Automatic Expectation and Variance Computing for Attacks on Feistel Schemes

Emmanuel Volte[1] and Valérie Nachef[1] and Nicolas Marrière[1]

Department of Mathematics, University of Cergy-Pontoise, CNRS UMR 8088
2 avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France
emmanuel.volte@u-cergy.fr
valerie.nachef@u-cergy.fr
nicolas.marriere@u-cergy.fr

Abstract. There are many kinds of attacks that can be mounted on block ciphers: differential attacks, impossible differential attacks, truncated differential attacks, boomerang attacks. We consider generic differential attacks used as distinguishers for various types of Feistel ciphers: they allow to distinguish a random permutation from a permutation generated by the cipher. These attacks are based on differences between the expectations of random variables defined by relations on the inputs and outputs of the ciphers. Sometimes, one has to use the value of the variance as well. In this paper, we will provide a tool that computes the exact values of these expectations and variances. We first explain thoroughly how these computations can be carried out by counting the number of solutions of a linear systems with equalities and non-equalities. Then we provide the first applications of this tool. For example, it enabled to discover a new geometry in 4-point attacks. It gave an explanation to some phenomena that can appear in simulations when the inputs and outputs have a small number of bits.

Key words: Generic attacks on Feistel type schemes, pseudo-random permutations, differential cryptanalysis

1 Introduction

Many symmetric block ciphers and hash functions are based on Feistel-type constructions. Classical Feistel ciphers have been intensively studied since the seminal work by Luby and Rackoff [21]. These ciphers allow to construct pseudo-random permutations from $2n$ bits to $2n$ bits using random round functions from n bits to n bits. This construction is used in DES [1, 2]. With generalized Feistel schemes, it is possible to construct pseudo-random functions from kn bits to kn bits using different kinds of round functions. When the round functions are from $(k-1)n$ bits to n bits, we obtain an unbalanced Feistel scheme with contracting functions. These contracting ciphers are studied in [23, 28]. When the round functions are from n bits to $(k-1)n$ bits, we have unbalanced Feistel schemes with expanding functions, see [16, 29, 31, 33]. MARS [10] has an expanding Feistel structure. Alternating Feistel schemes alternate contracting and expanding rounds. They are described in [4] and are used in the BEAR/LION block cipher [4]. There are also type-1, type-2 and type-3 Feistel schemes, see also [14, 35]. Type-1 Feistel schemes are used in CAST-256 [3] and type-2 Feistel schemes in RC-6 and CLEFIA [30, 32].

Many different kinds of attacks have been mounted on Feistel-type block ciphers. Differential cryptanalysis [6] exploits the fact that characteristics or differentials on the input will produce a given difference on the output more frequently with a scheme than with a random permutation. Whereas ordinary differential cryptanalysis analyzes the full difference between two texts, the truncated variant [20] considers differences that are only partially determined. Impossible cryptanalysis [5, 19] uses impossible differentials:a given difference on the input will imply that a particular difference will never happen on the output whereas it can occur with a non negligible probability with a random permutation. Impossible differential attacks on generalized Feistel schemes are studied in [9] when there is no condition on the round functions, and in [17, 18, 34] when the round functions are permutations. Impossible boomerang attacks on generalized Feistel ciphers, when the round functions are permutation, are described in [11]. Also Meet-in-the-middle attacks on Type-2 and Type-3 Feistel ciphers are described in [13].

Generic attacks on Feistel-type ciphers are (or make use of) distinguishers that allow to determine the maximal numbers of rounds of the scheme needed to distinguish a permutation computed by the scheme from a random permutation. Depending on the number of rounds, it is possible to find some relations between the input and output variables. These relations hold conditionally to equalities on some internal variables due to the structure of the Feistel scheme. The attacks consist of using m plaintext/ciphertexts pairs and in counting the number of tuples of these pairs that satisfy the relations between the input and output variables. Then, it is possible to compare $\mathcal{N}$, the number of such tuples obtained with a random permutation, with $\tilde{\mathcal{N}}$, the corresponding number for the studied scheme. The attacks are successful, i.e. we are able to distinguish a permutation generated by a Feistel-type scheme from a random permutation, in three cases. The first case occurs when $\tilde{\mathcal{N}}$ is significantly greater than $\mathcal{N}$. For example, attacks on unbalanced Feistel schemes with expanding functions used the fact that $\tilde{\mathcal{N}}$ is significantly greater than $\mathcal{N}$ [29, 27, 33]. The second case happens when $\tilde{\mathcal{N}}$ is significantly smaller than $\mathcal{N}$ (this is the case for impossible attacks). For the third case, $\mathcal{N}$ and $\tilde{\mathcal{N}}$ have the same order, but the difference $|\mathbb{E}(\tilde{\mathcal{N}}) - \mathbb{E}(\mathcal{N})|$ is larger than both standard deviations $\sigma(\mathcal{N})$ and $\sigma(\tilde{\mathcal{N}})$, where $\mathbb{E}$ denotes the expectation function. In that case, the attacks work thanks to the Chebychev formula, which states that for any random variable X, and any $\alpha > 0$, we have $\mathbb{P}\left(|X - \mathbb{E}(X)| \geq \alpha\sigma(x)\right) \leq \frac{1}{\alpha^2}$. Using this formula, it is then possible to construct a prediction interval for $\tilde{\mathcal{N}}$ for example, in which future computations will fall, with a good probability. It is important to notice that for our attacks, it is enough to compute $\mathbb{E}(\mathcal{N})$, $\mathbb{E}(\tilde{\mathcal{N}})$ and $\sigma(\mathcal{N})$. Suppose that for a given number of rounds, $|\mathbb{E}(\mathcal{N}) - \mathbb{E}(\tilde{\mathcal{N}})| \geq \sigma(\mathcal{N})$. Then we have two cases. If $\sigma(\tilde{\mathcal{N}})$ behaves like $\sigma(\tilde{\mathcal{N}})$ or is smaller than $\sigma(\mathcal{N})$, we will have $|\mathbb{E}(\mathcal{N}) - \mathbb{E}(\tilde{\mathcal{N}})| \geq \max(\sigma_{\mathcal{N}}, \sigma_{\tilde{\mathcal{N}}})$ and the attack is successful. If $\sigma(\tilde{\mathcal{N}})$ is greater than $\sigma(\mathcal{N})$, this will lead to an attack by the variance for the same number of rounds. In order to compute $\sigma(\mathcal{N})$, we need to take into account the fact that the structures obtained from the m plaintext/ciphertext tuples are not independent. However, their mutual dependence is very small. To compute $\sigma(\mathcal{N})$, we will use this well-known formula, see [12], p.97, that we will call the "Covariance Formula": if $x_1, \ldots x_n$, are random variables, then if V represents the variance, we have $V(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} V(x_i) + 2\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\left[\mathbb{E}(x_i\, x_j) - \mathbb{E}(x_i)\mathbb{E}(x_j)\right]$. The computation of standard deviation and the use of the covariance formula usually allow to attacks more rounds than other attacks. This technique has been used for classical Feistel schemes in [26] for contracting Feistel schemes in [28] and for generalized Feistel schemes in [22].

Nevertheless, the computation of the expectation and the variance is very tedious and in all the previously mentioned papers, the calculation has to be done for each case. Moreover, most of the time, it is not possible to give all the details and only estimations are provided. In order to get these estimates, some hypothesis have to be done on the dependency of random variables. This does not always fit exactly to simulations. Very often, the simulations confirm the theoretical analysis, but for some cases, it is not exactly the case. Sometimes, the simulations show that some attacks work better than expected. In a few cases, it is the contrary. This is probably due to the fact that computations are not complete since they are very laborious. Also, in previous computations, the authors used a O function. For some small values of n, the exact value of this O functions can bring important changes. For example,with small values of n, it is possible to obtain attacks with a better complexity, or to attack more rounds, as we will see in this paper. We emphasize that in this paper, we will provide exact values, unlike in [7, 8] where the authors provide estimates for several kinds of statistical attacks.

In this paper, we present a tool that allows to compute the exact values of expectations and variances of the random variables defined by the attacks. We consider Known Plaintext Attacks (KPA, but the tool can be adapted to Non Adaptive Chosen Plaintext Attacks (NCPA) as well. We prove formulas for the expectation and the variance. From the formulas, we show that the computations of these expectations and variances are based on finding the number of solutions of linear systems on equalities and non-equalities. Then a computer program calculates this number of solutions.
The link to this computer program is:
http://www.voltee.com/SitePerso/publications.html
As we will see on examples of attacks, this program can also help to detect new geometries for attacks. It is also adapted to most types of attacks since it can count the number of solutions of any linear system of equalities and non-equalities. In particular, this program can be used on differential attacks, and impossible differential attacks. The paper is organized as follows. In section 2, we introduce the notation and definition. In Sections 3 and 4, we prove how

to do the computations by finding the number of solutions of linear systems of equalities and non-equalities. In these sections, we provide formulas that give the expectation and the standard deviation, once we know the number of solutions of the systems related to the attack. The notation given here will be used in the sequel. The algorithm used to compute the number of solutions is given in Section 5. In Section 6, we present the exact values for the expectations and variances that we have obtain for several example of attacks and use these results to show that the attacks are successful. Section 7 contains the conclusion and perspectives.

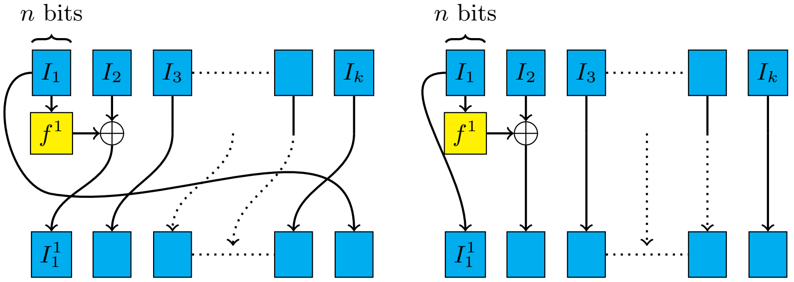
2 Notation

In our attacks, we want to distinguish a random permutation from kn bits to kn bits from a permutation produced by a Feistel-type ciphers using random functions from n bits to n bits. There are several possibilities. For example, with a classical Feistel scheme, at each round, only one function from n bits to n bits is used. For an expanding Feistel scheme, at each round, we need $k-1$ round functions from n bits to n bits. In our study, we will consider that we use only one round function per round. For example, for one usual round of an expanding Feistel scheme, we will introduce $k-1$ rounds in our computations. We now introduce the notation.

- k and n are integers greater or equal to 2.
- $N = 2^n$.
- $J = \{0,1\}^{kn}$. J is ordered in a natural way. $\text{card}(J) = |J| = N^k$.
- For a and b, $\delta_{ab} = 0$ if $a \neq b$ and $\delta_{aa} = 1$ (Kronecker symbol).
- $(a_1, a_2, \ldots, a_p) \not\ne\in E^p$ means that the a_i values are pairwise distinct elements of E. We sometimes denote by $\mathbf{a} = (a_1, \ldots, a_p)$ when there is no ambiguity.
- $\mathcal{B}_{kn}$ denotes the set of bijections from J to J. We have $|\mathcal{B}_{kn}| = 2^{kn}! = (N^k)!$
- Ψ^d is the set of the Feistel Schemes (for a certain type: balanced Feistel scheme, unbalanced Feistel scheme with expanding functions, generalized Feistel scheme of type 1, 2 or 3) with d **turns**, where each turn involves exactly one function from n bits to n bits. For example, with a balanced Feistel schemes, since at each round exactly one round function is used, the number of turns is identical to the number of rounds. For an unbalanced Feistel scheme with expanding functions defined from J to J, there are $(k-1)$ round functions from n bits to n bits at each round. In that case, if r is the number of rounds, the number of turns is $d = (k-1)r$, since in our computations, we consider that we use only one round function at each turn. We have $|\Psi^d| = 2^{nd2^n} = N^{dN}$
- When a bijection f is given, a couple $(I, S) \in J \times J$ (input / output) where $S = f(I)$, is called **a point**. When we have φ points, they are denoted by $(I(1), S(1)), \ldots, I(\varphi), S(\varphi))$.
- I and S are divided in k parts of n bits. We have $I = [I_1, I_2, \ldots, I_k]$ and $S = [S_1, S_2, \ldots, S_k]$.

- The internal functions are denoted by f_1, f_2, $\dots$, f_d (see figure 1). We always take the image of the first part, it means $I_1 = I_1^0$ for the first turn, I_1^1 for the second turn and so on.

Fig. 1. Two different possibilities for the first Feistel round



- Let J_m be the set of all the subsets of J with a cardinal equal to m. If $M \in J_m$, we have $|M| = m$. We say that $M(i)$ is the i-th element of M (for the same order as J). With M and a given bijection f, we can define a set of points: $M_f = \{(I, f(I)) \mid I \in M\}$.
- A φ**-condition** is an equality or a non-equality between xor of parts of two (or more) points $\big(I(1), S(1)\big), \big(I(2), S(2)\big), \dots, \big(I(\varphi), S(\varphi)\big)$. The general form can be defined as follow:

$$\oplus_{i\in\Phi}\Big(\oplus_{p\in C_1} I_p(i) \oplus_{q\in C_2} S_q(i)\Big) \underset{\neq}{\overset{=}{}} 0$$

  where Φ is a subset of $\{1, 2, \dots, \varphi\}$, C_1 and C_2 are subsets of $\{1, \dots, k\}$. Most often C_1 and C_2 have zero or one element.
- A φ**-attack** (A) is a finite set of φ-conditions.
- For an φ-attack (A), we define the random variable $\mathcal{N}$:

$$\mathcal{N} = \sum_{\substack{(i_1,\dots,i_\varphi)\\ \neq\in[1,m]^\varphi}} \mathcal{N}_{i_1,i_2,\dots,i_\varphi}$$

  where $\mathcal{N}_{i_1,i_2,\dots,i_\varphi} = 1$ if the φ-attack works (all the conditions are realized) on points $\big(I(i_1), S(i_1)\big), \big(I(i_2), S(i_2)\big), \dots, \big(I(i_\varphi), S(i_\varphi)\big)$ in M_f where $M \in_R J_m$ and $f \in_R B_{kn}$
- We write $\mathbf{I} = (I(1), \dots, I(\varphi)) \in J^\varphi$. The same notation applies for the outputs.
- In the same way, we define $\tilde{\mathcal{N}}$ by choosing again $M \in_R J_m$ and $f \in_R \Psi^d$
- We say that a φ-attack works if $|\mathbb{E}(\mathcal{N}) - \mathbb{E}(\tilde{\mathcal{N}})| \geq \sigma_{\mathcal{N}}$ (as explained in Section 1).

Example:
$n = 2$, $k = 2$, $N = 16$, $\varphi = 4$, $m = 4$, so $|J_m| = \binom{16}{4}$.

We consider the following φ-attack $\mathcal{A}$:

$$\begin{cases} I_1(1) \oplus I_1(2) = 0 \\ I_1(3) \oplus I_1(4) = 0 \\ I_1(1) \oplus I_1(3) \neq 0 \end{cases}$$

Then, for $M = \{0000, 0001, 0100, 0101\} \in J_m$, we have exactly 8 solutions for $\mathcal{A}$:

$$\begin{aligned}(i_1, i_2, i_3, i_4) \in \{\ & (0,1,2,3);(1,0,2,3);(0,1,3,2);(1,0,3,2);\\ & (2,3,0,1);(3,2,0,1);(2,3,1,0);(3,2,1,0)\}\end{aligned}$$

So, $\mathbb{E}(\mathcal{N}) = 8$.

3 Computing $\mathbb{E}(\mathcal{N})$ and $\mathbb{E}(\tilde{\mathcal{N}})$

3.1 Computation of $\mathbb{E}(\mathcal{N})$

Let (A) be a φ-attack and $\mathcal{N}$ the random variable: $\mathcal{N} = \sum_{\substack{(i_1,\ldots,i_\varphi)\\ \neq\in[1,m]^\varphi}} \mathcal{N}_{i_1,i_2,\ldots,i_\varphi}$.

Proposition 1. *Let* $P(N) = \ card\{\mathbf{I}, \mathbf{S} \neq\in J^\varphi \ satisfying\ (A)\}.$ *Then*
$$\mathbb{E}(\mathcal{N}) = \left(\frac{(N^k-\varphi)!}{N^k!}\right)^2 \frac{m!}{(m-\varphi)!}\, P(N)$$

Remark 1. $P(N)$ will be the value returned by our computer program that gives the number of solutions of system (A).

Proof. We have:

$$\mathbb{E}(\mathcal{N}) = \frac{\displaystyle\sum_{f\in\mathcal{B}_{nk}} \sum_{M\in J_m} \sum_{\substack{(i_1,\ldots,i_\varphi)\\ \neq\in[1,m]^\varphi}} n_{i_1,\ldots,i_\varphi,f,M}}{|\mathcal{B}_{kn}| \times |J_m|}$$

where $n_{i_1,\ldots,i_\varphi,f,M}$ is equal to 1 or 0 for the given f, M and $i_1, \ldots, i_\varphi$ whether or not the φ-attack is verified for the points $\big(M(i_1), f(M(i_1))\big), \ldots \big(M(i_\varphi), f(M(i_\varphi))\big)$. When $f \in \mathcal{B}_{kn}$ is given, we have:

$$\begin{aligned}\sum_{M\in J_m} \sum_{\substack{(i_1,\ldots,i_\varphi)\\ \neq\in[1,m]^\varphi}} n_{i_1,\ldots,i_\varphi,f,M} &= \sum_{M\in J_m} \sum_{\substack{(i_1,\ldots,i_\varphi)\\ \neq\in[1,m]^\varphi}} \sum_{\mathbf{I}\neq\in J^\varphi} n' \prod_{u=1}^{\varphi} \delta_{I(u)M(i_u)}\\ &= \sum_{\mathbf{I}\neq\in J^\varphi} n' \sum_{M\in J_m} \sum_{\substack{(i_1,\ldots,i_\varphi)\\ \neq\in[1,m]^\varphi}} \prod_{u=1}^{\varphi} \delta_{I(u)M(i_u)}\end{aligned}$$

where $n' = n'_{I(1),\ldots,I(\varphi),f}$ is equal to 1 or 0 for the given $\mathbf{I}$ and f. And,

$$\sum_{M\in J_m} \sum_{\substack{(i_1,\ldots,i_\varphi)\\ \neq\in[1,m]^\varphi}} \prod_{u=1}^{\varphi} \delta_{I(u)M(i_u)} = \mathrm{card}\{M \in J_m \mid \{I(1), \ldots, I(\varphi)\} \subset M\}$$

$$
\begin{aligned}
&= \frac{\binom{N^k-\varphi}{m-\varphi}}{|J_m|}|J_m| = \frac{\binom{N^k-\varphi}{m-\varphi}}{\binom{N^k}{m}}|J_m| \\
&= \frac{(N^k-\varphi)!}{(m-\varphi)!(N^k-m)!} \times \frac{m!(N^k-m)!}{N^k!}|J_m| \\
&= \frac{(N^k-\varphi)!}{N^k!}\frac{m!}{(m-\varphi)!}|J_m|
\end{aligned}
$$

Thus,

$$
\mathbb{E}(\mathcal{N}) = \frac{m!(N^k-\varphi)!}{|\mathcal{B}_{nk}|(m-\varphi)!N^k!} \sum_{f\in\mathcal{B}_{nk}} \sum_{\mathbf{I}\neq\in J^\varphi} n'_{I(1),\ldots,I(\varphi),f}
$$

Furthermore:

$$
n' = \sum_{\mathbf{S}\neq\in J^\varphi} n''_{I(1),\ldots,I(\varphi),S(1),\ldots,S(\varphi)} \prod_{u=1}^{\varphi} \delta_{S(u)f(I(u))}
$$

where $n''_{I(1),\ldots,I(\varphi),S(1),\ldots,S(\varphi)}$ equal 1 or 0 for the given $\mathbf{I}$ and $\mathbf{S}$. So:

$$
\sum_{f\in\mathcal{B}_{nk}} \sum_{\substack{\mathbf{I}\neq\in J^\varphi \\ \mathbf{S}\neq\in J^\varphi}} n'' \prod_{u=1}^{\varphi} \delta_{S(u)f(I(u))} = \sum_{\substack{\mathbf{I}\neq\in J^\varphi \\ \mathbf{S}\neq\in J^\varphi}} n'' \sum_{f\in\mathcal{B}_{nk}} \prod_{u=1}^{\varphi} \delta_{S(u)f(I(u))}
$$

And,

$$
\begin{aligned}
\sum_{f\in\mathcal{B}_{kn}} \prod_{u=1}^{\varphi} \delta_{S(u)f(I(u))} &= \mathrm{card}\{f\in\mathcal{B}_{nk} \mid \forall u \in \{1,\ldots,\varphi\},\ f(I(u)) = S(u)\} \\
&= (N^k-\varphi)!
\end{aligned}
$$

Finally,

$$
\begin{aligned}
\mathbb{E}(\mathcal{N}) &= \left(\frac{(N^k-\varphi)!}{N^k!}\right)^2 \frac{m!}{(m-\varphi)!} \sum_{\substack{\mathbf{I}\neq\in J^\varphi \\ \mathbf{S}\neq\in J^\varphi}} n''_{\mathbf{I},\mathbf{S}} \\
&= \left(\frac{(N^k-\varphi)!}{N^k!}\right)^2 \frac{m!}{(m-\varphi)!}\ \mathrm{card}\{\mathbf{I},\mathbf{S} \neq\in J^\varphi \text{ satisfying } (A)\} \\
&= \left(\frac{(N^k-\varphi)!}{N^k!}\right)^2 \frac{m!}{(m-\varphi)!}P(N)
\end{aligned}
$$

as claimed. □

3.2 Computation of $\mathbb{E}(\tilde{\mathcal{N}})$

Because of the introduction of new notations, we will state the proposition at the end of this subsection. As previously, we have $1 \leq u \leq \varphi$.

The same computation for $\mathbb{E}(\tilde{\mathcal{N}})$ gives:

$$\mathbb{E}(\tilde{\mathcal{N}}) = \frac{(N^k-\varphi)!}{N^k!} \frac{\frac{m!}{(m-\varphi)!}}{|\Psi^d|} \sum_{\substack{\mathbf{I} \neq\in J^\varphi \\ \mathbf{S} \neq\in J^\varphi}} n''_{\mathbf{I},\mathbf{S}} \times \mathrm{card}\{f \in \Psi^d \mid \forall u,\ f(I(u)) = S(u)\}$$

If $I(u)$ are distinct and f is a bijection with $f(I(u)) = S(u)$ for all u, then we have necessary $S(u)$ distinct, so we do not need to add this condition, and:

$$\mathbb{E}(\tilde{\mathcal{N}}) = \frac{(N^k-\varphi)!}{N^k!} \frac{\frac{m!}{(m-\varphi)!}}{|\Psi^d|} \underbrace{\sum_{\substack{\mathbf{I} \neq\in J^\varphi \\ \mathbf{S} \in J^\varphi}} n''_{\mathbf{I},\mathbf{S}} \times \mathrm{card}\{f \in \Psi^d \mid \forall u,\ f(I(u)) = S(u)\}}_{\Sigma_1}$$

For the Feistel scheme used to go from $I(u)$ to $S(u)$, we only have to know some information from the internal functions f^1, ..., f^d. For this, we need to introduce new variables that are the outputs of the internal functions.

Definition 1. *For all $u \in \{1, \dots, \varphi\}$ and all turn $r \in \{1, \dots, d\}$ $K_r(u) = f^r(I_1^{r-1}(u))$, with the following rule: $I_1^r(i) = I_1^r(j) \iff K_{r+1}(i) = K_{r+1}(j)$. We define $\mathbf{K} = K_r(u)_{1 \le u \le \varphi,\ 1 \le r \le d}$.*

Taking into account account this rule, how many different cases do we have to consider?
For each turn r we will consider the equalities between $I_1^{r-1}(1), \dots, I_1^{r-1}(\varphi)$. This corresponds to the number of partition of a set of φ elements. The number of partition of a set of φ elements is the Bell number B_φ, and the number of partitions with p subsets is the second type number of Stirling $S(\varphi, p)$. Moreover, we have the formula:

$$B_\varphi = \sum_{p=1}^{\varphi} S(\varphi, p)$$

When we want to compute $S(\varphi, p)$, there exist several kinds of partitions. For example, if $\varphi = 5$ and $p = 3$, we have $\binom{5}{3} = 10$ ways to have a group of 3 and two groups of 1, and $5 \times 3 = 15$ ways to have two groups of 2 and one group of 1. So $S(5, 3) = 25$. In that case, there are 2 kinds of partitions. Thus, in computing $S(\varphi, p)$, the number t will denote the chosen kind of partition. Thus we obtain:

$$\Sigma_1 = \sum_{p_1=1}^{\varphi} \dots \sum_{p_d=1}^{\varphi} \sum_{t_1=1}^{S(\varphi,p_1)} \dots \sum_{t_d=1}^{S(\varphi,p_d)} \mathrm{card}\{I \neq\in J^\varphi, f \in \Psi^d \text{ satisfying } (A)$$
$$\text{and induced equalities and non-equalities from } t_1, \dots, t_d\}$$

Let (A') be the system derived from (A) where we have added the equalities and non-equalities induced by the choice of $p_1, \dots, p_d$, and $t_1, \dots, t_d$, and where we have replaced the values of $\mathbf{S}$ in function of $\mathbf{I}$ and $\mathbf{K}$. For this system, the variables are only $I_i(u)$ and $K_r(u)$ (in total $k\varphi + d\varphi$ variables).

$$\begin{aligned}\Sigma_1 &= \sum_{(p_1,\ldots,p_d)} \sum_{(t_1,\ldots,t_d)} \frac{|\Psi^d|}{N^{p_1+p_2+\ldots p_d}} \mathrm{card}\{\mathbf{I} \not\neq\in J^\varphi, \mathbf{K} \text{ satisfying } (A')\} \\ &= \frac{|\Psi^d|}{N^{\varphi d}} \sum_{p_1,\ldots,p_d} \sum_{t_1,\ldots,t_d} \mathrm{card}\{\mathbf{I} \not\neq\in J^\varphi, \mathbf{K}, K'_1, \ldots, K'_{\varphi d-p} \text{ satisfying } (A')\}\end{aligned}$$

where K'_i are (artificial) other values taken by the round functions that enabled us to simplify the computation (we just increase by one the number of variables each time we have an equality between the variables $I_1^r(u)$). We can now state the result:

Proposition 2. *Let Q be the polynomial defined by:*

$$Q(N) = \sum_{(p_1,\ldots,p_d)} \sum_{(t_1,\ldots,t_d)} \mathit{card}\{\mathbf{I} \not\neq\in J^\varphi, \mathbf{K}, K'_1 \ldots K'_{\varphi d-p} \text{ satisfying } (A')\}.$$

Then: $\mathbb{E}(\tilde{\mathcal{N}}) = \dfrac{(N^k-\varphi)!}{N^k!} \dfrac{\frac{m!}{(m-\varphi)!}}{N^{\varphi d}} Q(N)$.

Remark 2. $Q(N)$ will be returned by our computer program that gives the number of solutions of the systems.

4 Computing $V(\mathcal{N})$

Proposition 3. *Let $X = \sum_{i=1}^n X_i$ be a random variable, where each X_i follow a Bernoulli distribution. Then,*

$$V(X) = -\mathbb{E}(X)^2 + \sum_{i,j} \mathbb{E}(X_i X_j)$$

Proof.

$$\begin{aligned}V(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 &= \mathbb{E}\left(\sum_{i=1}^n X_i^2 + \sum_{i\neq j} X_i X_j\right) - \mathbb{E}(X)^2 \\ &= \mathbb{E}(X) - \mathbb{E}(X)^2 + \sum_{i\neq j} \mathbb{E}(X_i X_j) = -\mathbb{E}(X)^2 + \sum_{i,j} \mathbb{E}(X_i X_j)\end{aligned}$$

□

Since $\mathcal{N} = \sum_{\mathbf{i} \not\neq\in \{1,\ldots,m\}^\varphi} \mathcal{N}_{\mathbf{i}}$, we have the corollary:

Corollary 1.

$$V(\mathcal{N}) = -\mathbb{E}(\mathcal{N})^2 + \sum_{\mathbf{i},\mathbf{j}} \mathbb{E}(\mathcal{N}_{\mathbf{i}} \mathcal{N}_{\mathbf{j}})$$

$$V(\tilde{\mathcal{N}}) = -\mathbb{E}(\tilde{\mathcal{N}})^2 + \sum_{\mathbf{i},\mathbf{j}} \mathbb{E}(\tilde{\mathcal{N}}_{\mathbf{i}} \tilde{\mathcal{N}}_{\mathbf{j}})$$

We now continue with the computation of $\sum_{\mathbf{i},\mathbf{j}} \mathbb{E}(\mathcal{N}_{\mathbf{i}}\mathcal{N}_{\mathbf{j}})$.

Proposition 4. *Let $P(N,m)$ be defined by:*

$$P(N,m) = \sum_{h=0}^{\varphi} \prod_{i=1}^{h} (N^k - 2\varphi + i)^2 \prod_{i=h+1}^{\varphi} (m - 2\varphi + i) \sum_{\substack{I,I' \neq\in J^{\varphi} \\ |I \cap I'| = h}} \sum_{\substack{S,S' \neq\in J^{\varphi} \\ S(i)=S'(i) \\ \Longleftrightarrow \\ I(i)=I'(i)}} n''_{I,S} n''_{I',S'} \quad (1)$$

Then

$$\sum_{\mathbf{i},\mathbf{j}} \mathbb{E}(\mathcal{N}_{\mathbf{i}}\mathcal{N}_{\mathbf{j}}) = \frac{\prod_{i=1}^{\varphi} (m - i + 1)}{\prod_{i=1}^{2\varphi} (N^k - i + 1)^2} P(N,m) \quad (2)$$

Remark 3. $P(N,m)$ will be returned by the computer program.

Proof. We have:

$$\begin{aligned}
\sum_{\mathbf{i},\mathbf{j}} \mathbb{E}(\mathcal{N}_{\mathbf{i}}\mathcal{N}_{\mathbf{j}}) &= \mathbb{E}(\sum_{\mathbf{i},\mathbf{j}} \mathcal{N}_{\mathbf{i}}\mathcal{N}_{\mathbf{j}}) \\
&= \frac{\sum_{f \in \mathcal{B}_{kn}} \sum_{M \in J_m} \sum_{\mathbf{i},\mathbf{j}} n_{\mathbf{i},f,M} n_{\mathbf{j},f,M}}{|\mathcal{B}_{kn}| \times |J_m|}
\end{aligned}$$

$$\begin{aligned}
\sum_{M \in J_m} \sum_{\mathbf{i},\mathbf{j}} n_{\mathbf{i},f,M} n_{\mathbf{j},f,M} &= \sum_{M \in J_m} \sum_{\mathbf{i},\mathbf{j}} \sum_{I \neq\in J^{\varphi}} \sum_{I' \neq\in J^{\varphi}} n_{\mathbf{i},f,M} n_{\mathbf{j},f,M} \prod_{u=1}^{\varphi} \delta_{I(u)M(i_u)} \delta_{I'(u)M(j_u)} \\
&= \sum_{M \in J_m} \sum_{\mathbf{i},\mathbf{j}} \sum_{I \neq\in J^{\varphi}} \sum_{I' \neq\in J^{\varphi}} n'_{I,f} n'_{I',f} \prod_{u=1}^{\varphi} \delta_{I(u)M(i_u)} \delta_{I'(u)M(j_u)} \\
&= \sum_{I \neq\in J^{\varphi}} \sum_{I' \neq\in J^{\varphi}} n'_{I,f} n'_{I',f} \sum_{M \in J_m} \underbrace{\sum_{\mathbf{i},\mathbf{j}} \prod_{u=1}^{\varphi} \delta_{I(u)M(i_u)} \delta_{I'(u)M(j_u)}}_{1 \text{ iff } I \subset M \text{ and } I' \subset M, 0 \text{ otherwise}} \\
&= \sum_{I \neq\in J^{\varphi}} \sum_{I' \neq\in J^{\varphi}} n'_{I,f} n'_{I',f} \operatorname{card}\{M \in J_m \mid I \subset M \text{ and } I' \subset M\} \\
&= \sum_{h=0}^{\varphi} \sum_{\substack{I,I' \neq\in J^{\varphi} \\ |I \cap I'| = h}} n'_{I,f} n'_{I',f} \underbrace{\binom{N^k - 2\varphi + h}{m - 2\varphi + h}}_{\Lambda} \\
&= \sum_{h=0}^{\varphi} \Lambda \sum_{\substack{I,I' \neq\in J^{\varphi} \\ |I \cap I'| = h}} \sum_{\substack{S,S' \neq\in J^{\varphi} \\ S(i)=S'(i) \\ \Longleftrightarrow \\ I(i)=I'(i)}} n''_{I,S} n''_{I',S'} \prod_{u=1}^{\varphi} \delta_{S(u)f(I(u))} \delta_{S'(u)f(I'(u))}
\end{aligned}$$

So, $\displaystyle\sum_{f\in\mathcal{B}_{kn}}\sum_{M\in J_m}\sum_{\mathbf{i},\mathbf{j}} n_{\mathbf{i},f,M}n_{\mathbf{j},f,M} =$

$$= \sum_{h=0}^{\varphi} \mathit{\Lambda} \sum_{\substack{I,I' \neq\in J^{\varphi} \\ |I\cap I'|=h}} \sum_{\substack{S,S' \neq\in J^{\varphi} \\ S(i)=S'(i) \\ \Longleftrightarrow \\ I(i)=I'(i)}} n''_{I,S}n''_{I',S'}\mathrm{card}\{f\in\mathcal{B}_{kn} \mid f(I)=S, f(I')=S'\}$$

$$= \sum_{h=0}^{\varphi} \mathit{\Lambda} \sum_{\substack{I,I' \neq\in J^{\varphi} \\ |I\cap I'|=h}} \sum_{\substack{S,S' \neq\in J^{\varphi} \\ S(i)=S'(i) \\ \Longleftrightarrow \\ I(i)=I'(i)}} n''_{I,S}n''_{I',S'}(N^k-2\varphi+h)!$$

$$= \sum_{h=0}^{\varphi} \frac{(N^k-2\varphi+h)!^2}{(N^k-m)!(m-2\varphi+h)!} \sum_{\substack{I,I' \neq\in J^{\varphi} \\ |I\cap I'|=h}} \sum_{\substack{S,S' \neq\in J^{\varphi} \\ S(i)=S'(i) \\ \Longleftrightarrow \\ I(i)=I'(i)}} n''_{I,S}n''_{I',S'}$$

So,

$$\sum_{\mathbf{i},\mathbf{j}} \mathbb{E}(\mathcal{N}_{\mathbf{i}}\mathcal{N}_{\mathbf{j}}) = \frac{m!}{(N^k!)^2}\sum_{h=0}^{\varphi} \frac{(N^k-2\varphi+h)!^2}{(m-2\varphi+h)!} \sum_{\substack{I,I' \neq\in J^{\varphi} \\ |I\cap I'|=h}} \sum_{\substack{S,S' \neq\in J^{\varphi} \\ S(i)=S'(i) \\ \Longleftrightarrow \\ I(i)=I'(i)}} n''_{I,S}n''_{I',S'}$$

$$= \frac{\displaystyle\prod_{i=1}^{\varphi}(m-i+1)}{\displaystyle\prod_{i=1}^{2\varphi}(N^k-i+1)^2} \sum_{h=0}^{\varphi}\prod_{i=1}^{h}(N^k-2\varphi+i)^2 \prod_{i=h+1}^{\varphi}(m-2\varphi+i) \sum_{\substack{I,I' \neq\in J^{\varphi} \\ |I\cap I'|=h}} \sum_{\substack{S,S' \neq\in J^{\varphi} \\ S(i)=S'(i) \\ \Longleftrightarrow \\ I(i)=I'(i)}} n''_{I,S}n''_{I',S'}$$

Thus

$$\sum_{\mathbf{i},\mathbf{j}} \mathbb{E}(\mathcal{N}_{\mathbf{i}}\mathcal{N}_{\mathbf{j}}) = \frac{\displaystyle\prod_{i=1}^{\varphi}(m-i+1)}{\displaystyle\prod_{i=1}^{2\varphi}(N^k-i+1)^2} P(N,m)$$

as claimed □

Corollary 2. *We have:* $V(\mathcal{N}) = -\mathbb{E}(\mathcal{N})^2 + \dfrac{\displaystyle\prod_{i=1}^{\varphi}(m-i+1)}{\displaystyle\prod_{i=1}^{2\varphi}(N^k-i+1)^2} P(N,m).$

5 The general algorithm to compute a mirror system

As we have seen previously, the main task to obtain the values of expectations and variances is to compute the number of solutions of systems of linear equalities and linear non-equalities. According to [25], we call such systems “Mirror

systems". In this paper, we have counted the number of solutions of a mirror system over $(\mathbb{Z}/2\mathbb{Z})^n$. This algorithm has some similarities with those used to compute the chromatic polynomial of a graph.
We suppose that the mirror system has no specificities, i.e. the right parts of the equalities and the non-equalities can be null or not, and the number of variables in each equality or non-equality is not necessary even.

Notations and example. We will illustrate our algorithm with one major example. We want to compute the number of solutions of the following mirror system with 8 variables A, B, C, D, E, G, H, I over the group $(\mathbb{Z}/2\mathbb{Z})^n$ of cardinal N. We write inside the system, and between parenthesis, the number of variables, and we put the $\sharp$ symbol in order to signify "number of solutions".

$$P(N) = \sharp \left\{ (8) \begin{array}{ccccccccl}
A & +B & +C & & +E & & & & = 0 \\
A & +B & & +D & & & & & = 0 \\
 & & C & +D & +E & & & & = 0 \\
A & & +C & +D & & & & & \neq 0 \\
 & B & +C & & +E & & & & \neq 0 \\
 & & & & & G & & +I & \neq 0 \\
 & & & & & G & +H & & \neq 0 \\
 & & & & & & H & +I & \neq 0
\end{array} \right.$$

Gaussian reduction. We transform the equalities to obtain a triangular system, thanks to a Gaussian reduction. Then we use these equalities to get rid of some the variables in the non-nequalities.
▷ Illustration:

$$P(N) = \sharp \left\{ (8) \begin{array}{ccccccccl}
A & +B & +C & & +E & & & & = 0 \\
 & & C & +D & +E & & & & = 0 \\
 & & & & 0 & & & & = 0 \\
 & B & & +D & +E & & & & \neq 0 \\
 & B & & +D & & & & & \neq 0 \\
 & & & & & G & & +I & \neq 0 \\
 & & & & & G & +H & & \neq 0 \\
 & & & & & & H & +I & \neq 0
\end{array} \right. \quad \text{(we get rid of } A \text{ and } C\text{)}$$

Elimination of all equalities. Each first variable of the independent linear equalities can only have one value when the other are fixed.
So we can eliminate all equalities and subtract to the number of variables, the number of independent equalities.
▷ Illustration: we have only one choice for the both variables A and C, when the others are fixed. So we can get rid of all the equalities, and the number of

variables becomes $8-2=6$. Now,

$$P(N) = \sharp \begin{cases} (6) & \begin{array}{lllllll} B & +D & +E & & & & \neq 0 \\ B & +D & & & & & \neq 0 \\ & & & G & & +I & \neq 0 \\ & & & G & +H & & \neq 0 \\ & & & & H & +I & \neq 0 \end{array} \end{cases}$$

Look for joint variables. Then we look for variables that appear always together in the non-equalities.

▷ Illustration: here we notice that B and D satisfy this property. We define a new variable, $F = B + D$. For every possibility for F, we will have N choices for (B, D). So:

$$P(N) = \sharp \begin{cases} (6) & \begin{array}{llllll} F & +E & & & & \neq 0 \\ F & & & & & \neq 0 \\ & & G & & +I & \neq 0 \\ & & G & +H & & \neq 0 \\ & & & H & +I & \neq 0 \end{array} \end{cases}$$

Split into independent systems of non-equalities. We now try to split the system into several independent systems. We attribute to each new system the number of variables involved in it. Then we will multiply the different polynomials obtained with theses new systems and we will end by multiplying with N^d where d are the remaining variables.

▷ Illustration:

$$P(N) = \sharp \begin{cases} (2) & \begin{array}{lll} F & +E & \neq 0 \\ F & & \neq 0 \end{array} \end{cases} \times \sharp \begin{cases} (3) & \begin{array}{llll} G & & +I & \neq 0 \\ G & +H & & \neq 0 \\ & H & +I & \neq 0 \end{array} \end{cases} \times N^{6-2-3}$$

Recursive final algorithm.

- If there is no inequality at all, in this case the number of solutions is N^v where v is the number of remaining variables.
- When there are non-equalities without variable, the number of solution is 0.
- If a variable appears only in one non-equality, the number of solutions is $N-1$ multiplied by the number of solution of the system with one less variable and without the concerned non-equality.
- In all other cases, we will use a fusion-like algorithm. We count the number of solutions of 2 new systems. The first one without the last non-equality, and the second one with the last non-equality transformed into an equality. Then we subtract the two polynomials.

▷ Illustration:

$$Q(N) = \sharp \begin{cases} (2) & \begin{array}{lll} F & +E & \neq 0 \\ F & & \neq 0 \end{array} \end{cases} = (N-1)\sharp \begin{cases} (1) \, F \neq 0 \end{cases} = (N-1)^2$$

$$\begin{aligned} R(N) &= \sharp\left\{(3)\begin{array}{lll} G & & +I \neq 0 \\ G & +H & \neq 0 \\ & H & +I \neq 0 \end{array}\right. \\ &= \sharp\left\{(3)\begin{array}{lll} G & & +I \neq 0 \\ G & +H & \neq 0 \end{array}\right. - \sharp\left\{(3)\begin{array}{lll} G & & +I \neq 0 \\ G & +H & \neq 0 \\ & H & +I = 0 \end{array}\right. \\ &= N(N-1)^2 - \sharp\left\{(2)\begin{array}{ll} G & +I \neq 0 \\ G & +I \neq 0 \end{array}\right. \\ &= N(N-1)^2 - N(N-1) = N(N-1)(N-2) \end{aligned}$$

Finally:

$$P(N) = Q(N) \times R(N) \times N = N^2(N-1)^3(N-2)$$

6 Application to several examples of attacks

6.1 Notation for Feistel-type schemes

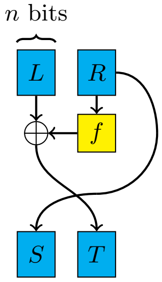
With Feistel type schemes, according to the structure of the scheme, internal variables are defined at each round. Conditions that are imposed on these internal variables will allow the differential path to propagate. Thus, once conditions on the input variables are settled, the conditions on the output variables will appear either at random or due to conditions satisfied by some internal variables. We consider two types of attacks: 2-point attacks, where we use plaintext/ciphertext pairs and φ-point attacks, where we use φ-tuples of plaintext/ciphertexts. These last attacks allow more possibilities of conditions on the inputs, the outputs and the internal variables. They were first introduced in [16] and then generalized in [29, 33].

6.2 Examples of 2-point attacks

Differential notation for 2-point attacks We use plaintext/ciphertext pairs. In KPA, on the input variables, the notation $[\mathbf{0}, \mathbf{0}, \mathit{\Delta}_3^0, \mathit{\Delta}_4^0, \ldots, \mathit{\Delta}_k^0]$ means that the pair of messages (i, j) satisfies $I_1(i) = I_1(j)$, $I_2(i) = I_2(j)$, and $I_s(i) \oplus I_s(j) = \mathit{\Delta}_s^0$, $3 \leq s \leq k$. The differential of the outputs i and j after round r is denoted by $[\mathit{\Delta}_1^r, \mathit{\Delta}_2^r, \ldots, \mathit{\Delta}_k^r]$. At each round, internal variables are defined by the structure of the scheme. In our attacks, we determine conditions that have to be satisfied by the outputs. When we have a scheme, these conditions are satisfied either at random or because the internal variables verify some equalities. Thus, we will impose conditions on the internal variables on some chosen rounds. When we impose conditions on the internal variables in order to get a differential characteristic, we use the notation $\boxed{0}$ to mean that the corresponding internal variables are equal in messages i and j. When we write 0 to specify that this condition propagates.

Classic Feistel scheme Ψ^5: "2-point attack" The first round of a classical Feistel scheme is represented in Figure 2.

Fig. 2. One round of a classical Feistel scheme



The input is denoted by $[I_1, I_2]$ and the output by $[S_1, S_2]$. For the message i, the input and the output are denoted by $[I_1(i), I_2(i)]$ and $[S_1(i), S_2(i)]$. We have m messages and we want to compute the expectation of the number $\mathcal{N}$ of 2-tuples of points satisfying the following relations:

$$\begin{cases} S_2(i) \neq S_2(j) \\ S_1(i) = S_1(j) \\ I_2(i) = I_2(j) \\ S_2(i) \oplus S_2(j) = I_1(i) \oplus I_1(j) (\neq 0) \end{cases}$$

Thanks to our tool, we obtain:

$$\mathbb{E}(\mathcal{N}) = \frac{1}{N^4(N^2-1)^2} \frac{m!}{(m-2)!}(-N^4 + N^5) = \frac{m(m-1)}{(N+1)^2(N-1)} \sim \frac{m^2}{N^3}$$

$$V(\mathcal{N}) = -\mathbb{E}(\mathcal{N})^2 + \frac{m(m-1)}{N^4(N^2-1)^2(N^2-2)^2(N^2-3)^2} P(N,m)$$

with

$$\begin{aligned} P(N,m) = {} & 2N^{13} - 2N^{12} - 20N^{11} + (18 - m + m^2)N^{10} + (86 - 2m - 2m^2)N^9 \\ & + (-84 + 19m - 7m^2)N^8 + (-144 - 28m + 20m^2)N^7 + (168 - 32m \\ & + 4m^2)N^6 + (24 + 112m - 44m^2)N^5 + (-48 - 68m + 28m^2)N^4 \end{aligned}$$

$$\begin{aligned} V(\mathcal{N}) = {} & \frac{2m(m-1)}{(N^2-3)^2(N^2-2)^2(N^2-1)^2(N+1)^2} \times \\ & \Big[\; N^{11} + N^{10} - 11N^9 - 12N^8 + (51 - 2m)N^7 + (2m + 53)N^6 + \\ & (2m^2 + 4m - 113)N^5 + (-16m - 102)N^4 + (108 - 8m^2 + 10m)N^3 + \\ & (32m + 84 + 2m^2)N^2 + (-36 + 6m^2 - 12m)N - 24 - 4m^2 - 16m \; \Big] \\ \sim {} & \frac{2m^2}{N^3} \end{aligned}$$

With a classical Feistel scheme, the wanted equalities can happen at random or due to conditions that are satisfied on internal variables and give a differential path as shown in table 1. However, the program allows to calculate the exact value for the expectation. In the computation of $\mathbb{E}(\tilde{\mathcal{N}})$, we have to count two mirror systems (beware we have switched left and right part of the scheme) that correspond to two differential paths:

Table 1. Attack on Ψ^5

round	Δ_1^0	$\mathbf{0}$
1	0	Δ_1^0
2	Δ_1^0	$\boxed{0}$
3	0	Δ_1^0
4	Δ_1^0	$\boxed{0}$
5	0	Δ_1^0

$$\left\{\begin{array}{l}
I_1(1) \oplus K_2(1) \oplus K_4(1) \oplus I_1(2) \oplus K_2(2) \oplus K_4(2) = 0\\
K_1(1) \oplus K_3(1) \oplus K_5(1) \oplus K_1(2) \oplus K_3(2) \oplus K_5(2) = 0\\
K_2(1) \oplus K_4(1) \oplus K_2(2) \oplus K_4(2) = 0\\
K_3(1) \oplus K_5(1) \oplus K_3(2) \oplus K_5(2) = 0\\
K_5(1) \oplus K_5(2) = 0\\
I_2(1) \oplus I_2(2) \neq 0\\
K_4(1) \oplus K_4(2) \neq 0
\end{array}\right.$$

Number of solutions: $N^9 - 2N^{10} + N^{11}$

$$\left\{\begin{array}{l}
I_1(1) \oplus K_2(1) \oplus K_4(1) \oplus I_1(2) \oplus K_2(2) \oplus K_4(2) = 0\\
K_1(1) \oplus K_3(1) \oplus K_5(1) \oplus K_1(2) \oplus K_3(2) \oplus K_5(2) = 0\\
K_2(1) \oplus K_4(1) \oplus K_2(2) \oplus K_4(2) = 0\\
K_3(1) \oplus K_5(1) \oplus K_3(2) \oplus K_5(2) = 0\\
K_4(1) \oplus K_4(2) = 0\\
K_5(1) \oplus K_5(2) = 0\\
I_2(1) \oplus I_2(2) \neq 0
\end{array}\right.$$

Number of solutions: $-N^{10} + N^{11}$

The total number of solutions is given by: $N^9 - 3N^{10} + 2N^{11}$

So :

$$\mathbb{E}(\tilde{\mathcal{N}}) = \frac{m(m-1)}{N^2(N^2-1)} \times \frac{N^9 - 3N^{10} + 2N^{11}}{N^{10}} = \frac{m(m-1)(2N+1)}{N^3(N+1)} \sim \frac{2m^2}{N^3}$$

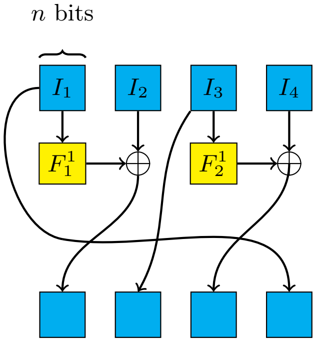
Thus the expectation for a classical Feistel scheme with 5 rounds is about twice the expectation we had for a random permutation as expected. This attack is taken from [24].

Also if $m \sim N^{3/2}$, then we can distinguish a permutation generated by classical Feistel scheme with 5 rounds from a random permutation and the attack is successful.

Remark 4. In this attack, the expectation is about the double for a Feistel cipher than for a random permutation, thus there is no need to compute the standard deviation. However, we can notice that here $\sigma(\mathcal{N}) \simeq \sqrt{\mathbb{E}(\mathcal{N})}$. In all 2-point attacks that we have studied, this is always the case.

Type-2 Feistel schemes with $k = 4$ and $r = 10$: "2-point attack"

Fig. 3. One round of a Type-2 Feistel scheme



Results for any n. In Figure 3, one round of a Type-2 is represented with $k = 4$.

The input and output are still denoted by $[I_1, I_2, I_3, I_4]$ and $[S_1, S_2, S_3, S_4]$. For the message i, the input and the output are denoted by $[I_1(i), I_2(i), I_3(i), I_4(i)]$ and $[S_1(i), S_2(i), S_3(i), S_4(i)]$. We have m messages and we want to compute the mean of value of the number $\mathcal{N}$ of pairs of points satisfying the following relations:

$$\begin{cases} I_1(i) = I_1(j) \\ S_4(i) \oplus S_4(j) = I_2(i) \oplus I_2(j) \end{cases}$$

For this attack, there are 10 mirror systems. Here is an example of one system, whose number of solution is give, by $N^{12} - 2N^{13} + N^{14}$.

$$\left\{\begin{array}{llll} I_1(i)\oplus I_1(j) & & & =0 \\ & I_2(i)\oplus I_2(j) & & \oplus S_4(i)\oplus S_4(j)=0 \\ & & & S_4(i)\ \oplus S_4(j)\neq 0 \\ & & S_1(i)\oplus S_1(j) & \neq 0 \end{array}\right.$$

Finally, the total number of solutions is $N^8 - N^{10} - N^{11} + N^{14}$ and the expectation is given by:

$$\mathbb{E}(\mathcal{N}) = \frac{m(m-1)}{N^8(N^4-1)^2}(N^8 - N^{10} - N^{11} + N^{14})$$

$$\mathbb{E}(\mathcal{N}) = \frac{m(m-1)(N^6 - N^3 - N^2 + 1)}{(N^4-1)^2} = \frac{m^2}{N^2} - \frac{m^2}{N^5} + O(\frac{1}{N^6}) \sim \frac{m^2}{N^2}$$

For the variance, we have

$$V(\mathcal{N}) = -\mathbb{E}(\mathcal{N})^2 + \frac{m(m-1)}{(N^4(N^4-1)(N^4-2)(N^4-3))^2}P(N, m)$$

with

$$P(N, m) = -36N^8m + 36N^8m^2 - 180N^9 + 150N^9m - 30N^9m^2 + 246N^{10}$$

$$-121N^{10}m - 19N^{10}m^2 - 1212N^{11} + 1058N^{11}m - 244N^{11}m^2 + 2592N^{12}$$
$$-2172N^{12}m + 408N^{12}m^2 - 1194N^{13} + 863N^{13}m - 133N^{13}m^2 + 1116N^{14}$$
$$-1094N^{14}m + 316N^{14}m^2 - 4308N^{15} + 3678N^{15}m - 732N^{15}m^2 + 5082N^{16}$$
$$-4128N^{16}m + 812N^{16}m^2 - 4308N^{17} + 3750N^{17}m - 798N^{17}m^2 + 3418N^{18}$$
$$-2842N^{18}m + 518N^{18}m^2 - 1244N^{19} + 947N^{19}m - 181N^{19}m^2 - 30N^{20} - 61N^{20}m$$
$$+33N^{20}m^2 - 44N^{21} - 26N^{21}m + 24N^{21}m^2 + 12N^{22} + 43N^{22}m - N^{22}m^2 + 52N^{23}$$
$$-20N^{23}m + 2N^{23}m^2 + 14N^{24} + 14N^{24}m - 10N^{24}m^2 + 12N^{25} - 2N^{25}m - 2N^{25}m^2$$
$$-22N^{26} - 2N^{27} - 2N^{28} - N^{28}m + N^{28}m^2 + 2N^{30}$$

This gives: $V(\mathcal{N}) \sim \frac{2N^{28}m^2}{N^{30}} = \frac{2m^2}{N^2}$, and the variance is about twice the expectation.

We now compute the expectation for the scheme. Here the number of round functions is 20. Thus the number of rounds is 10 but the number of turns is 20, as explained in section 2. We have for example the differential path given in table 2.

Table 2. Attack on a Type-2 Feistel scheme with $k = 4$ and 10 rounds.

round	$\mathbf{0}$	Δ_2^0	Δ_3^0	Δ_4^0
1	Δ_2^0	Δ_3^0	Δ_3^1	0
2	Δ_1^2	Δ_3^1	$\boxed{0}$	Δ_2^0
3	Δ_1^3	0	Δ_2^0	Δ_1^2
4	$\boxed{0}$	Δ_2^0	Δ_3^4	Δ_1^3
5	Δ_2^0	Δ_3^4	Δ_3^5	0
6	Δ_1^6	Δ_3^5	$\boxed{0}$	Δ_2^0
7	Δ_1^7	0	Δ_2^0	Δ_1^6
8	$\boxed{0}$	Δ_2^0	Δ_3^8	Δ_1^7
9	Δ_2^0	Δ_3^8	Δ_3^9	0
10	Δ_1^{10}	Δ_3^9	Δ_3^{10}	Δ_2^0

For the scheme, with our program, we find 3 different systems when we consider that the input must be different :
Mirror system 1 :

$$\begin{aligned} I_1(1) \oplus I_1(2) = 0 \\ K_1(1) \oplus K_6(1) \oplus K_9(1) \oplus K_{14}(1) \oplus K_{17}(1) \\ \oplus K_1(2) \oplus K_6(2) \oplus K_9(2) \oplus K_{14}(2) \oplus K_{17}(2) = 0 \\ I_2(1) \oplus I_2(2) \neq 0 \end{aligned}$$

Mirror system 2 :

$$
\begin{aligned}
I_1(1) \oplus I_1(2) = 0 \\
I_2(1) \oplus I_2(2) = 0 \\
K_1(1) \oplus K_6(1) \oplus K_9(1) \oplus K_{14}(1) \oplus K_{17}(1) \\
\oplus K_1(2) \oplus K_6(2) \oplus K_9(2) \oplus K_{14}(2) \oplus K_{17}(2) = 0 \\
I_3(1) \oplus I_3(2) \neq 0
\end{aligned}
$$

Mirror system 3 :

$$
\begin{aligned}
I_1(1) \oplus I_1(2) = 0 \\
I_2(1) \oplus I_2(2) = 0 \\
I_3(1) \oplus I_3(2) = 0 \\
K_1(1) \oplus K_6(1) \oplus K_9(1) \oplus K_{14}(1) \oplus K_{17}(1) \\
\oplus K_1(2) \oplus K_6(2) \oplus K_9(2) \oplus K_{14}(2) \oplus K_{17}(2) = 0 \\
I_4(1) \oplus I_4(2) \neq 0
\end{aligned}
$$

Then, from the first system, we find that the most likely path is when $I_1(1) = I_1(2)$ and all the following steps are different values :

$$
\begin{aligned}
I_1(1) \oplus I_1(2) = 0 \\
K_1(1) \oplus K_6(1) \oplus K_9(1) \oplus K_{14}(1) \oplus K_{17}(1) \\
\oplus K_1(2) \oplus K_6(2) \oplus K_9(2) \oplus K_{14}(2) \oplus K_{17}(2) = 0 \\
K_6(1) \oplus K_9(1) \oplus K_{14}(1) \oplus K_{17}(1) \oplus K_6(2) \oplus K_9(2) \oplus K_{14}(2) \oplus K_{17}(2) = 0 \\
I_2(1) \oplus I_2(2) \neq 0 \\
I_4(1) \oplus K_2(1) \oplus K_5(1) \oplus K_{10}(1) \oplus K_{13}(1) \oplus K_{18}(1) \\
\oplus I_4(2) \oplus K_2(2) \oplus K_5(2) \oplus K_{10}(2) \oplus K_{13}(2) \oplus K_{18}(2) \neq 0 \\
I_3(1) \oplus I_3(2) \neq 0 \\
I_3(1) \oplus K_3(1) \oplus K_8(1) \oplus K_{11}(1) \oplus K_{16}(1) \\
\oplus I_3(2) \oplus K_3(2) \oplus K_8(2) \oplus K_{11}(2) \oplus K_{16}(2) \neq 0 \\
I_4(1) \oplus K_2(1) \oplus I_4(2) \oplus K_2(2) \neq 0 \\
K_4(1) \oplus K_7(1) \oplus K_{12}(1) \oplus K_{15}(1) \oplus K_4(2) \oplus K_7(2) \oplus K_{12}(2) \oplus K_{15}(2) \neq 0 \\
I_3(1) \oplus K_3(1) \oplus I_3(2) \oplus K_3(2) \neq 0 \\
I_2(1) \oplus K_{17}(1) \oplus I_2(2) \oplus K_{17}(2) \neq 0 \\
K_4(1) \oplus K_4(2) \neq 0 \\
I_4(1) \oplus K_2(1) \oplus K_5(1) \oplus K_{10}(1) \oplus K_{13}(1) \oplus I_4(2) \\
\oplus K_2(2) \oplus K_5(2) \oplus K_{10}(2) \oplus K_{13}(2) \neq 0 \\
I_4(1) \oplus K_2(1) \oplus K_5(1) \oplus I_4(2) \oplus K_2(2) \oplus K_5(2) \neq 0
\end{aligned}
$$

$$
\begin{aligned}
K_4(1) \oplus K_7(1) \oplus K_{12}(1) \oplus K_4(2) \oplus K_7(2) \oplus K_{12}(2) \neq 0 \\
I_2(1) \oplus K_9(1) \oplus K_{14}(1) \oplus K_{17}(1) \oplus I_2(2) \oplus K_9(2) \oplus K_{14}(2) \oplus K_{17}(2) \neq 0 \\
I_3(1) \oplus K_3(1) \oplus K_8(1) \oplus K_{11}(1) \oplus I_3(2) \oplus K_3(2) \oplus K_8(2) \oplus K_{11}(2) \neq 0 \\
K_4(1) \oplus K_7(1) \oplus K_4(2) \oplus K_7(2) \neq 0 \\
I_4(1) \oplus K_2(1) \oplus K_5(1) \oplus K_{10}(1) \oplus I_4(2) \oplus K_2(2) \oplus K_5(2) \oplus K_{10}(2) \neq 0 \\
I_3(1) \oplus K_3(1) \oplus K_8(1) \oplus I_3(2) \oplus K_3(2) \oplus K_8(2) \neq 0 \\
I_2(1) \oplus K_{14}(1) \oplus K_{17}(1) \oplus I_2(2) \oplus K_{14}(2) \oplus K_{17}(2) \neq 0
\end{aligned}
$$

We have $N^{28} - 18N^{29} + 153N^{30} - 816N^{31} + 3060N^{32} - 8568N^{33} + 18564N^{34} - 31824N^{35} + 43758N^{36} - 48620N^{37} + 43758N^{38} - 31824N^{39} + 18564N^{40} - 8568N^{41} + 3060N^{42} - 816N^{43} + 153N^{44} - 18N^{45} + N^{46}$ solutions.

If we take into account all the systems and the paths, the total number of solutions is given by $Q(N) = -N^{33} + 5N^{34} - 4N^{35} - 35N^{36} + 149N^{37} - 321N^{38} + 464N^{39} - 482N^{40} + 352N^{41} - 161N^{42} + 33N^{43} + N^{46}$ and $\mathbb{E}(\tilde{\mathcal{N}}) = \dfrac{m(m-1)Q(N)}{N^4(N^4-1)(N^{20})^2} = \dfrac{m^2}{N^2} + \dfrac{33m^2}{N^5} + O(\dfrac{1}{N^6}) \sim \dfrac{m^2}{N^2}$.

The term $\frac{33m^2}{N^5}$ is due to the constraints on the internal variables that satisfy the differential paths plus the random path.

In this attack, both expectations are of the same order. In that case, the computations of $\mathbb{E}(\mathcal{N})$ and $\mathbb{E}(\tilde{\mathcal{N}})$ do not allow to conclude. Here we have that $|\mathbb{E}(\tilde{\mathcal{N}}) - \mathbb{E}(\mathcal{N})| \sim \frac{34m^2}{N^5}$. In order to obtain a successful attack, it is enough to have a number of messages such that this difference is greater than the standard deviation. Here, $V(\mathcal{N}) \sim 2\frac{m^2 N^{28}}{N^{30}} = \frac{2m^2}{N^2}$ and $\sigma(\mathcal{N}) \sim \sqrt{2}\frac{m}{N}$. This gives the condition $34\frac{m^2}{N^5} \geq \sqrt{2}\frac{m}{N} \Leftrightarrow m \geq \frac{\sqrt{2}}{34}N^4$. Thus if we use about N^4, i.e. 2^{4n} messages, we can distinguish a random permutation from a permutation generated by a Type-2 Feistel scheme with 10 rounds and $k = 4$. As we can notice, we can use less than N^4 messages (the full code book). In [22], the theoretical analysis provided an attack with the full code book.

Remark 5. As long as $\mathbb{E}(\mathcal{N})$ is significantly smaller than or equal to $\mathbb{E}(\tilde{\mathcal{N}})$, we do not need to compute the variance to conclude on the success of the attack. This happens when the number of conditions on the internal variables do no exceed the number of conditions on the outputs. When the two expectations have the same behavior, it is necessary to compute $\sigma(\mathcal{N})$ and to compare with the difference of the expectations. The difference of the expectations is related to the number of conditions we have on the internal variables. This means that we can add conditions as long $|\mathbb{E}(\tilde{\mathcal{N}}) - \mathbb{E}(\mathcal{N})| \geq \sigma(\mathcal{N})$. Of course, when we add conditions on the internal variables, we can attack more rounds.

Results for small values of n. Here we explain some phenomena that may appear with small value of n. Let us consider again type 2 Feistel schemes with $k = 4$

and $r = 10$. If we take $n = 8$ and $m = 2^{28}$, then we obtain the following value:

$$\begin{aligned}
&\mathbb{E}(\mathcal{N}) \approx 1\,099\,511\,558\,400\\
&\mathbb{E}(\tilde{\mathcal{N}}) \approx 1\,099\,513\,745\,758\\
&V(\mathcal{N}) \approx 2\,197\,953\,438\,347\\
&\sigma(\mathcal{N}) \approx 1\,482\,559\\
&\mathbb{E}(\tilde{\mathcal{N}}) - \mathbb{E}(\mathcal{N}) \approx 2\,187\,358
\end{aligned}$$

We can see that the difference of both expectations is greater than the standard deviation. This shows that in that case we do not need to take the maximal number of messages, i.e. 2^{32}, as seen previously.

We now study type 2 Feistel schemes with $k = 4$ and $r = 12$. The theoretical study of [22] showed that it was not possible to attack more than 10 rounds. However, for small values of n, we now show that it is still possible to mount a KPA on 12 rounds. We consider the following conditions on the inputs and outputs:

$$I_1(i) = I_1(j) \text{ and } I_2(i) \oplus I_2(j) = S_2(i) \oplus S_2(j)$$

Then we obtain for $P(N)$ and $V(\mathcal{N})$, the same values. But we have $Q(N) = N^{54} - N^{51} + 89N^{50} - 511N^{49} + 1390N^{48} - 2401N^{47}$. If we choose $n = 5$ and $m = 2^{20}$ (i.e. the maximal number of messages), we obtain: $\mathbb{E}(\tilde{\mathcal{N}}) - \mathbb{E}(\mathcal{N}) \approx 76\,098$ and $\sigma(\mathcal{N})) \approx 45\,610$. Again the difference of both expectations is greater then the standard deviation. This shows that for small values of n, it is possible to attack more rounds as expected.

6.3 Example of a 4-point Attack

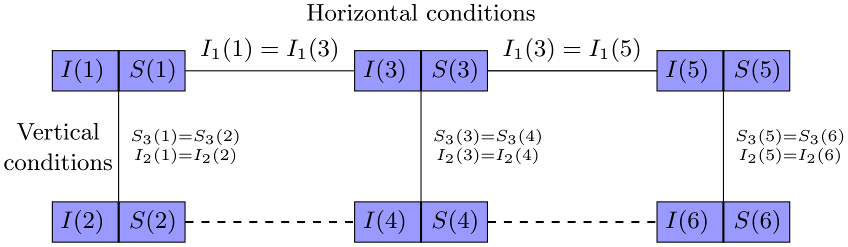
Differential notation for φ-point attacks We recall that a point is a pair (plaintext, ciphertext)=$[I_1, I_2, \ldots, I_k, S_1, S_2, \ldots, S_k]$. We impose some differential equalities on φ-tuples of points and we count the number of φ-tuples satisfying these equalities. This number of points will give the complexity of the attack. Δ denotes the Xor on coordinates of points. After round p, intermediate output of point $\alpha \in \{1, \ldots, \varphi\}$ is $[M_1^p(\alpha), M_2^p(\alpha), \ldots, M_k^p(\alpha)]$ We now define different kinds of equalitites:

1. "Horizontal equalities" on M_i^p: $M_i^p(1) = M_i^p(3) = \ldots = M_i^p(\varphi - 1)$
2. "Vertical equalities" on M_i^p: $M_i^p(1) = M_i^p(2)$, $M_i^p(3) = M_i^p(4)$, ... , $M_i^p(\varphi - 1) = M_i^p(\varphi)$.
3. "Differential equalities" on M_i^p: $M_i^p(1) \oplus M_i^p(2) = M_i^p(3) \oplus M_i^p(4) = ... = M_i^p(\varphi - 1) \oplus M_i^p(\varphi)$.

Figure 4 shows why we choose the terms of "vertical" and "horizontal" equalities.

To be more precise, when we write $[0, .\Delta_2^0, \Delta_3^0, \ldots, \Delta_k^0]$, this means that, on the input variables, a vertical conditions on the first coordinate and horizontal conditions on the second coordinate. The same notation applies to the internal

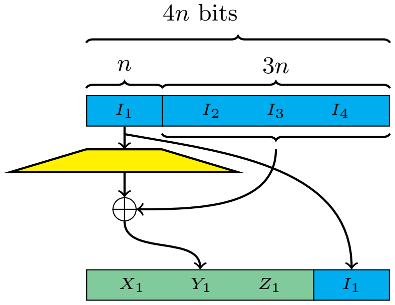
Fig. 4. Example of differential equalities for $\varphi = 6$



variable and the output variables. The differential path is constructed such that we always keep the differential equalities. In the differential path, when we impose a vertical condition we will write $\boxed{0}$ and when we impose an horizontal condition, we will set $\bullet$. We will write 0 and . when these conditions propagate.

Expanding Feistel schemes F_4^{10} ($k = 4$ and $r = 10$): "4-point attack"
We provide in Figure 6, the first round of an unbalanced Feistel scheme with expanding functions when $k = 4$.

Fig. 5. One round of an unbalanced Feistel scheme with expanding functions



The input is denoted by $[I_1, I_2, I_3, I_4]$ and the output by $[S_1, S_2, S_3, S_4]$. For the message i, the input and the output are denoted by $[I_1(i), I_2(i), I_3(i), I_4(i)]$ and
$[S_1(i), S_2(i), S_3(i), S_4(i)]$. We have m messages and we want to compute the ex-

pectation of the number $\mathcal{N}$ of 4-tuples of points satisfying the following relations:

$$\begin{cases} I_1(i) = I_1(j) \\ I_1(\ell) = I_1(p) \neq I_1(i) \\ I_2(i) = I_2(j) \\ I_2(\ell) = I_2(p) \neq I_2(i) \\ I_3(i) = I_3(j) \\ I_3(\ell) = I_3(p) \neq I_3(i) \\ I_4(i) \oplus I_4(j) = I_4(\ell) \oplus I_4(p) \neq 0 \end{cases} \qquad \begin{cases} S_1(i) \oplus S_1(j) = S_1(\ell) \oplus S_1(p) \neq 0 \\ S_2(i) = S_2(\ell) \\ S_2(j) = S_2(p) \neq S_2(i) \\ S_3(i) = S_3(\ell) \\ S_3(j) = S_3(p) \neq S_3(i) \\ S_4(i) = S_4(\ell) \\ S_4(j) = S_4(p) \neq S_4(i) \end{cases}$$

For this attack, there are many mirror systems. Here, we have 30 turns since, for each round, we need 3 round internal functions from n bits to n bits. The size of the systems do not allow to present examples. However, the systems are available through the computer program.
The total number of solutions is $P(N) = 4N^8 - 8N^9 + 4N^{10} - 4N^{12} + 8N^{13} - 4N^{14} + N^{16} - 2N^{17} + N^{18}$. So:

$$\begin{aligned} \mathbb{E}(\mathcal{N}) &= m(m-1)(m-2)(m-3) \times \\ &\quad \frac{4N^8 - 8N^9 + 4N^{10} - 4N^{12} + 8N^{13} - 4N^{14} + N^{16} - 2N^{17} + N^{18}}{(N^k(N^k-1)(N^k-2)(N^k-\varphi+1))^2} \\ &= m(m-1)(m-2)(m-3) \times \\ &\quad \frac{4N^8 - 8N^9 + 4N^{10} - 4N^{12} + 8N^{13} - 4N^{14} + N^{16} - 2N^{17} + N^{18}}{N^8(N^4-1)^2(N^4-2)^2(N^4-3)^2} \\ &\sim \frac{m^4}{N^{14}} \end{aligned}$$

We now explain the computation of the expectation for the scheme.

Among all the differential different paths, only 36 are significant. A path is not significant when the conditions on the internal variables are equivalent to the conditions on the output variables. It is significant when the conditions on the internal variables imply the conditions on the output variables.

We now give below the example of two differential paths:

As we mentioned before, in order to keep the differential equalities inside the path, we need to impose conditions on the internal variables. We call them "vertical conditions" and "horizontal conditions". The study of the different paths obtained by our computer program shows that there are also another kind of conditions that we can call "diagonal conditions". This definition is taken according to Figure 4. For example, on the internal variable X^1, this condition is defined by: $X^1(i) = X^1(p)$ and $X^1(j) = X^1(\ell)$. To indicate that we set a diagonal condition, we will write $\underline{\star}$ in the tables.

If we use these diagonal conditions, we can modify the previous paths in the following way and obtain new paths. Here, we give some ways to modify the differential paths using the diagonal conditions. There are many more possibilities and it is possible to find all if them. However, our computer program will provide the results as we will see below.

Table 3. F_4^{10} attack: example of two differential paths

round	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	Δ_4^0
1	0	0	Δ_4^0	0
2	0	Δ_4^0	0	0
3	$\bullet\Delta_4^0$	0	0	0
4	$\bullet\Delta_1^4$	Δ_2^4	Δ_3^4	$.\Delta_4^0$
5	$\bullet\Delta_1^5$	Δ_2^5	$.\ \Delta_3^5$	$.\Delta_1^4$
6	$\boxed{0}$	$.\Delta_2^6$	$.\Delta_5^6$	$.\Delta_1^5$
7	$\bullet\Delta_2^6$	Δ_3^6	Δ_1^5	0
8	$\bullet\Delta_1^8$	Δ_2^8	Δ_3^8	$.\Delta_2^6$
9	$\bullet\Delta_1^9$	Δ_2^9	$.\Delta_3^9$	$.\Delta_1^8$
10	Δ_1^{10}	$.\Delta_2^{10}$	$.\Delta_3^{10}$	$.\Delta_1^9$

round	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	Δ_4^0
1	0	0	Δ_4^0	0
2	0	Δ_4^0	0	0
3	$\bullet\Delta_4^0$	0	0	0
4	$\bullet\Delta_1^4$	Δ_2^4	Δ_3^4	$.\Delta_4^0$
5	$\boxed{0}$	Δ_2^5	$.\ \Delta_3^5$	$.\Delta_1^4$
6	$\boxed{0}$	Δ_3^5	Δ_1^4	0
7	$\bullet\Delta_3^5$	Δ_1^4	0	0
8	$\bullet\Delta_1^8$	Δ_2^8	Δ_3^8	$.\Delta_3^5$
9	$\bullet\Delta_1^9$	Δ_2^9	$.\Delta_3^9$	$.\Delta_1^8$
10	Δ_1^{10}	$.\Delta_2^{10}$	$.\Delta_3^{10}$	$.\Delta_1^9$

Table 4. F_4^{10} attack: path 1 with one, two or 3 $\underline{\star}$ conditions

round	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	Δ_4^0
1	0	0	Δ_4^0	0
2	0	Δ_4^0	0	0
3	$\underline{\star}\Delta_4^0$	0	0	0
4	$\underline{\star}\Delta_1^4$	Δ_2^4	Δ_3^4	$\star\Delta_4^0$
5	$\bullet\Delta_1^5$	Δ_2^5	$\star\Delta_3^5$	$\star\Delta_1^4$
6	$\boxed{0}$	Δ_2^6	Δ_5^6	$.\Delta_1^5$
7	$\bullet\Delta_2^6$	Δ_3^6	Δ_1^5	0
8	$\bullet\Delta_1^8$	Δ_2^8	Δ_3^8	$.\Delta_2^6$
9	$\bullet\Delta_1^9$	Δ_2^9	$.\Delta_3^9$	$.\Delta_1^8$
10	Δ_1^{10}	$.\Delta_2^{10}$	$.\Delta_3^{10}$	$.\Delta_1^9$

round	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	Δ_4^0
1	0	0	Δ_4^0	0
2	0	Δ_4^0	0	0
3	$\bullet\Delta_4^0$	0	0	0
4	$\underline{\star}\Delta_1^4$	Δ_2^4	Δ_3^4	$.\Delta_4^0$
5	$\bullet\Delta_1^5$	Δ_2^5	Δ_3^5	$\star\Delta_1^4$
6	$\boxed{0}$	Δ_2^6	Δ_5^6	$.\Delta_1^5$
7	$\bullet\Delta_2^6$	Δ_3^6	Δ_1^5	0
8	$\bullet\Delta_1^8$	Δ_2^8	Δ_3^8	$.\Delta_2^6$
9	$\bullet\Delta_1^9$	Δ_2^9	$.\Delta_3^9$	$.\Delta_1^8$
10	Δ_1^{10}	$.\Delta_2^{10}$	$.\Delta_3^{10}$	$.\Delta_1^9$

round	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	Δ_4^0
1	0	0	Δ_4^0	0
2	0	Δ_4^0	0	0
3	$\underline{\star}\Delta_4^0$	0	0	0
4	$\underline{\star}\Delta_1^4$	Δ_2^4	Δ_3^4	$\star\Delta_4^0$
5	$\underline{\star}\Delta_1^5$	Δ_2^5	$\star\Delta_3^5$	$\star\Delta_1^4$
6	$\boxed{0}$	$\star\Delta_2^6$	$\star\Delta_5^6$	$\star\Delta_1^5$
7	$\bullet\Delta_2^6$	Δ_3^6	Δ_1^5	0
8	$\bullet\Delta_1^8$	Δ_2^8	Δ_3^8	$.\Delta_2^6$
9	$\bullet\Delta_1^9$	Δ_2^9	$.\Delta_3^9$	$.\Delta_1^8$
10	Δ_1^{10}	$.\Delta_2^{10}$	$.\Delta_3^{10}$	$.\Delta_1^9$

This shows that all these attacks will succeed with high probability since for the same input and output conditions, we get much more paths than expected.

Moreover, these diagonal conditions can also be set on the input and output variables. Thus for the same scheme, there are many attacks with the same complexity. For the attack on F_4^{10}, we obtain 35 differential path besides the random one.

Remark 6. These "diagonal conditions" can also be used for the more general rectangle attacks as studied in [33].

The computation shows that of the numbers of solutions of all systems is given by:
$Q(N) = 48N^{114} - 320N^{115} + 876N^{116} - 1252N^{117} + 992N^{118} - 468N^{119} + 208N^{120} - 120N^{121} + 36N^{122}$

$$\begin{aligned}\mathbb{E}(\tilde{\mathcal{N}}) &= \frac{\frac{m!}{(m-4)!}Q(N)}{N^k(N^k-1)(N^k-2)(N^k-\varphi+1)N^{d\varphi}}\\ &= \frac{\frac{m!}{(m-4)!}Q(N)}{N^4(N^4-1)(N^4-2)(N^4-3)N^{120}} \sim \frac{36m^4}{N^{14}}\end{aligned}$$

Table 5. F_4^{10} attack: path 2 with one or two $\underline{\star}$ conditions

round	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	Δ_4^0
1	0	0	Δ_4^0	0
2	0	Δ_4^0	0	0
3	$\underline{\star}\Delta_4^0$	0	0	0
4	$\underline{\star}\Delta_1^4$	Δ_2^4	Δ_3^4	$\star\Delta_4^0$
5	$\boxed{0}$	Δ_2^5	$\star\Delta_3^5$	$\star\Delta_1^4$
6	$\boxed{0}$	Δ_3^5	Δ_1^4	0
7	$\bullet\Delta_3^5$	Δ_1^4	0	0
8	$\bullet\Delta_1^8$	Δ_2^8	Δ_3^8	$.\Delta_3^5$
9	$\bullet\Delta_1^9$	Δ_2^9	$.\Delta_3^9$	$.\Delta_1^8$
10	Δ_1^{10}	$.\Delta_2^{10}$	$.\Delta_3^{10}$	$.\Delta_1^9$

round	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	Δ_4^0
1	0	0	Δ_4^0	0
2	0	Δ_4^0	0	0
3	$\underline{\star}\Delta_4^0$	0	0	0
4	$\bullet\Delta_1^4$	Δ_2^4	Δ_3^4	$\star\Delta_4^0$
5	$\boxed{0}$	Δ_2^5	Δ_3^5	$.\Delta_1^4$
6	$\boxed{0}$	Δ_3^5	Δ_1^4	0
7	$\bullet\Delta_3^5$	Δ_1^4	0	0
8	$\bullet\Delta_1^8$	Δ_2^8	Δ_3^8	$.\Delta_3^5$
9	$\bullet\Delta_1^9$	Δ_2^9	$.\Delta_3^9$	$.\Delta_1^8$
10	Δ_1^{10}	$.\Delta_2^{10}$	$.\Delta_3^{10}$	$.\Delta_1^9$

round	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	Δ_4^0
1	0	0	Δ_4^0	0
2	0	Δ_4^0	0	0
3	$\bullet\Delta_4^0$	0	0	0
4	$\underline{\star}\Delta_1^4$	Δ_2^4	Δ_3^4	$.\Delta_4^0$
5	$\boxed{0}$	Δ_2^5	Δ_3^5	$\star\Delta_1^4$
6	$\boxed{0}$	Δ_3^5	Δ_1^4	0
7	$\bullet\Delta_3^5$	Δ_1^4	0	0
8	$\bullet\Delta_1^8$	Δ_2^8	Δ_3^8	$.\Delta_3^5$
9	$\bullet\Delta_1^9$	Δ_2^9	$.\Delta_3^9$	$.\Delta_1^8$
10	Δ_1^{10}	$.\Delta_2^{10}$	$.\Delta_3^{10}$	$.\Delta_1^9$

Thus if $m \sim N^{7/2}$, i.e. $m \sim 2^{7n/2}$, then we can distinguish a permutation generated by F_4^{10} from a random permutation and the attack is successful, since in that case $\mathbb{E}(\mathcal{N})$ is close to 1 and $\mathbb{E}(\tilde{\mathcal{N}})$ is close to 36.

Remark 7. In this attack, we do not need to compute the variance since with the right number of messages, the expectation for a scheme is 36 times the expectation for a random permutation.

Results for small values of n. The theoretical study of [33] shows that it is possible to get KPA up to $3k-1$ rounds, with a $2k+2$-point attacks. This attack needs $2^{(k-\frac{1}{2k+2})n}$ messages. When $k = 4$, the exact computation allows to show that for small values of n, it is possible to have a 4-point attack for 11 rounds that has a better complexity than the 10-point attack, and also that it is possible to attack 12 rounds instead of 11 rounds. Results for small n are summarized in Table 6.

Table 6. Improvements on the attacks for Unbalanced Feistel schemes with expanding functions.

round	n	m	$\mathbb{E}(\mathcal{N})$	$\mathbb{E}(\tilde{\mathcal{N}})$	$\sigma(\mathcal{N})$	$\lvert\mathbb{E}(\tilde{\mathcal{N}}) - \mathbb{E}(\mathcal{N}) - \sigma(\mathcal{N})\rvert$
11	16	2^{62}	16776704.0039	16802558.3906	8191.8749	17662.5117
11	8	2^{30}	254.0039	353.4039	31.8750	67.5250
12	7	2^{28}	16129.0001	16414.2110	254.0001	31.2108
12	6	2^{24}	3969.0004	4243.8287	126.0004	148.8277
12	4	2^{15}	14.0616	27.8061	7.5015	6.24292

7 Conclusion and perspectives

We summarize in this table the capacities of our program and the future improvements:

Scheme	Random permutation	Classical Feistel, Expanding Feistel, type 1 Feistel, type 2 Feistel, type 3 Feistel, Feistel with one to one functions	Misty	Contracting Feistel, Alternating Feistel
Expectation	$\surd$	$\surd$	to do (*)	to do
Standard deviation	$\surd$	to do	to do (*)	to do
Taylor expansion for expectation and standard deviation	$\surd$	to do (*)	to do (*)	to do (*)

(*) requires minor modifications in the computer program.

First applications:

- We have discover in section 6 new differential paths with diagonal conditions. This could lead to the study of new geometries for differential attacks.
- For the type 2 Feistel scheme with $k = 4$, the exact computation of the expectation and the standard deviation gives us better attacks than in previous papers or new attacks.
  - For $r = 10$ and $n = 8$, we only need 2^{28} messages instead of 2^{32} [22].
  - For $r = 12$ and $n = 5$ we attack the scheme with 2^{20} messages (new attack). In [22], it was possible to get a KPA up to 10 rounds.
- For unbalanced Feistel schemes with expanding functions with $k = 4$, the computation of the exact values for the expectations and standard deviation lead to the following improvements:
  - For $r = 11$ and $n \leq 16$, there exist 4-point attacks with a better complexity than the 10-point attacks of [33].
  - For $r = 12$ and $n \leq 7$, we have obtained new attacks. In [33], no attacks were provided for 12 rounds and $k = 4$.

We will also improve the efficiency of the program in order to make a complete and exact description of all possible differential attacks on a specific scheme.

References

1. Encryption Algorithm for Computer Data Protection. Technical Report Federal Register 40(52) 12134, National Bureau of Standards, March 1975.
2. Notice of a Proposed Federal Information Processing Data Encryption. Technical Report Federal Register 40(149) 12607, National Bureau of Standards, August 1975.
3. C. Adams, H. Heys, S. Tavares, and M. Wiener. The CAST-256 Encryption Algorithm. Technical report, AES Submission, 1998.
4. R. J. Anderson and E. Biham. Two Practical and Provably Secure Block Ciphers: BEAR and LION. In D. Gollman, editor, *Fast Software Encrytion – FSE '96*, volume 1039 of *Lecture Notes in Computer Science*, pages 113–120. Springer-Verlag, 1996.
5. E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In Jacques Stern, editor, *Advances in Cryptology – EUROCRYPT 99*, volume 1592 of *Lecture Notes in Computer Science*, pages 12–23. Springer-Verlag, 1999.
6. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.
7. C. Blondeau and B. Gérard. On Data Complexity of Statistical Attacks Agianst Block Ciphers. *Cryptology ePrint archive: 2009/64: Listing for 2009.*
8. C. Blondeau, B. Gérard, and J. P. Tillich. Accurate Estimates of the Data Complexity and Success Probability for Various Cryptanalysis. *Des. Codes Cryptography*, 59(1-3):3–34, 2011.
9. C. Bouillaguet, O. Dunkelman, G. Leurent, and P. A. Fouque. New Insights on Impossible Differential Cryptanalysis. In A. M. and S. Vaudenay, editors, *Selected Areas in Cryptographyl – SAC '11*, volume 7118 of *Lecture Notes in Computer Science*, pages 243–259. Springer-Verlag, 2011.
10. C. Burwick, D. Coppersmith, E. D´ Avignon, R. Gennaro, S. Halevi, C. Jutla, S. M. Jr. Matyas, L. O´ Connor, M. Peyravian, D. Safford, and N. Zunic. MARS - a candidate cipher for AES . Technical report, AES Submission, 1998.
11. J. Choy and H. Yap. Impossible Boomerang Attack for Block Cipher Structures. In T. Takagi and M. Mambo, editors, *Advances in Information and Computer Security*, volume 5824 of *Lecture Notes in Computer Science*, pages 22–37. Springer Berlin Heidelberg, 2009.
12. Paul G.Hoel, Sidney C.Port, and Charles J.Stone. *Introduction to Probability Theory.* Houghton Mifflin Company, 1971.
13. J. Guo, J. Jean, I. Nikolc, and Y. Sasaki. Meet-in-the-Middle Attacks on Generic Feistel Constructions. In P.Sarkar and T. Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014*, volume 8873 of *Lecture Notes in Computer Science*, pages 458–477. Springer-Verlag, 2014.
14. S. Ibrahim and M. A. Mararof. Diffusion Analysis of Scalable Feistel Networks. *World Academy of Science, Engineering and Technology*, 5:98–101, 2005.
15. J.Lu. Cryptanalyis of Block Ciphers. Technical Report 19, RHUL-MA, July 2008.
16. C. S. Jutla. Generalized Birthday Attacks on Unbalanced Feistel Networks. In H. Krawczyk, editor, *Advances in Cryptology – CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 186–199. Springer-Verlag, 1998.
17. J. Kim, S. Hong, and J. Lim". Impossible Differential Cryptanalysis Using Matrix Method . *Discrete Mathematics*, 310(5):988 – 1002, 2010.

18. L. R. Knudsen and V. Rijmen. On the Decorrelated Fast Cipher (DFC) and Its Theory. In L. R. Knudsen, editor, *Fast Software Encrytion – FSE '99*, volume 1636 of *Lecture Notes in Computer Science*, pages 81–94. Springer-Verlag, 1999.
19. Lars R. Knudsen. DEAL - A 128-bit Block Cipher. Technical Report 151, University of Bergen, Department of Informatics, Norway, February 1998.
20. L.R. Knudsen. Truncated and higher order differentials. In B. Preneel, editor, *Fast Software Encrytion – FSE '94*, volume 1008 of *Lecture Notes in Computer Science*, pages 291–311. Springer-Verlag, 1994.
21. M. Luby and C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.
22. Valérie Nachef, Emmanuel Volte, and Jacques Patarin. Differential Attacks on Generalized Feistel schemes. In Michel Abdalla, Cristina Nita-Rotaru, and Ricardo Dahab, editors, *CANS 2013*, volume 8257 of *Lecture Notes in Computer Science*, pages 1–19. Springer-Verlag, 2013.
23. M. Naor and O. Reingold. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *J. Cryptology*, 12(1):29–66, 1999.
24. J. Patarin. Generic Attacks on Feistel Schemes - Extended version. *Cryptology ePrint archive: 2008/036: Listing for 2008.*
25. J. Patarin. Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. *Cryptology ePrint archive: 2010/287: Listing for 2010.*
26. J. Patarin. Generic Attacks on Feistel Schemes. In C. Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 222–238. Springer-Verlag, 2001.
27. J. Patarin, V. Nachef, and C. Berbain. Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions - Extended version. *Cryptology ePrint archive: 2007/449: Listing for 2007.*
28. J. Patarin, V. Nachef, and C. Berbain. Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions. In X. Lai and K. Chen, editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 396–411. Springer-Verlag, 2006.
29. J. Patarin, V. Nachef, and C. Berbain. Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions. In K. Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 325–341. Springer-Verlag, 2007.
30. R. L. Rivest, M. Robshaw, R. Sidney, and Y. L. Yin. The RC6 Block Cipher . Technical report, AES Submission, 1998.
31. B. Schneier and J. Kelsey. Unbalanced Feistel Networks and Block Cipher Design. In D. Gollmann, editor, *Fast Software Encrytion – FSE '96*, volume 1039 of *Lecture Notes in Computer Science*, pages 121–144. Springer-Verlag, 1996.
32. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-bit blockcipher CLEFIA (extended abstract). In A. Biryukov, editor, *Fast Software Encrytion – FSE 2007*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer-Verlag, 2007.
33. E. Volte, V. Nachef, and J. Patarin. Improved Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions. In K. Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 94–111. Springer-Verlag, 2010.
34. X. Lai Y. Luo, Z. Wu and G. Gong. A Unified Method for Finding Impossible Differentials of Block Cipher Structures. 2009. http://eprint.iacr.org/.

35. Y. Zheng, T. Matsumoto, and H. Imai. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. In G. Brassard, editor, *Advances in Cryptology CRYPTO 89 Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 461–480. Springer New York, 1990.