $\mathcal{A} \in \mathcal{Z}^n$.
By choosing this set judiciously, we can maximize the advantage defined by

$$\mathrm{Adv}^n_{\mathcal{A}} = \left| \mathbf{Pr}_{\mathsf{D}_0^n}\left[\mathcal{A}\right] - \mathbf{Pr}_{\mathsf{D}_1^n}\left[\mathcal{A}\right] \right| \ . \tag{I.1}$$

Such a distinguisher can make two different types of mistakes. It can either output 1 when $\hat{\mathsf{D}} = \mathsf{D}_0$ or output 0 when $\hat{\mathsf{D}} = \mathsf{D}_1$. We denote the probability of these two events by

$$\alpha = \mathbf{Pr}_{\mathsf{D}_0^n}\left[\overline{\mathcal{A}}\right] \tag{I.2}$$

and

$$\beta = \mathbf{Pr}_{\mathsf{D}_1^n}\left[\mathcal{A}\right] \ . \tag{I.3}$$

With these notations, the advantage is such that:

$$\mathrm{Adv}^n_{\mathcal{A}} = \left|1 - 2P_e\right| \ , \tag{I.4}$$

where $P_e = \frac{1}{2}(\alpha + \beta)$ is overall probability of error. This can be seen as Bayesian approach, where one assigns prior probabilities to two hypothesis (see [Jun03a]). As

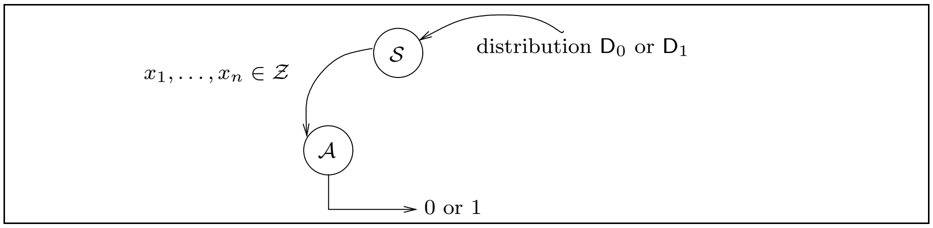

$\mathcal{S}$
distribution D_0 or D_1
$x_1, \ldots, x_n \in \mathcal{Z}$
$\mathcal{A}$
0 or 1

Figure I.1: A distinguisher between two distributions

for now we can consider that $P_e \leq \frac{1}{2}$, otherwise we would turn $\mathcal{A}$ in $\overline{\mathcal{A}}$ to get an overall probability of error less than $\frac{1}{2}$. Thus

$$\mathrm{Adv}_{\mathcal{A}}^{n} = 1 - 2P_e \ . \tag{I.5}$$

Thus maximizing $\mathrm{Adv}_{\mathcal{A}}^{n}$ is equivalent to minimizing the overall probability of error P_e.

2.3 Maximizing the advantage of the distinguisher

We are going to derive the set $\mathcal{A}$ that minimizes the overall probability of error (i.e. maximize the advantage of the distinguisher). The construction we make can also be considered like a proof of the Neyman-Pearson lemma (see [Jun03a] for more details). We have:

$$\begin{aligned} P_e &= \frac{1}{2}\left(\sum_{\mathbf{x}^n \in \overline{\mathcal{A}}} \mathbf{Pr}_{\mathsf{D}_0^n}[\mathbf{x}^n] + \sum_{\mathbf{x}^n \in \mathcal{A}} \mathbf{Pr}_{\mathsf{D}_1^n}[\mathbf{x}^n]\right) \\ &= \frac{1}{2}\left(1 - \sum_{\mathbf{x}^n \in \mathcal{A}} \mathbf{Pr}_{\mathsf{D}_0^n}[\mathbf{x}^n] + \sum_{\mathbf{x}^n \in \mathcal{A}} \mathbf{Pr}_{\mathsf{D}_1^n}[\mathbf{x}^n]\right) \\ &= \frac{1}{2} + \frac{1}{2}\sum_{\mathbf{x}^n \in \mathcal{A}} \left(\mathbf{Pr}_{\mathsf{D}_1^n}[\mathbf{x}^n] - \mathbf{Pr}_{\mathsf{D}_0^n}[\mathbf{x}^n]\right) \ . \end{aligned}$$

Thus minimizing P_e is equivalent to minimizing the sum of the last equation. It is minimal when $\mathcal{A}$ consists of all $\mathbf{x}^n$ such that the difference in the parenthesis is negative (see [Vau03]). The set that minimizes the overall probability of error is thus:

$$\mathcal{A} = \left\{\mathbf{x}^n \in \mathcal{Z}^n \ : \ \frac{\mathbf{Pr}_{\mathsf{D}_0^n}[\mathbf{x}^n]}{\mathbf{Pr}_{\mathsf{D}_1^n}[\mathbf{x}^n]} \geq 1\right\} \ , \tag{I.6}$$

with the convention that $\frac{p}{0} = +\infty$ for $p > 0$. Note that this set is well defined, as the $\frac{0}{0}$ case can be ignored.

This set defines a so called *decision function* $\delta : \mathcal{Z}^n \to \{0, 1\}$ such that

$$\forall \mathbf{x}^n \in \mathcal{Z}^n \quad \delta(\mathbf{x}^n) = 0 \Leftrightarrow \mathbf{x}^n \in \mathcal{A} \ .$$

The set $\mathcal{A}$ is called the *region of acceptance* of δ.

We summarize these results in the following definition.

Definition 1. ***(Optimal Binary Hypothesis Test).*** *The optimal decision rule to test $\hat{\mathsf{D}} = \mathsf{D}_0$ against $\hat{\mathsf{D}} = \mathsf{D}_1$ that minimizes the overall probability of error (i.e. maximizes the advantage of the distinguisher of Algorithm 1) is the following:*

$$\delta_{\text{opt}} = \begin{cases} 0 \text{ (i.e. accept } \hat{\mathsf{D}} = \mathsf{D}_0\text{) if } \mathrm{LR}(\mathbf{x}^n) \geq 1 \\ 1 \text{ (i.e. accept } \hat{\mathsf{D}} = \mathsf{D}_1\text{) if } \mathrm{LR}(\mathbf{x}^n) < 1 \end{cases} \tag{I.7}$$

where LR *is the likelihood ratio,*

$$\mathrm{LR}(\mathbf{x}^n) = \frac{\mathbf{Pr}_{\mathsf{D}_0^n}[\mathbf{x^n}]}{\mathbf{Pr}_{\mathsf{D}_1^n}[\mathbf{x^n}]}\ , \tag{I.8}$$

with the convention that $\frac{p}{0} = +\infty$ *for* $p > 0$ *(the* $\frac{0}{0}$ *case can be ignored).*

Intuitively, if we suppose that for some query we receive a value x that could not be generated by distribution D_0 (i.e. $\mathbf{Pr}_{\mathsf{D}_0}[x] = 0$) our distinguisher should choose at the end $\hat{\mathsf{D}} = \mathsf{D}_1$. We see that in such a situation, $\mathrm{LR}(\mathbf{x}^n) = 0$ and thus our distinguisher will make the right choice. Note that this result corresponds to the Neyman-Pearson lemma (see [JV03]).

2.4 On the optimality of the distinguisher

The best advantage of the distinguisher described in Algorithm 1 is reached when $\mathcal{A}$ is defined by equation (I.6). Unfortunately such a distinguisher can hardly be implemented as n grows. In order to take a decision it must keep in memory all the results of the n queries. We are going to optimize (in the sense of decreasing the needed memory, while keeping the same advantage) the distinguisher by using the fact that $X_1, \ldots, X_n$ are i.i.d. and by the use of $|\mathcal{Z}|$ counters, each one counting the number of occurrences of a certain symbol of $\mathcal{Z}$ in the sequence $\mathbf{x}^n$. Moreover, we will show that the best advantage of such a distinguisher is the same as the one described in Algorithm 1.

If we go back the definition of the *likelihood ratio*, we have:

$$\begin{aligned} \mathrm{LR}(\mathbf{x}^n) &= \frac{\mathbf{Pr}_{\mathsf{D}_0^n}[\mathbf{x}^n]}{\mathbf{Pr}_{\mathsf{D}_1^n}[\mathbf{x}^n]} \\ &= \prod_{i=1}^{n} \frac{\mathbf{Pr}_{\mathsf{D}_0}[x_i]}{\mathbf{Pr}_{\mathsf{D}_1}[x_i]} \\ &= \prod_{\substack{a \in \mathcal{Z} \\ \text{s.t. } N(a|\mathbf{x}^n) > 0}} \left(\frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]} \right)^{N(a|\mathbf{x}^n)} \end{aligned}$$

where $N(a|\mathbf{x}^n)$ is the number of times the symbol $a \in \mathcal{Z}$ occurs in the sequence $\mathbf{x}^n \in \mathcal{Z}^n$.

We thus see that the optimal decision rule is perfectly defined by $|\mathcal{Z}|$ counters, each one counting the number of occurrences of a particular symbol of $\mathcal{Z}$ in the sequence $x_1, x_2, \ldots, x_n$. Taking the logarithm of the *likelihood ratio*, we can define a new decision rule $\widetilde{\delta}$ (i.e. a new region of acceptance $\widetilde{\mathcal{A}}$) based on these counters:

```
Parameters: a complexity $n$, an acceptance region $\widetilde{\mathcal{A}}$
Input: a random Source $\mathcal{S}$ which generates realizations of a random variable $X$ following a distribution $\hat{\mathsf{D}}$
Initialize $|\mathcal{Z}|$ counters $u_1, u_2, \ldots, u_{|\mathcal{Z}|}$
for $i = 1, \ldots, n$ do
    Receive $x \in \mathcal{Z}$ from the Source
    Increment $u_x$
end for
if $(u_1, u_2, \ldots, u_{|\mathcal{Z}|}) \in \widetilde{\mathcal{A}}$
    Output 0
else
    Output 1
end if
```

Algorithm 2: Modeling of a distinguisher limited to n questions, using counters

Definition 2. ***(Optimal Binary Hypothesis Test Revisited).*** *The optimal decision rule to test $\hat{\mathsf{D}} = \mathsf{D}_0$ against $\hat{\mathsf{D}} = \mathsf{D}_1$ that minimizes the overall probability of error is the following:*

$$\widetilde{\delta}_{\text{opt}} = \begin{cases} 0 \text{ (i.e. accept } \hat{\mathsf{D}} = \mathsf{D}_0\text{) if } \mathrm{LLR}(N(a_1|\mathbf{x}^n), \ldots, N(a_{|\mathcal{Z}|}|\mathbf{x}^n)) \geq 0 \\ 1 \text{ (i.e. accept } \hat{\mathsf{D}} = \mathsf{D}_1\text{) if } \mathrm{LLR}(N(a_1|\mathbf{x}^n), \ldots, N(a_{|\mathcal{Z}|}|\mathbf{x}^n)) < 0 \end{cases} \tag{I.9}$$

where $N(a_i|\mathbf{x}^n)$ is the number of times the symbol a_i occurs in the sequence $\mathbf{x}^n \in \mathcal{Z}^n$ and where LLR *is the logarithmic likelihood ratio,*

$$\mathrm{LLR}(N(a_1|\mathbf{x}^n), \ldots, N(a_{|\mathcal{Z}|}|\mathbf{x}^n)) = \sum_{\substack{a \in \mathcal{Z} \\ \text{s.t. } N(a|\mathbf{x}^n) > 0}} N(a|\mathbf{x}^n) \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]} \,, \tag{I.10}$$

with the convention that $\log \frac{0}{p} = -\infty$ and $\log \frac{p}{0} = +\infty$ for $p > 0$ (Note that the $\log \frac{0}{0}$ case can be ignored).

From this consideration, it is now possible to derive the best distinguisher of two distributions (see Algorithm 2).
As the decision rule used in the new distinguisher is equivalent to the one used in the previous distinguisher, both offer the same advantage. In the next paragraph we will compute its exact value.

2.5 Computation of the Advantage of the Best Distinguisher

Let $\mathcal{M}_n$ and $\mathcal{M}_n^*$ be the vectors defined by

$$[\mathcal{M}_n]_{(x_1,x_2,\ldots,x_n)} = \mathbf{Pr}_{\mathsf{D}_0^n}[x_1, x_2, \ldots, x_n] \quad \text{and} \quad [\mathcal{M}_n^*]_{(x_1,x_2,\ldots,x_n)} = \mathbf{Pr}_{\mathsf{D}_1^n}[x_1, x_2, \ldots, x_n] \,.$$

This corresponds to n-wise distribution matrices in the decorrelation theory (see [Vau03]) in a simplified case as we have no input here, only outputs x_i.

The probability that the distinguisher outputs 0 when X follows distribution D_0 (resp. D_1) is $\sum_{\mathbf{x}^n \in \mathcal{A}} [\mathcal{M}_n]_{\mathbf{x}^n}$ (resp. $\sum_{\mathbf{x}^n \in \mathcal{A}} [\mathcal{M}_n^*]_{\mathbf{x}^n}$). The advantage is thus

$$\sum_{\mathbf{x}^n \in \mathcal{A}} \left([\mathcal{M}_n]_{\mathbf{x}^n} - [\mathcal{M}_n^*]_{\mathbf{x}^n} \right) .$$

We know that the set $\mathcal{A}$ maximizes this sum (as it minimizes its opposite), moreover this sum is null if it is taken over all possible values of $\mathbf{x}^n$. Thus the advantage is

$$\frac{1}{2} \sum_{\mathbf{x}^n \in \mathcal{Z}^n} \left| [\mathcal{M}_n]_{\mathbf{x}^n} - [\mathcal{M}_n^*]_{\mathbf{x}^n} \right| ,$$

which can be written down as

$$\boxed{\mathrm{Adv}^n_{\delta_{\mathrm{opt}}} = \frac{1}{2} \parallel \mathcal{M}_n - \mathcal{M}_n^* \parallel_1} ,$$

where the norm $\parallel \cdot \parallel_1$ of a vector A is defined by $\parallel A \parallel_1 = \sum_i |A_i|$.

2.6 Necessary number of queries for close distributions

In this section we try to anticipate the number of queries that the algorithm we have presented needs in order to distinguish D_0 from D_1, given a certain error probability P_e.

In the first part we will see how the LLR can be approximated by a normal law when $\mathsf{Supp}_{\mathsf{D}_0} = \mathsf{Supp}_{\mathsf{D}_1}$. In the second we compute the approximate number of queries considering that D_1 is the uniform distribution and that both distributions are close to each other.

Approximation of the LLR by a normal law

We start by introducing a definition which will allow to simplify some of the results we are going to obtain.

Definition 3. *The relative entropy or Kullback Leibler distance*[1] *between two distributions* D_0 *and* D_1 *is defined as*

$$D(\mathsf{D}_0 \parallel \mathsf{D}_1) = \sum_{x \in \mathcal{Z}} \mathbf{Pr}_{\mathsf{D}_0}[x] \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[x]}{\mathbf{Pr}_{\mathsf{D}_1}[x]} ,$$

with the convention that $0 \log \frac{0}{p} = 0$ *and* $p \log \frac{p}{0} = +\infty$ *for* $p > 0$.

[1] See [CT91] for more details

The following Theorem provides an important property of the Kullback Leibler distance (see [CT91] for a proof).

Theorem 1. *Considering the two distributions* D_0 *and* D_1 *we have*

$$D(\mathsf{D}_0 \parallel \mathsf{D}_1) \geq 0$$

with equality if and only if $\mathsf{D}_0 = \mathsf{D}_1$.

Still using the conventions proposed in Section 1 and in Definition 3, and considering that $0 \log p = 0$ for $p \geq 0$, we can write the LLR as:

$$\begin{aligned} \mathrm{LLR}(N(a_1|\mathbf{x}^n), \ldots, N(a_{|\mathcal{Z}|}|\mathbf{x}^n)) &= \sum_{a \in \mathcal{Z}} N(a|\mathbf{x}^n) \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]} \\ &= \sum_{a \in \mathcal{Z}} \sum_{i=1}^{n} 1_{x_i = a} \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]} \\ &= \sum_{i=1}^{n} \sum_{a \in \mathcal{Z}} 1_{x_i = a} \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]} . \end{aligned}$$

As the n queries are independent, we can consider the n random variables

$$\sum_{a \in \mathcal{Z}} 1_{x_i = a} \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]} , \ 1 \leq i \leq n$$

to be independent. The Central Limit Theorem then states that the LLR converges towards a normal distribution of mean $\mathbf{E}[\mathrm{LLR}]_j$ and of variance $\mathbf{Var}[\mathrm{LLR}]_j$, where j is equal to 0 (resp. 1) when $\hat{\mathsf{D}} = \mathsf{D}_0$ (resp. $\hat{\mathsf{D}} = \mathsf{D}_1$).

The mean (depending on the distribution) is

$$\begin{aligned} \mathbf{E}[\mathrm{LLR}]_j &= \sum_{i=1}^{n} \sum_{a \in \mathcal{Z}} \mathbf{E}_{1_{x_i = a}}[\log] \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]} \\ &= n \sum_{a \in \mathcal{Z}} \mathbf{Pr}_{\mathsf{D}_j}[a] \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]} . \end{aligned}$$

Using the *relative entropy* we obtain

$$\mathbf{E}[\mathrm{LLR}]_0 = nD(\mathsf{D}_0 \parallel \mathsf{D}_1) \tag{I.11}$$

and

$$\mathbf{E}[\mathrm{LLR}]_1 = -nD(\mathsf{D}_1 \parallel \mathsf{D}_0) . \tag{I.12}$$

Before going further we should note that these results hold because we supposed that $\mathsf{Supp}_{\mathsf{D}_0} = \mathsf{Supp}_{\mathsf{D}_1}$. Suppose now that this is not the case. Some $a \in \mathcal{Z}$ such that $\mathbf{Pr}_{\mathsf{D}_0}[a] = 0$ and $\mathbf{Pr}_{\mathsf{D}_1}[a] \neq 0$ can occur. We then have $D(\mathsf{D}_1 \parallel \mathsf{D}_0) = +\infty$ and thus $\mathbf{E}[\mathrm{LLR}]_1 = -\infty$. In the same situation, the value of $\mathbf{E}[\mathrm{LLR}]_0$ is finite. It is obvious that in such a situation the Central Limit Theorem cannot be used and this is why we have to suppose that $\mathsf{Supp}_{\mathsf{D}_0} = \mathsf{Supp}_{\mathsf{D}_1}$.

As the n queries are independent we also have:

$$\begin{aligned}
\mathbf{Var}[\mathrm{LLR}]_0 &= n\mathbf{Var}\left[\sum_{a\in\mathcal{Z}} 1_{x=a} \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]}\right] \\
&= n\left(\mathbf{E}\left[\sum_{a\in\mathcal{Z}}\sum_{a'\in\mathcal{Z}} 1_{x=a}1_{x=a'} \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]} \log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a']}{\mathbf{Pr}_{\mathsf{D}_1}[a']}\right] - D(\mathsf{D}_0 \parallel \mathsf{D}_1)^2\right) \\
&= n\left(\mathbf{E}\left[\sum_{a\in\mathcal{Z}} 1_{x=a} \left(\log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]}\right)^2\right] - D(\mathsf{D}_0 \parallel \mathsf{D}_1)^2\right) \\
&= n\left(\sum_{a\in\mathcal{Z}} \mathbf{Pr}_{\mathsf{D}_0}[a] \left(\log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]}\right)^2 - D(\mathsf{D}_0 \parallel \mathsf{D}_1)^2\right) .
\end{aligned}$$

A similar computation leads to:

$$\mathbf{Var}[\mathrm{LLR}]_1 = n\left(\sum_{a\in\mathcal{Z}} \mathbf{Pr}_{\mathsf{D}_1}[a] \left(\log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]}\right)^2 - D(\mathsf{D}_1 \parallel \mathsf{D}_0)^2\right) .$$

We summarize these results in the following proposition.

Proposition 1. *Considering that $X_1, \ldots, X_n$ are i.i.d. and that D_0 and D_1 have the same support, the Central Limit Theorem states that the* LLR *converges towards a normal distribution of mean*

$$\mathbf{E}[\mathrm{LLR}]_0 = nD(\mathsf{D}_0 \parallel \mathsf{D}_1) \geq 0 \tag{I.13}$$

or

$$\mathbf{E}[\mathrm{LLR}]_1 = -nD(\mathsf{D}_1 \parallel \mathsf{D}_0) \leq 0 \tag{I.14}$$

and of variance

$$\mathbf{Var}[LLR]_0 = n\left(\sum_{a\in\mathcal{Z}} \mathbf{Pr}_{\mathsf{D}_0}[a] \left(\log \frac{\mathbf{Pr}_{\mathsf{D}_0}[a]}{\mathbf{Pr}_{\mathsf{D}_1}[a]}\right)^2 - D(\mathsf{D}_0 \parallel \mathsf{D}_1)^2\right) \tag{I.15}$$

or

$$\mathbf{Var}\left[LLR\right]_1 = n\left(\sum_{a\in\mathcal{Z}} \mathbf{Pr}_{\mathsf{D}_1}\left[a\right]\left(\log\frac{\mathbf{Pr}_{\mathsf{D}_0}\left[a\right]}{\mathbf{Pr}_{\mathsf{D}_1}\left[a\right]}\right)^2 - D(\mathsf{D}_1 \parallel \mathsf{D}_0)^2\right)\ . \tag{I.16}$$

whether $\hat{D} = D_0$ or $\hat{D} = D_1$.

When we say that D_0 and D_1 can be distinguished, we mean that the distinguisher takes the right decision with a small probability of error P_e. Now that we have shown that the LLR can be approximated by a normal law, we can extend this concept.

Definition 4. *We will say that the two normal distributions given in Proposition 1 can be distinguished with a probability of error P_e when the underlying two distributions D_0 and D_1 can be distinguished with a probability of error P_e.*

Computation of the number of queries

In the preceeding paragraph, we have considered that $\mathsf{Supp}_{\mathsf{D}_0} = \mathsf{Supp}_{\mathsf{D}_1}$. Now, we also consider that both distributions are very close to each other and that D_1 is the uniform distribution.

Approximation 1. *Considering that D_0 is close to the uniform distribution D_1, we can write*

$$\forall a \in \mathcal{Z}\ :\ \mathbf{Pr}_{\mathsf{D}_0}\left[a\right] = \frac{1}{|\mathcal{Z}|} + \epsilon_a \quad \text{with} \quad |\epsilon_a| \ll \frac{1}{|\mathcal{Z}|} \tag{I.17}$$

We can now simplify the results obtained in Proposition 1.

Theorem 2. *Under the hypothesis of Proposition 1 and of Approximation 1 we have, at order two :*

$$\mathbf{E}\left[\mathrm{LLR}\right]_0 \approx -\mathbf{E}\left[\mathrm{LLR}\right]_1 \approx \frac{1}{2}n\left|\mathcal{Z}\right|\sum_{a\in\mathcal{Z}}\epsilon_a^2 \tag{I.18}$$

and

$$\mathbf{Var}\left[\mathrm{LLR}\right]_0 \approx \mathbf{Var}\left[\mathrm{LLR}\right]_1 \approx n\left|\mathcal{Z}\right|\sum_{a\in\mathcal{Z}}\epsilon_a^2\ . \tag{I.19}$$

Proof. If we make use of Proposition 1 and of Approximation 1, we have:

$$\begin{aligned}\mathbf{E}\left[\mathrm{LLR}\right]_0 &= n\sum_{a\in\mathcal{Z}}\left(\frac{1}{|\mathcal{Z}|}+\epsilon_a\right)\log\left(1+\left|\mathcal{Z}\right|\epsilon_a\right)\\ \mathbf{E}\left[\mathrm{LLR}\right]_1 &= n\sum_{a\in\mathcal{Z}}\frac{1}{|\mathcal{Z}|}\log\left(1+\left|\mathcal{Z}\right|\epsilon_a\right)\end{aligned}$$

and

$$\begin{aligned}
\textsf{\textbf{Var}}\left[\mathrm{LLR}\right]_0 &= n\left(\sum_{a\in\mathcal{Z}}\left(\frac{1}{|\mathcal{Z}|}+\epsilon_a\right)\left(\log\left(1+|\mathcal{Z}|\,\epsilon_a\right)\right)^2\right.\\
&\qquad\left.-\left(\sum_{a\in\mathcal{Z}}\left(\frac{1}{|\mathcal{Z}|}+\epsilon_a\right)\log\left(1+|\mathcal{Z}|\,\epsilon_a\right)\right)^2\right)\\
\textsf{\textbf{Var}}\left[\mathrm{LLR}\right]_1 &= n\left(\sum_{a\in\mathcal{Z}}\frac{1}{|\mathcal{Z}|}\left(\log\left(1+|\mathcal{Z}|\,\epsilon_a\right)\right)^2-\left(\sum_{a\in\mathcal{Z}}\frac{1}{|\mathcal{Z}|}\log\left(1+|\mathcal{Z}|\,\epsilon_a\right)\right)^2\right)\ .
\end{aligned}$$

If we develop these four results in Taylor series at order 2, we obtain the announced results. □

In the rest of this paragraph, we use the following notation:

$$\begin{aligned}
\mu &= \frac{1}{2}n\,|\mathcal{Z}|\sum_{a\in\mathcal{Z}}\epsilon_a^2\\
\sigma^2 &= n\,|\mathcal{Z}|\sum_{a\in\mathcal{Z}}\epsilon_a^2\ .
\end{aligned}$$

We can finally give the expected Theorem, that is the one that gives the number of necessary questions to distinguish D_0 and D_1 with a specific error probability.

Theorem 3. *If we assume that we are under the hypothesis of Proposition 1 and of Approximation 1 and that the number of queries* n *of the distinguisher is*

$$n = \frac{\mathsf{d}}{|\mathcal{Z}|\sum_{a\in\mathcal{Z}}\epsilon_a^2} \tag{I.20}$$

for some d*, then the probability of error* P_e *is*

$$P_e = 1-\Phi\left(\frac{\sqrt{\mathsf{d}}}{2}\right)\ , \tag{I.21}$$

where Φ *is the distribution function of a standard normal distribution, i.e.*

$$\Phi(x) = \int_{-\infty}^{x}\frac{1}{\sqrt{2\pi}}e^{-\frac{1}{2}z^2}dz\ .$$

Proof. Let d be such that

$$\mu = \frac{\sqrt{\mathsf{d}}}{2}\,\sigma\ .$$

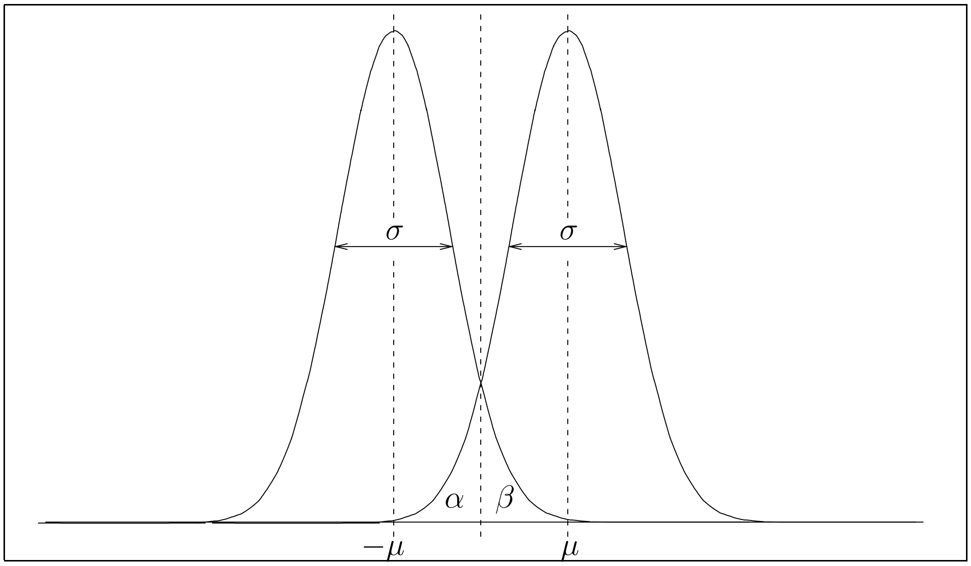


Figure I.2: The two normal distributions and the probabilities of error

We have

$$\begin{aligned}\mu = \frac{\sqrt{\mathsf{d}}}{2}\,\sigma \quad &\Leftrightarrow \quad \mu^2 = \frac{\mathsf{d}}{4}\,\sigma^2 \\ &\Leftrightarrow \quad \frac{1}{4}n^2\,|\mathcal{Z}|^2\left(\sum_{a\in\mathcal{Z}}\epsilon_a^2\right)^2 = \frac{\mathsf{d}}{4}n\,|\mathcal{Z}|\sum_{a\in\mathcal{Z}}\epsilon_a^2 \\ &\Leftrightarrow \quad n = \frac{\mathsf{d}}{|\mathcal{Z}|\displaystyle\sum_{a\in\mathcal{Z}}\epsilon_a^2}\ .\end{aligned}$$

□

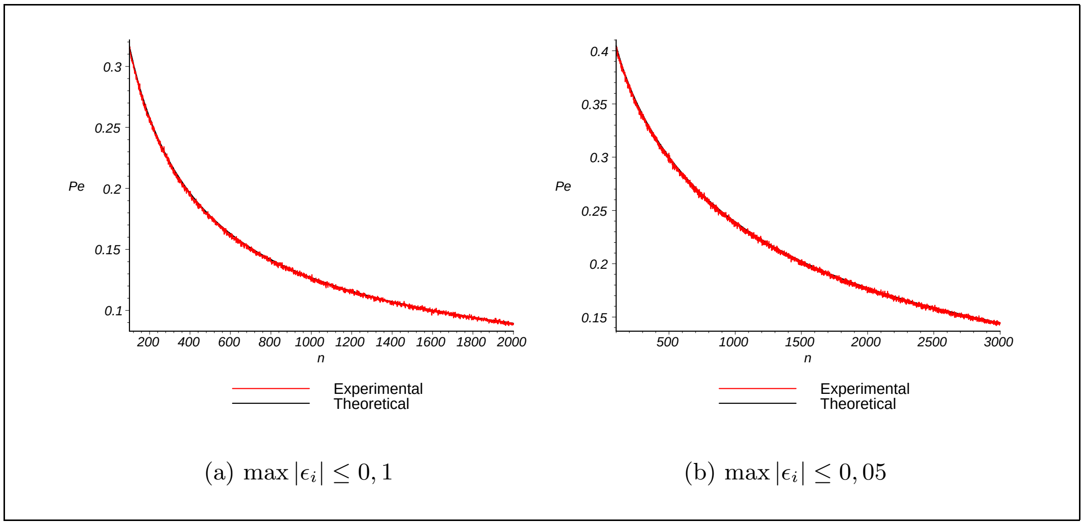
We now compute the probability of error. The two normal distributions $\mathcal{N}(\mu,\sigma)$ and $\mathcal{N}(-\mu,\sigma)$ can be distinguished with a probability of error (see Figure I.2)

$$
\begin{aligned}
P_e &= \frac{1}{2}(\alpha+\beta)\\
&= \frac{1}{2}\left(\int_{-\infty}^{0}\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}dx+\int_{0}^{+\infty}\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x+\mu)^2}{2\sigma^2}}dx\right)\\
&= \frac{1}{2}\left(\int_{-\infty}^{-\mu/\sigma}\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}dz+\int_{\mu/\sigma}^{+\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}dz\right)\\
&= \frac{1}{2}\left(1-\int_{-\mu/\sigma}^{\mu/\sigma}\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}dz\right)\\
&= \frac{1}{2}\left(1-2\int_{0}^{\mu/\sigma}\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}dz\right)\\
&= \frac{1}{2}\left(1-2\left(\int_{-\infty}^{\mu/\sigma}\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}dz-\frac{1}{2}\right)\right)\\
&= 1-\Phi\left(\frac{\mu}{\sigma}\right)\\
&= 1-\Phi\left(\frac{\sqrt{\mathsf{d}}}{2}\right)
\end{aligned}
$$

For instance, with $\mathsf{d}=1$, a distinguisher that asks $\frac{1}{|\mathcal{Z}|\sum_{a\in\mathcal{Z}}\epsilon_a^2}$ queries makes an error with a probability $P_e = 1-\Phi(\frac{1}{2})\approx 0.3085$.

Experimental results

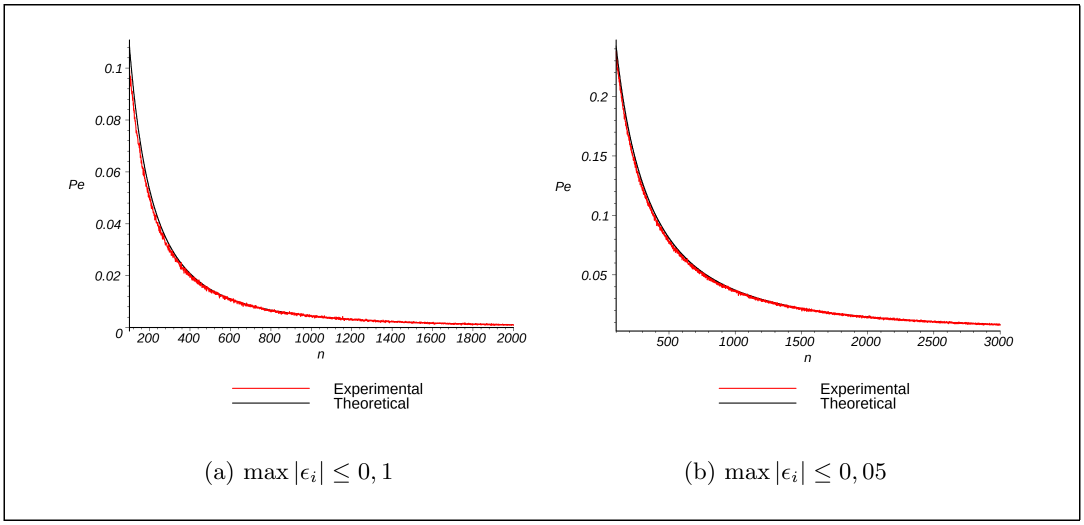
We provide here some experimental results. The program we use to test the accuracy of Theorem 3 works in the following way: it chooses at random a distribution of probability D_0. Then, for each allowed number of questions n, it computes d and the resulting theoretical probability of error $P_{e,\text{th}}$ using equations (I.20) and (I.21). Then it computes the experimental probability of $P_{e,\exp}$ by querying a Source implementing D_0 and a Source implementing D_1 (so that it can compute α and β experimentally). The results of these experiments are shown on Figure I.3 and I.4, depending on the cardinality of $\mathcal{Z}$.



(a) $\max|\epsilon_i| \leq 0,1$

(b) $\max|\epsilon_i| \leq 0,05$

Figure I.3: Accuracy of Theorem 3 when $|\mathcal{Z}| = 2$



(a) $\max|\epsilon_i| \leq 0,1$

(b) $\max|\epsilon_i| \leq 0,05$

Figure I.4: Accuracy of Theorem 3 when $|\mathcal{Z}| = 4$

The program we used was written in C, the random generator we used was the standard C generator. For each graph, the experimental curve was computed on the base of 200 iterations, each one simulating the distinguisher allowed to n queries, for $n = \{1, 2, 3, \ldots, 3000\}$.

2.7 Necessary number of queries for distant distributions

We have seen that it is possible to compute an approximation of the number of queries the distinguisher needs in the case where D_0 is close to D_1. We now consider that the two distributions are distant.

Definition 5. *We consider that* D_0 *and* D_1 *are distant when* $\mathsf{Supp}_{\mathsf{D}_0} \neq \mathsf{Supp}_{\mathsf{D}_1}$ *and when one of the two the following equations are verified:*

$$\forall a \in \mathsf{Supp}_{\mathsf{D}_0} \ : \ \mathbf{Pr}_{\mathsf{D}_0}[a] \geq \mathbf{Pr}_{\mathsf{D}_1}[a]$$

$$\forall a \in \mathsf{Supp}_{\mathsf{D}_1} \ : \ \mathbf{Pr}_{\mathsf{D}_1}[a] \geq \mathbf{Pr}_{\mathsf{D}_0}[a]$$

We now consider that $\mathsf{Supp}_{\mathsf{D}_0} \neq \mathsf{Supp}_{\mathsf{D}_1} = \mathcal{Z}$. To simplify the study we also consider that D_1 is the uniform distribution, so that the fact that these two distributions are distant implies that

$$\forall a \in \mathsf{Supp}_{\mathsf{D}_0} \ : \ \mathbf{Pr}_{\mathsf{D}_0}[a] \geq \mathbf{Pr}_{\mathsf{D}_1}[a] = \frac{1}{q} \ .$$

In such a situation, supposing that the generator implements D_1, it is possible that the distinguisher receives a sample $a \in \mathcal{Z}$ such that $\mathbf{Pr}_{\mathsf{D}_0}[a] = 0$. Regardless what it received before, it can then choose $\hat{\mathsf{D}} = \mathsf{D}_1$ with no doubt. In other terms, if the distinguisher receives a value a in the symmetric difference

$$\begin{aligned}
\mathsf{Supp}_{\mathsf{D}_0} \triangle \mathsf{Supp}_{\mathsf{D}_1} &= (\mathsf{Supp}_{\mathsf{D}_0} \cup \mathsf{Supp}_{\mathsf{D}_1}) - (\mathsf{Supp}_{\mathsf{D}_0} \cap \mathsf{Supp}_{\mathsf{D}_1}) \\
&= (\mathsf{Supp}_{\mathsf{D}_0} \cup \mathcal{Z}) - (\mathsf{Supp}_{\mathsf{D}_0} \cap \mathcal{Z}) \\
&= \mathcal{Z} - \mathsf{Supp}_{\mathsf{D}_0} \\
&= \overline{\mathsf{Supp}_{\mathsf{D}_0}}
\end{aligned}$$

it can take its decision. Thus the number of queries it needs can be considered to approximatively equal to the expected number of questions before receiving a value of the symmetric difference, when the distinguisher implements D_1. One can see that once such a value is received, the error probability P_e is 0.

Theorem 4. *If we assume that* D_0 *is distant from the uniform distribution* D_1 *and that the distinguisher asks* n *questions, then the probability of error is such that*

$$P_e \leq \left(\frac{|\mathsf{Supp}_{\mathsf{D}_0}|}{|\mathcal{Z}|}\right)^n \tag{I.22}$$

Proof. We have defined the probability of error to be

$$P_e = \frac{1}{2}(\alpha + \beta) \ .$$

We have:

$$\alpha = \mathbf{Pr}_{\mathsf{D}_0}\left[\overline{\mathcal{A}} \;\middle|\; \forall i\ \frac{\mathbf{Pr}_{\mathsf{D}_0}[x_i]}{\mathbf{Pr}_{\mathsf{D}_1}[x_i]} \geq 1\right] \mathbf{Pr}_{\mathsf{D}_0}\left[\forall i \frac{\mathbf{Pr}_{\mathsf{D}_0}[x_i]}{\mathbf{Pr}_{\mathsf{D}_1}[x_i]} \geq 1\right] + \mathbf{Pr}_{\mathsf{D}_0}\left[\overline{\mathcal{A}} \;\middle|\; \exists i\ \frac{\mathbf{Pr}_{\mathsf{D}_0}[x_i]}{\mathbf{Pr}_{\mathsf{D}_1}[x_i]} < 1\right] \mathbf{Pr}_{\mathsf{D}_0}\left[\exists i \frac{\mathbf{Pr}_{\mathsf{D}_0}[x_i]}{\mathbf{Pr}_{\mathsf{D}_1}[x_i]} < 1\right] .$$

The definition of $\mathcal{A}$ for the best distinguisher implies that

$$\mathbf{Pr}_{\mathsf{D}_0}\left[\overline{\mathcal{A}} \;\middle|\; \forall i\ \frac{\mathbf{Pr}_{\mathsf{D}_0}[x_i]}{\mathbf{Pr}_{\mathsf{D}_1}[x_i]} \geq 1\right] = 0 .$$

As the two distributions are distant, we also have

$$\mathbf{Pr}_{\mathsf{D}_0}\left[\exists i \frac{\mathbf{Pr}_{\mathsf{D}_0}[x_i]}{\mathbf{Pr}_{\mathsf{D}_1}[x_i]} < 1\right] = 0 ,$$

so that $\alpha = 0$. On the other hand, we have

$$\beta = \mathbf{Pr}_{\mathsf{D}_1}\left[\mathcal{A} \mid \forall i\ x_i \in \mathsf{Supp}_{\mathsf{D}_0}\right] \mathbf{Pr}_{\mathsf{D}_1}\left[\forall i\ x_i \in \mathsf{Supp}_{\mathsf{D}_0}\right] + \mathbf{Pr}_{\mathsf{D}_1}\left[\mathcal{A} \mid \exists i\ x_i \notin \mathsf{Supp}_{\mathsf{D}_0}\right] \mathbf{Pr}_{\mathsf{D}_1}\left[\exists i\ x_i \notin \mathsf{Supp}_{\mathsf{D}_0}\right] .$$

As the distinguisher makes no mistake when it receives a value in $\overline{\mathsf{Supp}_{\mathsf{D}_0}}$, we know that

$$\mathbf{Pr}_{\mathsf{D}_1}\left[\mathcal{A} \mid \exists i\ x_i \notin \mathsf{Supp}_{\mathsf{D}_0}\right] = 0 .$$

We thus have

$$\begin{aligned} \beta &\leq \mathbf{Pr}_{\mathsf{D}_1}\left[\forall i\ x_i \in \mathsf{Supp}_{\mathsf{D}_0}\right] \\ &= \left(\frac{\left|\mathsf{Supp}_{\mathsf{D}_0}\right|}{|\mathcal{Z}|}\right)^n \end{aligned}$$

which concludes the proof. □

To complete this section, we can note that if

$$\frac{1}{|\mathcal{Z}| \displaystyle\sum_{a \in \mathsf{Supp}_{\mathsf{D}_0} \cap \mathsf{Supp}_{\mathsf{D}_1}} \epsilon_a^2} \ll n_\triangle ,$$

the effect of the fact that $\mathsf{Supp}_{\mathsf{D}_0} \cap \mathsf{Supp}_{\mathsf{D}_1} \neq \emptyset$ can be neglected. Although this may happen only when $\mathcal{Z}$ is large enough, we can sum on $\mathsf{Supp}_{\mathsf{D}_0} \cap \mathsf{Supp}_{\mathsf{D}_1}$ instead of $\mathcal{Z}$, so that Theorem 3 is still valid.

3 Best distinguisher of a Couple of Random Variables

3.1 The problem

We consider a sequence of n iid pairs of random variables (X_i, Y_i) $1 \leq i \leq n$, each pair taking values in the set $\mathcal{Z} \times \mathcal{Z}$ (note that X_i and Y_i are dependent). We will concentrate on known plaintext attacks for which $X_1, \ldots, X_n$ are i.i.d. and uniformly distributed. When the distribution of the random variable X is uniform, the distribution of the random variable Y is defined by a so called *Matrix of transition* T such that

$$T_{x,y} = \mathbf{Pr}\left[Y = y | X = x\right] \ .$$

A random Generator implements a matrix of transition $\hat{T}$ which is either T or T^* (the ideal transition matrix). By querying it, we want to discover which one it implements. Like for the previous section, we will have to find the best distinguisher for this task (see Figure I.5).

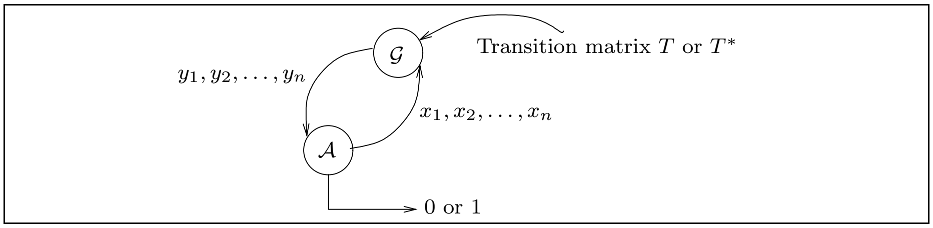


Figure I.5: A non-adaptative distinguisher between two transition matrices

3.2 Notation and convention

In this section we will focus on the distribution of couples (X, Y) taking values in $\mathcal{Z}^2$. We will consider such a couple like a random variable $Z = (X, Y)$. Therefore, n realizations will be denoted $z_i = (x_i, y_i)$ for $1 \leq i \leq n$.

We call support of a transition matrix T the subset Supp_T of $\mathcal{Z} \times \mathcal{Z}$ such that for all (x, y):

$$(x, y) \in \mathsf{Supp}_T \Leftrightarrow T_{x,y} \neq 0 \ .$$

3.3 The Best Decision Rule

In the previous section, we managed to find a distinguisher whose set of acceptance was dependent only on counters. In this section we are going to follow the same approach. In a first phase, we will maximize the advantage of our distinguisher in order to derive a set of acceptance $\mathcal{A}$ based on the n realizations of the random variable (X, Y), where X is uniformly distributed. In a second phase, we will use this set to find a new set of acceptance $\widetilde{\mathcal{A}}$ based on $|\mathcal{Z}|^2$ counters.

Finding a set of acceptance based on realizations

We consider the distinguisher described by Algorithm 3. We want to maximize its advantage given by

$$\mathrm{Adv}_{\mathcal{A}}^{n} = \left|\mathbf{Pr}_T\left[\mathcal{A}\right] - \mathbf{Pr}_{T^*}\left[\mathcal{A}\right]\right| \ . \tag{I.23}$$

This distinguisher can make two types of mistake. It can either output 1 when $\hat{T} = T$ or output 0 when $\hat{T} = T^*$. We denote the probability of these two events by

$$\alpha = \mathbf{Pr}_T\left[\overline{\mathcal{A}}\right] \tag{I.24}$$

and

$$\beta = \mathbf{Pr}_{T^*}\left[\mathcal{A}\right] \ . \tag{I.25}$$

As in the previous section, we can write the advantage using these notation in the following way:

$$\mathrm{Adv}_{\mathcal{A}}^{n} = 1 - 2P_e \tag{I.26}$$

where P_e is the overall probability of error, considered to be less than $\frac{1}{2}$, and such that $P_e = \frac{1}{2}(\alpha + \beta)$.

Still following the methodology used in the previous section, we can derive the set $\mathcal{A} \subset (\mathcal{Z} \times \mathcal{Z})^n$ maximizing the advantage. We find

$$\mathcal{A} = \left\{ \mathbf{z}^n \in (\mathcal{Z} \times \mathcal{Z})^n \ : \ \frac{\mathbf{Pr}_T\left[\mathbf{z}^n\right]}{\mathbf{Pr}_{T^*}\left[\mathbf{z}^n\right]} \geq 1 \right\} \ , \tag{I.27}$$

with the convention that $\frac{p}{0} = +\infty$ for $p > 0$. Note that the $\frac{0}{0}$ can be ignored.

We can express this result in function of the transition matrix T and T^*. Considering that the X_i's are uniformly distributed, we have:

$$\begin{aligned}
\frac{\mathbf{Pr}_T\left[\mathbf{z}^n\right]}{\mathbf{Pr}_{T^*}\left[\mathbf{z}^n\right]} &= \frac{\mathbf{Pr}_T\left[(X_i, Y_i) = (x_i, y_i) \ 1 \leq i \leq n\right]}{\mathbf{Pr}_{T^*}\left[(X_i, Y_i) = (x_i, y_i) \ 1 \leq i \leq n\right]} \\
&= \prod_{i=1}^{n} \frac{\mathbf{Pr}_T\left[(X_i, Y_i) = (x_i, y_i)\right]}{\mathbf{Pr}_{T^*}\left[(X_i, Y_i) = (x_i, y_i)\right]} \\
&= \prod_{i=1}^{n} \frac{T_{x_i, y_i}}{T^*_{x_i, y_i}} \ .
\end{aligned}$$

We summarize these results in the following definition.

Definition 6. ***(Optimal Binary Hypothesis Test using Transition Matrix).*** *The optimal decision rule to test $\hat{T} = T$ against $\hat{T} = T^*$ that minimizes the overall*

```
Parameters: a complexity $n$, an acceptance region $\mathcal{A}$
Input: an random Generator $\mathcal{G}$ which generates a realization of a random variable $Y$ according to a realization of $X$ at its input and to a transition matrix $\hat{T}$.
for $i = 1, \dots, n$ do
    Pick $x_i$ uniformly at random and send it to the Generator $\mathcal{G}$
    Receive $y_i \in \mathcal{Z}$
end for
if $((x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)) \in \mathcal{A}$
    Output 0
else
    Output 1
end if
```

Algorithm 3: Known plaintext attack based on a set of realizations

probability of error (i.e. maximizes the advantage of the distinguisher of Algorithm 3) is the following:

$$\delta_{\text{opt}} = \begin{cases} 0 \text{ (i.e. accept } \hat{T} = T\text{) if } \mathrm{LR}(\mathbf{z}^n) \geq 1 \\ 1 \text{ (i.e. accept } \hat{T} = T^*\text{) if } \mathrm{LR}(\mathbf{z}^n) < 1 \end{cases} \tag{I.28}$$

where LR *is the likelihood ratio,*

$$\mathrm{LR}(\mathbf{z}^n) = \prod_{i=1}^{n} \frac{T_{x_i,y_i}}{T^*_{x_i,y_i}} \ , \tag{I.29}$$

with the convention that $\frac{p}{0} = +\infty$ *for* $p > 0$ *(the* $\frac{0}{0}$ *case can be ignored).*

Finding a set of acceptance based on counters

Like in the previous section, the distinguisher we just computed can not be implemented as it uses a huge amount of memory. We will see that only counters are necessary in order to derive a distinguisher with the same advantage.

If we reconsider the definition of the LR, we have:

$$\begin{aligned} \mathrm{LR}(\mathbf{z}^n) &= \prod_{i=1}^{n} \frac{\mathbf{Pr}_T\left[(X_i, Y_i) = (x_i, y_i)\right]}{\mathbf{Pr}_{T^*}\left[(X_i, Y_i) = (x_i, y_i)\right]} \\ &= \prod_{\substack{a,b \in \mathcal{Z} \\ \text{s.t. } N((a,b)|\mathbf{z}^n) > 0}} \left(\frac{\mathbf{Pr}_T\left[(X, Y) = (a, b)\right]}{\mathbf{Pr}_{T^*}\left[(X, Y) = (a, b)\right]} \right)^{N((a,b)|(x_1,y_1)\dots(x_n,y_n))} \ , \end{aligned}$$

```
Parameters: a complexity $n$, an acceptance region $\widetilde{\mathcal{A}}$
Input: a random Generator $\mathcal{G}$ which generates a realization of a random variable $Y$ according to a realization of $X$ at its input and to a transition matrix $\hat{T}$.
Initialize a matrix $\mathcal{U}$ of $|\mathcal{Z}| \times |\mathcal{Z}|$ counters
for $i = 1, \dots, n$ do
    Pick $a \in \mathcal{Z}$ uniformly at random and send it to the Generator $\mathcal{G}$
    Receive $b \in \mathcal{Z}$ and increment $[\mathcal{U}]_{ab}$
end for
if $\mathcal{U} \in \widetilde{\mathcal{A}}$
    Output 0
else
    Output 1
end if
```

Algorithm 4: Known plaintext attack based on a set of counters

where $N((a,b)|(x_1,y_1)\dots(x_n,y_n))$ is the number of times the couple $(a,b) \in \mathcal{Z}^2$ occurs in the sequence $(x_1,y_1)\dots(x_n,y_n)$. The likelihood ratio is thus uniquely defined by $|\mathcal{Z}|^2$ counters. Let $\mathcal{U}$ be the $|\mathcal{Z}| \times |\mathcal{Z}|$ matrix such that

$$[\mathcal{U}]_{ab} = N((a,b)|(x_1,y_1),(x_2,y_2),\dots,(x_n,y_n)) \; .$$

Like in the previous section, we can take the logarithm of the likelihood ratio and consider it as a function of the counters. We denote it LLR, such that

$$\begin{aligned}
\mathrm{LLR}(\mathcal{U}) &= \sum_{\substack{a,b \in \mathcal{Z} \\ \text{s.t. } N((a,b)|\mathbf{z}^n)>0}} N((a,b)|\mathbf{z}^n) \log \frac{\mathbf{Pr}_T\left[(X,Y)=(a,b)\right]}{\mathbf{Pr}_{T^*}\left[(X,Y)=(a,b)\right]} \\
&= \sum_{\substack{a,b \in \mathcal{Z} \\ \text{s.t. } N((a,b)|\mathbf{z}^n)>0}} N((a,b)|\mathbf{z}^n) \log \frac{T_{a,b}}{T^*_{a,b}} \; ,
\end{aligned}$$

with the convention that $\log \frac{0}{p} = -\infty$ and $\log \frac{p}{0} = +\infty$ for $p > 0$. We note that the $\log \frac{0}{0}$ case still never occurs here as the sum is taken over (a,b) couples such that $N((a,b)|\mathbf{z}^n) > 0$. We can define a new decision rule $\widetilde{\delta}$ (i.e. a new set of acceptance $\widetilde{\mathcal{A}}$) based on the counters. The distinguisher associated with this new set $\widetilde{\mathcal{A}}$ is described by Algorithm 4. We summarize these results in the following definition.

Definition 7. ***(Optimal Binary Hypothesis Test using Transition Matrix Revisited).*** *The optimal decision rule to test $\hat{T} = T$ against $\hat{T} = T^*$ that minimizes the overall probability of error is the following:*

$$\widetilde{\delta}_{\mathrm{opt}} = \begin{cases} 0 \text{ (i.e. accept } \hat{T} = T\text{) if } \mathrm{LLR}(\mathcal{U}) \geq 0 \\ 1 \text{ (i.e. accept } \hat{T} = T^*\text{) if } \mathrm{LLR}(\mathcal{U}) < 0 \end{cases} \tag{I.30}$$

where $\mathcal{U}$ is the $|\mathcal{Z}| \times |\mathcal{Z}|$ matrix such that $[\mathcal{U}]_{ab} = N((a,b)|\mathbf{z}^n)$ and where LLR *is the logarithmic likelihood ratio,*

$$\mathrm{LLR}(\mathcal{U}) = \sum_{\substack{a,b \in \mathcal{Z} \\ \text{s.t. } N((a,b)|\mathbf{z}^n)>0}} N((a,b)|\mathbf{z}^n) \log \frac{T_{a,b}}{T^*_{a,b}} \ , \tag{I.31}$$

with the convention that $\log \frac{0}{p} = -\infty$ *and* $\log \frac{p}{0} = +\infty$ *for* $p > 0$ *(the* $\log \frac{0}{0}$ *case can be ignored).*

As in the previous case, it is clear that if the optimal distinguisher receives a couple (x, y) such that $T_{x,y} = 0$, it will eventually make the right choice (i.e. choose $\hat{T} = T^*$).

3.4 Computation of the advantage of the best distinguisher

The probability that the distinguisher outputs 0 when $\hat{T} = T$ (resp. $\hat{T} = T^*$) is $\sum_{(a,b)\in\mathcal{A}} \mathbf{Pr}_T[\mathbf{z}^n]$ (resp. $\sum_{(a,b)\in\mathcal{A}} \mathbf{Pr}_{T^*}[\mathbf{z}^n]$). The advantage is thus

$$\left| \sum_{\mathbf{z}^n \in \mathcal{A}} \left(\mathbf{Pr}_T[\mathbf{z}^n] - \mathbf{Pr}_{T^*}[\mathbf{z}^n] \right) \right| \ .$$

We know that this sum is maximum when it is taken over $\mathcal{A}$ and that it is null when it is taken over all possible values. Thus the advantage is:

$$\mathrm{Adv}^n_{\delta_{\mathrm{opt}}} = \frac{1}{2} \sum_{\mathbf{z}^n \in (\mathcal{Z}\times\mathcal{Z})^n} \left| \mathbf{Pr}_T[\mathbf{z}^n] - \mathbf{Pr}_{T^*}[\mathbf{z}^n] \right|$$

If $\mathcal{T}_n$ is the $|\mathcal{Z}^n| \times |\mathcal{Z}^n|$ matrix such that

$$[\mathcal{T}_n]_{(x_1,x_2,\ldots,x_n)(y_1,y_2,\ldots,y_n)} = \prod_{i=1}^{n} T_{x_i y_i} \ ,$$

we can write down the advantage as:

$$\boxed{\mathrm{Adv}^n_{\delta_{\mathrm{opt}}} = \frac{1}{2\,|\mathcal{Z}|^n} \parallel \mathcal{T}_n - \mathcal{T}^*_n \parallel_1} \ , \tag{I.32}$$

where the $\parallel \cdot \parallel_1$ norm of a matrix A is defined by $\parallel A \parallel_1 = \sum_{i,j} |A_{i,j}|$.

3.5 Necessary number of queries for close distributions

Like in the previous section, we try to anticipate the number of queries that our distinguisher needs in order to make the distinction between T and T^*, given a certain error probability P_e.

We follow an identical approach. We will approximate the LLR by a normal law in the case where $\mathsf{Supp}_T = \mathsf{Supp}_{T^*}$. Then we compute the number of queries supposing that T is close to T^*.

Approximation of the LLR by a normal law

We slightly modify the definition of the relative entropy so that it fits to the transition matrices we are manipulating.

Definition 8. *The relative entropy between two transition matrices T and T^* is defined as*

$$\mathcal{D}(T \parallel T^*) = \sum_{a,b\in\mathcal{Z}} T_{a,b} \log \frac{T_{a,b}}{T^*_{a,b}} \tag{I.33}$$

with the convention that $0 \log \frac{0}{p} = 0$ and $p \log \frac{p}{0} = +\infty$ for $p > 0$.

Using just the same conventions as in the previous section, we can write the LLR in the following way:

$$\begin{aligned} \mathrm{LLR}(\mathcal{U}) &= \sum_{a,b\in\mathcal{Z}} N((a,b)|\mathbf{z}^n) \log \frac{T_{a,b}}{T^*_{a,b}} \\ &= \sum_{a,b\in\mathcal{Z}} \sum_{i=1}^{n} 1_{(a,b)=(x_i,y_i)} \log \frac{T_{a,b}}{T^*_{a,b}} \\ &= \sum_{i=1}^{n} \sum_{a,b\in} 1_{(a,b)=(x_i,y_i)} \log \frac{T_{a,b}}{T^*_{a,b}} \ . \end{aligned}$$

As the n queries are independent, we can consider that the n random variables

$$\sum_{a,b\in\mathcal{Z}} 1_{(a,b)=(x_i,y_i)} \log \frac{T_{a,b}}{T^*_{a,b}} \ , \ 1 \le i \le n$$

are independent. The Central Limit Theorem then states that the LLR approaches a normal distribution of mean $\mathbf{E}\left[\mathrm{LLR}\right]_j$ and of variance $\mathbf{Var}\left[\mathrm{LLR}\right]_j$, where j is equal to 0 (resp. 1) when $\hat{T} = T$ (resp. $\hat{T} = T^*$).

The mean (depending on the distribution) is

$$\mathbf{E}\left[\mathrm{LLR}\right]_j = \sum_{i=1}^{n} \sum_{a,b\in\mathcal{Z}} \mathbf{E}\left[1_{(a,b)=(x_i,y_i)}\right] \log \frac{T_{a,b}}{T^*_{a,b}} \ ,$$

which gives

$$\mathbf{E}\left[\mathrm{LLR}\right] = \frac{n}{|\mathcal{Z}|} \mathcal{D}(T \parallel T^*) \tag{I.34}$$

and

$$\mathbf{E}\left[\mathrm{LLR}\right]^* = -\frac{n}{|\mathcal{Z}|}\mathcal{D}(T^* \parallel T)\ . \tag{I.35}$$

As the n queries are independent we also have:

$$\begin{aligned}
\mathbf{Var}\left[\mathrm{LLR}\right] &= n\mathbf{Var}\left[\sum_{a,b\in\mathcal{Z}} 1_{(a,b)=(x,y)} \log\frac{T_{a,b}}{T^*_{a,b}}\right] \\
&= n\Bigg(\mathbf{E}\left[\sum_{a,b\in\mathcal{Z}}\sum_{a',b'\in\mathcal{Z}} 1_{(a,b)=(x,y)}1_{(a',b')=(x,y)} \log\frac{T_{a,b}}{T^*_{a,b}}\log\frac{T_{a',b'}}{T^*_{a',b'}}\right] \\
&\qquad -\frac{1}{|\mathcal{Z}|^2}\mathcal{D}(T\parallel T^*)^2\Bigg) \\
&= n\left(\mathbf{E}\left[\sum_{a,b\in\mathcal{Z}} 1_{(a,b)=(x,y)}\left(\log\frac{T_{a,b}}{T^*_{a,b}}\right)^2\right] - \frac{1}{|\mathcal{Z}|^2}\mathcal{D}(T\parallel T^*)^2\right) \\
&= \frac{n}{|\mathcal{Z}|}\left(\sum_{a,b\in\mathcal{Z}} T_{a,b}\left(\log\frac{T_{a,b}}{T^*_{a,b}}\right)^2 - \frac{1}{|\mathcal{Z}|}\mathcal{D}(T\parallel T^*)^2\right)\ .
\end{aligned}$$

A similar computation leads to:

$$\mathbf{Var}\left[\mathrm{LLR}\right]^* = \frac{n}{|\mathcal{Z}|}\left(\sum_{a,b\in\mathcal{Z}} T^*_{a,b}\left(\log\frac{T_{a,b}}{T^*_{a,b}}\right)^2 - \frac{1}{|\mathcal{Z}|}\mathcal{D}(T^*\parallel T)^2\right)\ .$$

We summarize these results in the following proposition.

Proposition 2. *Considering that the n queries to the Oracle are independent and that T and T^* have the same support, the Central Limit Theorem states that the* LLR *approaches a normal distribution of mean*

$$\mathbf{E}\left[\mathrm{LLR}\right] = \frac{n}{|\mathcal{Z}|}\mathcal{D}(T\parallel T^*) \geq 0 \tag{I.36}$$

or

$$\mathbf{E}\left[\mathrm{LLR}\right]^* = -\frac{n}{|\mathcal{Z}|}\mathcal{D}(T^*\parallel T) \leq 0\ , \tag{I.37}$$

and of variance

$$\mathbf{Var}\left[LLR\right] = \frac{n}{|\mathcal{Z}|}\left(\sum_{a,b\in\mathcal{Z}} T_{a,b}\left(\log\frac{T_{a,b}}{T^*_{a,b}}\right)^2 - \frac{1}{|\mathcal{Z}|}\mathcal{D}(T\parallel T^*)^2\right)\ .$$

or

$$\mathsf{Var}\left[LLR\right]^* = \frac{n}{|\mathcal{Z}|}\left(\sum_{a,b\in\mathcal{Z}} T^*_{a,b}\left(\log\frac{T_{a,b}}{T^*_{a,b}}\right)^2 - \frac{1}{|\mathcal{Z}|}\mathcal{D}(T^* \parallel T)^2\right) .$$

whether $\hat{T} = T$ *or* $\hat{T} = T^*$*.*

Computation of the number of queries

Until now, we have only considered that $\mathsf{Supp}_T = \mathsf{Supp}_{T^*}$. Now, we also consider that T and T^* are close to each other and that T^* is an ideal transition matrix where all entries are equal to $\frac{1}{|\mathcal{Z}|}$.

Approximation 2. *Considering that* T *is close to* T^**, we can write*

$$\forall a,b\in\mathcal{Z}\ :\ T_{a,b} = \frac{1}{|\mathcal{Z}|} + \epsilon_{a,b} \quad \textit{with} \quad \epsilon_{a,b} \ll \frac{1}{|\mathcal{Z}|}\ . \tag{I.38}$$

The results of Proposition 2 can now be simplified.

Theorem 5. *Under the hypothesis of Proposition 2 and of Approximation 2 we have, at order two:*

$$\mathsf{E}\left[\mathrm{LLR}\right] \approx -\mathsf{E}\left[\mathrm{LLR}\right]^* \approx \frac{1}{2}n\sum_{a,b\in\mathcal{Z}}\epsilon^2_{a,b} \tag{I.39}$$

and

$$\mathsf{Var}\left[\mathrm{LLR}\right] \approx \mathsf{Var}\left[\mathrm{LLR}\right]^* \approx n\sum_{a,b\in\mathcal{Z}}\epsilon^2_{a,b}\ . \tag{I.40}$$

Proof. Using the approximations we have:

$$\begin{aligned}
\mathsf{E}\left[\mathrm{LLR}\right] &= \frac{n}{|\mathcal{Z}|}\sum_{a,b\in\mathcal{Z}}\left(\frac{1}{|\mathcal{Z}|}+\epsilon_{a,b}\right)\log\left(1+|\mathcal{Z}|\,\epsilon_{a,b}\right)\\
\mathsf{E}\left[\mathrm{LLR}\right]^* &= \frac{n}{|\mathcal{Z}|}\sum_{a,b\in\mathcal{Z}}\frac{1}{|\mathcal{Z}|}\log\left(1+|\mathcal{Z}|\,\epsilon_{a,b}\right)
\end{aligned}$$

and

$$\begin{aligned}
\mathsf{Var}\left[\mathrm{LLR}\right] =& \frac{n}{|\mathcal{Z}|}\left(\sum_{a,b\in\mathcal{Z}}\left(\frac{1}{|\mathcal{Z}|}+\epsilon_{a,b}\right)\left(\log\left(1+|\mathcal{Z}|\,\epsilon_{a,b}\right)\right)^2\right.\\
&\left.-\left(\sum_{a,b\in\mathcal{Z}}\left(\frac{1}{|\mathcal{Z}|}+\epsilon_{a,b}\right)\log\left(1+|\mathcal{Z}|\,\epsilon_{a,b}\right)\right)^2\right)\\
\mathsf{Var}\left[\mathrm{LLR}\right]^* =& \frac{n}{|\mathcal{Z}|}\left(\sum_{a,b\in\mathcal{Z}}\frac{1}{|\mathcal{Z}|}\left(\log\left(1+|\mathcal{Z}|\,\epsilon_{a,b}\right)\right)^2-\left(\sum_{a,b\in\mathcal{Z}}\frac{1}{|\mathcal{Z}|}\log\left(1+|\mathcal{Z}|\,\epsilon_{a,b}\right)\right)^2\right)\ .
\end{aligned}$$

If we develop these four results in Taylor series at order 2, we obtain the announced results. □

In the rest of this paragraph we adopt the following notations:

$$\begin{aligned}\mu &= \frac{1}{2} n \sum_{a,b\in\mathcal{Z}} \epsilon_{a,b}^2 \\ \sigma^2 &= n \sum_{a,b\in\mathcal{Z}} \epsilon_{a,b}^2 \ .\end{aligned}$$

We now give the expected theorem which gives the necessary number of questions to distinguish T from T^* given a specific probability of error.

Theorem 6. *If we assume that we are under the hypothesis of Proposition 2 and of Approximation 2 and that the number of queries* n *of the distinguisher is*

$$n = \frac{\mathsf{d}}{\sum_{a,b\in\mathcal{Z}} \epsilon_{a,b}^2} \tag{I.41}$$

for some d*, then the probability of error* P_e *is*

$$P_e = 1 - \Phi\left(\frac{\sqrt{\mathsf{d}}}{2}\right) \ , \tag{I.42}$$

where Φ *is the distribution function of a standard normal distribution, i.e.*

$$\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}z^2} dz \ .$$

Proof. The proof is exactly the same as the one of Theorem 3. The only change is the definition of μ and σ. □

3.6 Illustration in the case of a Linear Cryptanalysis

In the case of a standard linear cryptanalysis, the cardinal of $\mathcal{Z}$ is 2. The variable X (resp. Y) is in reality the product of a mask and of an input block (resp. an output block) of a permutation. Thus both the sum of the rows and of the columns must be equal to 1. The shape of the transition matrix is

$$T = \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix} \ ,$$

where $p = \mathsf{\mathbf{Pr}}\left[X = Y\right]$. If T is supposed to be close to an ideal transition matrix T^*, we obtain:

$$T = \begin{pmatrix} 1/2+\epsilon & 1/2-\epsilon \\ 1/2-\epsilon & 1/2+\epsilon \end{pmatrix} .$$

In [Mat94a], Matsui applies its linear cryptanalysis on 14-rounds DES. The linear expression holds with a probability $1/2 + 1.19 \cdot 2^{-21}$. With our notation, it means that $\epsilon = 1.19 \cdot 2^{-21}$. Matsui also shows that in that case, 2^{43} plaintexts are needed to conclude the attack. Theorem 6 allows to compute the corresponding probability of error in such a case. It gives:

$$P_e = 0.0461958570 .$$

3.7 Necessary number of queries for distant distributions

We studied the case where T is close to T^*. We now consider the opposite case, that is when T and T^* are distant from each other.

Definition 9. *We consider that T and T^* are distant when $\mathsf{Supp}_T \neq \mathsf{Supp}_{T^*}$ and when one of the two the following equations are verified:*

$$\forall (x,y) \in \mathsf{Supp}_T \ : \ T_{x,y} \geq T^*_{x,y}$$

$$\forall (x,y) \in \mathsf{Supp}_{T^*} \ : \ T^*_{x,y} \geq T_{x,y}$$

Theorem 7. *If we assume that T is distant from the uniform transition matrix T^* and that the distinguisher asks n questions, then the probability of error is such that*

$$P_e \leq \left(\frac{|\mathsf{Supp}_T|}{|\mathcal{Z}|^2} \right)^n \tag{I.43}$$

Proof. The proof is identical to the one of Theorem 4. □

Chapter II

The tools of Generalized Linear Cryptanalysis

1 Introduction and notation

In section 2 we are going to introduce a fundamental mapping from a a finite extension F_{q^m} of a finite field F_q. Some of its fundamental properties are also introduced. In section 3 we will use it in order to define a transition matrix.

In what follows, F_{q^m} is a finite extension of a finite field F_q. We can consider F_{q^m} as a vector space over F_q, of dimension m. The set $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathsf{F}_{q^m}$ will denote a base of this vector space, i.e. every element α of F_{q^m} can be uniquely written

$$\alpha = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_m\alpha_m \quad \text{with} \quad c_i \in \mathsf{F}_q \ \ \forall\, 1 \leq i \leq m \ .$$

2 Trace

Definition 10. ***(Trace)*** *The trace $\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\alpha)$ of an element $\alpha \in \mathsf{F}_{q^m}$ over F_q is defined by*

$$\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \ . \tag{II.1}$$

If F_q is the prime subfield of F_{q^m} (i.e. q is prime), the trace is called absolute trace and simply denoted $\mathbf{Tr}_{\mathsf{F}_{q^m}}(\alpha)$.

We give here some useful properties of the trace function, proofs can be found in [LN83].

Theorem 8. *The trace function satisfies the following properties:*

1. $\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\alpha+\beta) = \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\alpha) + \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\beta)$ *for all* $\alpha, \beta \in \mathsf{F}_{q^m}$*;*
2. $\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(c\alpha) = c\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\alpha)$ *for all* $c \in \mathsf{F}_q$ *and* $\alpha \in \mathsf{F}_{q^m}$*;*

3. *$\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}$ is a linear transformation from F_{q^m} onto F_q, where both F_{q^m} and F_q are viewed as vector spaces over F_q;*

4. *$\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a) = ma$ for all $a \in \mathsf{F}_q$;*

5. *$\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\alpha^q) = \mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\alpha)$ for all $\alpha \in \mathsf{F}_{q^m}$.*

We give another theorem which is also taken from [LN83].

Theorem 9. ***(Transitivity of trace)*** *The trace function is transitive, i.e. :*

$$\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\alpha) = \mathsf{Tr}_{\mathsf{F}_{q^n}/\mathsf{F}_q}\left(\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_{q^n}}(\alpha)\right) \tag{II.2}$$

for all $\alpha \in \mathsf{F}_{q^m}$ and for all integer n such that n divides m.

The following Theorem of the trace will be fundamental during our generalization of linear cryptanalysis. It states that the trace is a *balanced* transformation.

Theorem 10. *Let $\mathbf{X}$ be a random variable, uniformly distributed over F_{q^m} viewed as a vector space over F_q. In other terms we can write*

$$\mathbf{X} = \begin{pmatrix} X_0 \\ \vdots \\ X_{m-1} \end{pmatrix}$$

where the X_i's are iid random variables uniformly distributed over F_q. Then the random variable $\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{X})$ is a uniformly distributed over F_q, i.e.

$$\mathsf{Pr}_{\mathbf{X}\in_U \mathsf{F}_{q^m}}\left[\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{X}) = c\right] = \frac{1}{q} \quad \textit{for all} \quad c \in \mathsf{F}_q\ .$$

Proof. As $\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}$ is a mapping from F_{q^m} onto F_q, there exists $\mathbf{C} \in \mathsf{F}_{q^m}$ such that

$$\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{C}) = c\ .$$

Thus we have:

$$\begin{aligned}\mathsf{Pr}_{\mathbf{X}\in_U \mathsf{F}_{q^m}}\left[\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{X}) = c\right] &= \mathsf{Pr}_{\mathbf{X}\in_U \mathsf{F}_{q^m}}\left[\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{X}) = \mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{C})\right] \\ &= \mathsf{Pr}_{\mathbf{X}\in_U \mathsf{F}_{q^m}}\left[\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{X} - \mathbf{C}) = 0\right]\ ,\end{aligned}$$

using the trace linearity. The trace of an element is equal to 0 when this element is a root of (II.1). As this polynomial is of degree q^{m-1}, there are at most q^{m-1} roots among the q^m elements of F_{q^m}. So

$$\begin{aligned}\mathsf{Pr}_{\mathbf{X}\in_U \mathsf{F}_{q^m}}\left[\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{X}) = c\right] &\leq \frac{q^{m-1}}{q^m} \\ &= \frac{1}{q}\ .\end{aligned}$$

As

$$\sum_{c\in\mathsf{F}_q} \mathbf{Pr}_{\mathbf{X}\in_U \mathsf{F}_{q^m}} \left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{X}) = c\right] = 1$$

we can conclude that

$$\mathbf{Pr}_{\mathbf{X}\in_U \mathsf{F}_{q^m}} \left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(\mathbf{X}) = c\right] = \frac{1}{q}\ .$$

□

3 A transition matrix using the trace

3.1 Definition

In this section we are going to define a specific transition matrix $\mathbf{LT}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$ where a, b are elements of the field F_{q^m} and f is a function over F_{q^m}. This matrix will be used to study the non-linearity of the function f. We will then see how this concept generalizes the linear characteristic LP defined in the context of a linear cryptanalysis.

Then we will use the study made in the first part of this work, together with the notion of trace, to study the non linearity of the S-Box of AES.

Definition 11. ***(Linear Transition Matrix)*** *Let f be a function over F_{q^m}. The linear transition matrix $\mathbf{LT}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$ of f from F_{q^m} over F_q and for $a, b \in \mathsf{F}^*_{q^m}$ is a $q\times q$ matrix such that*

$$\left[\mathbf{LT}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)\right]_{i,j} = \mathbf{Pr}_{X\in\mathsf{F}_{q^m}}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bf(X)) = j | \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) = i\right] \quad \text{(II.3)}$$

where the probability holds over the uniform distribution of the random variable X. If F_q is the prime field of F_{q^m} (i.e. q is prime), the Linear Characteristic Matrix is simply denoted $\mathbf{LT}^{f}_{\mathsf{F}_{q^m}}(a,b)$.

Example. We consider the case where f is C^*, the random permutation uniformly distributed over F_{q^m}. We have:

$$\begin{aligned}
\mathbf{E}_{C^*}\left[[\mathbf{LT}^{C^*}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)]_{i,j}\right] &= \mathbf{E}_X\left[\mathbf{Pr}_{C^*}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bC^*(X)) = j | \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) = i\right]\right] \\
&= \sum_{x\in F} \mathbf{Pr}_{C^*}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bC^*(x)) = j | \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(ax) = i\right] \\
&\qquad \times \mathbf{Pr}_X[X = x] \\
&= 1/q\ .
\end{aligned}$$

In what follows we consider that $\boxed{q = 2^n}$.

If we take the specific case where $n = 1$, f is a permutation C and denote by p the value of the coefficient of the first row, first column of the linear characteristic matrix, we obtain

$$\begin{aligned} p &= \left[\mathsf{LT}^{C}_{\mathsf{F}_{2^m}}(a,b)\right]_{00} \\ &= \mathsf{Pr}_{X\in\mathsf{F}_{2^m}}\left[\mathsf{Tr}_{\mathsf{F}_{2^m}}(bC(X)) = 0 | \mathsf{Tr}_{\mathsf{F}_{2^m}}(aX) = 0\right] \\ &= \mathsf{Pr}_{X\in\mathsf{F}_{2^m}}\left[\mathsf{Tr}_{\mathsf{F}_{2^m}}(bC(X)) = \mathsf{Tr}_{\mathsf{F}_{2^m}}(aX)\right] \ , \end{aligned}$$

as $\mathsf{F}_2 = \{0,1\}$. The linear characteristic one usually defines in the context of linear cryptanalysis compares two bits, which is exactly what we do when we consider the case where $n = 1$.

In what follows we will also need the following definition.

Definition 12. ***(Linear Bias Matrix)*** *Let f be a function over F_{q^m} and $\mathsf{LT}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$ its transition matrix for $a, b \in \mathsf{F}^*_{q^m}$. The linear bias matrix $\mathsf{LB}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$ of f corresponding to the given linear transition matrix is defined as*

$$\mathsf{LB}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b) = \mathsf{LT}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b) - \mathbf{U} \tag{II.4}$$

where $\mathbf{U}$ is a $q \times q$ matrix such that all entries are equal to $\frac{1}{q}$.

3.2 A fundamental property on linear transition matrices

In this paragraph, we consider the situation of Figure II.1.

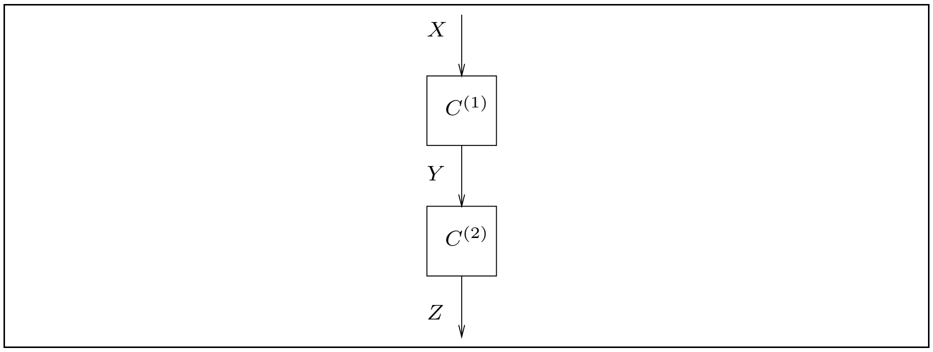


Figure II.1: Two rounds of a typical block cipher

Our objective is to determine the transition matrix on two rounds $C^{(2)} \circ C^{(1)}$ given the transition matrices of each individual round.

Property 1. *Consider the situation described on Figure II.1, where $C^{(1)}$ and $C^{(2)}$ are two fixed permutations over F_{q^m}. Suppose that, for every $a, b, c \in \mathsf{F}^*_{q^m}$, the chain $\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) \to \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bY) \to \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(cZ)$ is a Markov chain. Then:*

$$\mathbf{LT}^{C^{(2)}\circ C^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,c) = \mathbf{LT}^{C^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b) \times \mathbf{LT}^{C^{(2)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(b,c) \tag{II.5}$$

Proof. We have:

$$\begin{aligned}
&\left[\mathbf{LT}^{C^{(2)}\circ C^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,c)\right]_{i,j} \\
&= \mathbf{Pr}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(cZ) = j \mid \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) = i\right] \\
&= q\,\mathbf{Pr}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(cZ) = j, \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) = i\right] \\
&= \sum_{k\in\mathsf{F}_q} \mathbf{Pr}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(cZ) = j, \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) = i \mid \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bY) = k\right] .
\end{aligned}$$

Using the fact that $\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) \to \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bY) \to \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(cZ)$ is a Markov chain we conclude that:

$$\begin{aligned}
\left[\mathbf{LT}^{C^{(2)}\circ C^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,c)\right]_{i,j} &= \sum_{k\in\mathsf{F}_q} \mathbf{Pr}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(cZ) = j \mid \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bY) = k\right] \\
&\qquad \mathbf{Pr}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) = i \mid \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bY) = k\right] \\
&= \sum_{k\in\mathsf{F}_q} \mathbf{Pr}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(cZ) = j \mid \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bY) = k\right] \\
&\qquad \mathbf{Pr}\left[\mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bY) = k \mid \mathbf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) = i\right] \\
&= \sum_{k\in\mathsf{F}_q} \left[\mathbf{LT}^{C^{(2)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(b,c)\right]_{k,j} \left[\mathbf{LT}^{C^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)\right]_{i,k}
\end{aligned}$$

which concludes the proof. □

In what follows, we will consider that the hypothesis of Property 1 is always verified.

3.3 Some useful properties

In this paragraph, we denote by $\mathbf{U}$ the $q \times q$ matrix such that $[\mathbf{U}]_{i,j} = \frac{1}{q}$ for all $i, j \in \{0, \ldots, q-1\}$. We also consider two $q \times q$ transition matrices $\mathbf{LT}$ and $\mathbf{LT}^{'}$ of some permutations and their corresponding bias matrices $\mathbf{LB}$ and $\mathbf{LB}$, such that :

$$\mathbf{LT} = \mathbf{U} + \mathbf{LB} \quad \text{and} \quad \mathbf{LT}^{'} = \mathbf{U} + \mathbf{LB}^{'} .$$

We denote $[\mathsf{LB}]_{i,j} = \epsilon_{i,j}$ and $[\mathsf{LB}^{'}]_{i,j} = \delta_{i,j}$ for $i, j \in \{0, \dots, q-1\}$. We also denote by P a random permutation matrix. We recall there are exactly $q!$ such $q \times q$ transition matrices. We call P the associated permutation of $\{0, \dots, p-1\}$ such that:

$$[P \times \mathsf{LT}]_{i,j} = [\mathsf{LT}]_{\mathsf{P}(i),j} \ .$$

Finally, M denotes any $q \times q$ matrix.

Property 2. *For any transition matrices* LT *and* $\mathsf{LT}^{'}$ *and any permutation matrix* P *we have:*

$$\mathsf{LT} = P \times \mathsf{LT}^{'} \quad \Leftrightarrow \quad \mathsf{LB} = P \times \mathsf{LB}^{'} \ .$$

Proof. We have:

$$\begin{aligned} \mathsf{LT} = P \times \mathsf{LT}^{'} &\Leftrightarrow \mathsf{LT} - \mathsf{U} = P \times \mathsf{LT}^{'} - \mathsf{U} \\ &\Leftrightarrow \mathsf{LB} = P \times \left(\mathsf{LT}^{'} - \mathsf{U}\right) \\ &\Leftrightarrow \mathsf{LB} = P \times \mathsf{LB}^{'} \ . \end{aligned}$$

□

Property 3. *For any* $q \times q$ *matrix* M *we have:*

$$\| P \times M \|_2^2 = \| M \times P \|_2^2 = \| M \|_2^2$$

Proof. We have:

$$\| P \times M \|_2^2 = \sum_{i,j} [M]^2_{\mathsf{P}(i),j} = \sum_{i,j} [M]^2_{i,j} = \| M \|_2^2 \ .$$

□

Property 4. *For any transition matrix* LT *of some permutation, and the corresponding bias matrix* LB*, we have:*

$$\mathsf{U} \times \mathsf{LT} = \mathsf{LT} \times \mathsf{U} = \mathsf{U} \quad \textit{and} \quad \mathsf{U} \times \mathsf{LB} = \mathsf{LB} \times \mathsf{U} = 0 \ .$$

Proof. We have:

$$[\mathsf{U} \times \mathsf{LT}]_{i,j} = \sum_{l} [\mathsf{U}]_{i,l} [\mathsf{LT}]_{l,j} = \frac{1}{q} \sum_{l} [\mathsf{LT}]_{l,j} = \frac{1}{q}$$

as LT is a transition matrix. The equality holds for $\mathsf{LT} \times \mathsf{U}$ because LT is the transition matrix of a permutation, thus the coefficients of a column also sum to one. The other equality is a corollary of the previous one. □

Property 5. *Considering two transition matrices* LT *and* $\mathsf{LT}^{'}$ *of two permutations and their corresponding bias matrices* LB *and* $\mathsf{LB}^{'}$*, we have:*

$$\mathsf{LT} \times P \times \mathsf{LT}^{'} = \mathsf{U} + \mathsf{LB} \times P \times \mathsf{LB}^{'}$$

Proof. Using property 4 we have:

$$\begin{aligned}\mathsf{LT} \times P \times \mathsf{LT}^{'} &= (\mathsf{U} + \mathsf{LB}) \times P \times (\mathsf{U} + \mathsf{LB}^{'}) \\ &= \mathsf{U} \times P \times \mathsf{U} + \mathsf{U} \times P \times \mathsf{LB}^{'} + \mathsf{LB} \times P \times \mathsf{U} + \mathsf{LB} \times P \times \mathsf{LB}^{'} \\ &= \mathsf{U} + \mathsf{U} \times \mathsf{LB}^{'} + \mathsf{LB} \times \mathsf{U} + \mathsf{LB} \times P \times \mathsf{LB}^{'} \\ &= \mathsf{U} + \mathsf{LB} \times P \times \mathsf{LB}^{'}\end{aligned}$$

□

Corollary 1.

$$\| \mathsf{LT} \times P \times \mathsf{LT}^{'} - \mathsf{U} \|_2 = \| \mathsf{LB} \times P \times \mathsf{LB}^{'} \|_2 \ .$$

From what we have just seen we conclude that in order to evaluate the efficency of a transition matrix of the the type $P_1 \times \mathsf{LT} \times P_2 \times \mathsf{LT}^{'}$, it is sufficient to compute the euclidian norm of the matrix $\mathsf{LB} \times P_2 \times \mathsf{LB}^{'}$ as the previous properties show that:

$$\begin{aligned}\| P_1 \times \mathsf{LT} \times P_2 \times \mathsf{LT}^{'} - \mathsf{U} \|_2^2 &= \| P_1 \times (\mathsf{LT} \times P_2 \times \mathsf{LT}^{'} - \mathsf{U}) \|_2^2 \\ &= \| \mathsf{LT} \times P_2 \times \mathsf{LT}^{'} - \mathsf{U} \|_2^2 \\ &= \| \mathsf{LB} \times P_2 \times \mathsf{LB}^{'} \|_2^2 \ .\end{aligned}$$

In the next paragraph, we study the mean of the last expression, considering every possible permutation matrix.

3.4 A first generalization of the piling-up lemma

The generalization

The following theorem states that the value of $\| \mathsf{LB} \times P \times \mathsf{LB}^{'} \|_2^2$ is proportional to the product of both euclidian norm of LB and $\mathsf{LB}^{'}$ if we consider the mean on every possible permutation matrix P. In the next chapters we will see that the bias matrix corresponding to the succession of a permutation, a key xoring and an another permutation (typical in a block cipher) can be written

$$\mathsf{LB} \times P \times \mathsf{LB}^{'}$$

where LB and $\mathsf{LB}^{'}$ correspond to the bias matrices of two layers, separated by a key xoring, represented by the permutation P. The next theorem can thus be considered like a generalization of the classic piling-up lemma of standard linear cryptanalysis.

Theorem 11. ***Generalized Piling-up lemma*** *We consider two bias matrices* LB *and* $\mathsf{LB}^{'}$ *corresponding to the bias matrices of some permutations. We also consider* P*, a random permutation matrix uniformly distributed. We have:*

$$\mathsf{E}_P \left[\| \mathsf{LB} \times P \times \mathsf{LB}^{'} \|_2^2 \right] = \frac{1}{q-1} \| \mathsf{LB} \|_2^2 \cdot \| \mathsf{LB}^{'} \|_2^2 \ .$$

Proof. We have:

$$[\mathsf{\mathbf{LB}} \times P \times \mathsf{\mathbf{LB}}^{'}]_{i,j} = \sum_{l} \epsilon_{i,l}\delta_{\mathsf{P}(l),j} \ .$$

Thus

$$\| \ \mathsf{\mathbf{LB}} \times P \times \mathsf{\mathbf{LB}}^{'} \ \|_2^2 = \sum_{i,j}\sum_{l,l'} \epsilon_{i,l}\delta_{\mathsf{P}(l),j}\epsilon_{i,l'}\delta_{\mathsf{P}(l'),j} \ .$$

We can compute the expectation of the last expression:

$$\begin{aligned}
\mathsf{\mathbf{E}}_P\left[\| \ \mathsf{\mathbf{LB}} \times P \times \mathsf{\mathbf{LB}}^{'} \ \|_2^2\right] &= \frac{1}{q!}\sum_{\mathsf{P}}\sum_{i,j}\sum_{l,l'} \epsilon_{i,l}\delta_{\mathsf{P}(l),j}\epsilon_{i,l'}\delta_{\mathsf{P}(l'),j} \\
&= \frac{1}{q!}\sum_{\mathsf{P}}\sum_{i,j}\sum_{l} \epsilon_{i,l}^2\delta_{\mathsf{P}(l),j}^2 + \frac{1}{q!}\sum_{\mathsf{P}}\sum_{i,j}\sum_{\substack{l,l' \\ l\neq l'}} \epsilon_{i,l}\delta_{\mathsf{P}(l),j}\epsilon_{i,l'}\delta_{\mathsf{P}(l'),j} \\
&= \frac{1}{q!}\sum_{i,j}\sum_{l} \epsilon_{i,l}^2 \sum_{\mathsf{P}} \delta_{\mathsf{P}(l),j}^2 + \frac{1}{q!}\sum_{i,j}\sum_{\substack{l,l' \\ l\neq l'}} \epsilon_{i,l}\epsilon_{i,l'} \sum_{\mathsf{P}} \delta_{\mathsf{P}(l),j}\delta_{\mathsf{P}(l'),j} \ .
\end{aligned}$$

However, we also have:

$$\begin{aligned}
\sum_{\mathsf{P}} \delta_{\mathsf{P}(l),j}^2 &= \sum_{\mathsf{P}}\left(\sum_{u} 1_{\mathsf{P}(l)=u}\right)\delta_{\mathsf{P}(l),j}^2 \\
&= \sum_{\mathsf{P}}\sum_{u} 1_{\mathsf{P}(l)=u}\delta_{u,j}^2 \\
&= \sum_{u}\delta_{u,j}^2 \sum_{\mathsf{P}} 1_{\mathsf{P}(l)=u} \\
&= (q-1)!\sum_{u}\delta_{u,j}^2 \ ,
\end{aligned}$$

and

$$\begin{aligned}
\sum_{\mathsf{P}} \delta_{\mathsf{P}(l),j}\delta_{\mathsf{P}(l'),j} &= \sum_{\mathsf{P}} \left(\sum_{\substack{u,u'\\ u\neq u'}} 1_{\substack{\mathsf{P}(l)=u\\ \mathsf{P}(l')=u'}} \right) \delta_{\mathsf{P}(l),j}\delta_{\mathsf{P}(l'),j} \\
&= \sum_{\mathsf{P}} \sum_{\substack{u,u'\\ u\neq u'}} 1_{\substack{\mathsf{P}(l)=u\\ \mathsf{P}(l')=u'}} \delta_{u,j}\delta_{u',j} \\
&= \sum_{\substack{u,u'\\ u\neq u'}} \delta_{u,j}\delta_{u',j} \sum_{\mathsf{P}} 1_{\substack{\mathsf{P}(l)=u\\ \mathsf{P}(l')=u'}} \\
&= (q-2)! \sum_{\substack{u,u'\\ u\neq u'}} \delta_{u,j}\delta_{u',j} \\
&= (q-2)! \sum_{u} \delta_{u,j} \sum_{\substack{u'\\ u'\neq u}} \delta_{u',j} \\
&= -(q-2)! \sum_{u} \delta_{u,j}^2 \ .
\end{aligned}$$

Thus :

$$\begin{aligned}
\mathbf{E}_P \left[\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2^2 \right] &= \frac{1}{q} \sum_{i,j} \sum_{l,u} \epsilon_{i,l}^2 \delta_{u,j}^2 - \frac{1}{q(q-1)} \sum_{i,j} \sum_{\substack{l,l'\\ l\neq l'}} \epsilon_{i,l}\epsilon_{i,l'} \sum_{u} \delta_{u,j}^2 \\
&= \frac{1}{q} \left(\sum_{i,l} \epsilon_{i,l}^2 \right) \left(\sum_{u,j} \delta_{u,j}^2 \right) \\
&\qquad - \frac{1}{q(q-1)} \sum_{i,j} \sum_{u} \sum_{l} \delta_{u,j}^2 \epsilon_{i,l} \sum_{\substack{l'\\ l\neq l'}} \epsilon_{i,l'} \\
&= \frac{1}{q} \| \mathbf{LB} \|_2^2 \cdot \| \mathbf{LB}' \|_2^2 + \frac{1}{q(q-1)} \sum_{i,j} \sum_{u} \sum_{l} \delta_{u,j}^2 \epsilon_{i,l}^2 \\
&= \frac{1}{q} \| \mathbf{LB} \|_2^2 \cdot \| \mathbf{LB}' \|_2^2 + \frac{1}{q(q-1)} \left(\sum_{i,l} \epsilon_{i,l}^2 \right) \left(\sum_{u,j} \delta_{u,j}^2 \right) \\
&= \frac{1}{q-1} \| \mathbf{LB} \|_2^2 \cdot \| \mathbf{LB}' \|_2^2 \ .
\end{aligned}$$

□

As we are going to see, this theorem offers only limited accuracy. We can notice that it is very easy to obtain an upper bound on $\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2^2$. We thus obtain a lower bound on the number of needed queries.

Property 6. *We consider two bias matrices* LB *and* $\mathsf{LB}^{'}$ *corresponding to the bias matrix of some permutation. We also consider* P*, a permutation matrix. We have:*

$$\| \mathsf{LB} \times P \times \mathsf{LB}^{'} \|_2^2 \leq \| \mathsf{LB} \|_2^2 \cdot \| \mathsf{LB}^{'} \|_2^2 \ . \tag{II.6}$$

Proof. The euclidian norm $\| \cdot \|_2$ is a matrix norm, thus

$$\| \mathsf{LB} \times P \times \mathsf{LB}^{'} \|_2^2 \leq \| \mathsf{LB} \|_2^2 \cdot \| P \times \mathsf{LB}^{'} \|_2^2 \ .$$

Using Property 3, we conclude that

$$\| \mathsf{LB} \times P \times \mathsf{LB}^{'} \|_2^2 \leq \| \mathsf{LB} \|_2^2 \cdot \| \mathsf{LB}^{'} \|_2^2 \ .$$

□

Practical tests on the accuracy of the piling-up lemma

In the next chapter we will see that the permutation matrix P_k resulting from a subkey xoring will have the following shape:

$$[P_k]_{i,j} = [I]_{i \oplus k,j} \quad \forall i,j,k \in \mathsf{F}_q \ ,$$

where I the identity matrix and where k is a random variable uniformly distributed on F_q. Suppose now that we want an approximation of the bias matrix corresponding to one round with a bias matrix LB, followed by a subkey xoring which implies a permutation matrix P_k, followed by another round with a bias matrix $\mathsf{LB}^{'}$. Using Property 2 with know that the bias matrix of the whole system is simply $\mathsf{LB} \times P_k \times \mathsf{LB}^{'}$. Suppose that we want to compute the euclidian norm of this matrix. As the permutation matrix is unknown, we use the piling-up lemma in order to approximate the needed value. We can then wonder about the accuracy of the result.

In order to test the accuracy of Theorem 11, we propose some practical results, shown on Figure II.2. Here we represent

$$\mathrm{err}_q = \max_k \left(\frac{\left| \| \mathsf{LB} \times P_k \times \mathsf{LB}^{'} \|_2^2 - \frac{1}{q-1} \| \mathsf{LB} \|_2^2 \| \mathsf{LB}^{'} \|_2^2 \right|}{\frac{1}{q-1} \| \mathsf{LB} \|_2^2 \| \mathsf{LB}^{'} \|_2^2} \right) \tag{II.7}$$

in function of $\epsilon_{\max}$, the maximum value of any entry of bias matrices. Both LB and $\mathsf{LB}^{'}$ are chosen randomly, according to this specification. Equation (II.7) represents the worst case, i.e. the case where the theorem has the worst precision. On Figure II.2 we show the results of several experiments (modifying the value of $\epsilon_{\max}$) in three different cases, whether q is 2, 4 or 16.

We first notice that the theorem is not an approximation but a perfect result in the case where $q = 2$, i.e. we can write:

$$\| \mathsf{LB} \times P_k \times \mathsf{LB}^{'} \|_2^2 \ = \ \| \mathsf{LB} \|_2^2 \| \mathsf{LB}^{'} \|_2^2 \quad \forall k \in \mathsf{F}_2 \ .$$

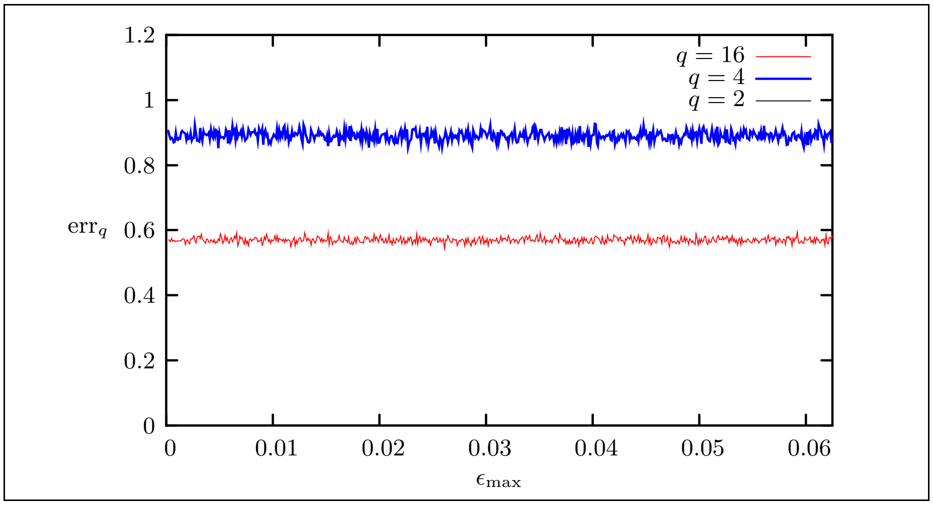


Figure II.2: Accuracy of the generalized piling-up lemma when q is 2, 4 or 16

We see that the bigger the cardinal of the arrival field of the trace, the worst precision we obtain in the worst case. We also see that the worst case seems somehow independent of $\epsilon_{\max}$ (the maximum value of all entries of the bias matrix).

Another interesting results are shown on Figure II.4 and II.5. Considering the case $q = 4$, it seems that the variable err_q^k defined by

$$\mathrm{err}_q^k = \frac{\left| \| \mathbf{LB} \times P_k \times \mathbf{LB}^{'} \|_2^2 - \frac{1}{q-1} \| \mathbf{LB} \|_2^2 \| \mathbf{LB}^{'} \|_2^2 \right|}{\frac{1}{q-1} \| \mathbf{LB} \|_2^2 \| \mathbf{LB}^{'} \|_2^2} \tag{II.8}$$

can take four different types of values. We see on Figure II.4 that $\mathrm{err}_q^k \approx 0.57$, 0.41 , 0.25 or 0.16. A similar results can be obtained for $q = 16$, where err_q^k seems to take sixteen different types of values.

It also seems that that those typical values cannot be linked to particular value of k. For example when $q = 4$ and $k = 0$, err_4^0 is approximatively equal to 0.57 one time over four. We cannot conclude anything though, as the bias matrix used for the study where chosen at random, which in a real attack is not going to be the case.

In order to complete this practical study, we compute err_q^k when $\mathbf{LB}$ and $\mathbf{LB}^{'}$ are not computed at random but defined by AES substitution box and using the masks (0x08,0x55) and (0x08,0x9B) respectively. In the next section we show how to compute these two matrices:

$$\mathsf{LB} = \begin{pmatrix} -0.062500 & -0.062500 & 0.187500 & -0.062500 \\ 0.062500 & 0.031250 & -0.062500 & -0.031250 \\ 0.000000 & 0.000000 & -0.093750 & 0.093750 \\ 0.000000 & 0.031250 & -0.031250 & 0.000000 \end{pmatrix},$$

$$\mathsf{LB}' = \begin{pmatrix} -0.062500 & -0.062500 & -0.062500 & 0.187500 \\ 0.062500 & -0.031250 & 0.031250 & -0.062500 \\ 0.000000 & 0.093750 & 0.000000 & -0.093750 \\ 0.000000 & 0.000000 & 0.031250 & -0.031250 \end{pmatrix}.$$

The obtained results are shown on Figure II.3.

k	0	1	2	3
err_q^k	0.093688	0.736686	0.874753	0.505917

Figure II.3: Values of err_q^k when LB and LB' are defined by AES S-box

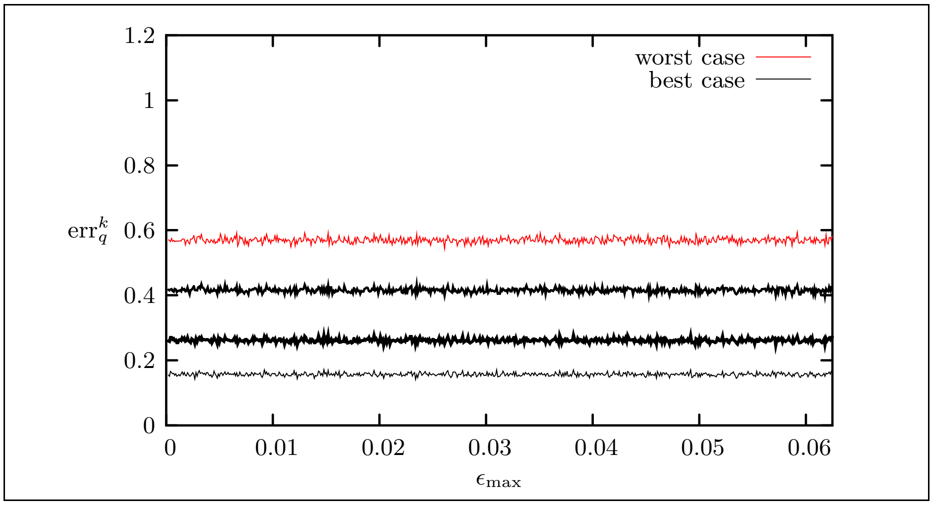


Figure II.4: Mean distance between the true bias and the bias approximated by the piling-up lemma, when $q = 4$

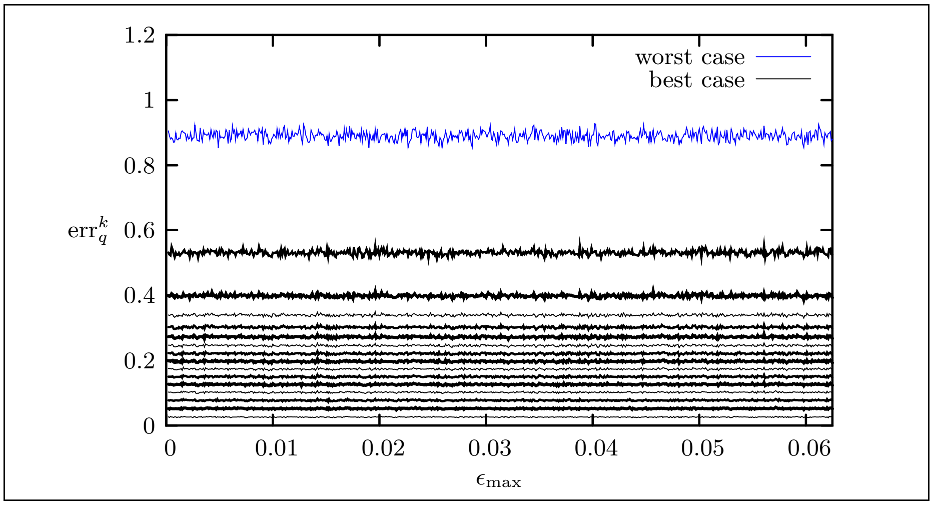


Figure II.5: Mean distance between the true bias and the bias approximated by the piling-up lemma, when $q = 16$

3.5 Why there is no second generalization of the piling-up lemma (yet)

We try to provide here an another type of generalization. Whereas the previous study gives an equality on $\mathbf{E}_P\left[\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2^2\right]$, this study tries to give a lower bound on $\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2^2$, independent of P. In other words, this will corresponds to an upper bound on the number of needed plaintext/ciphertext couples for generalized cryptanalysis. This research is motivated by the fact that the preceeding generalization accuracy seems very limited.

A mathematical property of definite positive matrices

Definition 13. ***Positive Definite Matrix*** *A $q \times q$ real matrix A is called positive definite if*

$$x^T A x > 0 \tag{II.9}$$

for all nonzero vectors $x \in \mathcal{R}^q$, where x^T denotes the transpose.

The following theorem is proved in [Dan01]. It gives a lower bound on the trace of the product of two positive definite matrices.

Theorem 12. *If A and B are two $q \times q$ positive definite matrices then*

$$q\left(|A| \cdot |B|\right)^{\frac{m}{q}} \leq tr\left(A^m B^m\right) \tag{II.10}$$

for any positive integer m, and where $|\cdot|$ denotes the matrix determinant.

We will make use of a specific case of the preceeding theorem.

Corollary 2. *If A and B are two $q \times q$ positive definite matrices then*

$$tr\,(AB) \;\geq\; q(|A|\,|B|)^{\frac{1}{q}}\ , \tag{II.11}$$

where $|\cdot|$ denotes the matrix determinant.

Definition 14. *Let A be a $q \times q$ real matrix. A is said to be nonsingular iff $|A| \neq 0$, where $|\cdot|$ denotes the determinant of a matrix.*

One last property about positive definite matrices will be used.

Property 7. *For any nonsingular matrix M, the matrix $M^{\mathrm{T}}M$ is positive definite.*

Proof. For any vector $x \neq 0$,

$$\begin{aligned} x^{\mathrm{T}}(M^{\mathrm{T}}M)x &= (Mx)^{\mathrm{T}}(Mx) \\ &= \parallel Mx \parallel_2^2 \end{aligned}$$

But

$$\begin{aligned} \parallel Mx \parallel_2^2 = 0 &\Leftrightarrow \ Mx = 0 \\ &\Leftrightarrow \ 0 \text{ is an eigen value of M} \\ &\Leftrightarrow \ |M| = 0 \end{aligned}$$

which is impossible as M is nonsingular. □

Where we generalize the piling-up lemma and explain why it doesn't work

In this generalization, we search for a lower bound on $\parallel \mathsf{LB} \times P \times \mathsf{LB}' \parallel_2^2$, which would be independent of P. The following theorem gives such a bound for nonsingular matrices.

Theorem 13. *Let A and B be two real nonsingular $q \times q$ matrices and let P be a permutation matrix. We have:*

$$\parallel A \times P \times B \parallel_2^2 \geq \; q(|A|\,|B|)^{\frac{2}{q}}\ . \tag{II.12}$$

Proof. We have:

$$\begin{aligned} \parallel A \times P \times B \parallel_2^2 &= \operatorname{tr}\left((A \times P \times B) \times (A \times P \times B)^T\right) \\ &= \operatorname{tr}\left(A \times P \times B \times B^T \times P^T \times A^T\right) \\ &= \operatorname{tr}\left(A^T \times A \times P \times B \times B^T \times P^T\right) \\ &= \operatorname{tr}\left(A^T \times A \times (P \times B) \times (P \times B)^T\right) \end{aligned}$$

Let $A' = A^T \times A$ and $B' = (P \times B) \times (P \times B)^T$. By Property 7, as A is nonsingular, then A' is positive definite. As B is non singular, we have $|P \times B| = |P|\,|B| \neq 0$ as $|P| \neq 0$ and $|B| \neq 0$. Thus $P \times B$ is nonsingular. Following Property 7, this implies that B' is positive definite. We thus can apply Theorem 12:

$$\begin{aligned}
\| A \times P \times B \|_2^2 &= \operatorname{tr}\left(A' \times B'\right) \\
&\geq n(\left|A'\right| \left|B'\right|)^{\frac{1}{n}} \\
&= n(\left|A^T \times A\right| \left|P \times B \times B^T \times P^T\right|)^{\frac{1}{n}} \\
&= n(|A|^2\,|B|^2 \left|P \times P^T\right|)^{\frac{1}{n}} \\
&= n(|A|^2\,|B|^2\,|I|)^{\frac{1}{n}} \\
&= n(|A|\,|B|)^{\frac{2}{n}} .
\end{aligned}$$

□

The last theorem could gives us a very useful bound, namely that

$$\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2^2 \geq\ q(|\mathbf{LB}| \left|\mathbf{LB}'\right|)^{\frac{2}{q}} .$$

The only problem is that a linear bias matrix is such that the sum of all columns gives 0, so that the determinant of any linear bias matrix is null. These kind of matrices are thus always singular, Theorem 13 does NOT apply to them. However, it is still possible to give some kind of generalization of the piling-up lemma.

Theorem 14. ***(Another generalization of the piling-up lemma)*** *We consider two $q \times q$ bias matrices $\mathbf{LB}$ and $\mathbf{LB}'$ corresponding to the bias matrices of some permutations. We also consider P a permutation matrix. If there exists two nonsingular $q \times q$ matrices A and B such that*

$$\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2 \geq \| A \times P \times B \|_2 ,$$

then

$$\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2^2 \geq\ q(|A|\,|B|)^{\frac{2}{q}} .$$

Proof. We know that $\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2 \geq \| A \times P \times B \|_2$. As A and B are nonsingular, then we can apply Theorem 13 and obtain the announced result. □

Why this is not a generalization (yet)

We have seen that it is somehow possible to find a lower bound on $\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2$ under the condition to find two appropriate nonsingular matrices A and B such that $\| \mathbf{LB} \times P \times \mathbf{LB}' \|_2 \geq \| A \times P \times B \|_2$. However, finding such matrices doesn't seems to be an easy task, and this why Theorem 14 cannot be considered as a true generalization.

4 Case study : The AES S-box

In this section, we are going to test experimentally the results obtained in the past sections. $\mathsf{LT}^S_{\mathsf{F}_{2^8}/\mathsf{F}_q}$ (resp. $\mathsf{LT}^*_{\mathsf{F}_{2^8}/\mathsf{F}_q}$) will denote the transition matrix of the permutation of F_{2^8} defined by the S-box of AES (resp. the random permutation of F_{2^8} uniformly distributed C^*). The corresponding bias matrices will be denoted $\mathsf{LB}^S_{\mathsf{F}_{2^8}/\mathsf{F}_q}$ and $\mathsf{LB}^*_{\mathsf{F}_{2^8}/\mathsf{F}_q}$ respectively. We note that $\mathsf{LT}^S_{\mathsf{F}_{2^8}/\mathsf{F}_q}$ (and thus $\mathsf{LB}^S_{\mathsf{F}_{2^8}/\mathsf{F}_q}$) depends on the applied mask on the AES S-box. If the mask is denoted (a, b), the corresponding transition matrix will be denoted $\mathsf{LT}^S_{\mathsf{F}_{2^8}/\mathsf{F}_q}(a, b)$. Similarly, the corresponding bias matrix will be denoted $\mathsf{LB}^S_{\mathsf{F}_{2^8}/\mathsf{F}_q}(a, b)$. To simplify notations, we will drop the subscript on these definitions. However we should keep in mind that q is the cardinal of the trace arrival space, such that $\log(q)$ should divide 8, as the AES S-box is defined over 2^8.

Our experiment consists in two parts. In the first one, we look for the best couples (a, b) such that the number of queries needed to distinguish LT^S from LT^* is minimal (given a fixed probability of error). In the second one, we consider an oracle which implements either LT^S or LT^*. Our distinguisher asks n questions to it and takes a decision $\widehat{\mathsf{LT}}$. We iterate this algorithm and compute the number of errors it makes.

4.1 Finding the best mask

We use Algorithm 5 in order to find the best masks, i.e. those that minimize the number of questions needed to distinguish LT^S from LT^*.

When LB^S is close to LB^*, we recall that this number is computed according to the following equation:

$$n = \frac{1}{\| \mathsf{LB}^S \|_2^2},$$

which corresponds to a probability of error $P_e = 1 - \Phi\left(\frac{1}{2}\right) \approx 0.3085$ (see Theorem 6). When LB^S is far from LB^* (which we consider to be the case when LT^S has some 0 entry), the number of query is computed according to the following equation (see Theorem 7):

$$n \leq \frac{\log P_e}{\log \frac{|\mathsf{Supp}_T|}{q^2}}$$

For the computations we fix P_e to $1 - \Phi\left(\frac{1}{2}\right)$ and consider that the bound approximates the necessary number of queries. In the algorithm $n(a, b)$ corresponds to this experimental computation when the mask used on AES S-box is (a, b).

```
Parameters: An S-box $S$ defining a permutation over $\mathsf{F}_{q^m}$, a $(q^m-1)\times(q^m-1)$ matrix $n$ s.t. $n(a,b)$ is the evaluation of the number of queries needed to distinguish $\mathsf{LT}^S(a,b)$ from $\mathsf{LT}^*$.
Input: The cardinal of the arrival space of the trace $q$.
for every $(a,b) \in \mathsf{F}^*_{q^m} \times \mathsf{F}^*_{q^m}$ do
    for every $X \in \mathsf{F}_{q^m}$ do
        Compute $i \leftarrow \mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX)$
        Compute $j \leftarrow \mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bS(X))$
        Increment $[\mathsf{LT}(a,b)]_{i,j}$
    end for
    Compute $\mathsf{LT}(a,b) \leftarrow \frac{1}{q^{m-1}}\mathsf{LT}(a,b)$
    Compute the bias matrix $\mathsf{LB}(a,b)$ corresponding to $\mathsf{LT}(a,b)$
    if $\mathsf{LT}$ is distant from $\mathsf{LT}^*$ then
        Compute $n(a,b) \leftarrow \frac{1.67}{2\log q - \log\left|\mathsf{Supp}_{\mathsf{LT}}\right|}$
    else
        Compute $n(a,b) \leftarrow \| \mathsf{LB}(a,b) \|_2^{-2}$
    end if
end for
Display $(n(a,b),a,b)$ sorted by increasing $n(a,b)$
```

Algorithm 5: Finding the best couples (a,b)

F_2		F_{2^2}		F_{2^4}	
(a,b)	$n(a,b)$	(a,b)	$n(a,b)$	(a,b)	$n(a,b)$
(0x01,0x1E)	64.000000	(0x08,0x55)	13.128205	(0x 4,0x 8)	3.328335
(0x01,0x4A)	64.000000	(0x08,0x9B)	13.128205	(0x 4,0x21)	3.328335
(0x01,0x54)	64.000000	(0x08,0xCE)	13.128205	(0x 4,0x29)	3.328335
(0x01,0x66)	64.000000	(0x21,0x55)	13.128205	(0x 4,0x41)	3.328335
(0x01,0x78)	64.000000	(0x21,0x9B)	13.128205	(0x 4,0x49)	3.328335
(0x02,0x 3)	64.000000	(0x21,0xCE)	13.128205	(0x 4,0x60)	3.328335
(0x02,0x15)	64.000000	(0x97,0x55)	13.128205	(0x 4,0x68)	3.328335
(0x02,0x25)	64.000000	(0x97,0x9B)	13.128205	(0x 4,0x97)	3.328335
(0x02,0x26)	64.000000	(0x97,0xCE)	13.128205	(0x 4,0x9F)	3.328335
(0x02,0x33)	64.000000	(0x9F,0x55)	13.128205	(0x 4,0xB6)	3.328335
(0x03,0x 8)	64.000000	(0x9F,0x9B)	13.128205	(0x 4,0xBE)	3.328335
...	...	...	...	...	...
(0xFF,0xD9)	∞	(0xFC,0x7E)	170.666672	(0xFF,0x74)	4.456977
(0xFF,0xFE)	∞	(0xFC,0xB9)	170.666672	(0xFF,0x7A)	4.456977
(0xFF,0xFF)	∞	(0xFC,0xC7)	170.666672	(0xFF,0x7F)	4.456977

Figure II.6: First ten best masks (and worst three) when q is 2, 2^2 or 2^4

Figure II.6 presents the results when q is $1, 2$ or 4 respectively.
We can also see that making a bad mask choice in F_{2^4} is harmless (as the number of

questions needed is almost the same in the best case and in the worst case) whereas this choice is important in F_2.

4.2 Experimental probability of error

In this section we will first study the probability that the distinguisher decides that the Generator implements LT^* whereas it implements LT^S, which is the α probability of error defined in a past section. Then we will study the overall probability of error. In both cases, we consider three possible values of q.

Probability of error α

The first error we will study is the one where our distinguisher decides that the Generator implements the ideal transition matrix whereas it does not. The configuration is shown on Figure II.7.

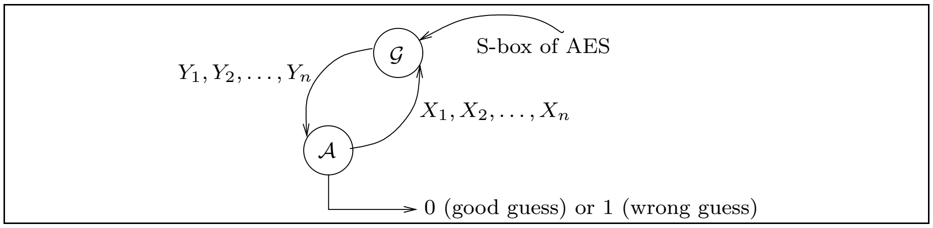


Figure II.7: Computing experimental α error

The idea is to iterate the experiment and compute an experimental probability of error depending on the complexity n (i.e. the number of allowed queries to the Generator). In other terms we compute the experimental value of α.
We apply this algorithm for the usual three different cases, i.e. when q is 2, 4 or 16. For each case the mask (a, b) is chosen according to the best result of Algorithm 5. The results of our experiments are given in Figure II.8. As one could expect, as the linear transition matrix of S contains some 0 when $q = 16$, the α error is 0 in that case.

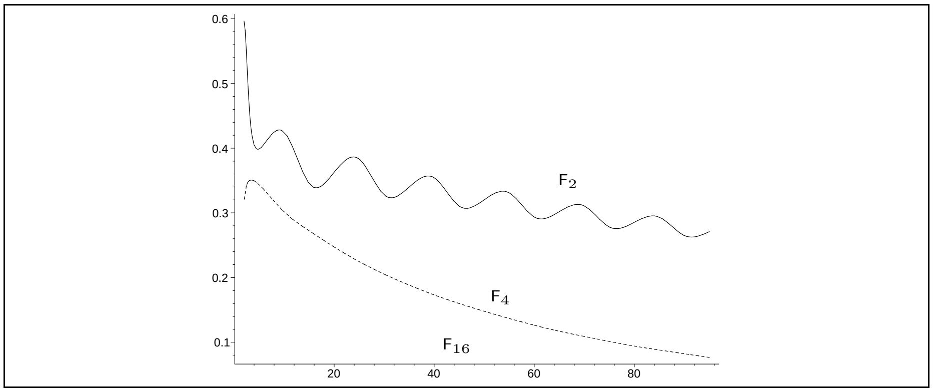


Figure II.8: Experimental α error in function of the number of allowed questions to the Generator

Parameters: A complexity n, a mask $(a, b) \in F^* \times F^*$, the corresponding transition matrix for the S-box $\mathsf{LT}^S_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a, b)$
Input: a Generator $\mathcal{G}$ which implements the AES S-box and outputs $S(X)$ for any query X.

```
for $i = 1, \ldots, n$ do
    Pick $X$ uniformly at random
    Compute $x_i \leftarrow \mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX)$
    Send $X$ to the Generator $\mathcal{G}$ and receive $Y$
    Compute $y_i \leftarrow \mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bY)$
end for
Compute LR $= q^n \prod_{i=1}^{n} [\mathsf{LT}^S_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a, b)]_{x_i, y_i}$
if LR $\geq 1$ then
    Output 0
else
    Output 1
end if
```

Algorithm 6: Experimental probability of error α

Overall probability of error

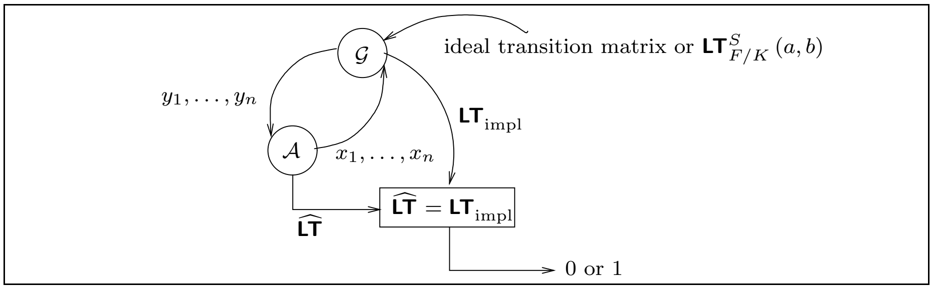

$\mathcal{G}$
ideal transition matrix or $\mathsf{LT}^{S}_{F/K}(a,b)$
$y_1,\ldots,y_n$
$\mathsf{LT}_{\text{impl}}$
$\mathcal{A}$
$x_1,\ldots,x_n$
$\widehat{\mathsf{LT}} = \mathsf{LT}_{\text{impl}}$
$\widehat{\mathsf{LT}}$
0 or 1

Figure II.9: Experimental overall probability of error

In an another approach we can compute an experimental overall probability of error. We consider a special type of Generator, shown on Figure II.9. It implements either the transition matrix $\mathsf{LT}^{S}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$ or the ideal transition matrix. The distinguisher asks n questions to it and then guess what the Generator implements. It can then ask a last question, namely what to Generator implements. The distinguisher then outputs 0 if its guess is right, 1 otherwise. This algorithm is iterated in order to obtain an experimental probability of error. Algorithm 7 implements it.

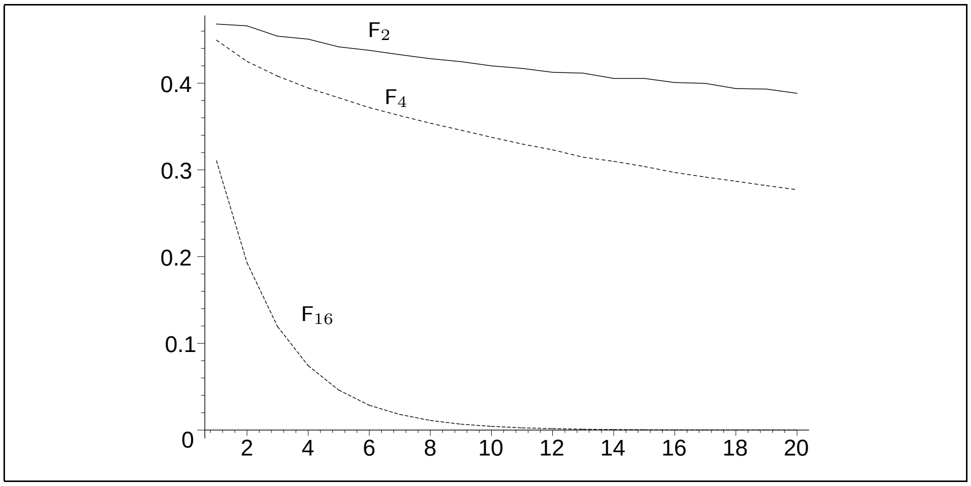


Figure II.10: Experimental overall probability of error function of the number of queries

```
**Parameters:** A complexity $n$, a mask $(a,b) \in F^* \times F^*$, the corresponding transition matrix for the S-box $\mathsf{LT}^{S}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$
**Input:** An Generator $\mathcal{G}$ which implements either the ideal transition matrix or $\mathsf{LT}^{S}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$ with equal probabilities
for $i = 1, \ldots, n$ do
    Pick $X$ uniformly at random
    Compute $x_i \leftarrow \mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX)$
    Send $x_i$ to the Generator $\mathcal{G}$ and reive $y_i$
end for
Compute $\mathrm{LR} = q^n \prod_{i=1}^{n} [\mathsf{LT}^{S}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)]_{x_i,y_i}$
if $\mathrm{LR} \geq 1$ then
    Set $\widehat{\mathsf{LT}} \leftarrow \mathsf{LT}^{S}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$
else
    Set $\widehat{\mathsf{LT}} \leftarrow \mathsf{LT}^*$
end if
Receive $\mathsf{LT}_{\mathrm{impl}}$ from the Generator $\mathcal{G}$
if $\widehat{\mathsf{LT}} = \mathsf{LT}_{\mathrm{impl}}$ then
    Output 0
else
    Output 1
end if
```

Algorithm 7: Experimental overall probability of error

Chapter III

Generalized Linear Cryptanalysis of a simple cipher

1 Description of the cipher

We now introduce a very simple SPN, represented on Figure $III.1$, which is inspired from a little cipher presented in [Hey99]. The block and the subkey are 16 bits long. The cipher is made of 3 identical rounds (a key xoring, an S-box layer and a permutation) followed by a round without permutation and an additional key xoring. The substitution box is AES S-box, it is represented on Figure III.2 in hexadecimal.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure III.2: The cipher's S-box $S(xy)$ where x designs a row and y a column

The permutation is described on Figure III.3. In that table, a number represents a

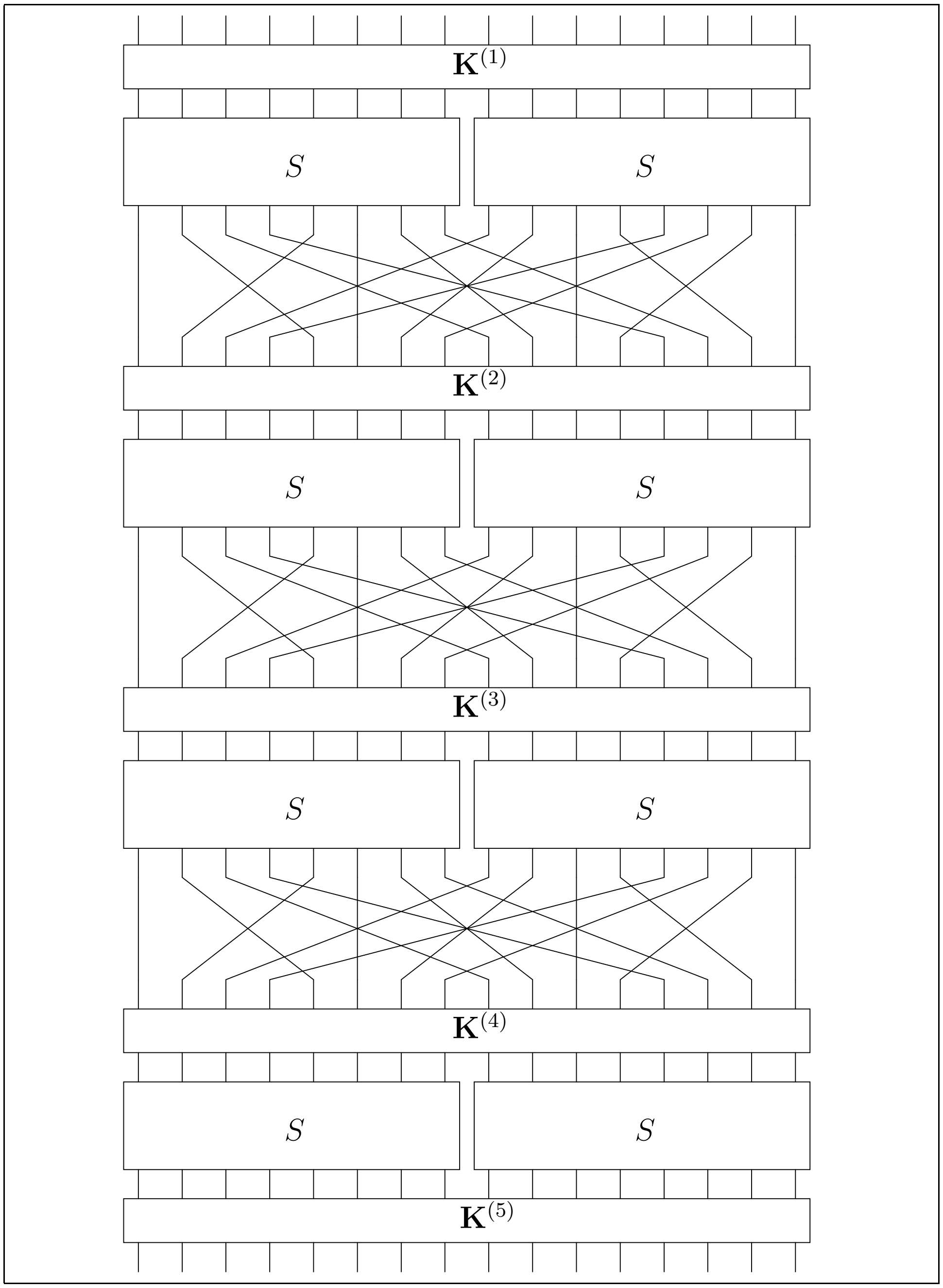


Figure III.1: A simple SPN

bit position, 1 being the leftmost bit.

input	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
output	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Figure III.3: The cipher's permutation

The key layer corresponds to a a bitwise xor between the subkey bits and the text bits. We consider the five subkeys of the cipher to be independent.

2 Notations

The input and the output of the cipher will be denoted $\mathbf{X}$ and $\mathbf{Y}$ respectively. The key of round $i \in \{1, 2, 3, 4, 5\}$ will be denoted $\mathbf{K}^{(i)}$. These values will be considered vectors of four elements in F_{16}, that is:

$$\mathbf{X} = \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix} \quad , \quad \mathbf{Y} = \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} \quad \text{and} \quad \mathbf{K}^{(i)} = \begin{pmatrix} K_0^{(i)} \\ K_1^{(i)} \\ K_2^{(i)} \\ K_3^{(i)} \end{pmatrix} \quad .$$

The input of round i will be denoted $\mathbf{X}^{(i)}$ and its output $\mathbf{Y}^{(\mathbf{i})}$. We thus have $\mathbf{X}^{(1)} = \mathbf{X}$ and $\mathbf{Y}^{(4)} = \mathbf{Y}$. When studying one single round, the output of the key-layer will be denoted $\mathbf{U}$ and the output of S-boxes layer $\mathbf{V}$. The most significant bit will always be on the left.

The definition of the transition matrix has to be slightly modified so it is adapted to our cipher. We will consider that it is defined in the following way :

$$[\mathsf{LT}^{C}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a}, \mathbf{b})]_{i,j} = \mathsf{Pr}\left[\mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{b} \cdot \mathbf{Y}) = j \mid \mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a} \cdot \mathbf{X}) = i\right] \ ,$$

where the $\cdot$ operation denotes the scalar product and where $\mathbf{a}$ and $\mathbf{b}$ are 16 bits masks considered like vectors of four elements in F_{16} :

$$\mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} \quad .$$

As the departure field of the trace is F_{16}, we can study two cases, whether the arrival space F_q is F_2 or F_4.

3 Unbalanced linear expressions vs. biased transition matrices

In a classical linear cryptanalysis, the attacker tries to find an unbalanced linear expression on the first four rounds of the cipher, the last subkey $\mathbf{K}^{(5)}$ excepted. In order to do this one would approximate the S-box by a linear expression, use it to approximate a full round of the cipher and then make use of the Piling-up Lemma in order to approximate the whole cipher without the last subkey layer. A good approximation involves a unbalanced linear expression. A linear expression is unbalanced when the LP coefficient is far from 0.

In our generalization, linear expressions will be replaced by transition matrices. In order to find good masks on the whole cipher starting with goods masks on S-boxes we had to generalize the Piling-up lemma. Before we use this we start by an exhaustive search on all possible transition matrices (i.e. all possible input/output masks $(\mathbf{a}, \mathbf{b})$) in order to find the best one (i.e. the one for which the euclidian norm of the corresponding bias matrix is maximum) for the first rounds of the cipher. This is what we do in the next paragraph. As the LP was a measure on the efficacity of a particular linear expression, it is replaced here by the inverse of the euclidian norm of the bias matrix. When this value is high, the matrix is close to the ideal transition matrix (i.e. the input/output mask is inefficient). When this value is low the matrix is biased.

4 Exhaustive search on input/output masks

We thus try to find biased transition matrices on the cipher without the last subkey and the last S-box layer. We have to use an exhaustive search on all possible $(\mathbf{a}, \mathbf{b})$ values. We should note that this search is key dependent, i.e. the matrices that we are looking for will depend on the key values. This should not be the case as the biased transition matrix used during the attack should be efficient for any possible keys. The idea will be to find some key-dependent biased transition matrices and then select the most effective ones, that is those that stay effective even if the subkeys of the cipher change.

We thus first fix the subkey values. For our experiment we have chosen the following random values

$$(\mathbf{K}^{(1)}, \mathbf{K}^{(2)}, \mathbf{K}^{(3)}, \mathbf{K}^{(4)}, \mathbf{K}^{(5)}) = (\texttt{0x3f3b}, \texttt{0xa1d5}, \texttt{0x095a}, \texttt{0x71bb}, \texttt{0xd18e}) .$$

The best input/output masks (i.e. those that define the most biased transition matrices) are :

- (0x3600,0xd994) in F_2 (with $n(a, b) \approx 894$),

- (0x3600,0xd994), (0x9100,0xd994) and (0xa700,0xd994) in F_4 (with $n(a,b) \approx 687$).

In order to find them, 128 SUN Ultra 10 where used during approximately 3 days for each field.

5 Analysis of the cipher

In order to make the cryptanalysis of the cipher in F_{16}, we first have to represent it in a different way. Whereas the permutation is a linear transformation in F_2, it is not linear anymore in F_{16}. We will thus *group* the bits by group of 4 and try to represent the permutation in a suitable way for the attack. We consider here one round of the cipher (i.e. one key layer, one S-box layer and one permutation layer). We see that it can be represented like on Figure III.4. We have splitted the permutation into three permutations. The resulting round is equivalent to the previous one.
We now denote by S_1 the S-box containing the AES S-box and the first part of the permutation. On Figure III.5 we show the resulting round of the cipher, followed by the key layer of the following round.

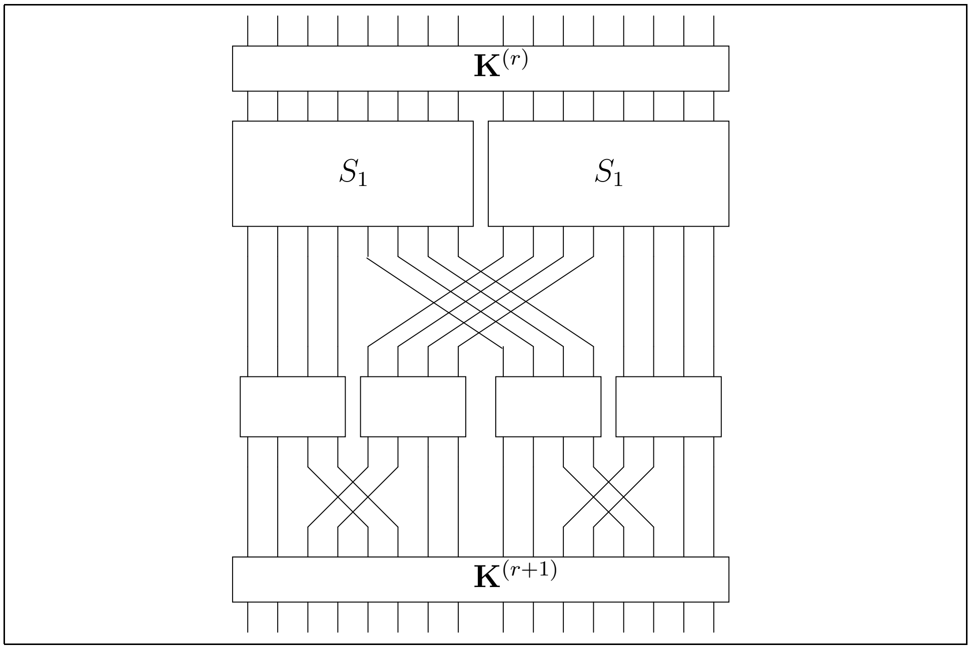


Figure III.5: Second analysis of one round of the cipher

We consider now the cipher part consisting of the last permutation and the key layer $\mathbf{K}^{(r+1)}$. In order to simplify the notation, we just name the key $\mathbf{K}$. This part is equivalent to a key layer $\tilde{\mathbf{K}}$ followed by the same permutation (see Figure III.6) such that:

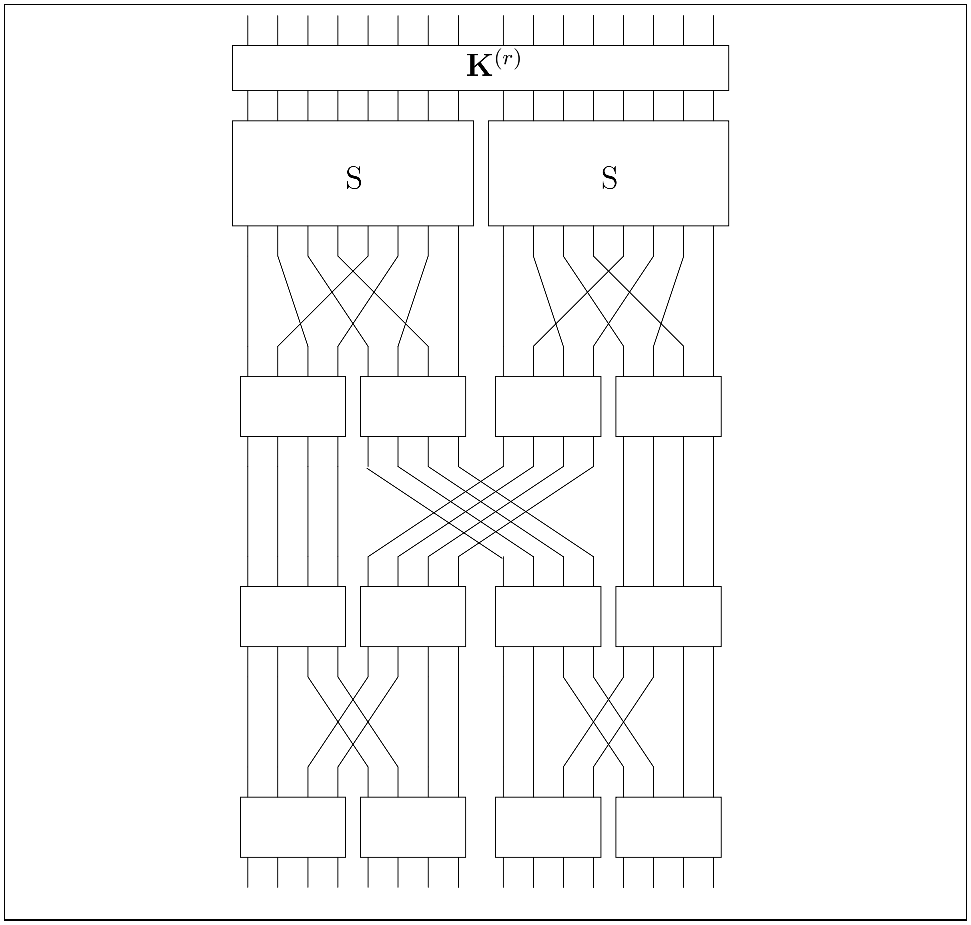


Figure III.4: First analysis of one round of the cipher

$$\begin{pmatrix} \tilde{K}_0 \\ \vdots \\ \tilde{K}_{15} \end{pmatrix} = \begin{pmatrix} P & 0 \\ 0 & P \end{pmatrix} \times \begin{pmatrix} K_0 \\ \vdots \\ K_{15} \end{pmatrix} ,$$

with $K_0, \ldots, K_{15}, \tilde{K}_0, \ldots, \tilde{K}_{15} \in \mathsf{F}_2$ and

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

After this inversion between the key layer and the permutation, we can integrate the last permutation of round r into the s-box layer of round $r+1$. We show the final cipher on Figure III.8. On this cipher we see three types of S-box : S_1, S_2 and S_3. According to the previous analysis, these S-boxes are such that :

- $S_1 \equiv S$ followed by the first part of the initial permutation

- $S_2 \equiv$ the last part of the initial permutation followed by S, followed by the first part of the initial permutation

- $S_3 \equiv$ the last part of the initial permutation followed by S.

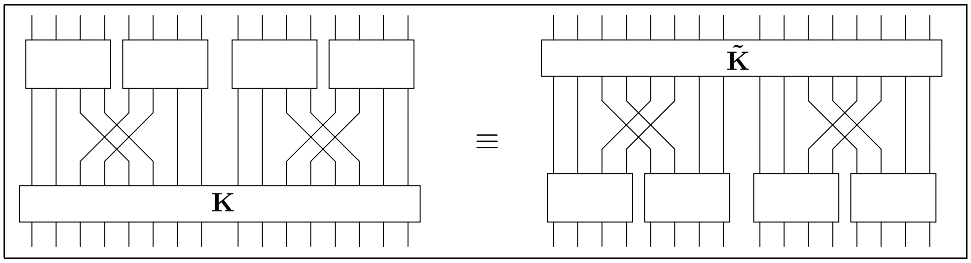


Figure III.6: Third analysis of the cipher

6 A transition matrix on one round of the cipher

6.1 The study

We consider here one round of the cipher (the analyzed version). We denote by $\mathbf{X}$ the round input and by $\mathbf{Y}$ the round output. We also name $\mathbf{U}$ and $\mathbf{V}$ the input and the output of the round S-box respectively. Here we simply denote by $\mathbf{K}$ the round subkey and by S_i the round S-box. We summarize these notations on Figure III.7.

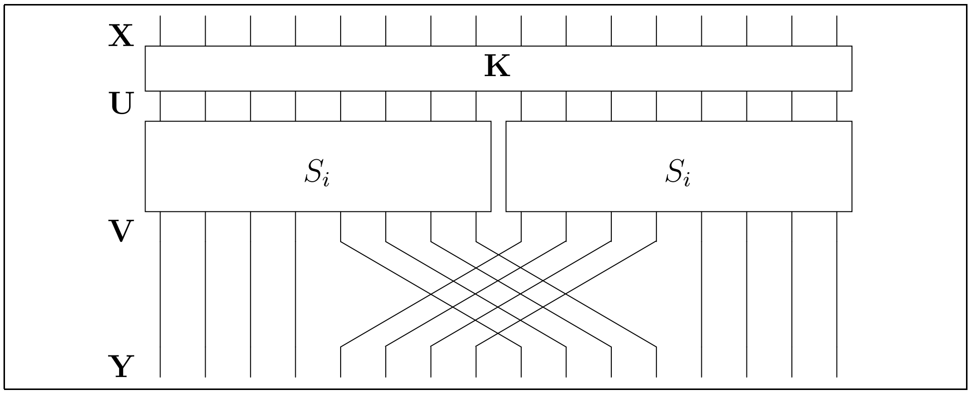


Figure III.7: One round of the analyzed SPN

We can now try to compute a transition matrix on one round R :

$$\begin{aligned}
[\mathsf{LT}^{\mathsf{R}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b})]_{i,j} &= \mathsf{Pr}_{\mathbf{X}}\left[\mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{b}\cdot\mathbf{Y}) = j \mid \mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a}\cdot\mathbf{X}) = i\right] \\
&= \mathsf{Pr}_{\mathbf{X}}\left[\mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{b}\cdot\mathbf{Y}) = j \mid \mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a}\cdot(\mathbf{U}\oplus\mathbf{K})) = i\right] \\
&= \mathsf{Pr}_{\mathbf{X}}\left[\mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{b}\cdot\mathbf{Y}) = j \mid \mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a}\cdot\mathbf{U}) = i\oplus k\right] \ ,
\end{aligned}$$

with $k = \mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a}\cdot\mathbf{K})$. As $\mathbf{K}$ is a random variable uniformly distributed in F_{16} and as the trace is a balanced transformation from F_{16} onto F_q (see Th. 10), k is a random variable of F_q uniformly distributed. Thus:

$$[\mathsf{LT}^{\mathsf{R}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b})]_{i,j} = \mathsf{Pr}_{\mathbf{X}}\left[\mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\tilde{\mathbf{b}}\cdot\mathbf{V}\right) = j \mid \mathsf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a}\cdot\mathbf{U}) = i\oplus k\right]$$

with

$$\tilde{\mathbf{b}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \times \mathbf{b} \ .$$

We thus finally have

$$[\mathsf{LT}^{\mathsf{R}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b})]_{i,j} = \left[\mathsf{LT}^{\mathsf{S}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a},\tilde{\mathbf{b}}\right)\right]_{i\oplus k,j}$$

for every i and j of F_q. If I is the $q\times q$ identity matrix, we denote by P_k the matrix of permutation such that

$$[P_k]_{i,j} = [I]_{i\oplus k,j} \quad \forall\, i,j,k \in \mathsf{F}_q \ .$$

For one round of the cipher, we thus obtain

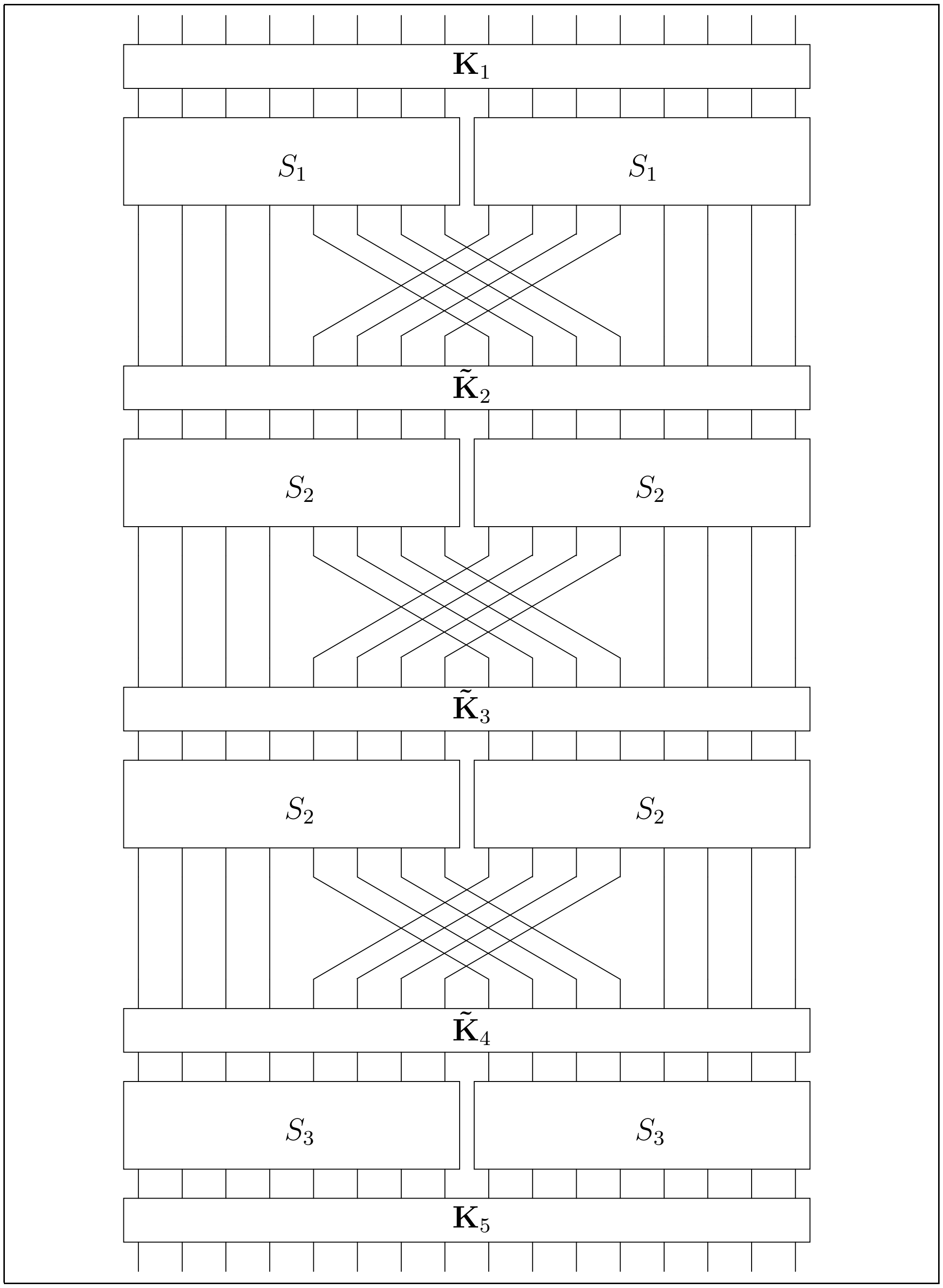


Figure III.8: The new equivalent shape of the simple SPN, with linear transformations in F_{16}

$$\boxed{\mathbf{LT}^{\mathsf{R}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a},\mathbf{b}\right) = P_k \times \mathbf{LT}^{\mathsf{S}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a},\tilde{\mathbf{b}}\right)} \tag{III.1}$$

We can note that if

$$\mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} b_0 \\ 0 \\ b_2 \\ 0 \end{pmatrix}$$

(i.e. only one S-box is active) we obtain :

$$\boxed{\mathbf{LT}^{\mathsf{R}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a},\mathbf{b}\right) = P_k \times \mathbf{LT}^{S_i}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a},\tilde{\mathbf{b}}\right)} \tag{III.2}$$

The general case is slightly more difficult to solve. What we want to obtain is an expression of $\mathbf{LT}_{\mathsf{F}_{16}/\mathsf{F}_q}$ which would involve the transition matrices of the S-boxes, and not the transition matrix of the S-box layer. We thus have to give an equation that allows to compute the transition matrix of the S-box layer according to the transition matrix of the S-box. In the following equations, we simply denote $\mathbf{LT}_{\mathsf{F}_{16}/\mathsf{F}_q}$ and $\mathbf{Tr}_{\mathsf{F}_{16}/\mathsf{F}_q}$ by $\mathbf{LT}$ and $\mathbf{Tr}$ respectively. If we use the notations

$$\mathbf{a}_{01} = \begin{pmatrix} a_0 \\ a_1 \\ 0 \\ 0 \end{pmatrix} , \mathbf{a}_{23} = \begin{pmatrix} 0 \\ 0 \\ a_2 \\ a_3 \end{pmatrix} , \mathbf{b}_{01} = \begin{pmatrix} b_0 \\ b_1 \\ 0 \\ 0 \end{pmatrix} , \mathbf{b}_{23} = \begin{pmatrix} 0 \\ 0 \\ b_2 \\ b_3 \end{pmatrix} ,$$

so that $\mathbf{a} = \mathbf{a}_{01} \oplus \mathbf{a}_{23}$ and that $\mathbf{b} = \mathbf{b}_{01} \oplus \mathbf{b}_{23}$ we have:

$$
\begin{aligned}
&\left[\mathbf{LT}^{\mathsf{S}}(\mathbf{a},\mathbf{b})\right]_{i,j} \\
&\quad= \mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}\cdot\mathbf{V}) = j \mid \mathbf{Tr}(\mathbf{a}\cdot\mathbf{U}) = i\right] \\
&\quad= q\,\mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}\cdot\mathbf{V}) = j, \mathbf{Tr}(\mathbf{a}\cdot\mathbf{U}) = i\right] \\
&\quad= q\sum_{l\in\mathsf{F}_q}\mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}\cdot\mathbf{V}) = j, \mathbf{Tr}(\mathbf{a}\cdot\mathbf{U}) = i, \mathbf{Tr}(\mathbf{b}_{01}\cdot\mathbf{V}) = l\right] \\
&\quad= q\sum_{l\in\mathsf{F}_q}\mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}_{23}\cdot\mathbf{V}) = j\oplus l, \mathbf{Tr}(\mathbf{a}\cdot\mathbf{U}) = i, \mathbf{Tr}(\mathbf{b}_{01}\cdot\mathbf{V}) = l\right] \\
&\quad= q\sum_{l,m\in\mathsf{F}_q}\mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}_{23}\cdot\mathbf{V}) = j\oplus l, \mathbf{Tr}(\mathbf{a}\cdot\mathbf{U}) = i,\right. \\
&\qquad\qquad\qquad\qquad\left.\mathbf{Tr}(\mathbf{b}_{01}\cdot\mathbf{V}) = l, \mathbf{Tr}(\mathbf{a}_{01}\cdot\mathbf{U}) = m\right] \\
&\quad= q\sum_{l,m\in\mathsf{F}_q}\mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}_{23}\cdot\mathbf{V}) = j\oplus l, \mathbf{Tr}(\mathbf{a}_{23}\cdot\mathbf{U}) = i\oplus m,\right. \\
&\qquad\qquad\qquad\qquad\left.\mathbf{Tr}(\mathbf{b}_{01}\cdot\mathbf{V}) = l, \mathbf{Tr}(\mathbf{a}_{01}\cdot\mathbf{U}) = m\right] \\
&\quad= q\sum_{l,m\in\mathsf{F}_q}\mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}_{01}\cdot\mathbf{V}) = l, \mathbf{Tr}(\mathbf{a}_{01}\cdot\mathbf{U}) = m\right] \\
&\qquad\qquad\qquad\mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}_{23}\cdot\mathbf{V}) = j\oplus l, \mathbf{Tr}(\mathbf{a}_{23}\cdot\mathbf{U}) = i\oplus m\right] \\
&\quad= \frac{1}{q}\sum_{l,m\in\mathsf{F}_q}\mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}_{01}\cdot\mathbf{V}) = l \mid \mathbf{Tr}(\mathbf{a}_{01}\cdot\mathbf{U}) = m\right] \\
&\qquad\qquad\qquad\mathbf{Pr}\left[\mathbf{Tr}(\mathbf{b}_{23}\cdot\mathbf{V}) = j\oplus l \mid \mathbf{Tr}(\mathbf{a}_{23}\cdot\mathbf{U}) = i\oplus m\right] \\
&\quad= \frac{1}{q}\sum_{l,m\in\mathsf{F}_q}\left[\mathbf{LT}^{\mathsf{S}}(\mathbf{a}_{01},\mathbf{b}_{01})\right]_{m,l}\left[\mathbf{LT}^{\mathsf{S}}(\mathbf{a}_{23},\mathbf{b}_{23})\right]_{i\oplus m,j\oplus l}
\end{aligned}
$$

If we set $u = i\oplus m$, we obtain:

$$
\begin{aligned}
\left[\mathsf{LT}^{\mathsf{S}}(\mathbf{a},\mathbf{b})\right]_{i,j} &= \frac{1}{q}\sum_{l,u\in\mathsf{F}_q}\left[\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{01},\mathbf{b}_{01})\right]_{i\oplus u,l}\left[\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{23},\mathbf{b}_{23})\right]_{u,j\oplus l} \\
&= \frac{1}{q}\sum_{l\in\mathsf{F}_q}\left(\sum_{u\in\mathsf{F}_q}\left[\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{23},\mathbf{b}_{23})\times P_j\right]_{u,l}\left[P_i\times\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{01},\mathbf{b}_{01})\right]_{u,l}\right) \\
&= \frac{1}{q}\sum_{l\in\mathsf{F}_q}\left(\sum_{u\in\mathsf{F}_q}\left[P_j\times{}^{T}\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{23},\mathbf{b}_{23})\right]_{l,u}\left[P_i\times\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{01},\mathbf{b}_{01})\right]_{u,l}\right) \\
&= \frac{1}{q}\sum_{l\in\mathsf{F}_q}\left[P_j\times{}^{T}\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{23},\mathbf{b}_{23})\times P_i\times\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{01},\mathbf{b}_{01})\right]_{l,l} \\
&= \frac{1}{q}\operatorname{Tr}\left(P_j\times{}^{T}\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{23},\mathbf{b}_{23})\times P_i\times\mathsf{LT}^{\mathrm{S}}(\mathbf{a}_{01},\mathbf{b}_{01})\right)\ .
\end{aligned}
$$

Finally, for one S-box layer of the cipher and when both S-boxes are active, we have:

$$
\boxed{\left[\mathsf{LT}^{\mathsf{S}}\left(\mathbf{a},\tilde{\mathbf{b}}\right)\right]_{i,j} = \frac{1}{q}\operatorname{Tr}\left(P_j\times{}^{T}\mathsf{LT}^{\mathrm{S}}\left(\mathbf{a}_{23},\tilde{\mathbf{b}}_{23}\right)\times P_i\times\mathsf{LT}^{\mathrm{S}}\left(\mathbf{a}_{01},\tilde{\mathbf{b}}_{01}\right)\right)}\ . \qquad \text{(III.3)}
$$

We can now give an expression for $\mathsf{LB}^{\mathsf{S}}\left(\mathbf{a},\tilde{\mathbf{b}}\right)$ (using Property 5):

$$
\begin{aligned}
\left[\mathsf{LB}^{\mathsf{S}}\left(\mathbf{a},\tilde{\mathbf{b}}\right)\right]_{i,j} &= \left[\mathsf{LT}^{\mathsf{S}}\left(\mathbf{a},\tilde{\mathbf{b}}\right)\right]_{i,j} - \frac{1}{q} \\
&= \frac{1}{q}\operatorname{Tr}\left(P_j\times{}^{T}\mathsf{LT}^{\mathrm{S}}\left(\mathbf{a}_{23},\tilde{\mathbf{b}}_{23}\right)\times P_i\times\mathsf{LT}^{\mathrm{S}}\left(\mathbf{a}_{01},\tilde{\mathbf{b}}_{01}\right)\right) - \frac{1}{q} \\
&= \frac{1}{q}\operatorname{Tr}\left(P_j\times{}^{T}\mathsf{LT}^{\mathrm{S}}\left(\mathbf{a}_{23},\tilde{\mathbf{b}}_{23}\right)\times P_i\times\mathsf{LT}^{\mathrm{S}}\left(\mathbf{a}_{01},\tilde{\mathbf{b}}_{01}\right) - \mathbf{U}\right) \\
&= \frac{1}{q}\operatorname{Tr}\left(P_j\times{}^{T}\mathsf{LB}^{\mathrm{S}}\left(\mathbf{a}_{23},\tilde{\mathbf{b}}_{23}\right)\times P_i\times\mathsf{LB}^{\mathrm{S}}\left(\mathbf{a}_{01},\tilde{\mathbf{b}}_{01}\right)\right)
\end{aligned}
$$

Thus:

$$
\boxed{\left[\mathsf{LB}^{\mathsf{S}}\left(\mathbf{a},\tilde{\mathbf{b}}\right)\right]_{i,j} = \frac{1}{q}\operatorname{Tr}\left(P_j\times{}^{T}\mathsf{LB}^{\mathrm{S}}\left(\mathbf{a}_{23},\tilde{\mathbf{b}}_{23}\right)\times P_i\times\mathsf{LB}^{\mathrm{S}}\left(\mathbf{a}_{01},\tilde{\mathbf{b}}_{01}\right)\right)} \qquad \text{(III.4)}
$$

6.2 Conclusions of the study

We have seen that the transition matrix of on round of the cipher can be written in the following way:

$$\mathsf{LT}^{\mathsf{R}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b}) = P_k \times \mathsf{LT}^{\mathsf{S}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a},\tilde{\mathbf{b}}\right) \ .$$

When only one S-box of the round is active, for example when

$$\mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} b_0 \\ 0 \\ b_2 \\ 0 \end{pmatrix} \ ,$$

then this equations becomes

$$\mathsf{LT}^{\mathsf{R}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b}) = P_k \times \mathsf{LT}^{S_i}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a},\tilde{\mathbf{b}}\right) \ .$$

When both S-boxes are active, we obtain:

$$\left[\mathsf{LT}^{\mathsf{S}}\left(\mathbf{a},\tilde{\mathbf{b}}\right)\right]_{i,j} = \frac{1}{q}\,\mathrm{Tr}\left(P_j \times {}^T\mathsf{LT}^{\mathrm{s}}\left(\mathbf{a}_{23},\tilde{\mathbf{b}}_{23}\right) \times P_i \times \mathsf{LT}^{\mathrm{s}}\left(\mathbf{a}_{01},\tilde{\mathbf{b}}_{01}\right)\right) \ ,$$

which leads to

$$\left[\mathsf{LB}^{\mathsf{S}}\left(\mathbf{a},\tilde{\mathbf{b}}\right)\right]_{i,j} = \frac{1}{q}\,\mathrm{Tr}\left(P_j \times {}^T\mathsf{LB}^{\mathrm{s}}\left(\mathbf{a}_{01},\tilde{\mathbf{b}}_{01}\right) \times P_i \times \mathsf{LB}^{\mathrm{s}}\left(\mathbf{a}_{01},\tilde{\mathbf{b}}_{01}\right)\right) \ .$$

From this study we also conclude that

$$\mathsf{LB}^{\mathsf{R}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b}) = P_k \times \mathsf{LB}^{\mathsf{S}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a},\tilde{\mathbf{b}}\right) \ ,$$

and thus that

$$\parallel \mathsf{LB}^{\mathsf{R}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b}) \parallel_2 = \parallel \mathsf{LB}^{\mathsf{S}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a},\tilde{\mathbf{b}}\right) \parallel_2 \ ,$$

So finding the best mask on one round of the cipher is equivalent to finding the best mask on the S-box layer of the cipher, which is in turn equivalent to finding the best mask on the S-box when only one is active. If both S-boxes are active, we have provided a formula that gives the value of the transition matrix of the S-box layer given the transition matrix of the S-box.

7 Piling-up rounds

7.1 Piling-up two rounds

We consider here two successive rounds $\mathsf{R}^{(r)}$ and $\mathsf{R}^{(r+1)}$. The previous study permits to find the transition matrix of $\mathsf{R}^{(r)}$ and the transition matrix of $\mathsf{R}^{(r+1)}$, both according the the corresponding subkeys k_k and k_{r+1}. We have :

$$\begin{aligned} \mathsf{LT}^{\mathsf{R}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\mathbf{a}^{(r+1)}\right) &= P_{k_r} \times \mathsf{LT}^{\mathsf{S}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\tilde{\mathbf{a}}^{(r+1)}\right) \ , \\ \mathsf{LT}^{\mathsf{R}^{(r+1)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r+1)},\mathbf{a}^{(r+2)}\right) &= P_{k_{r+1}} \times \mathsf{LT}^{\mathsf{S}^{(r+1)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r+1)},\tilde{\mathbf{a}}^{(r+2)}\right) \ . \end{aligned}$$

Using Property 1, the transition matrix on two rounds is thus :

$$\mathsf{LT}^{\mathsf{R}^{(r+1)}\circ\mathsf{R}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\mathbf{a}^{(r+2)}\right) = P_{k_r} \times \mathsf{LT}^{\mathsf{S}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\tilde{\mathbf{a}}^{(r+1)}\right) \times P_{k_{r+1}} \times \mathsf{LT}^{\mathsf{S}^{(r+1)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r+1)},\tilde{\mathbf{a}}^{(r+2)}\right) \; .$$

Using Property 5, this leads to

$$\mathsf{LB}^{\mathsf{R}^{(r+1)}\circ\mathsf{R}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\mathbf{a}^{(r+2)}\right) = P_{k_r} \times \mathsf{LB}^{\mathsf{S}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\tilde{\mathbf{a}}^{(r+1)}\right) \times P_{k_{r+1}} \times \mathsf{LB}^{\mathsf{S}^{(r+1)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r+1)},\tilde{\mathbf{a}}^{(r+2)}\right) \; .$$

What we are interested in is $\parallel \mathsf{LB}^{\mathsf{R}^{(r+1)}\circ\mathsf{R}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\mathbf{a}^{(r+1)}\right) \parallel_2^2$ as this is a measure on the efficency of the chosen mask for generalized linear cryptanalysis. This is where the generalized piling-up lemma becomes useful. Whereas $P_{k_{r+1}}$ and P_{k_r} cannot be any permutation matrix, we will consider that the Theorem 11 holds anyhow. Thus, we will consider that:

$$\begin{aligned}&\parallel \mathsf{LB}^{\mathsf{R}^{(r+1)}\circ\mathsf{R}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\mathbf{a}^{(r+2)}\right) \parallel_2^2 \\ &\qquad\approx \frac{1}{q-1} \parallel \mathsf{LB}^{\mathsf{S}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\tilde{\mathbf{a}}^{(r+1)}\right) \parallel_2^2 \cdot \parallel \mathsf{LB}^{\mathsf{S}^{(r+1)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r+1)},\tilde{\mathbf{a}}^{(r+2)}\right) \parallel_2^2\end{aligned}$$

7.2 Piling-up several rounds

Piling-up several rounds is just as easy as piling-up two rounds several times. In order to apply generalized linear cryptanalysis, we need a good approximation on the first 3 rounds of the cipher followed by the fourth round key. We simply denote $\mathsf{LB}_{\mathsf{F}_{16}/\mathsf{F}_q}$ the corresponding bias matrix. We have:

$$\begin{aligned}\mathsf{LB}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b}) &= P_{k_4} \times \mathsf{LB}^{\mathsf{R}^{(3)}\circ\mathsf{R}^{(2)}\circ\mathsf{R}^{(1)}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b}) \\ &= P_{k_4} \times \left(\prod_{r=1}^{3} \mathsf{LB}^{\mathsf{R}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\mathbf{a}^{(r+1)}\right)\right) \; ,\end{aligned}$$

with $\mathbf{a}^{(1)} = \mathbf{a}$ and $\mathbf{a}^{(4)} = \mathbf{b}$. Applying the piling-up lemma several times, we obtain:

$$
\begin{aligned}
\| \,\textsf{\textbf{LB}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b})\, \|_2^2 &= \| \prod_{r=1}^{3} \textsf{\textbf{LB}}^{\mathsf{R}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\mathbf{a}^{(r+1)}\right) \|_2^2 \\
&= \| \prod_{r=1}^{3} P_{k_r} \times \textsf{\textbf{LB}}^{\mathsf{S}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\tilde{\mathbf{a}}^{(r+1)}\right) \|_2^2 \\
&= \| \textsf{\textbf{LB}}^{\mathsf{S}^{(1)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(1)},\tilde{\mathbf{a}}^{(2)}\right) \\
&\qquad \times \prod_{r=2}^{3} P_{k_r} \times \textsf{\textbf{LB}}^{\mathsf{S}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\tilde{\mathbf{a}}^{(r+1)}\right) \|_2^2 \\
&\approx \left(\frac{1}{q-1}\right)^2 \prod_{r=1}^{3} \| \textsf{\textbf{LB}}^{\mathsf{S}^{(r)}}_{\mathsf{F}_{16}/\mathsf{F}_q}\left(\mathbf{a}^{(r)},\tilde{\mathbf{a}}^{(r+1)}\right) \|_2^2 \ .
\end{aligned}
$$

Finally, with $\mathbf{a}^{(1)} = \mathbf{a}$ and $\mathbf{a}^{(4)} = \mathbf{b}$:

$$
\begin{aligned}
\| \textsf{\textbf{LB}}(\mathbf{a},\mathbf{b}) \|_2^2 \approx \left(\frac{1}{q-1}\right)^2 \| \textsf{\textbf{LB}}^{\mathsf{S}^{(1)}}\left(\mathbf{a}^{(1)},\tilde{\mathbf{a}}^{(2)}\right) \|_2^2 \\
\cdot \| \textsf{\textbf{LB}}^{\mathsf{S}^{(2)}}\left(\mathbf{a}^{(2)},\tilde{\mathbf{a}}^{(3)}\right) \|_2^2 \cdot \| \textsf{\textbf{LB}}^{\mathsf{S}^{(3)}}\left(\mathbf{a}^{(3)},\tilde{\mathbf{a}}^{(4)}\right) \|_2^2 \ .
\end{aligned}
$$

In the case where we can manage to have only one active substitution box per round, this equation becomes:

$$
\begin{aligned}
\| \textsf{\textbf{LB}}(\mathbf{a},\mathbf{b}) \|_2^2 \approx \left(\frac{1}{q-1}\right)^2 \| \textsf{\textbf{LB}}^{S_1}\left(\mathbf{a}^{(1)},\tilde{\mathbf{a}}^{(2)}\right) \|_2^2 \\
\cdot \| \textsf{\textbf{LB}}^{S_2}\left(\mathbf{a}^{(2)},\tilde{\mathbf{a}}^{(3)}\right) \|_2^2 \cdot \| \textsf{\textbf{LB}}^{S_2}\left(\mathbf{a}^{(3)},\tilde{\mathbf{a}}^{(4)}\right) \|_2^2 \ .
\end{aligned}
$$

In the last equation we made a slight abuse of notation. When computing $\| \textsf{\textbf{LB}}^{S_1}\left(\mathbf{a}^{(1)},\tilde{\mathbf{a}}^{(2)}\right) \|_2^2$ for example, we only consider the two non zero coordinates of $\mathbf{a}^{(1)}$ and $\tilde{\mathbf{a}}^{(2)}$ to obtain a mask on the active substitution box.

8 Finding the best path

We have to find a path, i.e. a sequence of input/output masks $\mathbf{a} = \mathbf{a}^{(1)} \rightarrow \mathbf{a}^{(2)} \rightarrow \mathbf{a}^{(3)} \rightarrow \mathbf{a}^{(4)} = \mathbf{b}$ such that the value of $n(\mathbf{a},\mathbf{b}) = \| \textsf{\textbf{LB}}_{\mathsf{F}_{16}/\mathsf{F}_q}(\mathbf{a},\mathbf{b}) \|_2^{-2}$ is minimum. Finding such a sequence is not a trivial problem. A possible strategy was proposed by

Matsui (see [Mat94b]) and then improved by Otha, Moriai and Aoki (see [OMA95]). Their solution applies well to a cipher following a Feistel scheme, which is not the case here. Thus, we propose an alternative. Algorithm 8 gives an efficient way to find the best possible characteristic on our cipher.

Parameters: The number of rounds r_{tot}. A list $\left(n_{\min}^{(1)}, \dots, n_{\min}^{(r_{\text{tot}})}\right)$, where all entry correspond to the approximate number of queries allowed for a particular round. An interval length δ.

```
main():
for each $\mathbf{a}^{(1)}$ do
    call sub(1)
end for
/* If this line is reach, no characteristic has been found */
Exit

sub($r$):
for each $\mathbf{a}^{(r+1)}$ do
    if $n(\mathbf{a}^{(r)}, \mathbf{a}^{(r+1)}) \in [n_{\min}^{(r)}; n_{\min}^{(r)} + \delta[$ then
        if $r = r_{\text{tot}}$ then
            Display $\left(\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \dots, \mathbf{a}^{(r)}\right)$ and $\left(n(\mathbf{a}^{(1)}, \mathbf{a}^{(2)}), \dots, n(\mathbf{a}^{(r)}, \mathbf{a}^{(r+1)})\right)$ and Exit
        else
            call sub($r + 1$)
        end if
    end if
end for
```

Algorithm 8: Finding the best characteristic

Remember that the objective is to find the characteristic such that the value of $\prod_{r=1}^{r_{\text{tot}}} n(\mathbf{a}^{(r)}, \mathbf{a}^{(r+1)})$ is minimal. Notice that on one round r, the number of questions $n(\mathbf{a}^{(r)}, \mathbf{a}^{(r+1)})$ is always smaller than the minimum number of questions on one substitution box (say $n_{\text{S-box}}$). The key of this algorithm is to determine the initial values $n_{\min}^{(1)}, \dots, n_{\min}^{(r)}$. Before we explain how to determine them, some clarification on the algorithm.

During the execution of `sub(r)`, we search for the output mask $\mathbf{a}^{(r+1)}$ of round r. The only masks that are accepted by the algorithm are those such that $n(\mathbf{a}^{(r)}, \mathbf{a}^{(r+1)}) \approx n_{\min}^{(r)}$. If such a mask is accepted, then procedure `sub` is called recursively, unless the searched mask was the last (i.e. we were looking for $\mathbf{b}$) which implies that we found the characteristic.

Here is how to choose $n_{\min}^{(1)}, \dots, n_{\min}^{(r)}$ in order to find the best characteristic. First

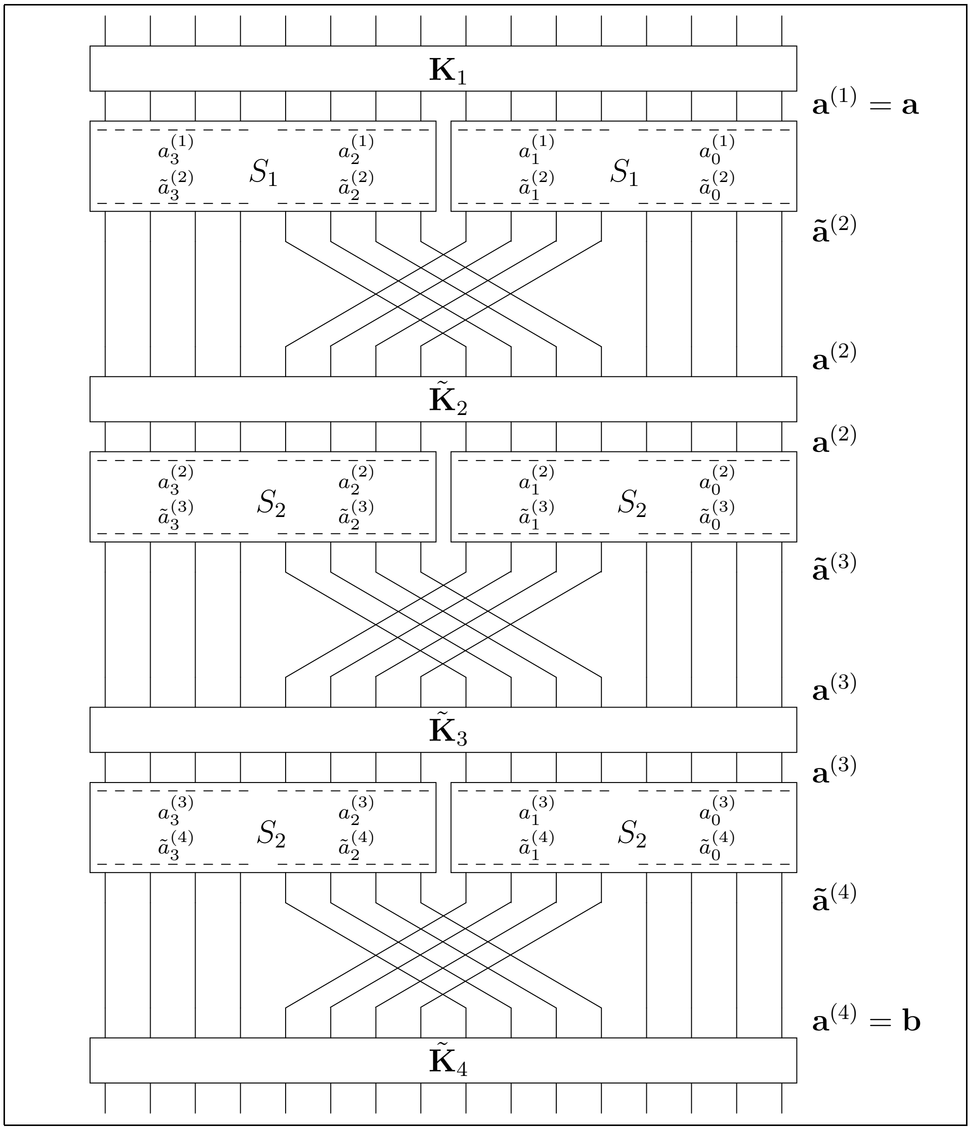

$\mathbf{K}_1$
$\mathbf{a}^{(1)} = \mathbf{a}$
$a_3^{(1)}$ $\tilde{a}_3^{(2)}$ S_1 $a_2^{(1)}$ $\tilde{a}_2^{(2)}$
$a_1^{(1)}$ $\tilde{a}_1^{(2)}$ S_1 $a_0^{(1)}$ $\tilde{a}_0^{(2)}$
$\tilde{\mathbf{a}}^{(2)}$
$\mathbf{a}^{(2)}$
$\tilde{\mathbf{K}}_2$
$\mathbf{a}^{(2)}$
$a_3^{(2)}$ $\tilde{a}_3^{(3)}$ S_2 $a_2^{(2)}$ $\tilde{a}_2^{(3)}$
$a_1^{(2)}$ $\tilde{a}_1^{(3)}$ S_2 $a_0^{(2)}$ $\tilde{a}_0^{(3)}$
$\tilde{\mathbf{a}}^{(3)}$
$\mathbf{a}^{(3)}$
$\tilde{\mathbf{K}}_3$
$\mathbf{a}^{(3)}$
$a_3^{(3)}$ $\tilde{a}_3^{(4)}$ S_2 $a_2^{(3)}$ $\tilde{a}_2^{(4)}$
$a_1^{(3)}$ $\tilde{a}_1^{(4)}$ S_2 $a_0^{(3)}$ $\tilde{a}_0^{(4)}$
$\tilde{\mathbf{a}}^{(4)}$
$\mathbf{a}^{(4)} = \mathbf{b}$
$\tilde{\mathbf{K}}_4$

Figure III.9: Path through the cipher

we initialize each of these values to $n_{\text{S-box}}$, the minimum number of questions on the substitution box. The we start the algorithm. If it finds a characteristic, we know it is the best. If it does not, we must increment one of the $n_{\text{min}}^{(i)}$'s in order to search through different branches. If the search succeeds, we know the characteristic is the best as $\prod_{r=1}^{r_{\text{tot}}} n(\mathbf{a}^{(r)}, \mathbf{a}^{(r+1)}) \approx \prod_{r=1}^{r_{\text{tot}}} n_{\text{min}}^{(r)}$ and as no characteristic can be found for smaller values of the $n_{\text{min}}^{(i)}$'s. If the search gives no result, we try all possible permutations of the values of $n_{\text{min}}^{(i)}$'s. If again, no result is found, we iterate. Algorithm 9 gives in a more formal way the method used to find the good initial values of the $n_{\text{min}}^{(i)}$'s.

Using this algorithm, we found the two following best paths:

- (0x0200, 0x4080) in F_2 with $n(a,b) \approx 475'000$. The path found is the following:

$$(\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \mathbf{a}^{(3)}, \mathbf{a}^{(4)}) = (\texttt{0x0200}, \texttt{0x0010}, \texttt{0x0200}, \texttt{0x4080}) \ .$$

- (0x5000, 0x0004) in F_4 with $n(a,b) \approx \left(\frac{1}{3}\right)^2 * 3800 \approx 422$. The path found is the following:

$$(\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \mathbf{a}^{(3)}, \mathbf{a}^{(4)}) = (\texttt{0x5000}, \texttt{0x0010}, \texttt{0x0005}, \texttt{0x0004}) \ .$$

9 And what was that all about?

After the results we have just presented, we decided to experiment our cryptanalysis on the cipher. Unfortunately, linear cryptanalysis (as well classic as generalized) in ineffective in the present case. Concretely, independently of number of plaintext/ciphertext couples at our disposal, the rank of the good subkey in the sorted list of all possible subkey for the last round is always too high (although it decreases as the number of couples increases). It is thus necessary to test un high number of wrong key before the good one is discovered. Even when using all possible plaintext/ciphertext couples (i.e. 2^{16} couples), the good subkey is not necessarily at the first position, which means that the cryptanalysis is not better than an exhaustive key search. These bad results are due to the excellent quality of AES substitution boxes against linear cryptanalysis and to the low number of possible plaintext/ciphertext couples at our disposal.

Can we conclude that our generalization of linear cryptanalysis is useless ? When a cipher is strong against linear cryptanalysis, is it automatically strong against our generalization ? In the next section we investigate both questions.

10 On the limitations of this generalization

In this section, we prove a result that seems to show that somehow, the power of generalized cryptanalysis (as we defined it) is limited when the power of classical

```
find_initial_values():
$\mathcal{A} \leftarrow ((n_{\text{S-box}}, \ldots, n_{\text{S-box}}))$
$\mathcal{B} \leftarrow \emptyset$
do
    for each element $\left(n_{\min}^{(1)}, \ldots, n_{\min}^{(r_{\text{tot}})}\right) \in \mathcal{A}$ do
        for each permutation $\sigma$ of the set $\{1, 2, \ldots, r_{\text{tot}}\}$ do
            if $\left(n_{\min}^{(\sigma(1))}, \ldots, n_{\min}^{(\sigma(r_{\text{tot}}))}\right) \notin \mathcal{B}$ then
                $\mathcal{B} \leftarrow \mathcal{B} \cup \left(n_{\min}^{(\sigma(1))}, \ldots, n_{\min}^{(\sigma(r_{\text{tot}}))}\right)$
            end if
        end for
    end for
    for each element $\left(n_{\min}^{(1)}, \ldots, n_{\min}^{(r_{\text{tot}})}\right) \in \mathcal{B}$ do
        Search of a characteristic with initial values $\left(n_{\min}^{(\sigma(1))}, \ldots, n_{\min}^{(\sigma(r_{\text{tot}}))}\right)$
    end for
$\mathcal{A} \leftarrow$ next_set($\mathcal{A}$)
$\mathcal{B} \leftarrow \emptyset$
while no characteristic has been found

next_set($\mathcal{A}$):
for each element $\left(n_{\min}^{(1)}, \ldots, n_{\min}^{(r_{\text{tot}})}\right) \in \mathcal{A}$ do
    $\mathcal{A} \leftarrow \mathcal{A} \setminus \left(n_{\min}^{(1)}, \ldots, n_{\min}^{(r_{\text{tot}})}\right)$
    for each $i \in \{1, \ldots, r_{\text{tot}} - 1\}$ do
        if $n_{\min}^{(i)} + \delta \leq n_{\min}^{(i+1)}$ do
            $\mathcal{A} \leftarrow \mathcal{A} \cup \left(n_{\min}^{(1)}, \ldots, n_{\min}^{(i)} + \delta, n_{\min}^{(i+1)}, \ldots, n_{\min}^{(r_{\text{tot}})}\right)$
        end if
        Sort $\mathcal{A}$ by increasing value of $\prod_{i=1}^{r_{\text{tot}}} n_{\min}^{(i)}$
    end for
end for
```

Algorithm 9: Finding the best initial values for the search for the best characteristic

linear cryptanalysis is limited.

Theorem 15. *Consider a permutation C over $\{0,1\}^n$. Let $\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)$ be the transition matrix defined by*

$$\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y} = \mathsf{Pr}_{Z\in\mathsf{F}_{2^m}}\left[\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(bC(Z)) = y \mid \mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(aZ) = x\right]$$

such that $n > 1$ and such that n divides m. Let $\epsilon_{x,y}$ be the x,y entry of the corresponding bias matrix. If there exists some $B > 0$ such that for all $a, b \in \mathsf{F}_2^*$ we have

$$\left(2\mathsf{Pr}_{Z\in\mathsf{F}_{2^m}}\left[\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_2}(aZ) = \mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_2}(bC(Z))\right] - 1\right)^2 \leq B \tag{III.5}$$

then

$$\sum_{x,y\in\mathsf{F}_{2^n}} \epsilon^2_{x,y} \leq 2^{2n}B\ .$$

Proof. If equation (III.5) is true, we also have:

$$\left(2\mathsf{Pr}_{Z\in\mathsf{F}_{2^m}}\left[\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_2}(\alpha aZ) = \mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_2}(\beta bC(Z))\right] - 1\right)^2 \leq B$$

for all $\alpha, \beta \in \mathsf{F}_{2^n}$. Using the transitivity of the trace (see Theorem 9), this implies:

$$\left(2\mathsf{Pr}_{Z\in\mathsf{F}_{2^m}}\left[\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(\alpha aZ)\right) = \mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(\beta bC(Z))\right)\right] - 1\right)^2 \leq B$$

Using Theorem 8, as α and β are elements of F_{2^n}, we have:

$$\left(2\mathsf{Pr}_{Z\in\mathsf{F}_{2^m}}\left[\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\alpha\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(aZ)\right) = \mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\beta\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(bC(Z))\right)\right] - 1\right)^2 \leq B$$

Considering the probabilistic part of the last equation, we have:

$$\begin{aligned}
&\mathsf{Pr}_{Z\in\mathsf{F}_{2^m}}\left[\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\alpha\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(aZ)\right) = \mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\beta\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(bC(Z))\right)\right] \\
&\quad = \sum_{z\in\mathsf{F}_{2^m}} 1_{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\alpha\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(az)\right)=\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\beta\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(bC(z))\right)}\mathsf{Pr}\left[Z = z\right] \\
&\quad = \frac{1}{2^m}\sum_{z\in\mathsf{F}_{2^m}}\sum_{x,y\in\mathsf{F}_{2^n}} 1_{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)=\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}\ 1_{\substack{x=\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(az)\\ y=\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(bC(z))}} \\
&\quad = \frac{1}{2^m}\sum_{x,y\in\mathsf{F}_{2^n}} 1_{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)=\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}\sum_{z\in\mathsf{F}_{2^m}} 1_{\substack{x=\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(az)\\ y=\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(bC(z))}}
\end{aligned}$$

Noticing that

$$\mathsf{Pr}_{Z\in\mathsf{F}_{2^m}}\left[\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(bC(Z)) = y, \mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(aZ) = x\right] = \frac{1}{2^m}\sum_{z\in\mathsf{F}_{2^m}} 1_{\substack{x=\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(az)\\ y=\mathsf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(bC(z))}}$$

we have:

$$\begin{aligned}\mathbf{Pr}_{Z\in \mathsf{F}_{2^m}}\left[\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\alpha \mathbf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}\left(aZ\right)\right) = \mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}\left(\beta \mathbf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}\left(bC(Z)\right)\right)\right] \\ = \frac{1}{2^n}\sum_{x,y\in \mathsf{F}_{2^n}} 1_{\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)=\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}\left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}\left(a,b\right)\right]_{x,y}\end{aligned}$$

Going back to the initial expression, we thus obtain:

$$\left(\frac{2}{2^n}\sum_{x,y\in \mathsf{F}_{2^n}} 1_{\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)=\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}\left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}\left(a,b\right)\right]_{x,y} - 1\right)^2 \leq B \qquad \text{(III.6)}$$

Noticing that

$$1_{i=j} = \frac{(-1)^{i+j}+1}{2}$$

for $i, j \in \mathsf{F}_2$ we can compute the preceeding sum:

$$\begin{aligned}&\sum_{x,y\in \mathsf{F}_{2^n}} 1_{\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)=\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}\left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}\left(a,b\right)\right]_{x,y} \\ &= \sum_{x,y\in \mathsf{F}_{2^n}} \frac{1}{2}\left((-1)^{\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)+\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}+1\right)\left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}\left(a,b\right)\right]_{x,y} \\ &= \frac{1}{2}\sum_{x,y\in \mathsf{F}_{2^n}} (-1)^{\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)+\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}\left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}\left(a,b\right)\right]_{x,y} + \frac{2^n}{2}\end{aligned}$$

Considering the last equality and equation (III.6), we obtain:

$$\left(\frac{1}{2^n}\sum_{x,y\in \mathsf{F}_{2^n}} (-1)^{\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)+\mathbf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}\left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}\left(a,b\right)\right]_{x,y}\right)^2 \leq B \qquad \text{(III.7)}$$

We can develop the left term of equation (III.7) (remember that + and − are equivalent in F_2):

$$\left(\frac{1}{2^n}\sum_{x,y\in\mathsf{F}_{2^n}}(-1)^{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)+\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y}\right)^2$$

$$= \frac{1}{2^{2n}}\sum_{x,y\in\mathsf{F}_{2^n}}\sum_{x',y'\in\mathsf{F}_{2^n}}(-1)^{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)+\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}(-1)^{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x')+\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y')}$$
$$\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y}\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x',y'}$$

$$= \frac{1}{2^{2n}}\sum_{x,y\in\mathsf{F}_{2^n}}\sum_{x',y'\in\mathsf{F}_{2^n}}(-1)^{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)+\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)-\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x')-\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y')}$$
$$\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y}\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x',y'}$$

$$= \frac{1}{2^{2n}}\sum_{x,y\in\mathsf{F}_{2^n}}\sum_{x',y'\in\mathsf{F}_{2^n}}(-1)^{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha(x-x'))+\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta(y-y'))}$$
$$\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y}\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x',y'}$$

We can notice that:

$$\sum_{\alpha,\beta\in\mathsf{F}_{2^n}}(-1)^{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha(x-x'))+\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta(y-y'))} = \begin{cases}2^{2n} & \text{when } x = x' \text{ and } y = y'\\ 0 & \text{otherwise.}\end{cases}$$

So that:

$$\sum_{\alpha,\beta\in\mathsf{F}_{2^n}}\left(\frac{1}{2^n}\sum_{x,y\in\mathsf{F}_{2^n}}(-1)^{\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\alpha x)+\mathsf{Tr}_{\mathsf{F}_{2^n}/\mathsf{F}_2}(\beta y)}\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y}\right)^2$$
$$= \sum_{x,y\in\mathsf{F}_{2^n}}\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]^2_{x,y}$$

The last equality and equation (III.7) give:

$$\sum_{x,y\in\mathsf{F}_{2^n}}\left[\mathsf{LT}^C_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]^2_{x,y} \le 2^{2n}B \qquad \text{(III.8)}$$

We are almost done. We have:

$$\begin{aligned}
&\sum_{x,y\in\mathsf{F}_{2^n}} \epsilon_{x,y}^2 \\
&\quad= \sum_{x,y\in\mathsf{F}_{2^n}} \left(\left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y} - \frac{1}{2^n}\right)^2 \\
&\quad= \sum_{x,y\in\mathsf{F}_{2^n}} \left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y}^2 - \frac{2}{2^n}\sum_{x,y\in\mathsf{F}_{2^n}} \left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y} + \sum_{x,y\in\mathsf{F}_{2^n}} \frac{1}{2^{2n}} \\
&\quad= \sum_{x,y\in\mathsf{F}_{2^n}} \left[\mathbf{LT}^{C}_{\mathsf{F}_{2^m}/\mathsf{F}_{2^n}}(a,b)\right]_{x,y}^2 - 1
\end{aligned}$$

Using equation (III.8) we obtain:

$$\sum_{x,y\in\mathsf{F}_{2^n}} \epsilon_{x,y}^2 \le 2^{2n}B$$

which finishes this (long) proof.

□

The preceeding theorem proves that when a cipher is strong against linear cryptanalysis, that is when the value of

$$\left(2\mathbf{Pr}_{Z\in\mathsf{F}_{2^m}}\left[\mathbf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_2}(aZ) = \mathbf{Tr}_{\mathsf{F}_{2^m}/\mathsf{F}_2}(bC(Z))\right] - 1\right)^2$$

is low, it makes sure that the value of

$$\sum_{x,y\in\mathsf{F}_{2^n}} \epsilon_{x,y}^2$$

is also relatively low. Given the definition of the transition matrices used in this study (see Chapter II, Definition 11), this also means that the cipher is strong against generalized cryptanalysis (but to a lesser extent). But the range of application of Theorem 15 is limited to this particular definition. It would be sufficient to define the transition matrices in some other way in order to leave its range of applicability. In the next chapter we give an example of such transition matrices.

Chapter IV

Further improvements and Conclusion

1 On the universality of our generalization

1.1 A new kind of transition matrices

At the beginning of chapter II we decide to use specific types of transition matrices (although some of the results of the chapter hold of any kind of transition matrices). Namely we defined $q \times q$ transition matrices in the following way:

$$\left[\mathsf{LT}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)\right]_{i,j} = \mathsf{Pr}_{X \in \mathsf{F}_{q^m}}\left[\mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(bf(X)) = j | \mathsf{Tr}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(aX) = i\right] ,$$

where f is function over F_{q^m} and a, b are elements of $\mathsf{F}^*_{q^m}$. This choice, although not completely arbitrary, can be changed by something more appropriate. For example, an easy way to eliminate the problem of the limitation proved in Theorem 15 is to make use of what we call *differential linear transition matrices*:

$$\left[\Delta\mathsf{LT}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right]_{i,j} = \mathsf{Pr}_{X_1,X_2 \in \mathsf{F}_{q^m}}\left[\psi(Y_2 \oplus Y_1) = j \mid \phi(X_2 \oplus X_1) = i\right] ,$$

where ψ and ϕ are linear functions from F_{q^m} onto F_q, where $Y_i = f(X_i)$ and where the X_i's independent and uniformly distributed. We consider the configuration represented on Figure IV.1.
We have:

$$Y_i = f(X_i) = C(X_i \oplus K)$$

where K represent a fixed subkey, and C a fixed permutation over F_{q^m}. In order to simplify notations, we can consider that $\phi = \psi$. Typically, f represents a round a block cipher. We can easily prove that differential linear transition matrix does not depend on K:

$$\begin{aligned} X_2 \oplus X_1 &= (U_2 \oplus K) \oplus (U_1 \oplus K) \\ &= U_2 \oplus U_1 \ . \end{aligned}$$

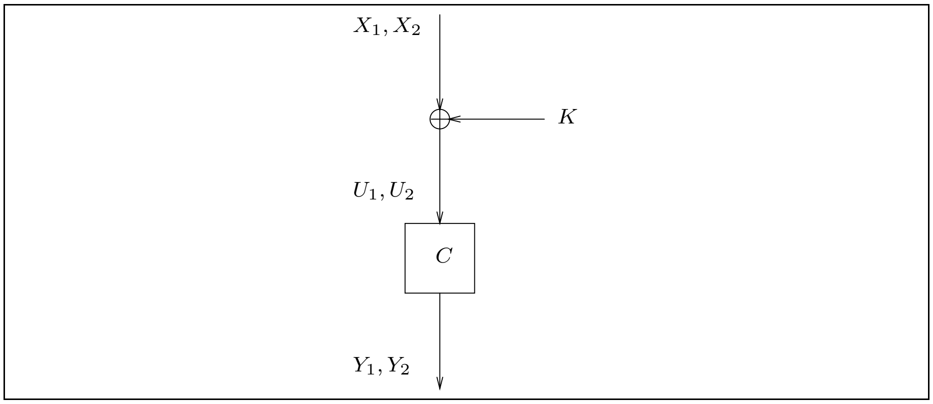


Figure IV.1: Application of differential linear transition matrices

Thus:

$$\begin{aligned}\left[\Delta\mathsf{LT}^{f}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right]_{i,j} &= \mathsf{Pr}_{X_1,X_2\,\in\,\mathsf{F}_{q^m}}\left[\psi(Y_2\oplus Y_1)=j \mid \psi(U_2\oplus U_1)=i\right]\\ &= \left[\Delta\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right]_{i,j}\ .\end{aligned}$$

We see that the subkeys will be discarded in the computation of the differential linear transition matrix of one round, which will thus only depend on the permutation C. Consider two rounds represented on Figure IV.2.
We have:

$$\begin{aligned}\left[\Delta\mathsf{LT}^{\mathsf{R}^{(2)}\circ\mathsf{R}^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right]_{i,j} &= \mathsf{Pr}_{X_1,X_2}\left[\psi(Y_2\oplus Y_1)=j \mid \psi(X_2\oplus X_1)=i\right]\\ &= q\ \mathsf{Pr}_{X_1,X_2}\left[\psi(Y_2\oplus Y_1)=j, \psi(X_2\oplus X_1)=i\right]\\ &= \sum_{k\in\mathsf{F}_q}\mathsf{Pr}_{X_1,X_2}\left[\psi(Y_2\oplus Y_1)=j, \psi(X_2\oplus X_1)=i \mid \psi(Z_2\oplus Z_1)=k\right]\end{aligned}$$

We suppose that the chain $\psi(X_2 \oplus X_1) \rightarrow \psi(Z_2 \oplus Z_1) \rightarrow \psi(Y_2 \oplus Y_1)$ is a Markov chain (just as we did in chapter II, Property 1), we obtain:

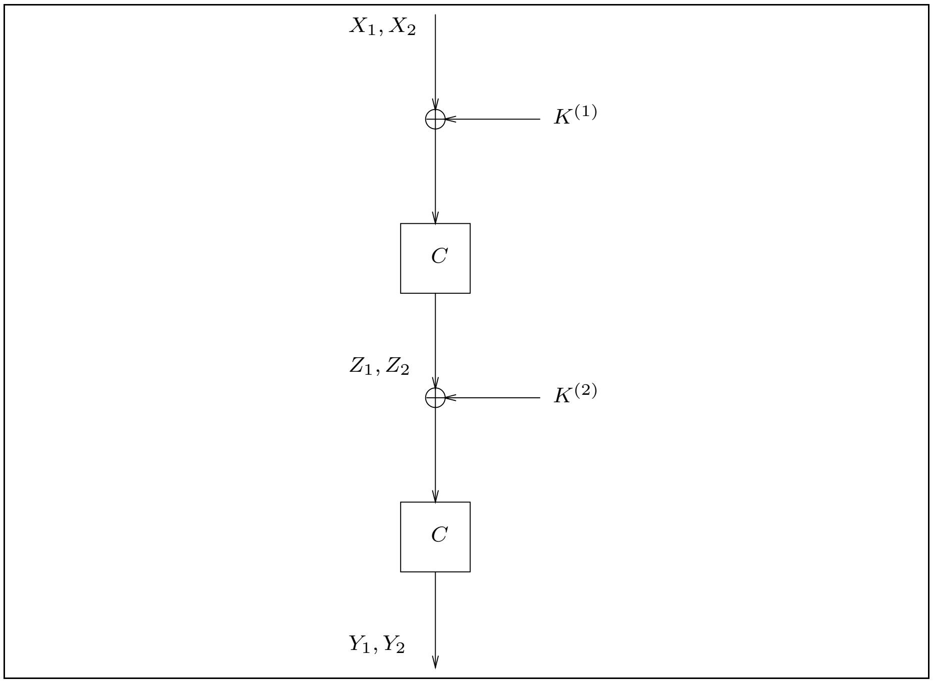


Figure IV.2: Differential linear transition matrix on two rounds

$$\begin{aligned}
\left[\Delta\mathsf{LT}^{\mathsf{R}^{(2)}\circ\mathsf{R}^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right]_{i,j} &= \sum_{k\in\mathsf{F}_q} \mathbf{Pr}\left[\psi(Y_2 \oplus Y_1) = j \mid \psi(Z_2 \oplus Z_1) = k\right] \\
&\qquad \mathbf{Pr}\left[\psi(X_2 \oplus X_1) = i \mid \psi(Z_2 \oplus Z_1) = k\right] \\
&= \sum_{k\in\mathsf{F}_q} \mathbf{Pr}\left[\psi(Y_2 \oplus Y_1) = j \mid \psi(Z_2 \oplus Z_1) = k\right] \\
&\qquad \mathbf{Pr}\left[\psi(Z_2 \oplus Z_1) = k \mid \psi(X_2 \oplus X_1) = i\right] \\
&= \sum_{k\in\mathsf{F}_q} \left[\Delta\mathsf{LT}^{\mathsf{R}^{(2)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right]_{k,j} \left[\Delta\mathsf{LT}^{\mathsf{R}^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right]_{i,k}
\end{aligned}$$

And thus:

$$\Delta\mathsf{LT}^{\mathsf{R}^{(2)}\circ\mathsf{R}^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q} = \Delta\mathsf{LT}^{\mathsf{R}^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q} \times \Delta\mathsf{LT}^{\mathsf{R}^{(2)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q} \ .$$

As we know that the differential linear transition matrix on one round does only depend on C, we obtain:

$$\Delta\mathsf{LT}^{\mathsf{R}^{(2)}\circ\mathsf{R}^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q} = \left(\Delta\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right)^2 \ . \tag{IV.1}$$

Since the first chapter, we know that the efficiency of such a transition matrix is given by the norm of the corresponding bias matrix. We have:

$$\begin{aligned}\| \Delta\mathsf{LB}^{\mathsf{R}^{(2)}\circ\mathsf{R}^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q} \|_2 &= \| \Delta\mathsf{LT}^{\mathsf{R}^{(2)}\circ\mathsf{R}^{(1)}}_{\mathsf{F}_{q^m}/\mathsf{F}_q} - \mathbf{U} \|_2 \\ &= \| \left(\Delta\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right)^2 - \mathbf{U} \|_2 \\ &= \| \left(\Delta\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q} - \mathbf{U}\right)^2 \|_2 \\ &= \| \left(\Delta\mathsf{LB}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}\right)^2 \|_2 \ ,\end{aligned}$$

using Property 4.

We see that the transition matrix on several rounds does not depend on the subkeys, which is a good thing as the matrix we want to obtain should work with just the same efficiency regardless of the key that was used to crypt the plaintexts. Nevertheless, we still need a generalization of the piling-up lemma here, as we did not express the norm of the bias matrix on several rounds in function of the norm of the bias matrices of each individual round.

1.2 Some interesting properties

Going back on the definitions of the transition matrices LT and $\Delta\mathsf{LT}$, we will consider in this paragraph that

$$\left[\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)\right]_{i,j} = \mathsf{Pr}_{X\in\mathsf{F}_{q^m}}\left[\mathsf{Tr}\left(bC(X)\right) = j | \mathsf{Tr}\left(aX\right) = i\right] \ ,$$

and that

$$\left[\Delta\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)\right]_{i,j} = \mathsf{Pr}_{X_1,X_2\,\in\,\mathsf{F}_{q^m}}\left[\mathsf{Tr}\left(b(Y_2\oplus Y_1)\right) = j \mid \mathsf{Tr}\left(a(X_2\oplus X_1)\right) = i\right] \ ,$$

with the usual notations. In other words we consider that ϕ and ψ correspond to the trace function. In this particular case, some interesting properties can be found.

Property 8. *For $i,j \in \mathsf{F}_q$ we have:*

$$\left[\Delta\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)\right]_{i,j} = \frac{1}{q}\sum_{l,k\in\mathsf{F}_q}\left[\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)\right]_{l,k}\left[\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)\right]_{l+i,k+j}$$

Proof. In order to simplify notations, we simply write $\Delta\mathsf{LT}$ instead of $\Delta\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$ and LT instead of $\mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a,b)$. We also drop the subscript on the trace function. We have:

$$\begin{aligned}
&[\Delta\mathsf{LT}]_{i,j} \\
&= q\ \mathsf{Pr}\left[\mathsf{Tr}\left(b(Y_2 \oplus Y_1)\right) = j\ ,\ \mathsf{Tr}\left(a(X_2 \oplus X_1)\right) = i\right] \\
&= \sum_{l \in \mathsf{F}_q} \mathsf{Pr}\left[\mathsf{Tr}\left(b(Y_2 \oplus Y_1)\right) = j\ ,\ \mathsf{Tr}\left(a(X_2 \oplus X_1)\right) = i\ \mid\ \mathsf{Tr}\left(X_1\right) = l\right] \\
&= q \sum_{l \in \mathsf{F}_q} \mathsf{Pr}\left[\mathsf{Tr}\left(b(Y_2 \oplus Y_1)\right) = j\ ,\ \mathsf{Tr}\left(a(X_2 \oplus X_1)\right) = i\ ,\ \mathsf{Tr}\left(aX_1\right) = l\right] \\
&= \sum_{l,k \in \mathsf{F}_q} \mathsf{Pr}\left[\mathsf{Tr}\left(b(Y_2 \oplus Y_1)\right) = j\ ,\ \mathsf{Tr}\left(a(X_2 \oplus X_1)\right) = i\ ,\right. \\
&\qquad\qquad \left.\mathsf{Tr}\left(aX_1\right) = l\ \mid\ \mathsf{Tr}\left(bY_1\right) = k\right] \\
&= q \sum_{l,k \in \mathsf{F}_q} \mathsf{Pr}\left[\mathsf{Tr}\left(bY_2\right) = k + j\ ,\ \mathsf{Tr}\left(aX_2\right) = l + i\ ,\right. \\
&\qquad\qquad \left.\mathsf{Tr}\left(aX_1\right) = l\ ,\ \mathsf{Tr}\left(bY_1\right) = k\right] \\
&= \frac{1}{q} \sum_{l,k \in \mathsf{F}_q} \mathsf{Pr}\left[\mathsf{Tr}\left(bY_1\right) = k\ \mid\ \mathsf{Tr}\left(aX_1\right) = l\right] \\
&\qquad\qquad \mathsf{Pr}\left[\mathsf{Tr}\left(bY_2\right) = k + j\ \mid\ \mathsf{Tr}\left(aX_2\right) = l + i\right]
\end{aligned}$$

which concludes the proof. □

An another interesting remark is the following:

Property 9. *We the usual notations, we have:*

$$\parallel \Delta\mathsf{LB}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a, b) \parallel_2 \leq \parallel \mathsf{LT}^{C}_{\mathsf{F}_{q^m}/\mathsf{F}_q}(a, b) \parallel_2^2\ .$$

Proof. As in the precedent proof, we decide to simplify the notations. Using Property 8 we obtain:

$$\begin{aligned}
[\Delta\mathsf{LB}]_{i,j} &= [\Delta\mathsf{LT}]_{i,j} - \frac{1}{q} \\
&= \frac{1}{q} \sum_{l,k} \left([\mathsf{LT}]_{l,k} [\mathsf{LT}]_{l+i,k+j} - \frac{1}{q^2} \right)\ .
\end{aligned}$$

Thus:

$$\begin{aligned}
q^2 \parallel \Delta \mathbf{LB} \parallel_2^2 &= \sum_{i,j} \left(\sum_{l,k} \left([\mathbf{LT}]_{l,k} [\mathbf{LT}]_{l+i,k+j} - \frac{1}{q^2} \right) \right)^2 \\
&= \sum_{i,j} \sum_{l,k} \sum_{l',k'} \left([\mathbf{LT}]_{l,k} [\mathbf{LT}]_{l+i,k+j} - \frac{1}{q^2} \right) \left([\mathbf{LT}]_{l',k'} [\mathbf{LT}]_{l'+i,k'+j} - \frac{1}{q^2} \right) \\
&= \sum_{i,j} \sum_{l,k} \sum_{l',k'} [\mathbf{LT}]_{l,k} [\mathbf{LT}]_{l+i,k+j} [\mathbf{LT}]_{l',k'} [\mathbf{LT}]_{l'+i,k'+j} - q^2 \qquad \text{(IV.2)}
\end{aligned}$$

We also have:

$$\sum_{l,k} [\mathbf{LT}]_{l,k} [\mathbf{LT}]_{l+i,k+j} - \frac{1}{2} \parallel \mathbf{LT} \parallel_2^2 = \frac{1}{2} \sum_{l,k} \left(2 [\mathbf{LT}]_{l,k} [\mathbf{LT}]_{l+i,k+j} - [\mathbf{LT}]_{l,k}^2 \right) \qquad \text{(IV.3)}$$

As

$$0 \geq \left([\mathbf{LT}]_{l,k} - [\mathbf{LT}]_{l+i,k+j} \right)^2 = [\mathbf{LT}]_{l,k}^2 - 2 [\mathbf{LT}]_{l,k} [\mathbf{LT}]_{l+i,k+j} + [\mathbf{LT}]_{l+i,k+j}^2 \ ,$$

equation (IV.3) becomes:

$$\begin{aligned}
\sum_{l,k} [\mathbf{LT}]_{l,k} [\mathbf{LT}]_{l+i,k+j} - \frac{1}{2} \parallel \mathbf{LT} \parallel_2^2 &\geq \frac{1}{2} \sum_{l,k} [\mathbf{LT}]_{l+i,k+j}^2 \\
&= \frac{1}{2} \parallel \mathbf{LT} \parallel_2^2
\end{aligned}$$

and thus:

$$\sum_{l,k} [\mathbf{LT}]_{l,k} [\mathbf{LT}]_{l+i,k+j} \geq \parallel \mathbf{LT} \parallel_2^2 \ . \qquad \text{(IV.4)}$$

From equations (IV.2) and (IV.4) we obtain:

$$\begin{aligned}
q^2 \parallel \Delta \mathbf{LB} \parallel_2^2 &\leq q^2 \parallel \mathbf{LT} \parallel_2^4 - q^2 \\
&\leq q^2 \parallel \mathbf{LT} \parallel_2^4
\end{aligned}$$

which concludes the proof. □

We have to admit that those results, apart from making the link between two theories, are not very useful when comes the time of cryptanalysis. But they may be a start for finding some theory that (for example) would make use of both definitions in order to generalize the piling-up lemma. The aim was also to show that the transition matrices we defined in Chapter II are not unique, and can be replaced an another type of transition matrices.

Finding the best type of transition matrix for a particular cipher is the starting point for studies of great interest !

2 Conclusion

In this diploma work, we expose several ideas that generalize Matsui's linear cryptanalysis. Whether some generalizations had already been done, none of them proposed a way to widen the space cardinal of the linear expressions, which is our proposal. Following this idea we replace linear expressions by linear transition matrices. A critical measure on linear expression is the notion of bias. The study on distinguishers we make in chapter I allows us to extend it, giving a similar measure on transition matrices. All the results given in chapter I and some results given in chapter II are true regardless the exact definition of the transition matrix (see section 1 for more details). The only assumption is that the matrices are transition matrices (i.e. that their lines and columns sum to 1).

From that point, we made the choice of restricting the study to specific types of transition matrices. More precisely, we defined a specific type of transition matrices using the trace operator on finite fields. This operator is an elegant way to generalize the notion of scalar product. Still in chapter II we tried to generalize one of the central notions of linear cryptanalysis, the piling-up lemma. The generalization we propose is of course linked to the exact definition of the transition matrices we are using and thus to the trace function.

Finally, in chapter III, we use the tools of the past chapters to cryptanalyze a simple cipher. We show how to find a transition matrix on several rounds of the cipher, given the transition matrices on the individual rounds, using the generalization of the piling-up lemma. We also take a look at an another complex problem faced by the cryptanalyst, namely how to find the transition matrices on individual rounds such that a transition matrix on several rounds can indeed be derived.

The theory we have presented here is general enough to open new doors on very exciting future work. We give some examples in the present chapter . . .

Bibliography

[BS90] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems (extended abstract). In Advances in Cryptology - CRYPTO'90, volume 537 of LNCS, pages 2–21. Springer-Verlag, 1990.

[CT91] Thomas M. Cover and Joy A. Thomas. Elements of Information Theory. Wiley Series in Telecommunications, 1991.

[Dan01] F. Dannan. Matrix and operator inequalities. Journal of Inequalities in Pure and Applied Mathematics, 2(3), 2001. Available on `http://jipam.vu.edu.au/v1n1/`.

[DR02] J. Daemen and V. Rijmen. The Design of Rijndael. Information Security and Cryptography. Springer, 2002.

[GC90] H. Gilbert and G. Chasse. A statistical attack of the FEAL cryptosystem. In Advances in Cryptology - CRYPTO'90, volume 537 of LNCS, pages 22–33. Springer-Verlag, 1990.

[Hey99] H.M. Heys. A tutorial on linear and differential cryptanalysis. Available on `http://www.engr.mun.ca/~howard/`, 1999.

[HKM95] C. Harpes, G. Kramer, and J.L. Massey. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. In Advances in Cryptology - EUROCRYPT'95, volume 921 of LNCS, pages 24–38. Springer-Verlag, 1995.

[HM97] C. Harpes and J. Massey. Partitioning cryptanalysis. In Fast Software Encryption FSE'97, volume 1267 of LNCS, pages 13–27. Springer-Verlag, 1997.

[Jun01] P. Junod. On the complexity of Matsui's attack. In Selected Areas in Cryptography, SAC'01, volume 2259 of LNCS, pages 199–211. Springer-Verlag, 2001.

[Jun03a] P. Junod. On the optimality of linear, differential and sequential distinguishers. In Advances in Cryptology - EUROCRYPT'03, volume 2656 of LNCS, pages 17–32. Springer-Verlag, 2003.

[Jun03b] P. Junod. On the optimality of linear, differential and sequential distinguishers (full version). Available on `http://eprint.iacr.org` and on `http://crypto.junod.info`, 2003.

[JV03] P. Junod and S. Vaudenay. Optimal key ranking procedures in a statistical cryptanalysis. In Proceedings of Fast Software Encryption - FSE'03, LNCS. Springer-Verlag, 2003. To appear.

[Lan02] S. Lang. Algebra. Springer-Verlag, 2002. Rev. 3rd ed.

[LN83] R. Lidl and H. Niederreiter. Finite Fields. Cambridge University Press, 1983.

[Mat93] M. Matsui. Linear cryptanalysis method for DES cipher. In Advances in Cryptology - EUROCRYPT'93, volume 765 of LNCS, pages 386–397. Springer-Verlag, 1993.

[Mat94a] M. Matsui. The first experimental cryptanalysis of the Data Encryption Standard. In Advances in Cryptology - CRYPTO'94, volume 839 of LNCS, pages 1–11. Springer-Verlag, 1994.

[Mat94b] M. Matsui. On correlation between the order of S-boxes and the strength of DES. In Advances in Cryptology - EUROCRYPT'94, volume 950 of LNCS, pages 366–375. Springer-Verlag, 1994.

[MG00] M. Minier and H. Gilbert. Stochastic cryptanalysis of Crypton. In Fast Software Encryption FSE'00, volume 1978 of LNCS, pages 121–133. Springer-Verlag, 2000.

[Miy89] S. Miyaguchi. The FEAL–8 cryptosystem and a call for attack. In Advances in Cryptology - CRYPTO'89, volume 435 of LNCS, pages 624–627. Springer-Verlag, 1989.

[Miy90] S. Miyaguchi. The FEAL cipher family. In Advances in Cryptology - CRYPTO'90, volume 537 of LNCS, pages 627–638. Springer-Verlag, 1990.

[MVV97] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. Handbook of applied cryptography. The CRC Press series on discrete mathematics and its applications. CRC-Press, 1997.

[MY92] M. Matsui and A. Yamagishi. A new method for known plaintext attack of FEAL cipher. In Advances in Cryptology - EUROCRYPT'92, volume 658 of LNCS, pages 81–91. Springer-Verlag, 1992.

[Nat77] National Bureau of Standards, U. S. Department of Commerce. Data Encryption Standard, 1977.

[OMA95] K. Ohta, S. Moriai, and K. Aoki. Improving the search algorithm for the best linear expression. In Advances in Cryptology - CRYPTO'95, LNCS, pages 157–170. Springer-Verlag, 1995.

[Par03] M.G. Parker. Generalised S-Box nonlinearity, 2003. Available on `http://www.ii.uib.no/~matthew/`.

[Sch94] B. Schneier. Applied cryptography: protocols, algorithms and source code in C. John Wiley and Sons, 1994.

[SM87] A. Shimizu and S. Miyaguchi. Fast data encipherment algorithm FEAL. In Advances in Cryptology - EUROCRYPT'87, volume 304 of LNCS, pages 267–280. Springer-Verlag, 1987.

[TCG91] A. Tardy-Corfdir and H. Gilbert. A known plaintext attack of FEAL and FEAL-6. In Advances in Cryptology - CRYPTO'91, volume 576 of LNCS, pages 172–182. Springer-Verlag, 1991.

[Vau03] S. Vaudenay. Decorrelation: a theory for block cipher security. 2003. To appear in the Journal of Cryptology, available on `http://lasecwww.epfl.ch`.

[Zha02] X. Zhan. Matrix inequalities, volume 1790 of Lecture Notes in Mathematics. Springer-Verlag, 2002. Available on `http://link.springer.de/series/lnm`.