Security of Random Feistel Schemes with 5 or more Rounds

Jacques Patarin

Université de Versailles
45 avenue des Etats-Unis
78035 Versailles Cedex - France

Abstract. We study cryptographic attacks on random Feistel schemes. We denote by m the number of plaintext/ciphertext pairs, and by k the number of rounds. In their famous paper [3], M. Luby and C. Rackoff have completely solved the cases $m \ll 2^{n/2}$: the schemes are secure against all adaptive chosen plaintext attacks (CPA-2) when $k \geq 3$ and against all adaptive chosen plaintext and chosen ciphertext attacks (CPCA-2) when $k \geq 4$ (for this second result a proof is given in [9]).
In this paper we study the cases $m \ll 2^n$. We will use the "coefficients H technique" of proof to analyze known plaintext attacks (KPA), adaptive or non-adaptive chosen plaitext attacks (CPA-1 and CPA-2) and adaptive or non-adaptive chosen plaitext and chosen ciphertext attacks (CPCA-1 and CPCA-2). In the first part of this paper, we will show that when $m \ll 2^n$ the schemes are secure against all KPA when $k \geq 4$, against all CPA-2 when $k \geq 5$ and against all CPCA-2 attacks when $k \geq 6$. This solves an open problem of [1], [14], and it improves the result of [14] (where more rounds were needed and $m \ll 2^{n(1-\varepsilon)}$ was obtained instead of $m \ll 2^n$). The number 5 of rounds is minimal since CPA-2 attacks on 4 rounds are known when $m \geq O(2^{n/2})$ (see [1], [10]). Furthermore, in all these cases we have always obtained an explicit majoration for the distinguishing probability. In the second part of this paper, we present some improved generic attacks. For $k = 5$ rounds, we present a KPA with $m \simeq 2^{3n/2}$ and a non-adaptive chosen plaintext attack (CPA-1) with $m \simeq 2^n$. For $k \geq 7$ rounds we also show some improved attacks against random Feistel generators (with more than one permutation to analyze and $\geq 2^{2n}$ computations).

1 Introduction

A "Luby - Rackoff construction with k rounds", which is also known as a "random Feistel cipher" is a Feistel cipher in which the round functions $f_1, \ldots, f_k$ are independently chosen as truly random functions (see section 2 for precise definitions).

Since the famous original paper [3] of M. Luby and C. Rackoff, these constructions have inspired a considerable amount of research. In [8] and [14] a summary of existing works on this topic is given.

We will denote by k the number of rounds and by n the integer such that the Feistel cipher is a permutation of $2n$ bits → $2n$ bits. In [3] it was proved that when $k \geq 3$ these Feistel ciphers are secure against all adaptative chosen plaintext attacks (CPA-2) when the number of queries (i.e. plaintext/ciphertext pairs obtained) is $m \ll 2^{n/2}$. Moreover when $k \geq 4$ they are secure against all adaptative chosen plaintext and chosen ciphertext attacks (CPCA-2) when the number of queries is $m \ll 2^{n/2}$ (a proof of this second result is given in [9]).

These results are valid if the adversary has unbounded computing power as long as he does only m queries.

These results can be applied in two different ways: directly using k truly random functions $f_1, \ldots, f_k$ (that requires significant storage), or in a hybrid setting, in which instead of using k truly random functions $f_1, \ldots, f_k$, we use k pseudo-random functions. These two ways are both interesting for cryptography. The first way gives "locally random permutations" where we have proofs of security without any unproven hypothesis (but we need a lot of storage), and the second way gives constructions for block encryption schemes where the security can be relied on a pseudo-random number generator, or on any one-way function.

In this paper, we will study security when $m \ll 2^n$, instead of $m \ll 2^{n/2}$ for the original paper of M. Luby and C. Rackoff. For this we must have $k \geq 5$, since for $k \leq 4$ some CPA-2 attacks when $m \geq O(2^{n/2})$ exist (see [1], [10]). Moreover the bound $m \ll 2^n$ is the larger bound that we can get, since an adversary with unlimited computing power can always distinguish a k-round random Feistel scheme from a random permutation with $O(k \cdot 2^n)$ queries and $O(2^{kn2^n})$ computations by simply guessing all the round functions (it is also possible to do less computing with the same number of queries by using collisions, see [13]).

The bound $m \ll 2^{n/2}$ is called the 'birthday bound', i.e. it is about the square root of the optimal bound against an adversary with unbounded computing power. In [1] W. Aiello and R. Venkatesan have found a construction of locally random functions ('Benes') where the optimal bound ($m \ll 2^n$) is obtained instead of the birthday bound. However here the functions are not permutations. Similarly, in [4], U. Maurer has found some other construction of locally random functions (not permutations) where he can get as close as wanted to the optimal bound (i.e. $m \ll 2^{n(1-\epsilon)}$ and for all $\epsilon > 0$ he has a construction). In [8] the security of unbalanced Feistel schemes is studied and a security proof in $2^{n(1-\epsilon)}$ is obtained, instead of $2^{n/2}$, but for much larger round functions (from $2n$ bits to ϵ bits, instead of n bits to n bits). This bound is basically again the birthday bound for these functions.

In this paper we will show that 5-round random Feistel schemes resist all CPA-2 attacks when $m \ll 2^n$ and that 6-round random Feistel schemes resist all CPCA-2 attacks when $m \ll 2^n$. Here we are very near the optimal bound, and we have permutations. This solves an open problem of [1], [10]. It also significantly improves the results of [6] in which the 2^n security is only obtained when the number of rounds tends to infinity, and the result of [14] where $2^{n(1-\epsilon)}$ security was proved for CPA-2 after 7 rounds (instead of 5 here) and for CPCA-2 after 10 rounds (instead of 6 here). Moreover we will obtain in this paper some explicit and simple majorations for the distinguishing probabilities. We will also present some improved generic attacks. All these results are summarized in appendix A.

2 Notations

General notations

- $I_n = \{0,1\}^n$ denotes the set of the 2^n binary strings of length n. $|I_n| = 2^n$.
- The set of all functions from I_n to I_n is F_n. Thus $|F_n| = 2^{n \cdot 2^n}$.
- For any $f, g \in F_n$, $f \circ g$ denotes the usual composition of functions.
- For any $a, b \in I_n$, $[a, b]$ will be the string of length $2n$ of I_{2n} which is the concatenation of a and b.
- For $a, b \in I_n$, $a \oplus b$ stands for bit by bit exclusive or of a and b.
- Let f_1 be a function of F_n. Let L, R, S and T be four n-bit strings in I_n. Then by definition
$$\Psi(f_1)[L, R] = [S, T] \overset{\text{def}}{\Leftrightarrow} \begin{cases} S = R \\ T = L \oplus f_1(R) \end{cases}$$
- Let $f_1, f_2, \ldots, f_k$ be k functions of F_n. Then by definition:
$$\Psi^k(f_1, \ldots, f_k) = \Psi(f_k) \circ \cdots \circ \Psi(f_2) \circ \Psi(f_1).$$

The permutation $\Psi^k(f_1, \ldots, f_k)$ is called a 'Feistel scheme with k rounds' or shortly Ψ^k. When $f_1, \ldots, f_k$ are randomly and independently chosen in F_n, then $\Psi^k(f_1, \ldots, f_k)$ is called a 'random Feistel scheme with k rounds' or a 'Luby-Rackoff construction with k rounds'.

We will first study 4 rounds (with some limitations on the inputs/outputs), then prove our cryptographic results by adding one or two rounds.

Notations for 4 rounds

- We will denote by $[L_i, R_i]$, $1 \le i \le m$, the m cleartexts. These cleartexts can be assumed to be pairwise distinct, i.e. $i \ne j \Rightarrow L_i \ne L_j$ or $R_i \ne R_j$.
- We call "index" any integer between 1 and m.
- $[R_i, X_i]$ is the output after one round, i.e.
$$\forall i, 1 \le i \le m, X_i = L_i \oplus f_1(R_i).$$
- $[X_i, Y_i]$ is the output after two rounds, i.e.
$$\forall i, 1 \le i \le m, Y_i = R_i \oplus f_2(X_i) = R_i \oplus f_2(L_i \oplus f_1(R_i)).$$
- $[Y_i, S_i]$ is the output after three rounds, i.e.
$$\forall i, 1 \le i \le m, S_i = X_i \oplus f_3(Y_i) = L_i \oplus f_1(R_i) \oplus f_3(Y_i).$$
- $[S_i, T_i]$ is the output after 4 rounds, i.e.
$$\forall i, 1 \le i \le m, T_i = Y_i \oplus f_4(S_i).$$

Notations for 5 rounds We keep the same notations for L_i, R_i, X_i, Y_i. Now $Z_i = X_i \oplus f_3(Y_i)$, and $[S_i, T_i]$ is still the output: $S_i = Y_i \oplus f_4(Z_i)$ and $T_i = Z_i \oplus f_5(S_i)$.

Part I: Security results

3 The general proof strategy

We will first study the properties of 4-round schemes. Our result on 4-round schemes for proving KPA security will be:

Theorem 31 (4 rounds) *For random values $[L_i, R_i]$, $[S_i, T_i]$, $1 \le i \le m$, such that the $[L_i, R_i]$, $1 \le i \le m$, are pairwise distinct, with probability $\ge 1 - \beta$ we have:*

1. *the number H of $(f_1, f_2, f_3, f_4) \in F_n^4$ such that $\forall i$, $1 \le i \le m$,*
$$\Psi^4(f_1, f_2, f_3, f_4)[L_i, R_i] = [S_i, T_i]$$
satisfies:
$$H \ge \frac{|F_n|^4}{2^{2nm}}(1 - \alpha).$$
2. *α and β can be chosen $\ll 1$ when $m \ll 2^n$.*

For 5 rounds, we will have :

Theorem 32 (5 rounds) *There are some values $\alpha > 0$ and $\beta > 0$ and there is a subset $E \subset I_{2n}^m$ such that:*

1. *for all pairwise distinct $[L_i, R_i]$, $1 \le i \le m$, and for all sequences $[S_i, T_i]$, $1 \le i \le m$, of E the number H of $(f_1, f_2, f_3, f_4, f_5) \in F_n^5$ such that $\forall i$, $1 \le i \le m$,*
$$\Psi^5(f_1, f_2, f_3, f_4, f_5)[L_i, R_i] = [S_i, T_i]$$
satisfies:
$$H \ge \frac{|F_n|^5}{2^{2nm}}(1 - \alpha).$$
2. *$|E| \ge (1 - \beta) \cdot 2^{2nm}$, and α and β can be chosen $\ll 1$ when $m \ll 2^{n(1-\varepsilon)}$, $\forall \varepsilon > 0$.*

Remark

1. Here the set E does not depend on the $[L_i, R_i]$, and it will give security against CPA-2. If E depends on the $[L_i, R_i]$, we will obtain security against CPA-1 only.
2. Instead of fixing a set E, as in theorem 32, we can formulate a similar theorem in term of expectancy of the deviation of H from the average value (see[15]: there is a formulation for CPA-1 and another for CPA-2). From these formulas we will get security when $m \ll 2^n$.

For 6 rounds, we will have :

Theorem 33 (6 rounds) *There are some values $\alpha > 0$ and $\beta > 0$ and there is a subset $E \subset I_n^{4m}$ such that:*

1. *for all $[L_i, R_i, S_i, T_i]$, $1 \leq i \leq m$, of E, the number H of $(f_1, f_2, f_3, f_4, f_5, f_6) \in F_n^6$ such that $\forall i$, $1 \leq i \leq m$,*
$$\Psi^6(f_1, f_2, f_3, f_4, f_5, f_6)[L_i, R_i] = [S_i, T_i]$$
satisfies:
$$H \geq \frac{|F_n|^6}{2^{2nm}}(1 - \alpha).$$
2. *For all super distinguishing circuit Φ with m oracle gates, the probability that $[L_i, R_i, S_i, T_i](\Phi)$, $1 \leq i \leq m$, be in E is $\geq 1 - \beta$, when Φ acts on a random permutation f of $I_{2n} \rightarrow I_{2n}$ (here $[L_i, R_i, S_i, T_i](\Phi)$, $1 \leq i \leq m$, denotes the successive $[S_i, T_i] = f[L_i, R_i]$ or $[L_i, R_i] = f^{-1}[S_i, T_i]$, $1 \leq i \leq m$, that will appear).*
3. *α and β can be chosen $\ll 1$ when $m \ll 2^n$.*

Now from these theorems and from the general "coefficients H technique" theorems given in [11], [12], we will get immediately that when $m \ll 2^n$, Ψ^4 is secure against all KPA, Ψ^5 against all CPA-2 and Ψ^6 against all CPCA-2.

4 Circles

One of the terms of the the deviation of Ψ^k from random permutations will be the probability to get "circles" in the variables, as we will explain below.

Definition We will say that we have 'a circle in R, X, Y' if there are k indices $i_1, \ldots, i_k$ with $k \geq 3$ and such that:

1. $i_1, i_2, \ldots, i_{k-1}$ are pairwise distinct and $i_k = i_1$.
2. $\forall \lambda$, $1 \leq \lambda \leq k - 2$ we have at least one of the three following conditions:
   - $R_{i_\lambda} = R_{i_{\lambda+1}}$ and $(X_{i_{\lambda+1}} = X_{i_{\lambda+2}}$ or $Y_{i_{\lambda+1}} = Y_{i_{\lambda+2}})$

   or • $X_{i_\lambda} = X_{i_{\lambda+1}}$ and $(R_{i_{\lambda+1}} = R_{i_{\lambda+2}}$ or $Y_{i_{\lambda+1}} = Y_{i_{\lambda+2}})$

   or • $Y_{i_\lambda} = Y_{i_{\lambda+1}}$ and $(R_{i_{\lambda+1}} = R_{i_{\lambda+2}}$ or $X_{i_{\lambda+1}} = X_{i_{\lambda+2}})$

Example If $R_1 = R_2$ and $X_1 = X_2$, then we have a circle in R, X, Y. If $R_1 = R_2$, $X_2 = X_3$, $Y_3 = Y_1$ then we have a circle in R, X, Y.

We will prove the following theorems.

Theorem 41 (For 4 rounds) *When $[L_i, R_i]$, $1 \leq i \leq m$, are pairwise distinct and randomly chosen, the probability p to obtain a circle in R, X, Y with at least one equation in Y when f_1, f_2 are randomly chosen in F_n satisfies:*

$$p \leq \frac{3m^2}{2 \cdot 2^{2n}} + \frac{3m^3}{2^{3n}} \cdot \frac{1}{1 - \frac{2m}{2^n}}.$$

Theorem 42 (For 5 rounds) *For all pairwise distinct* $[L_i, R_i]$, $1 \leq i \leq m$ *and for all value* λ, *such that* $\lambda > 0$ *and* $2m\sqrt{\lambda} < 2^n$, *we have: the probability* p *to obtain a circle in* X, Y, Z *with at least one equation* $Z_i = Z_j$ *when* f_1, f_2, f_3 *are randomly chosen in* F_n *satisfies:*

$$p \leq \frac{1}{\lambda} + \frac{m(m-1)}{2 \cdot 2^{2n}} + \frac{m(m-1)(m-2)}{2^{3n}} + \frac{4\lambda m^4}{2^{4n}} \cdot \frac{1}{1 - \frac{2m\sqrt{\lambda}}{2^n}}.$$

Corollary 41 *From this theorem 42 we get immediately that if* $m \ll 2^n$, *then (*λ *can be chosen such that),* p *is very small. So when* $m \ll 2^n$, *the probability to have a circle in* X, Y, Z *with at least one equation* $Z_i = Z_j$ *is negligible.*

Remark In [15] we show that the condition 'with at least one equation $Z_i = Z_j$' is important: sometime we cannot avoid some circles in X, Y.

With 6 rounds, we can get a simpler formula:

Theorem 43 (For 6 rounds) *For all* $[L_i, R_i]$, $1 \leq i \leq m$ *(such that* $i \neq j \Rightarrow L_i \neq L_j$ *or* $R_i \neq R_j$*), the probability* p *to obtain a circle in* X, Y, Z *with at least one equation in* Z *when* f_1, f_2, f_3, f_4 *are randomly chosen in* F_n *satisfies:*

$$p \leq \frac{3m^2}{2^{2n}} + \frac{11m^3}{2^{3n}} \cdot \frac{1}{1 - \frac{2m}{2^n}}.$$

Proof of theorem 41, 42, 43 are given in the extended version of this paper ([15]). A basic tool for these proofs is:

Theorem 44 $\forall \lambda > 0$, *for all pairwise distinct* $[L_i, R_i]$, $1 \leq i \leq m$, *when* f_1 *is randomly chosen in* F_n *we have a probability* $\geq 1 - \frac{1}{\lambda}$ *that the number* N *of* (i, j), $i < j / X_i = X_j$ *satisfies:*

$$N \leq \frac{\lambda m(m-1)}{2 \cdot 2^n}.$$

Proof This result comes immediately from this lemma:

Lemma 41 *For all* $[L_i, R_i]$, $1 \leq i \leq m$, *(such that* $i \neq j \Rightarrow L_j or R_i \neq R_j$*) the number of* (f_1, i, j) *such that* $X_i = X_j$, $i < j$, *is* $\leq |F_n| \cdot \frac{m(m-1)}{2 \cdot 2^n}$.

Proof of lemma 41 $X_i = X_j$ means $L_i \oplus f_1(R_i) = L_j \oplus f_1(R_j)$. This implies $R_i \neq R_j$ (because $L_i = L_j$ and $R_i = R_j \Rightarrow i = j$). Thus, when (i, j) is fixed, the number of f_1 such that $X_i = X_j$ is exactly $\frac{|F_n|}{2^n}$ if $R_i \neq R_j$, and exactly 0 if $R_i = R_j$. Therefore, since we have at most $m(m-1)/2$ values (i, j), $i < j / R_i \neq R_j$, the total number of (f_1, i, j) such that $X_i = X_j$ is $\leq |F_n| \frac{m(m-1)}{2 \cdot 2^n}$ as claimed.

5 Properties of H with 4 rounds

We give here the main ideas. See the extended version of this paper for more details ([15]). We will first prove that if the $[Y_i, S_i]$ are given, $1 \leq i \leq m$, (i.e. the output after 3 rounds), then the S_i variables will look random as long as $m \ll 2^n$ (but the Y_i variables will not look random in general). Then, with one more round and the same argument, we will obtain that the $[S_i, T_i]$ variables will look random as long as $m \ll 2^n$. We want to evaluate the number H of f_1, f_2, f_3 such that: $\forall i$, $1 \leq i \leq m$, $S_i = L_i \oplus f_1(R_i) \oplus f_3(Y_i)$ with $Y_i = R_i \oplus f_2(L_i \oplus f_1(R_i))$ (1).

Remarks

1. If $Y_i = Y_j$ with $i \neq j$, then $S_i \neq S_j$. So the S_i variables are not perfectly random in I_n when the Y_i are given. However, here we just say that the $[Y_i, S_i]$ must be pairwise distinct, since Ψ^k is a permutation.
2. If S_i is a constant ($\forall i$, $1 \leq i \leq m$, $S_i = 0$ for example), then all the Y_i variables must be pairwise distinct, and in (1) f_3 is then fixed on exactly m points. However the probability for f_1, f_2 to be such that all the Y_i are pairwise distinct is very small. So in this case $H \ll \frac{|F_n|^3}{2^{nm}}$.
3. Let us consider that instead of (1) we had to evaluate the number J of f_1, f_2, f_3 such that $\forall i$, $1 \leq i \leq m$, $S_i = f_3(Y_i)$ with $Y_i = R_i \oplus f_2(L_i \oplus f_1(R_i))$ (i.e. here we do not have the term $L_i \oplus f_1(R_i)$). Then, for random L_i, R_i and for random f_1, f_2, f_3, we will have about 2 times more collisions $S_i = S_j$ compared with a random variable S_i. So if S_i is random, $J \ll \frac{|F_n|^3}{2^{nm}}$ in this case. For (1) we will prove (among other results) that, unlike here for J, when the S_i are random, we always have $H \simeq \frac{|F_n|^3}{2^{nm}}$.

Analysis of (1) (In appendix B an example is given on what we do here) We will consider that all the Y_i are given (as well as the L_i, R_i, S_i), and we want to study how H can depend on the values S_i. If H has almost always the same value for all the S_i, then (by summation on all the Y_i) we will get $H \simeq \frac{|F_n|^3}{2^{nm}}$, and for all $[L_i, R_i]$ the S_i will look random, as wanted, when f_1, f_2, f_3 are randomly chosen in F_n (this is an indirect way to evaluate H).

In (1), when we have a new value Y_i, whatever S_i is, f_3 is exactly fixed on this point Y_i by (1). However if Y_i is not a new value, we have $Y_i = Y_j \Rightarrow L_i \oplus f_1(R_i) = L_j \oplus f_1(R_j) \oplus S_i \oplus S_j$. For each equation $Y_i = Y_j$, we will introduce a value $\lambda_{k(i,j)} = S_i \oplus S_j$. We want to evaluate the number H' of (f_1, f_2) such that: $\forall i$, $1 \leq i \leq m$, $f_2(L_i \oplus f_1(R_i)) = R_i \oplus Y_i$ (2).

We will fix the points (i, j) where $X_i = X_j$, i.e. we look for solutions (f_1, f_2) such that $X_i = X_j$ exactly on these (i, j), and, again, we want to evaluate how the number H' of (f_1, f_2) can depend on the values S_i (i.e. on the values λ_k).

We will group the equations (2) by the same $f_1(R_i)$, i.e. by "blocks in R, X, Y": two indices i and j are in the same block if we can go from i to j by equations $R_k = R_l$, or $X_k = X_l$, or $Y_k = Y_l$ (Since $X_k = X_l \Rightarrow f_1(R_k) = f_1(R_l) \oplus L_k \oplus L_l$ and $Y_k = Y_l \Rightarrow f_1(R_k) = f_1(R_l) \oplus L_k \oplus L_l \oplus \lambda_{k(i,j)}$, from these relations, we can replace the variable $f_1(R_k)$ by the variable $f_1(R_l)$ instead).

Finally, the only dependencies on the λ_k come when we want to evaluate the number H'' of f_1 such that: $\forall i$, $1 \leq i \leq \alpha$, X_i are pairwise distinct, where α is the number of X_i that we want pairwise distinct (if wanted we can assume $\alpha \leq O\left(\frac{m^2}{2^n}\right)$ since variables with no equation in R, X or Y create no problem). Each X_i has an expression like this: $X_i = f_1(R_j) \oplus \lambda_k \oplus L'_l$ (where L'_l is an expression in $\oplus$ of some L_i values), or like this: $X_i = f_1(R_j) \oplus L'_l$. This gives a number of solutions for f_1 that depends only of the fact that some equations of degree one in the λ_k variables are satisfied or not.

(These equations are $X_i \oplus X_j = X_k \oplus X_l$ where i, j are in the same block in R, X, Y and k, l are in the same block in R, X, Y, so these equations can be written only the L_i and λ_k variables).

Example In the example given in appendix B, $\lambda_1 = L_1 \oplus L_4 \oplus L_5 \oplus L_7$ is one of these equations, that can be true or not when the λ_i values are fixed (here it comes from $X_1 \oplus X_2 \oplus X_5 \oplus X_7$).

Analysis of the dependencies in the λ_k First, we can notice that if the system has no solution due to an incompatibility (for example if we want $X_1 = f_1(R_1) \oplus L_1$ and $X_2 = f_1(R_1) \oplus \lambda_1$ to be distinct) then we have a circle in R, X, Y with at least one equation in Y. The probability to get such circles has been evaluated in section 4 and is negligible if $m \ll 2^n$. So we will assume that we have no incompatibility in the system that says that the X_i variables considered are pairwise distinct. Let μ be the number of variables λ_k that satisfied at least one of these equations among the $\left(\frac{\alpha^2}{2}\right)$ equations considered for the evaluation of f_1. Each of the μ special λ_k values can have at most α exceptional relations. So for a λ like this, we have: $H \leq H^* \left(1 - \frac{\alpha}{2^n}\right)^{-\mu}$. The value $\left(1 - \frac{\alpha}{2^n}\right)^{-\mu}$ can be $\gg 1$, but since we have μ exceptional relations of degree one on μ variables λ_i, the weight W_λ of these λ values (i.e. the number of f_1, f_2, f_3 that give these values multiplied by the number of these values) satisfies:

$$W_\lambda \leq \frac{1}{2^{n\mu}} C^{\mu}_{\frac{\alpha^2}{2}} \left(1 - \frac{\alpha}{2^n}\right)^{-\mu} \text{ (we denote by } A_\mu \text{ this expression).}$$

(since we have $\leq \frac{\alpha^2}{2}$ possible equations). We have:

$$A_{\mu+1} \geq A_\mu \Leftrightarrow \left(\frac{\alpha^2}{2} - \mu\right)\left(1 - \frac{\alpha}{2^n}\right)^{-1} \geq 2^n(\mu + 1) \Leftrightarrow \mu \leq \text{ about } \frac{\alpha^2}{2 \cdot 2^n}.$$

So the weight W_λ becomes negligible as soon as $\mu \gg \frac{\alpha^2}{2 \cdot 2^n}$.

Remark If these μ variables λ_i generate almost all the possible relations with these variables, then the weight of these variables is even smaller since we just have to choose these μ variables among the α variables and then they are fixed (since almost all the equations are satisfied, many of these equations give equivalent values for the special λ_i). So we will have a C^{μ}_{α} instead of $C^{\mu}_{\frac{\alpha^2}{2}}$.

Finally we have obtain:

Theorem 51 *Let $\mathcal{F}$ be the set of values that we fix: i.e. in $\mathcal{F}$ we have the values of the Y_i, and all the indices (i, j) where we have all the equations $X_i = X_j$. Then if S and S' are two sequences of values of I_n^m such that:*

1. *$\forall i, j$, $Y_i = Y_j \Rightarrow S_i \neq S_j$ (and $S'_i \neq S'_j$).*
2. *No circle in R, X, Y can be created from the equalities $Y_i = Y_j \Rightarrow S_i \oplus S_j = X_i \oplus X_j$ and $R_k = R_l \Rightarrow X_k \oplus X_l = L_k \oplus L_l$.*

Then the number $H_{\mathcal{F}}$ of f_1, f_2, f_3 solutions satisfies:

$$|H_{\mathcal{F}}(S) - H_{\mathcal{F}}(S')| \leq H_{\mathcal{F}}(S) \cdot (q + r)$$

where $q = \frac{m^2}{2 \cdot 2^n}$ comes from the λ_i with very few special equalities, and r is a very small term related to the weight of the λ_i with a lot of special equalities (as we have seen r is negligible when $m \ll 2^n$).

We can do the same for $[S_i, T_i]$, as we did for $[Y_i, S_i]$. So, since by summation, we must obtain all the $(f_1, \ldots, f_4)$ with no circles, from theorem 51 we will get our results. Here the set E' depends on E, so this works for non-adaptive attacks. For adaptive attacks see [15] (then we have to eliminate some equations by conditions in $[S_i, T_i]$ independently of $[L_i, R_i]$, or to study the expectancy of the deviation of H).

Remark Another possibility is to use the result of [5]: with 2 times more rounds, security in CPA-1 can be changed in security in CPCA-2. However we would get like this CPCA-2 for 10 rounds (exactly as in [14]) instead of 6 rounds.

6 Comparing [14] and this paper

Technically the main differences between [14] and this paper are:

1. Here we introduce a condition: no more than $\frac{\lambda m(m-1)}{2^n}$indices (i, j), $i < j$ such that $X_i = X_j$ (instead of no more than θ pairwise distinct indices such that $X_{i_1} = X_{i_2} = \ldots = X_{i_\theta}$ of [14]). this gives us security when $m \ll 2^n$ (instead of $m \ll 2^{n(1-\varepsilon)}$ or $m \ll \frac{2^n}{n}$ of [14]).
2. In [14], 3 rounds are needed for half the variables to look random, and then 4 more rounds for the $[S_i, T_i]$. Here we show that the S_i will look random after 4 rounds even if the Z_i are public (with a probability near 1 when $m \ll 2^n$). So for the T_i we can use the same result with only one more round. Like this, we need less rounds in this paper compared with [14].
3. In this paper we study λ_k that come for Ψ^4 from $Y_i \oplus Y_j = 0$ (or similarly $Z_i \oplus Z_j = 0$ for Ψ^5) while in [14] all possible λ_k can be fixed.

Part II: Best found attacks

7 Generic attacks on Ψ^5

We will present here the two best generic attacks that we have found on Ψ^5:

1. A CPA-1 attack on Ψ^5 with $m \simeq 2^n$ and $\lambda = O(2^n)$ computations (This is an improvement compared with $m \simeq 2^{3n/2}$ and $\lambda = O(2^{3n/2})$ of [13]).
2. A KPA on Ψ^5 with $m \simeq 2^{3n/2}$ and $\lambda = O(2^{3n/2})$computations (This is an improvement compared with $m \simeq 2^{7n/4}$ and $\lambda = O(2^{7n/4})$ of [13]).

1. CPA-1 attack on Ψ^5.
   Let us assume that R_i =constant, $\forall i$, $1 \leq i \leq m$, $m \simeq 2^n$. We will simply count the number N of (i,j), $i < j$ such that $S_i = S_j$ and $L_i \oplus T_i = L_j \oplus T_j$. This number N will be about double for Ψ^5 compared with a truly random permutation.
   Proof:
   If $S_i = S_j$,
   $L_i \oplus T_i = L_j \oplus T_j \Leftrightarrow L_i \oplus Z_i = L_j \oplus Z_j \Leftrightarrow f_1(R_1) \oplus f_3(Y_i) = f_1(R_1) \oplus f_3(Y_j)$
   $\Leftrightarrow f_3(R_1 \oplus f_2(L_i \oplus f_1(R_1))) = f_3(R_1 \oplus f_2(L_j \oplus f_1(R_1))) \quad (\#)$.
   This will occur if $f_2(L_i \oplus f_1(R_1)) = f_2(L_j \oplus f_1(R_1))$, or if these values are distinct but have the same images by f_3, so the probability is about two times larger.

   Remarks
   (a) By storing the $S_i||L_i \oplus T_i$ values and looking for collisions, the complexity is in $\lambda \simeq O(2^n)$.
   (b) With a single value for R_i, we will get very few collisions. However this attack becomes significant if we have a few values R_i and for all these values about 2^n values L_i.
2. KPA on Ψ^5.
   The CPA attack can immediately be transformed in a KPA: for random $[L_i, R_i]$, we will simply count the number N of (i,j), $i < j$ such that $R_i = R_j$, $S_i = S_j$, and $L_i \oplus T_i = L_j \oplus T_j$. We will get about $\frac{m(m-1)}{2^{3n}}$ such collisions for Ψ^5, and about $\frac{m(m-1)}{2 \cdot 2^{3n}}$ for a random permutation. This KPA is efficient when m^2 becomes not negligible compared with 2^{3n}, i.e. when $m \geq$ about $2^{3n/2}$.

Remark These attacks are very similar with the attacks on 5-round Feistel schemes described by Knudsen (cf [2]) in the case where (unlike us) f_2 and f_3 are permutations (therefore, not random functions). Knudsen attacks are based on this theorem:

Theorem 71 (Knudsen, see [2]) *Let $[L_1, R_1]$ and $[L_2, R_2]$ be two inputs of a 5-round Feistel scheme, and let $[S_1, T_1]$ and $[S_2, T_2]$ be the outputs. Let us assume that the round functions f_2 and f_3 are permutations (therefore they are not random functions of F_n). Then, if $R_1 = R_2$ and $L_1 \neq L_2$, it is impossible to have simultaneously $S_1 = S_2$ and $L_1 \oplus L_2 = T_1 \oplus T_2$.*

Proof This comes immediately from (#) above.

8 Generic attacks on Ψ^k generators, $k \geq 6$

Ψ^k has always an even signature. This gives an attack in 2^{2n} if we want to distinguish Ψ^k from random permutations (see [13]) and if we have all the possible cleartext/ciphertext. In this appendix, we will present the best attacks that we know when we want to distinguish Ψ^k from random permutations with an even signature, or when we do not have exactly all the possible cleartext/ciphertext.

1. KPA with k even.
   Let (i,j) be two indices, $i \neq j$, such that $R_i = R_j$ and $S_i \oplus S_j = L_i \oplus L_j$. From [10] or [11] p.146, we know the exact value of H in this case, when k is even. We have:
   $$H = H^* \left(1 + \frac{1}{2^{(\frac{k}{2}-2)n}} - \frac{1}{2^{(\frac{k}{2}-1)n}} - \frac{2}{2^{\frac{kn}{2}}} + \frac{1}{2^{(k-1)n}}\right)$$
   where
   $$H^* = \frac{|F_n|^k}{2^{2nm}} \cdot \frac{1}{1-\frac{1}{2^{2n}}}$$
   i.e. H^* is the average value of H on two cleartext/ciphertext. So there is a small deviation, of about $\frac{1}{2^{(\frac{k}{2}-2)n}}$, from the average value.
   So in a KPA, when the $[L_i, R_i]$ are chosen at random, and if the f_i functions are chosen at random, we will get slightly more (i,j), $i<j$, with $R_i = R_j$ and $S_i \oplus S_j = L_i \oplus L_j$ from a Ψ^k (with k even) than from a truly random permutation. This can be detected if we have enough cleartext/ciphertext pairs from many Ψ^k permutations. In first approximation, these relations will act like independent Bernoulli variables (in reality the equations are not truly independent, but this is expected to create only a modification of second order).
   If we have N possibilities for (i,j), $i<j$, and if X is the number of (i,j), $i<j/R_i = R_j$ and $S_i \oplus S_j = L_i \oplus L_j$, we expect to have:
   $E(X) \simeq \frac{N}{2^{2n}}$
   $V(X) \simeq \frac{N}{2^{2n}}$
   $\sigma(X) \simeq \frac{\sqrt{N}}{2^n}$.
   We want $\sigma(X) \leq \frac{N}{2^{(\frac{k}{2}-2)n}} \cdot \frac{1}{2^{2n}}$ in order to distinguish Ψ^k from a random permutation. So we want $\frac{\sqrt{N}}{2^n} \leq \frac{N}{2^{\frac{k}{2}n}}$ i.e. $N \geq 2^{(k-2)n}$.
   However, if we have μ available permutations, with about 2^{2n} cleartext/ciphertext for each of these permutations, then $N \simeq 2^{4n}\mu$ (here we know these μ permutations almost on every possible cleartext. If not, μ will be larger and we will do more computations). $N \geq 2^{(k-2)n}$ gives $\mu \geq 2^{(k-6)n}$. This is an attack with $2^{(k-6)n}$ permutations and $2^{2n}\mu \simeq 2^{(k-4)n}$ computations.
2. KPA with k odd.
   In [15], a KPA with k odd is given (it has the same properties as the attack above for k even).

9 Conclusion

For a block cipher from $2n$ bits → $2n$ bits, we generally want to have no better attack than attacks with $\geq 2^{2n}$ computations. If this block cipher is a Feistel scheme we then need to have ≥ 6 rounds since (as shown in this paper) there is a generic attack on 5 rounds with 2^n computations in CPA-1 and $2^{3n/2}$ computations in KPA.

In this paper we have also shown that however, in the model where the adversaries have unlimited computing power but have access to only m cleartext/ciphertext pairs, the maximum possible security (i.e. $m \ll 2^n$) is obtained already for 5 rounds for CPA-1 and CPA-2 attacks. This solves an open problem of [1] and [14]. Moreover 6-round Feistel schemes can resist all CPCA-1 and CPCA-2 attacks when $m \ll 2^n$ (For CPCA-1 or CPCA-2 the case $k = 5$ rounds is still unclear: we only know that the security is between $m \ll 2^{n/2}$ and $m \ll 2^n$). When 2^{2n} is small (for example to generate 1000 pseudorandom permutations with an even signature of 30 bits → 30 bits) then more than 6 rounds are needed. In this paper we have studied such attacks, and we have extended the "coefficients H technique" to various cryptographic attacks.

We think that our proof strategy is very general and should be also efficient in the future to study different kinds of functions or permutation generators, such as, for example, Feistel schemes with a different group law than $\oplus$, or unbalanced Feistel schemes.

References

1. W. Aiello and R. Venkatesan. *Foiling Birthday Attacks in Length-Doubling Transformations-Benes: A Non-Reversible Alternative to Feistel. EUROCRYPT '96* (Lecture Notes in Computer Science 1070), pp. 307–320, Springer-Verlag.
2. L. R. Knudsen. *DEAL - A 128 bit Block Cipher. Technical Report* #151, University of Bergen, Departement of Informatics, Norway, February 1998.
3. M. Luby and C. Rackoff. *How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing*, vol. 17, n2, pp. 373–386, April 1988.
4. U. Maurer. *A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators. EUROCRYPT '92*, pp. 239–255, Springer-Verlag.
5. U. Maurer. *Indistinguishability of Random Systems. EUROCRYPT '02* (Lecture Notes in Computer Science 2332), pp. 110–132, Springer-Verlag.
6. U. Maurer and K. Pietrzak. *The security of Many-Round Luby-Rackoff Pseudo-Random Permutations. EUROCRYPT '03*, pp. –, Springer-Verlag.
7. V. Nachev. *Random Feistel schemes for $m = 3$*, available from the author at: Valerie.nachef@math.u-cergy.fr.
8. M. Naor and O. Reingold. *On the Construction of pseudo-random perlutations: Luby-Rackoff revisited. Journal of Cryptology*, vol. 12, 1999, pp. 29–66. Extended abstract was published in Proc. 29th Ann. ACM Symp. on Theory of Computing, 1997, pp. 189–199.
9. J. Patarin. *Pseudorandom Permutations based on the DES Scheme. Eurocode '90*, LNCS 514, pp. 193–204, Springer-Verlag.

10. J. Patarin. *New results on pseudorandom permutation generators based on the DES scheme. Crypto '91*,pp. 301–312, Springer-Verlag.
11. J. Patarin. *Etude des générateurs de permutations bass sur le schma du DES. Ph. D. Thesis*, Inria, Domaine de Voluceau, Le Chesnay, France, 1991.
12. J. Patarin. *About Feistel Schemes with 6 (or More) Rounds. Fast Software Encryption 1998*, pp. 103–121.
13. J. Patarin. *Generic Attacks on Feistel Schemes. Asiacrypt '01* (Lecture Notes in Computer Science 2248), pp. 222–238, Springer-Verlag.
14. J. Patarin. *Luby-Rackoff: 7 Rounds are Enough for $2^{n(1-\epsilon)}$ Security. Crypto '03* (Lecture Notes in Computer Science 2729), pp.513–529, Springer-Verlag.
15. J. Patarin. *Extended version of this paper*, avaible from the author.
16. B. Schneier and J. Kelsey. *Unbalanced Feistel Networks and Block Cipher Design. FSE '96* (Lecture Notes in Computer Science 1039), pp. 121–144, Springer-Verlag.

Appendices

A Summary of the known results on random Feistel schemes

KPA denotes known plaintext attacks. CPA-1 denotes non-adaptive chosen plaintext attacks. CPA-2 denotes adaptive chosen plaintext attacks. CPCA-1 denotes non-adaptive chosen plaintext and ciphertext attacks. CPCA-2 denotes adaptive chosen plaintext and chosen ciphertext attacks. Non-Homogeneous properties are defined in [12].

This figure 1 present the best known results against unbounded adversaries limited by m oracle queries.

	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2	Non-Homogeneous
Ψ	1	1	1	1	1	1
Ψ^2	$2^{n/2}$	2	2	2	2	2
Ψ^3	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	3	2
Ψ^4	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	2
Ψ^5	2^n	2^n	2^n	$\geq 2^{n/2}$	$\geq 2^{n/2}$	2
Ψ^6	2^n	2^n	2^n	2^n	2^n	4 *
$\Psi^k, k \geq 6$	2^n	2^n	2^n	2^n	2^n	$\leq \left(\frac{k}{2}-1\right)^2$ **

Fig. 1. Minimum number m of queries to distinguish Ψ^k from a random permutation of $I_n \rightarrow I_n$. For simplicity we denote 2^α for $O(2^\alpha)$ i.e. when we have security as long as $m \ll 2^\alpha$. $\geq$ means best security proved.

* ≤ 4 comes from [13] and ≥ 4 comes from [7].
** with k even and with $(k-2)(k-4)$ exceptional equations, so if $k \geq 7$ we need more than one permutation for this property.

	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2
Ψ	1	1	1	1	1
Ψ^2	$2^{n/2}$	2	2	2	2
Ψ^3	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	3
Ψ^4	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
Ψ^5	$\leq 2^{3n/2}$	2^n	2^n	$\leq 2^n$	$\leq 2^n$
Ψ^6	$\leq 2^{2n}$	$\leq 2^{2n}$	$\leq 2^{2n}$	$\leq 2^{2n}$	$\leq 2^{2n}$
Ψ^7	$\leq 2^{3n}$	$\leq 2^{3n}$	$\leq 2^{3n}$	$\leq 2^{3n}$	$\leq 2^{3n}$
Ψ^8	$\leq 2^{4n}$	$\leq 2^{4n}$	$\leq 2^{4n}$	$\leq 2^{4n}$	$\leq 2^{4n}$
$\Psi^k, k \geq 6$ *	$\leq 2^{(k-4)n}$	$\leq 2^{(k-4)n}$	$\leq 2^{(k-4)n}$	$\leq 2^{(k-4)n}$	$\leq 2^{(k-4)n}$

Fig. 2. Minimum number λ of computations needed to distinguish a generator Ψ^k (with one or many such permutations available) from random permutations with an even signature of $I_n \rightarrow I_n$. For simplicity we denote α for $O(\alpha)$. $\leq$ means best known attack.

* If $k \geq 7$ these attacks analyze about $2^{(k-6)n}$ permutations of the generator and if $k \leq 6$ only one permutation is needed.

History for Ψ^5 For Ψ^5 the best results of security against CPA-2 was:

- In 1988: $m \ll 2^{n/2}$ (cf [3]).
- In 1998: $m \ll 2^{3n/4}$ (cf [12]).
- In 2003: $m \ll 2^{5n/6}$ (cf [13]).
- In 2004: $m \ll 2^n$ (cf this paper).

However CPCA-2 for Ψ^5 is still unclear: so far we only have the original result of Luby and Rackoff $m \ll 2^{n/2}$.

B Example for theorem 31

We will illustrate here theorem 31 on a small toy example. Let $1, 2, 3, 4, 5, 6, 7$ be our indices ($m = 7$). Let us assume that f_1 is fixed such that $R_4 = R_1$, and $R_7 = R_5$, are our only equations $R_i = R_j$ $i > j$. Let us assume that the Y_i are given, and that $Y_4 = Y_2$, and $Y_7 = Y_3$ are the only equations $Y_i = Y_j$, $i > j$.Then we want to show that λ_1 and λ_2 look random, where $\lambda_1 = X_4 \oplus X_2$ and $\lambda_2 = X_7 \oplus X_3$ when f_1, f_2 are randomly chosen. For this, we fix λ_1 and λ_2, $\lambda_1 \neq 0$, $\lambda_2 \neq 0$, and we look for the number H of (f_1, f_2) that give these values. We want to prove that this number H does not depend significantly on λ_1 and λ_2 (except for well detected values of small weight). H is the number of (f_1, f_2) such that (here we put only pairwise distinct R_i variables):

1. $f_1(R_2) = f_1(R_1) \oplus L_2 \oplus L_4 \oplus \lambda_1$ and $f_1(R_5) = f_1(R_3) \oplus L_3 \oplus L_7 \oplus \lambda_2$ (these two equations do not create any problem: they just fix f_1 on two points).
2. **<u>Block $R_1 Y$:</u>**

   $f_2(L_1 \oplus f_1(R_1)) = R_1 \oplus Y_1$

$f_2(L_4 \oplus \lambda_1 \oplus f_1(R_1)) = R_2 \oplus Y_2$
$f_2(L_4 \oplus f_1(R_1)) = R_1 \oplus Y_2.$

Block R_3Y:

$f_2(L_3 \oplus f_1(R_3)) = R_3 \oplus Y_3$
$f_2(L_3 \oplus L_5 \oplus L_7 \oplus \lambda_2 \oplus f_1(R_3)) = R_5 \oplus Y_5$
$f_2(L_3 \oplus f_1(R_3) \oplus \lambda_2) = R_5 \oplus Y_3.$

Block R_6Y:

$f_2(L_6 \oplus f_1(R_6)) = R_6 \oplus Y_6$

Let us assume that, for example, all the $R_i \oplus Y_i$ are pairwise distinct. Then we want to evaluate the number of functions f_1 such that all the X_i are pairwise distinct. These conditions are more difficult to analyze since here we do not want equalities, but non equalities.

- If $\lambda_1 \in \{0, L_1 \oplus L_4\}$, or $\lambda_2 \in \{0, L_5 \oplus L_7\}$, we have no solution (these values give a circle in R, X, Y).
- For the X_i to be pairwise distinct, we must choose f_1 such that: $f_1(R_1) \oplus f_1(R_3)$ is not in A, where A is a set of 9 values (or less if we have collisions): $A = \{L_1 \oplus L_3, L_4 \oplus \lambda_1 \oplus L_3, L_4 \oplus L_3, L_1 \oplus L_3 \oplus L_5 \oplus L_7 \oplus \lambda_2, L_4 \oplus \lambda_1 \oplus L_3 \oplus L_5 \oplus L_7 \oplus \lambda_2, L_4 \oplus L_3 \oplus L_5 \oplus L_7 \oplus \lambda_2, L_1 \oplus L_3 \oplus \lambda_2, L_4 \oplus \lambda_1 \oplus L_3 \oplus \lambda_2, L_4 \oplus L_3 \oplus \lambda_2\}$. In the proof of theorem 31, we analyze the possible dependencies of $|A|$ with the λ_i values.

C Examples of unusual values of $\boldsymbol{H}$ for $\boldsymbol{\Psi^5}$

Example 1: Large value for H

With $m = 2$, when $R_1 = R_2$, $S_1 = S_2$ and $L_1 \oplus L_2 = T_1 \oplus T_2$, then

$$H = \frac{|F_n|^5}{2^{2nm}} \left(2 - \frac{1}{2^n}\right).$$

So here the value of H is about double than average with only $m = 2$.

Remark: $\forall k \in \mathbf{N}^*$, Ψ^k has always such large H with small m ($m \leq \left(\frac{k}{2} - 1\right)^2$ if k is even), we say that "Ψ^k is not homogeneous": see [12]. However, when $k \geq 7$, the probability that such inputs/outputs exist is generally negligible if we study only one single specific permutation.

Example 2: Small value for H

Here our example cannot be with $m \ll 2^{n/2}$ since we know that we always have

$$H \geq \frac{|F_n|^5}{2^{2nm}} \left(1 - \frac{m(m-1)}{2^n}\right)$$

(the proof is the same for Ψ^4 and Ψ^5).

However, we will show that when $m \to 2^{n/2}$, H can be much smaller than average (i.e. $m \to 2^n$ is not necessary, $m \to 2^{n/2}$ is enough). In this example 2, we will assume:

1. $\forall i, j,\ 1 \leq i \leq j \leq m,\ R_i = R_j\ (= R_1)$.
2. $\forall i, j,\ 1 \leq i \leq j \leq m,\ S_i = S_j\ (= S_1)$.
3. $\forall i, j,\ 1 \leq i \leq j \leq m,\ i \neq j \Rightarrow L_i \oplus L_j \neq T_i \oplus T_j$ (in example 3 below we will not need this condition 3).

To get condition 3, we may assume, for example, that $\forall i,\ 1 \leq i \leq m,\ L_i = i \oplus \varphi(i)$ and $T_i = \varphi(i)$, where φ is well chosen. So $L_i \oplus L_j = T_i \oplus T_j \Leftrightarrow i = j$.

From 1 we have: $\forall i, j,\ 1 \leq i \leq j \leq m,\ X_i \oplus X_j = L_i \oplus L_j$.

From 2 we have: $\forall i, j,\ 1 \leq i \leq j \leq m,\ Z_i \oplus Z_j = T_i \oplus T_j$.

H is the number of f_1, f_2, f_3, f_4, f_5 such that: $\forall i,\ 1 \leq i \leq m$,

$$L_i \oplus f_1(R_1) = X_i$$

$$R_1 \oplus f_2(L_i \oplus f_1(R_1)) = Y_i$$

$$X_i \oplus f_3(Y_i) = Z_i$$

$$Y_i \oplus f_4(T_i \oplus f_5(S_1)) = S_1$$

$$Z_i \oplus f_5(S_1) = T_i$$

So H is $|F_n|^2$ times the number of f_2, f_3, f_4 such that: $\forall i,\ 1 \leq i \leq m$,

$$\begin{cases} Y_i = R_1 \oplus f_2(L_i \oplus f_1(R_1)) = S_1 \oplus f_4(T_i \oplus f_5(S_1)) \\ f_3(Y_i) = L_i \oplus T_i \oplus f_1(R_1) \oplus f_5(S_1) \end{cases}$$

Since all the $L_i \oplus T_i$ are pairwise distinct, all the Y_i must be pairwise distinct. So for Y_i, $1 \leq i \leq m$, we have exactly: $2^n(2^n-1)(2^n-2)\ldots(2^n-m+1)$ solutions.

Now when Y_i, $1 \leq i \leq m$, are fixed, f_2, f_3 and f_4 are fixed on exactly m pairwise distinct points. So $H = \frac{|F_n|^5}{2^{3nm}} 2^n(2^n-1)(2^n-2)\ldots(2^n-m+1)$.

Let H^* be the average value of H (when the $[S_i, T_i]$ are pairwise distinct).

$$H^* = \frac{|F_n|^5}{2^{2n}(2^{2n}-1)(2^n-2)\ldots(2^{2n}-m+1)} \geq \frac{|F_n|^5}{2^{2nm}}.$$

So here:

$$\frac{H}{H^*} \leq (1-\frac{1}{2^n})(1-\frac{2}{2^n})\ldots(1-\frac{m-1}{2^n})$$

$$ln\left(\frac{H}{H^*}\right) \simeq -\frac{1+2+\ldots+(m-1)}{2^n} = -\frac{m(m-1)}{2^n}.$$

So when $m(m-1)$ is not negligible compared with 2^n, H will be significatively smaller than H^*, as claimed.

Remark 1 Here $R_i \oplus S_i$ is not random (since $R_i \oplus S_i$is constant), and $L_i \oplus T_i$ is not random (in example 3 below we will remove this condition on $L_i \oplus T_i$). These hypothesis are generally unrealistic in a cryptographic attack, where $\forall i$, $1 \leq i \leq m$, L_i or T_i, and R_i or S_i, cannot be chosen.

Remark 2 If we start, as here, from $[L_i, R_i]$ values with R_i constant, then the X_i values are pairwise distinct, so the Y_i values are perfectly random (if we define Y_i only from the relation $Y_i = R_i \oplus f_2(X_i)$). However, the Z_i values are not perfectly random (since the probability to have $Z_i \oplus Z_j = L_i \oplus L_j$ is the probability to have $f_3(Y_i) = f_3(Y_j)$ so is about double than average). Similarly, the $[S_i, T_i]$ values are not perfectly random since the probability to have $S_i = S_j$ and $T_i \oplus T_j = L_i \oplus L_j$ is in relation with the probability to have $f_3(Y_i) = f_3(Y_j)$, so is about double than average. We will use again this idea in example 3 below.

Remark 3 Here when $m \to 2^{n/2}$, we can have circles in Y, S, (and circles in R, Y) and this is a way to explain why in this example H can be much smaller than H^*.

Example 3: Small value for H, with random L_i and T_i

In this example 3, we will assume:

1. $\forall i, j$, $1 \leq i \leq j \leq m$, $R_i = R_j$ $(= R_1)$.
2. $\forall i, j$, $1 \leq i \leq j \leq m$, $S_i = S_j$ $(= S_1)$.
3. Let $A_i = L_i \oplus T_i$. Then A_i, $1 \leq i \leq m$, is random. More precisely it will be enough to assume that the number N of collisions $A_i = A_j$, $i < j$, is $< \frac{m(m-1)}{2 \cdot 2^n ln2}$ to show that H is small compared with the average value H^*. For random values A_i we have $N \simeq \frac{m(m-1)}{2 \cdot 2^n}$, so it is the case ($\frac{1}{ln2} \simeq 1,44$).

As in example 2, H is $|F_n|^2$ times the number of f_2, f_3, f_4 such that: $\forall i$, $1 \leq i \leq m$,

$$\begin{cases} Y_i = R_1 \oplus f_2(L_i \oplus f_1(R_1)) = S_1 \oplus f_4(T_i \oplus f_5(S_1)) \\ f_3(Y_i) = L_i \oplus T_i \oplus f_1(R_1) \oplus f_5(S_1) \end{cases}.$$

Since all the $L_i \oplus f_1(R_1)$ are pairwise distinct, and all the $T_i \oplus f_5(S_1)$ are pairwise distinct, f_2 and f_4 are fixed on exactly m points when Y_i, $1 \leq i \leq m$, is fixed.

So H is $\frac{|F_n|^4}{2^{2nm}}$ times the number of Y_i, f_3 such that: $\forall i$, $1 \leq i \leq m$, $f_3(Y_i) = L_i \oplus T_i \oplus f_1(R_1) \oplus f_5(S_1)$.

Let A_i be a sequence of values of I_n, $1 \leq i \leq m$. We want to evaluate the number h of Y_i, f_3 such that: $\forall i$, $1 \leq i \leq m$, $f_3(Y_i) = A_i$. Let h^* be the average value for h (average on all sequences A_i). We have $h^* = |F_n|$. For random values Y_i, and random functions f_3, A_i will have about 2 times more collisions $A_i = A_j$, $i < j$, than average sequences A_i.

So h for random values A_i is $\ll h^*$, and h for values A_i with 2 times more collisions than average is $\gg h^*$. This shows that if in this example 3 $L_i \oplus T_i$ is random, then $H \ll H^*$.