About Feistel Schemes with Six (or More) Rounds

Jacques Patarin

Bull PTS
68, route de Versailles - BP45
78431 Louveciennes Cedex - France
J.Patarin@frlv.bull.fr

Abstract. This paper is a continuation of the work initiated in [2] by M. Luby and C. Rackoff on Feistel schemes used as pseudorandom permutation generators. The aim of this paper is to study the qualitative improvements of "strong pseudorandomness" of the Luby-Rackoff construction when the number of rounds increase. We prove that for 6 rounds (or more), the success probability of the distinguisher is reduced from $\mathcal{O}\left(\frac{m^2}{2^n}\right)$ (for 3 or 4 rounds) to at most $\mathcal{O}\left(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}}\right)$. (Here m denotes the number of cleartext or ciphertext queries obtained by the enemy in a dynamic way, and $2n$ denotes the number of bits of the cleartexts and ciphertexts).
We then introduce two new concepts that are stronger than strong pseudorandomness: "very strong pseudorandomness" and "homogeneous permutations". We explain why we think that those concepts are natural, and we study the values k for which the Luby-Rackoff construction with k rounds satisfy these notions.

1 Introduction

In their famous paper [2], M. Luby and C. Rackoff provided a construction of pseudorandom permutations and strong pseudorandom permutations. ("Strong pseudorandom permutations" are also called "super pseudorandom permutations": here the distinguisher can access the permutation *and* the inverse permutation at points of its choice.) The basic building block of the Luby-Rackoff construction (L-R construction) is the so called Feistel permutation based on a pseudorandom function defined by the key. Their construction consists of four rounds of Feistel permutations (for strong pseudorandom permutations) or three rounds of Feistel permutations (for pseudorandom permutations). Each round involves an application of a different pseudorandom function. This L-R construction is very attractive for various reasons: it is elegant, the proof does not involve any unproven hypothesis, almost all (secret key) block ciphers in use today are based on Feistel schemes, and the number of rounds is very small (so that their result may suggest ways of designing faster block ciphers).

The L-R construction inspired a considerable amount of research. One direction of research was to improve the security bound obtained in the "main

S. Vaudenay (Ed.): Fast Software Encryption – FSE'98, LNCS 1372, pp. 103–121, 1998.

lemma" of [2] p. 381, *i.e.* to decrease the success probability of the distinguisher. It was noticed (in [1] and [7]) that in a L-R construction with 3 or 4 rounds, the security bound given in [2] was almost optimal. It was conjectured that for more rounds, this security could be greatly improved ([7], [10]). However, the analysis of these schemes appears to be very technical and difficult, so that some transformations in the L-R construction were suggested, in order to simplify the proofs ([1], [3], [4], [10]). However, by doing this, we lose the simplicity of the original L-R construction.

In this paper, we study again this original L-R construction. In [9], it was shown that the success probability of the distinguisher is reduced from $\mathcal{O}\left(\frac{m^2}{2^n}\right)$ for 3 or 4 rounds of a L-R construction, to at most $\mathcal{O}\left(\frac{m^3}{2^{2n}}\right)$ for 5 rounds (pseudorandom permutations) or 6 rounds (strong pseudorandom permutations) of a L-R construction. (In these expressions, m denotes the number of cleartext or ciphertext queries obtained by the enemy, and $2n$ denotes the number of bits of the cleartexts and ciphertexts).

In part I of this paper, we further improve this result: we show that, for 6 rounds (or more), the success probability of the distinguisher is at most $\mathcal{O}\left(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}}\right)$. Moreover, we know that a powerful distinguisher is always able to distinguish a L-R construction from a random permutation when $m \geq 2^n$ (as noticed in [1], [3], [7]). Then, in part II of this paper, we introduce two new concepts about permutation generators: "very strong pseudorandomness" and "homogeneous permutations". These concepts both imply that the generator is a strong pseudorandom generator. We explain why we feel that it is natural to introduce these notions, and we characterize the values k such that the L-R constructions with k rounds satisfy (or not) these notions.

Finally we formulate a few open problems and we conclude.

Part I: Improved security bounds for Ψ^6

2 Notations

(These notations are similar to those of [3], [9] and [10].)

- I_n denotes the set of all n-bit strings, $I_n = \{0,1\}^n$.
- F_n denotes the set of all functions from I_n to I_n, and B_n denotes the set of all such permutations ($B_n \subset F_n$).
- Let x and y be two bit strings of equal length, then $x \oplus y$ denotes their bit-by-bit exclusive-or.
- For any $f, g \in F_n$, $f \circ g$ denotes their composition.
- For $a, b \in I_n$, $[a, b]$ is the string of length $2n$ of I_{2n} which is the concatenation of a and b.
- Let f_1 be a function of F_n. Let L, R, S and T be elements of I_n. Then by definition:

$$\Psi(f_1)[L, R] = [S, T] \Leftrightarrow [(S = R) \; and \; (T = L \oplus f_1(R))].$$

– Let f_1, f_2, ..., f_k be k functions of F_n. Then by definition:

$$\Psi^k(f_1, ..., f_k) = \Psi(f_k) \circ ... \circ \Psi(f_2) \circ \Psi(f_1).$$

(When f_1, ..., f_k are randomly chosen in F_n, Ψ^k is the L-R construction with k rounds.)
– We assume that the definitions of permutation generators, distinguishing circuits, normal and inverse oracle gates are known. These definitions can be found in [2] or [3] for example.
– Let ϕ be a distinguishing circuit. We will denote by $\phi(F)$ its output (1 or 0) when its oracle gates are given the values of a function F.

3 Our new theorem for Ψ^6 and related work

In [2], M. Luby and C. Rackoff demonstrated how to construct a pseudorandom permutation generator from a pseudorandom function generator. Their generator was mainly based on the following theorem (called "main lemma" in [2] p. 381):

Theorem 1 (M. Luby and C. Rackoff). *Let ϕ be a distinguishing circuit with m oracle gates such that its oracle gates are given the values of a function F from I_{2n} to I_{2n}. Let P_1 be the probability that $\phi(F) = 1$ when f_1, f_2, f_3 are three independent functions randomly chosen in F_n and $F = \Psi^3(f_1, f_2, f_3)$. Let P_1^* be the probability that $\phi(F) = 1$ when F is a function randomly chosen in F_{2n}. Then for all distinguishing circuits ϕ:*

$$|P_1 - P_1^*| \leq \frac{m^2}{2^n},$$

i.e. the security is guaranteed until $m = \mathcal{O}(2^{\frac{n}{2}})$.

In [9], we proved the following theorem:

Theorem 2 (J. Patarin, [9]). *Let ϕ be a super distinguishing circuit with m oracle gates (a super distinguishing circuit can have normal or inverse oracle gates). Let P_1 be the probability that $\phi(F) = 1$ when $f_1, f_2, f_3, f_4, f_5, f_6$ are six independent functions randomly chosen in F_n and $F = \Psi^6(f_1, f_2, f_3, f_4, f_5, f_6)$. Let P_1^{**} be the probability that $\phi(F) = 1$ when F is a permutation randomly chosen in B_{2n}. Then:*

$$|P_1 - P_1^{**}| \leq \frac{5m^3}{2^{2n}},$$

i.e. the security is guaranteed until $m = \mathcal{O}(2^{\frac{2n}{3}})$.

Moreover, in [7] p. 310, we presented the following conjecture:

Conjecture: *For Ψ^5, or perhaps Ψ^6 or Ψ^7, and for any distinguishing circuit with m oracle gates, $|P_1 - P_1^*| \leq \frac{30m}{2^n}$ (the number 30 is just an example).*

As far as we know, nobody has yet proved this conjecture (if the conjecture is true, then the security is guaranteed until $m = \mathcal{O}(2^n)$). As mentioned in [1] and [3], the technical problems in analysing L-R construction with improved bounds seem to be very difficult (moreover, our conjecture may be wrong...). However, this part I makes a significant advance in the direction of this conjecture:

Theorem 3 (J. Patarin, this conference FSE'98). *Using the same notations as in theorem 2:*

$$|P_1 - P_1^{**}| \leq \frac{47m^4}{2^{3n}} + \frac{17m^2}{2^{2n}},$$

i.e. the security is guaranteed until $m = \mathcal{O}(2^{\frac{3n}{4}})$.

To prove this theorem 3, we first prove this "basic result":

"Basic result": *Let $[L_i, R_i]$, $1 \leq i \leq m$, be m distinct elements of I_{2n} ("distinct" means that if $i \neq j$, then $L_i \neq L_j$ or $R_i \neq R_j$). Let $[S_i, T_i]$, $1 \leq i \leq m$, be also m distinct elements of I_{2n}. Then the number H of 6-uples of functions $(f_1, ..., f_6)$ of F_n^6 such that:*

$$\forall i,\ 1 \leq i \leq m, \Psi^6(f_1, ..., f_6)[L_i, R_i] = [S_i, T_i]$$

satisfies:

$$H \geq \frac{|F_n|^6}{2^{2nm}}\Big(1 - \frac{47m^4}{2^{3n}} - \frac{16m^2}{2^{2n}}\Big).$$

Proof of the "basic result": The proof of the "basic result" is given in the next section.

Proof of theorem 3: The proof of theorem 3 is a direct consequence of the "basic result" and the general theorems of the proof techniques given in [6] or [8] or [9].

Remark: It can be noticed that – to prove theorem 3 – we just need a general minoration of H (such as in the "basic result") and we do not need both a general minoration and majoration of H. This is particularly important since, as we will see in section 6, no general majoration of H exists near the value $\frac{|F_n|^6}{2^{2nm}}$.

4 Proof of the "basic result": $H \geq \frac{|F_n|^6}{2^{2nm}}\left(1 - \frac{47m^4}{2^{3n}} - \frac{16m^2}{2^{2n}}\right)$

4.1 Definition of (C)

Let $[X_i, P_i]$ and $[Q_i, Y_i]$, $1 \leq i \leq m$, be the values such that:

$$\Psi^2(f_1, f_2)[L_i, R_i] = [X_i, P_i]$$

and

$$\Psi^4(f_1, f_2, f_3, f_4)[L_i, R_i] = [Q_i, Y_i]$$

(*i.e.* $[L_i, R_i]$ are the inputs, $[X_i, P_i]$ are the values after two rounds, $[Q_i, Y_i]$ are the values after four rounds, and $[S_i, T_i]$ are the output values after six rounds).

We denote by (C) the following set of equations:

$$(C) \quad \forall i, j,\ 1 \le i \le m,\ 1 \le j \le m,\ i \ne j,\ \begin{cases} R_i = R_j \Rightarrow X_i \oplus L_i = X_j \oplus L_j \\ S_i = S_j \Rightarrow Y_i \oplus T_i = Y_j \oplus T_j \\ X_i = X_j \Rightarrow P_i \oplus R_i = P_j \oplus R_j \\ Y_i = Y_j \Rightarrow Q_i \oplus S_i = Q_j \oplus S_j \\ P_i = P_j \Rightarrow X_i \oplus Q_i = X_j \oplus Q_j \\ Q_i = Q_j \Rightarrow P_i \oplus Y_i = P_j \oplus Y_j \end{cases}$$

Then, from [9], p. 145 or [8], p. 134, we know that the exact value for H is:

$$H = \sum_{(X,Y,P,Q) \text{ satisfying } (C)} \frac{|F_n|^6}{2^{6mn}} \cdot 2^{n(r+s+x+y+p+q)},$$

where:

- r is the number of independent equations $R_i = R_j$, $i \ne j$,
- s is the number of independent equations $S_i = S_j$, $i \ne j$,
- x is the number of independent equations $X_i = X_j$, $i \ne j$,
- y is the number of independent equations $Y_i = Y_j$, $i \ne j$,
- p is the number of independent equations $P_i = P_j$, $i \ne j$,
- and q is the number of independent equations $Q_i = Q_j$, $i \ne j$.

Remark: When m is small compared to $2^{n/2}$, and when the equalities in the R_i and S_j variables do not have special "patterns", then it is possible to prove that the dominant terms in the value of H above correspond to $x = y = p = q = 0$. Then the number of (X, Y, P, Q) satisfying (C) is about $\frac{2^{4nm}}{2^{n(r+s)}}$, so that:

$$H \simeq \frac{2^{4nm}}{2^{n(r+s)}} \cdot \frac{|F_n|^6}{2^{6nm}} \cdot 2^{n(r+s)} \simeq \frac{|F_n|^6}{2^{2nm}},$$

as expected.

However, we will see in section 6 that, when the equalities in R_i and S_j have special "patterns" (even for small values of m), then the value of H can be much larger than that (but never much smaller, as shown by the basic result).

Moreover, when m is not small compared to $2^{n/2}$, then the dominant terms in the value of H no longer correspond to $x = y = p = q = 0$.

These two facts may explain why the proof of the "basic result" is so difficult.

4.2 Plan of the proof

To prove the "basic result", we proceed as follows: we define two sets E and D, $D \subset E \subset I_n^4$, and a function $\Lambda : D \to I_n^4$ such that the three lemmas below are satisfied.

Lemma 4. *$\forall (X,Y,P,Q) \in E$, $\Lambda(X,Y,P,Q)$ satisfies all the equations (C).*

($\Lambda(X,Y,P,Q)$ will be often denoted by (X',Y',P',Q').)

Lemma 5. *$\forall (X',Y',P',Q') \in \Lambda(E)$, the number of $(X,Y,P,Q) \in E$ such that $\Lambda(X,Y,P,Q) = (X',Y',P',Q')$ is $\leq 2^{n(r+s+x'+y'+p'+q')}$, where:*

- *r is the number of independent equations $R_i = R_j$, $i \neq j$,*
- *s is the number of independent equations $S_i = S_j$, $i \neq j$,*
- *x' is the number of independent equations $X'_i = X'_j$, $i \neq j$,*
- *y' is the number of independent equations $Y'_i = Y'_j$, $i \neq j$,*
- *p' is the number of independent equations $P'_i = P'_j$, $i \neq j$,*
- *q' is the number of independent equations $Q'_i = Q'_j$, $i \neq j$*

Lemma 6.

$$|E| \geq 2^{4nm}\Big(1 - \frac{47m^4}{2^{3n}} - \frac{16m^2}{2^{2n}}\Big).$$

Then the "basic result" is just a consequence of these three lemmas, as follows.

As we said in section 4.1,

$$H = \sum_{(X,Y,P,Q) \text{ satisfying } (C)} \frac{|F_n|^6}{2^{6mn}} . 2^{n(r+s+x+y+p+q)}.$$

Thus, from lemma 4:

$$H \geq \sum_{(X',Y',P',Q') \in \Lambda(E)} \frac{|F_n|^6}{2^{6mn}} . 2^{n(r+s+x'+y'+p'+q')}.$$

Therefore, from lemma 5, H is greater than

$$\sum_{(X',Y',P',Q') \in \Lambda(E)} \frac{|F_n|^6}{2^{6mn}} . \big|\{(X,Y,P,Q) \in E,\ \Lambda(X,Y,P,Q) = (X',Y',P',Q')\}\big|$$

i.e.

$$H \geq \frac{|E| . |F_n|^6}{2^{6nm}}.$$

Finally, from lemma 6:

$$H \geq \frac{|F_n|^6}{2^{2nm}}\Big(1 - \frac{47m^4}{2^{3n}} - \frac{16m^2}{2^{2n}}\Big),$$

as claimed.

We will now below define Λ and prove lemma 4, lemma 5 and lemma 6.

4.3 General remarks

Remark 1: Since the proof below is rather long and technical, we suggest the interested reader to first read the proof of theorem 2, which is more simple (this proof can be found in the extended version of [9], available from the author), because our proof of lemma 4, 5 and 6 below is essentially an improvement of this previous result.

Remark 2: Figure 1 below shows how we define Λ (*i.e.* X', Y', P', Q') below. In a way, our aim can be described as follows: we must transform "most" (X, Y, P, Q) into a (X', Y', P', Q') that satisfies (C) (and the three lemmas). Roughly speaking, things can be seen as follows: we must handle the fact that *two* exceptional equations in X, P, Q or Y can occur (in order to have a proof in $\mathcal{O}\left(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}}\right)$ as wanted). However, the probability that *three* exceptional equations occur between four given indices i, j, k, ℓ is assumed to be negligible. (In Luby-Rackoff proof of theorem 1, the probability that *one* exceptional equation occurs between the intermediate variables was negligible, but no more here. Similarly, in our previous proof of theorem 2, the probability that *two* exceptional equations occur between the intermediate variable was negligible, but no more here.)

Remark 3: Only *two* exceptional equations in X, P, Q or Y can occur between three of four given indices, but the total number of exceptional equations in X, P, Q or Y can be huge. For example, if $m = 2^{0.7n}$, then the number of equations $X_i = X_j$, $i \neq j$, is expected to be about $\frac{m^2}{2^n} = \frac{2^{1.4n}}{2^n} = 2^{0.4n}$.

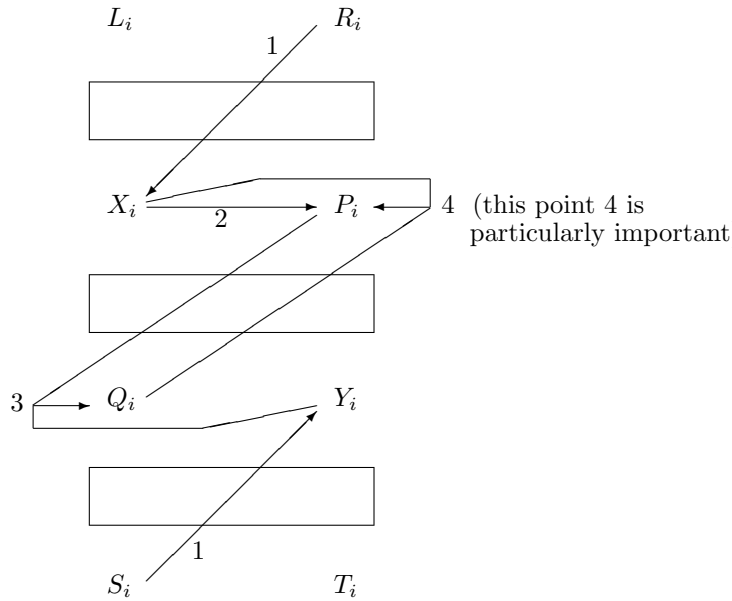


Figure 1: General view of the construction of Λ.

4.4 Definition of Λ

D is the domain of Λ (*i.e.* the set of all (X, Y, P, Q) for which Λ is defined). E will be a subset of D.

Definition of X'
Let $X = (X_1, ..., X_m)$ be an element of I_n^m. Similarly, let Y, P, Q be three elements of I_n^m. For all i, $1 \leq i \leq m$, let:

- i_R be the smallest integer, $1 \leq i_R \leq i$, such that $R_i = R_{i_R}$.
- i_S be the smallest integer, $1 \leq i_S \leq i$, such that $S_i = S_{i_S}$.

Then $X' = (X'_1, ..., X'_m)$ is (by definition) the element of I_n^m such that:

$$\forall i,\ 1 \leq i \leq m,\ X'_i = X_{i_R} \oplus L_i \oplus L_{i_R}.$$

Definition of Y'
Similarly, $Y' = (Y'_1, ..., Y'_m)$ is by definition the element of I_n^m such that:

$$\forall i,\ 1 \leq i \leq m,\ Y'_i = Y_{i_S} \oplus T_i \oplus T_{i_S}.$$

Note: These definitions of X' and Y' are shown with the two arrows numbered "1" in figure 1.

Definition of P^*
P^* is an intermediate variable that we use before defining P'. (In figure 1, the definition of P^* is shown with the arrow numbered "2", and the definition of P', that we do below, is shown with the arrow numbered "4"). For all i, $1 \leq i \leq m$, let i_X be the smallest integer, $1 \leq i_X \leq i$, such that $X'_i = X'_{i_X}$.

Then $P^* = (P_1^*, ..., P_m^*)$ is (by definition) the element of I_n^m such that:

$$\forall i,\ 1 \leq i \leq m,\ P_i^* = P_{i_X} \oplus R_i \oplus R_{i_X}.$$

Definition of Q'
Q' is now defined by a combined effect of P^* and Y'. (This is shown in figure 1 by the arrow numbered "3"). Before this, we need a definition of "Q^*-chain" and "Q^*-cycle".

Q^*-chain: Let i be an index, $1 \leq i \leq m$. Then, by definition, Q^*-*chain*(i) is the set of all indices j, $1 \leq j \leq m$, such that it is possible to go from i to j by a chain of equalities of the type $(P_k^* = P_\ell^*)$ or $(Y'_\alpha = Y'_\beta)$.

We also denote by $\min_{Q^*}(i)$ the smallest index in Q^*-*chain*(i).

Remark: If we have $(P_j^* \neq P_i^*)$ and $(Y'_j \neq Y'_i)$ for all $j \neq i$, then $\min_{Q^*}(i) = i$.

Q^*-cycles: Let ℓ be an even integer, $\ell \geq 2$. We call *Q^*-ℓ-cycle* a set of ℓ equations of the form $\begin{cases} Y'_{i_1} = Y'_{i_2} \\ P^*_{i_2} = P^*_{i_3} \\ \vdots \\ Y'_{i_{\ell-1}} = Y'_{i_\ell} \\ P^*_{i_\ell} = P^*_{i_1} \end{cases}$, where i_1, i_2, ..., i_ℓ are ℓ pairwise distinct indices.

We also call *Q^*-cycle* any *Q^*-ℓ-cycle*.

If (X, Y, P, Q) are such that a *Q^*-cycle* exists, then Q' and Λ are not defined (*i.e.* $(X, Y, P, Q) \notin E$). On the other hand, if no such *Q^*-cycle* exists, then from all the implications of the following type:

$$\begin{cases} P^*_\alpha = P^*_\beta \Rightarrow X'_\alpha \oplus Q'_\alpha = X'_\beta \oplus Q'_\beta & (*) \\ Y'_\gamma = Y'_\delta \Rightarrow Q'_\gamma \oplus S_\gamma = Q'_\delta \oplus S_\delta & (**) \end{cases}$$

it is possible to write all the Q'_i, $1 \leq i \leq m$, from the values $Q'_{\min_{Q^*}(i)}$, Y', P^*, S and X'. Q' is thus defined as follows:

1. $\forall i$, $1 \leq i \leq m$, $Q'_{\min_{Q^*}(i)} = Q_{\min_{Q^*}(i)}$.
2. If $i \neq \min_{Q^*}(i)$, then Q'_i is uniquely defined from equations $(*)$ and $(**)$, and from the definition of $Q'_{\min_{Q^*}(i)}$ given in 1.

Definition of g: To simplify the notations, we write: $\forall i$, $1 \leq i \leq m$, $Q'_i = Q_{\min_{Q^*}(i)} \oplus g(i, S, X')$. (Caution: g and $\min_{Q^*}(i)$ depend on Y' and P^*, and more precisely on the indices with equalities in Y' and P^*.)

Definition of P'

We now define P' (this definition of P' is particularly important, especially case 2 below) by a combined effect of X' and Q', and by keeping the equalities in P^* (*i.e.* if $P^*_i = P^*_j$, then $P'_i = P'_j$). Before this, we need a definition of "totalchain".

Totalchain: Let i be an index, $1 \leq i \leq m$. Then, by definition, *totalchain*(i) is the set of all indices j, $1 \leq j \leq m$, such that it is possible to go from i to j by a chain of equalities of the type $(X'_\alpha = X'_\beta)$ or $(Q'_\gamma = Q'_\delta)$ or $(P^*_\varepsilon = P^*_\zeta)$.

For an integer i, $1 \leq i \leq m$, P'_i is now defined in 8 cases:

Case 1: There is no equality of the type $Q'_\alpha = Q'_\beta$, with α and β in *totalchain*(i) and $\alpha \neq \beta$. Then (by definition) $P'_i = P^*_i$.

Remark: If i is the only index of *totalchain*(i), then we are in a particular case of this first case, and then $P'_i = P^*_i = P_i$.

Case 2: There are exactly two elements i and j, $i < j$, in *totalchain*(i), and they are linked only by the equality $Q'_i = Q'_j$. (This second case is particularly sensible: it is the most difficult case for the proof). Then there are two subcases:

Subcase 1: $\forall k,\ 1 \leq k \leq m,\ k \neq j,\ P_i^* \oplus Y_i' \oplus Y_j' \neq P_k^*$.

$$\text{Then (by definition):} \quad \begin{cases} P_i' = P_i^* \\ P_j' = P_i^* \oplus Y_i' \oplus Y_j' \end{cases}$$

Subcase 2: $\exists k,\ 1 \leq k \leq m,\ k \neq j,\ P_i^* \oplus Y_i' \oplus Y_j' = P_k^*$.

$$\text{Then (by definition):} \quad \begin{cases} P_i' = P_j^* \oplus Y_i' \oplus Y_j' \\ P_j' = P_j^* \end{cases}$$

Remark: This case 2 was the most difficult case to handle to improve theorem 2 in order to obtain theorem 3. The problem comes from the fact that $Q_i' = Q_j'$ might create an equality $P_a' = P_b'$, and $P_a' = P_b'$ might create $Q_i' = Q_j'$, and to prove lemma 5 we must know very precisely what equalities created what. In the definition given in this case 2, the problem is solved by introducing subcase 1 and 2, *i.e.* roughly speaking by selecting the subcase that creates the less trouble.

Case 3: There are exactly four distinct elements i, j, k, ℓ, in $totalchain(i)$, and they are linked only by the following three equalitites: $(Q_i' = Q_k')$ and $(X_i' = X_j')$ and $(X_k' = X_\ell')$.

$$\text{Then (by definition), if } i < k\text{:} \quad \begin{cases} P_i' = P_i^* \\ P_j' = P_j^* \\ P_k' = P_i^* \oplus Y_i' \oplus Y_k' \\ P_\ell' = P_i^* \oplus Y_i' \oplus Y_k' \oplus R_k \oplus R_\ell \end{cases}$$

$$\text{and if } k < i\text{:} \quad \begin{cases} P_k' = P_k^* \\ P_\ell' = P_\ell^* \\ P_i' = P_k^* \oplus Y_i' \oplus Y_k' \\ P_j' = P_k^* \oplus Y_i' \oplus Y_k' \oplus R_i \oplus R_j. \end{cases}$$

Case 4: There are exactly three distinct elements i, j, k in $totalchain(i)$, and they are linked only by the following two equalities: $(X_i' = X_j')$ and $(Q_i' = Q_k')$.

$$\text{Then (by definition):} \quad \begin{cases} P_i' = P_i^* \\ P_j' = P_j^* \\ P_k' = P_i^* \oplus Y_i' \oplus Y_k'. \end{cases}$$

Case 5: There are exactly three distinct elements i, j and k in $totalchain(i)$, and they are linked only by equalities in Q' (*i.e.* $Q_i' = Q_j' = Q_k'$).

Let $\alpha = \inf(i, j, k)$.

$$\text{Then (by definition): } \forall \beta \in \{i, j, k\},\ P_\beta' = P_\alpha^* \oplus Y_\alpha' \oplus Y_\beta'.$$

Case 6: There are exactly three distinct elements i, j, k in $totalchain(i)$, and they are linked only by the following two equations: $(P_i^* = P_j^*)$ and $(Q_i' = Q_k')$.

$$\text{Then (by definition):} \quad \begin{cases} P_i' = P_i^* \\ P_j' = P_j^* (= P_i') \\ P_k' = P_i^* \oplus Y_i' \oplus Y_k'. \end{cases}$$

Case 7: There are exactly three distinct elements i, j, k in $totalchain(i)$, and they are linked only by the two following equations: $(Q'_i = Q'_j)$ and $(Y'_i = Y'_k)$.

$$\text{Then (by definition):} \quad \begin{cases} P'_i = P^*_i \\ P'_k = P^*_k \\ P'_j = P^*_i \oplus Y'_i \oplus Y'_j. \end{cases}$$

Case 8: There are exactly four distinct elements i, j, k, ℓ in $totalchain(i)$, and they are linked only by the three following equations: $(Q'_i = Q'_j)$ and $(Y'_i = Y'_k)$ and $(Y'_j = Y'_\ell)$.

$$\text{Then (by definition):} \quad \begin{cases} P'_i = P^*_i \\ P'_j = P^*_i \oplus Y'_i \oplus Y'_j \\ P'_k = P^*_k \\ P'_\ell = P^*_\ell. \end{cases}$$

If there exists an index i that lies in none of these eight cases, then Λ and P' are not defined (*i.e.* $(X, Y, P, Q) \notin E$).

4.5 Proof of the three lemmas

It is possible to prove that the function Λ defined above satisfies lemmas 4, 5 and 6 of section 4.2 (with a subset E of D). Due to the lack of space, we do not give details, but the complete proof is available from the author.

Part II: Homogeneous permutations, very strong pseudorandom permutations

5 Definitions

Let G be a permutation generator, such that G involves ℓ different pseudorandom functions of F_n to compute a permutation of B_{2n}. We denote by K the set of all ℓ-uples of functions $(f_1, ..., f_\ell)$ of F_n (*i.e.* $K = F_n^\ell$). Thus G associates to each $k \in K$ a permutation $G(k)$ of B_{2n}. K can be seen as the set of the keys of G, and $k \in K$ as a secret key.

Let α_1, ..., α_m be m distinct elements of I_{2n}, and let β_1, ..., β_m be also m distinct elements of I_{2n}. We denote by $H(\alpha_1, ..., \alpha_m, \beta_1, ..., \beta_m)$ the number of keys k of K such that:

$$\forall i,\ 1 \leq i \leq m,\ G(k)(\alpha_i) = \beta_i.$$

Definition 7. *We say that G is a "homogeneous" permutation generator if there exist a function $\varepsilon(m, n) : \mathbf{N}^2 \to \mathbf{R}$ such that, for any integer m:*

1. *For all α_1, ..., α_m being m distinct elements of I_{2n}, and for all β_1, ..., β_m being m distinct elements of I_{2n}, we have:*

$$\left| H(\alpha_1, ..., \alpha_m, \beta_1, ..., \beta_m) - \frac{|K|}{2^{2nm}} \right| \leq \varepsilon(m,n) \frac{|K|}{2^{2nm}}.$$

2. *For any polynomial $P(n)$ and any $\alpha > 0$, an integer n_0 exists such that:*

$$\forall n \geq n_0,\ \forall m \leq P(n),\ \varepsilon(m,n) \leq \alpha.$$

Remark: This notion of "homogeneous" permutations is a very natural notion: roughly speaking, a permutation generator is homogeneous when for all set of m cleartext/ciphertext pairs, there are always about the same number of possible keys that send all the cleartexts on the ciphertexts.

Definition 8. *We say that G is a "very strong" permutation generator if – with the same notations as above – the function $\varepsilon(m,n)$ satisfies condition 2, and the following condition 1' (instead of condition 1):*

1'. *For all α_1, ..., α_m being m distinct elements of I_{2n}, and for all β_1, ..., β_m being m distinct elements of I_{2n}, we have:*

$$H(\alpha_1, ..., \alpha_m, \beta_1, ..., \beta_m) \geq \frac{|K|}{2^{2nm}} (1 - \varepsilon(m,n)).$$

Theorem 9. *If G is a "homogeneous permutation generator", then G is a "very strong permutation generator".*

Theorem 10. *If G is a "very strong permutation generator", then G is a "strong permutation generator".*

Proof: Theorem 9 is an obvious consequence of the definitions. Theorem 10 corresponds to the technique of proof we used in part I. (This way of proving strong pseudorandomness was first explicitely used in [6].)

As a result, for permutation generators, we have:

$$Homogeneous \Rightarrow Very\ Strong \Rightarrow Strong \Rightarrow Pseudorandom.$$

Interpretations:
In order to distinguish (with a non-negligible probability) permutations generated by a homogeneous permutation generator, from truly random permutations of B_{2n}, an enemy must know a large number of cleartext/ciphertext pairs. (More precisely, this number must increase faster than any polynomial in n, **whatever** the cleartext/ciphertext pairs may be.)

Remark 1: Related (but not equivalent) notions can be found in [11] ("multipermutations") and in [5].

Remark 2: In some very special cases, this property of "homogeneity" may be useful and "strong peusorandomness" is not enough. For example, let us assume that the enemy has a spy inside the encryption team. Let us also assume that the aim of the enemy is to distinguish the encryption algorithm from a truly random permutation, and that his spy has access to the whole database of cleartext/ciphertext pairs, but can only send very few such pairs to help distinguishing. In such a case, "homogeneity" may be a more natural property than strong pseudorandomness. However, we introduced the concepts of "homogeneity" and "very strong pseudorandomness" because they are very natural in the proofs, and not with applications in mind.

6 Examples

6.1 Ψ^4 is not homogeneous

Example 1 (with $m = 2$):
As shown in [7] p. 314 (or in [1] p. 309), if $\Psi^4[L_1, R_1] = [S_1, T_1]$ and $\Psi^4[L_2, R_2] = [S_2, T_2]$, and $R_1 = R_2$, $L_1 \neq L_2$, then the probability that $S_1 \oplus S_2 = L_1 \oplus L_2$ is about twice what it would be with a truly random permutation of B_{2n} (instead of Ψ^4). In [7] (and [1]), this result was used to show that the security bound given by Luby and Rackoff for Ψ^4 in a chosen-cleartext attack is tight (the attack requires $\simeq \sqrt{2^n}$ messages to ensure $S_i \oplus S_j = L_i \oplus L_j$).

Here, we use this result to show that Ψ^4 is not homogeneous, and the non-homogeneity property appears with only two (very special) messages.

Remark: However, Ψ^4 is a very strong permutation generator (and for Ψ^4, we can take $\varepsilon(m, n) = \frac{m^2}{2^n}$). (As mentioned above, the proof of strong pseudorandomness of Ψ^4 given in [6] is also a proof of very strong pseudorandomness.)

Example 2 (with $m = 4$):
Let $R_1 = R_3$, $R_2 = R_4 = R_1 \oplus \alpha$, $S_1 = S_2$, $S_3 = S_4 = S_1 \oplus \alpha$, $L_1 = L_2$, $L_3 = L_4 = L_1 \oplus \alpha$, $T_1 = T_3$, $T_2 = T_4 = T_1 \oplus \alpha$.

Then the value H for Ψ^4 with these R, L, S, T is at least about $\frac{|F_n|^4}{2^{6n}}$ (instead of about $\frac{|F_n|^4}{2^{8n}}$ as expected if it was homogeneous). The proof of a similar property will be done in details for Ψ^6 below.

6.2 Ψ^5 is not homogeneous

If $\Psi^5[L_1, R_1] = [S_1, T_1]$ and $\Psi^5[L_2, R_2] = [S_2, T_2]$, and if $R_1 = R_2$ and $L_1 \neq L_2$, then the probability that $S_1 = S_2$ and $L_1 \oplus L_2 = T_1 \oplus T_2$ is about twice what it would be with a truly random permutation of B_{2n} (instead of Ψ^5). Therefore Ψ^5 is not homogeneous, and the non-homogeneity property appears with only two (very special) messages.

Remark: However, since here we have two equations and two indices ($S_i = S_j$ and $L_i \oplus L_j = T_i \oplus T_j$), this non-homogeneity property would require about $m = 2^n$ messages in a chosen-cleartext attack (instead of the $\sqrt{2^n}$ messages above for Ψ^4).

6.3 Ψ^6 is not homogeneous

Example 1 (with $m = 4$):
Let $\Psi^6[L_i, R_i] = [S_i, T_i]$ for $i = 1, 2, 3, 4$. Then if $L_1 = L_2$, $L_3 = L_4$, $R_1 = R_3$ and $R_2 = R_4$, it is possible to prove that the probability that $S_1 = S_2$, $S_3 = S_4$, $L_1 \oplus L_3 = S_1 \oplus S_3$ and $T_1 \oplus T_2 = T_3 \oplus T_4 = R_1 \oplus R_2$ is at least about twice what it would be with a truly random permutation of B_{2n} (instead of Ψ^6). The proof can be done as explained in example 2 below. Therefore, Ψ^6 is not homogeneous.

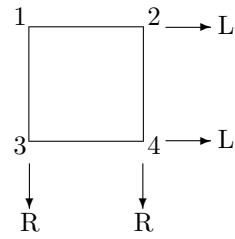
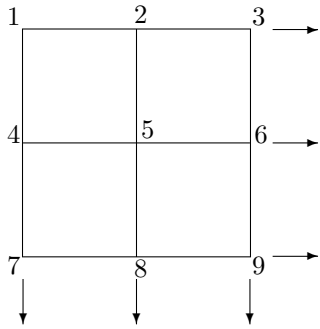


Figure 2: Modelisation of the equations $L_1 = L_2$, $L_3 = L_4$, $R_1 = R_3$ and $R_2 = R_4$.

Example 2 (with $m = 9$):



$$\oplus = \begin{cases} 0 & \text{for } S,\ L,\ (X,\ Q) \\ \alpha \text{ or } \beta \text{ or } \alpha \oplus \beta & \text{for } R,\ T,\ (Y,\ P) \end{cases}$$

($\oplus$ of 2 elements on the same line)

$$\oplus \text{ of 2 elements on the same column} = \begin{cases} 0 & \text{for } R,\ T,\ (Y,\ P) \\ \alpha' \text{ or } \beta' \text{ or } \alpha' \oplus \beta' & \text{for } S,\ L,\ (X,\ Q) \end{cases}$$

Figure 3: Modelisation of the equations in S, L, R, T (and in the X, Y, P, Q that we will consider).

Let $\Psi^6[L_i, R_i] = [S_i, T_i]$ for $1 \leq i \leq 9$. Let $\alpha \neq 0$ and $\beta \neq 0$ be two distinct values of I_n. Similarly, let $\alpha' \neq 0$ and $\beta' \neq 0$ be two distinct values of I_n. We

study the values of H when

$$\begin{cases} L_1 = L_2 = L_3 \\ L_4 = L_5 = L_6 = L_1 \oplus \alpha' \\ L_7 = L_8 = L_9 = L_1 \oplus \beta' \\ R_1 = R_4 = R_7 \\ R_2 = R_5 = R_8 = R_1 \oplus \alpha \\ R_3 = R_6 = R_9 = R_1 \oplus \beta \end{cases} \text{ and } \begin{cases} S_1 = S_2 = S_3 \\ S_4 = S_5 = S_6 = S_1 \oplus \alpha' \\ S_7 = S_8 = S_9 = S_1 \oplus \beta' \\ T_1 = T_4 = T_7 \\ T_2 = T_5 = T_8 = T_1 \oplus \alpha \\ T_3 = T_6 = T_9 = T_1 \oplus \beta. \end{cases}$$

(All these relations are represented in figure 3).

Then – as we will see below – for such L, R, S, T values, the value of H is at least $\frac{|F_n|^6}{2^{14n}}$, instead of $\frac{|F_n|^6}{2^{18n}}$ as expected if it was homogeneous Therefore, Ψ^6 is not homogeneous.

Proof: We consider (X, Y, P, Q) values such that:

$$\begin{cases} X_1 = X_2 = X_3 \\ X_4 = X_5 = X_6 = X_1 \oplus \alpha' \\ X_7 = X_8 = X_9 = X_1 \oplus \beta' \\ Y_1 = Y_4 = Y_7 \\ Y_2 = Y_5 = Y_8 = Y_1 \oplus \alpha \\ Y_3 = Y_6 = Y_9 = Y_1 \oplus \beta \end{cases} \text{ and } \begin{cases} Q_1 = Q_2 = Q_3 \\ Q_4 = Q_5 = Q_6 = Q_1 \oplus \alpha' \\ Q_7 = Q_8 = Q_9 = Q_1 \oplus \beta' \\ P_1 = P_4 = P_7 \\ P_2 = P_5 = P_8 = P_1 \oplus \alpha \\ P_3 = P_6 = P_9 = P_1 \oplus \beta. \end{cases}$$

(All these relations are also represented in figure 3).

All the L_i, R_i, S_i, T_i, X_i, Y_i, Q_i, P_i, $1 \leq i \leq 9$, can be written from L_1, R_1, S_1, T_1, X_1, Y_1, Q_1, P_1.

Moreover, whatever the values are for L_1, R_1, S_1, T_1, X_1, Y_1, Q_1 and P_1, it is easy to verify that all the conditions (C) are satisfied (these conditions were explicitly written in section 4.1 for Ψ^6).

For example, $R_1 = R_4 \Rightarrow X_1 \oplus L_1 = X_4 \oplus L_4$, since $X_1 \oplus X_4 = \alpha' = L_1 \oplus L_4$.

Similarly, $Q_7 = Q_9 \Rightarrow P_7 \oplus Y_7 = P_9 \oplus Y_9$, since $P_7 \oplus P_9 = \beta = Y_7 \oplus Y_9$.

Therefore, from the exact value of H (given in section 4.1), and by considering only such (X, Y, P, Q), we have:

$$H \geq 2^{4n} \cdot \frac{|F_n|^6}{2^{54n}} \cdot 2^{n(6+6+6+6+6+6)} = \frac{|F_n|^6}{2^{14n}},$$

as claimed (instead of $H \simeq \frac{|F_n|^6}{2^{18n}}$ if Ψ^6 was homogeneous).

6.4 $\forall k \in \mathbf{N}^*$, Ψ^k is not homogeneous

For simplicity, we assume that k is even (the proof is very similar when k is odd). Let $k = 2\lambda$. Let $\Psi^k[L_i, R_i] = [S_i, T_i]$ for $1 \leq i \leq m$. We essentially generalize to Ψ^k the construction given in example 2 for Ψ^6.

The exact value of H is:

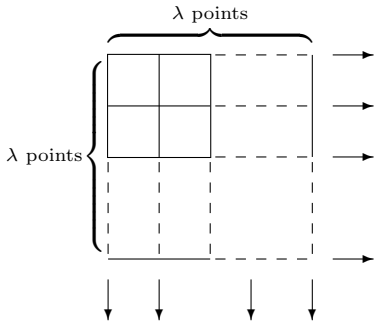
$$H = \sum_{(X^{(1)},\ldots,X^{(k-2)}) \text{ satisfying } (C)} \frac{|F_n|^k}{2^{knm}} \cdot 2^{n(r+s+x^{(1)}+\ldots+x^{(k-2)})},$$

where the $X^{(1)}$, ..., $X^{(k-2)}$ variables are the intermediate round variables, and where (C) denotes the conditions on the equalities (*i.e.* $R_i = R_j \Rightarrow X_i^{(1)} \oplus L_i = X_j^{(1)} \oplus L_j$, etc). The proof of this formula is not difficult and is given in [8], p. 134.

We take $m = \lambda^2 (= \frac{k^2}{4})$.

Let α_1, ..., $\alpha_{\lambda-1}$ be $\lambda - 1$ pairwise distinct and non-zero values of I_n. Let α'_1, ..., $\alpha'_{\lambda-1}$ be also $\lambda - 1$ pairwise distinct and non-zero values of I_n.

We study the value H when L_i, R_i, S_i, T_i, $1 \leq i \leq m$, satisfy the equalities modelised in figure 4. (For simplicity, we do not write these equalities explicitly).



$$\oplus = \begin{cases} 0 & \text{for } S,\ L,\ X^{(1)},\ ...,\ X^{(k-3)} \\ \alpha_i \oplus \alpha_j & \text{for } R,\ T,\ X^{(2)},\ ...,\ X^{(k-2)} \end{cases}$$

($\oplus$ of 2 elements on the same line)

$$\oplus \text{ of 2 elements on the same column} = \begin{cases} 0 & \text{for } R,\ T,\ X^{(2)},\ ...,\ X^{(k-2)} \\ \alpha'_i \oplus \alpha'_j & \text{for } S,\ L,\ X^{(1)},\ ...,\ X^{(k-3)} \end{cases}$$

Figure 4: Modelisation of the equations in S, L, R, T (and in the $X^{(1)}$, ..., $X^{(k-2)}$ that we will consider).

In the exact formula given above for H, we study the corresponding terms for values of $X^{(1)}$, ..., $X^{(k-2)}$ that satisfy the equalities represented in figure 4. We find

$$H \geq 2^{(k-2)n} \cdot \frac{|F_n|^k}{2^{knm}} \cdot 2^{nk\lambda(\lambda-1)},$$

so that, with $m = \lambda^2 = \frac{k^2}{4}$,

$$H \geq 2^{(k-2)n} \cdot \frac{|F_n|^k}{2^{2mn}}$$

(instead of $\frac{|F_n|^k}{2^{2nm}}$ if Ψ^k was homogeneous). Therefore, Ψ^k is not homogeneous, as claimed.

In conclusion:

$$\Psi^k \textit{ is very strong pseudorandom} \Leftrightarrow k \geq 4.$$

$$\Psi^k \textit{ is never homogeneous} \text{ (this was a surprise for us).}$$

Remark 1: The fact that Ψ^k is never homogeneous may explain why the proofs about the quality of pseudorandomness of the Ψ^k construction (such as theorem 3 of section 3) are so difficult.

Remark 2: In section 6.4, in order to give an explicit construction with a non homogeneous property, we have taken $m = \frac{k^2}{4} = \mathcal{O}(k^2)$, where k is the number of rounds of the L-R construction, so m increases when k increases. It is possible to prove that this increase was a necessity: when m is fixed, then all the values of H are converging to the same value when k tends to infinity. (This property can be proved with "Markov chain" theory for example).

7 Open problems

	Pseudorandom	Strong pseudo-random	Very strong pseudorandom	Homogeneous
Ψ	No	No	No	No
Ψ^2	No	No	No	No
Ψ^3	$= \mathcal{O}(\frac{m^2}{2^n})$	No	No	No
Ψ^4	$= \mathcal{O}(\frac{m^2}{2^n})$	$= \mathcal{O}(\frac{m^2}{2^n})$	$= \mathcal{O}(\frac{m^2}{2^n})$	No
Ψ^5	$\leq \mathcal{O}(\frac{m^3}{2^{2n}})$	$\leq \mathcal{O}(\frac{m^2}{2^n})$	$\leq \mathcal{O}(\frac{m^2}{2^n})$	No
Ψ^k, $k \geq 6$	$\leq \mathcal{O}(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}})$	$\leq \mathcal{O}(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}})$	$\leq \mathcal{O}(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}})$	No

Figure 5: Known results about the qualities of the Ψ^k pseudorandom permutations.

In figure 5, we represented the known results about the qualities of the L-R constructions with k rounds. For example, we see in this figure that Ψ^3 is not strong pseudorandom (this is written "No"), but that it is pseudorandom with an advantage of $\mathcal{O}(\frac{m^2}{2^n})$ for the best chosen-cleartext attack.

We also see that Ψ^5 is very strong pseudorandom, with an advantage of at most $\mathcal{O}(\frac{m^3}{2^{2n}})$ in a chosen-cleartext attack, and of at most $\mathcal{O}(\frac{m^2}{2^n})$ in a chosen-ciphertext and chosen-cleartext attack. "At most" means that we do not know if these $\mathcal{O}(\frac{m^3}{2^{2n}})$ and $\mathcal{O}(\frac{m^2}{2^n})$ bounds are reached or not: it is an open problem.

Similar open problems are shown in figure 5, when the "$\leq$" symbol appears.

It was conjectured in 1991 that, for Ψ^6 or Ψ^7, the advantage is negligible as long as m is negligible compared to 2^n. This is still unproven, as well as the following property:

When $k \to +\infty$, m must be $\Omega(2^n)$ to obtain a non-negligible advantage.

Another open problem that we mentioned is the following:

Is it possible to design homogeneous permutation generators ?

8 Conclusion

In order to improve the proved security bounds of pseudorandom permutations or pseudorandom functions, various authors have suggested new designs for the

permutation generators ([1], [3], [4], [10]). This comes from the fact that proofs are much easier to obtain in these modified schemes than in the original L-R construction.

However, in [1] and [4], the functions with improved security bounds are no longer bijections, and in [3] and [10], the design of the permutations if sensibly less simple, compared to the L-R construction. Should we conclude that these new constructions really have better security properties than the L-R construction ? Should we therefore develop new, fast, and secure encryption schemes based on these new constructions ? Or is it only a "technical problem", and is the L-R construction in fact as secure as these constructions, but with more difficult proofs ? This question is not completely solved yet. However, we have seen in this paper that the security properties of the L-R construction with six (or more) rounds are in fact better than what was proved before about them.

Nevertheless, we have defined two new natural notions about the quality of strong pseudorandom permutations: the concept of "very strong pseudorandomness" and the concept of "homogeneous permutations". We have seen that no L-R construction gives homogeneous permutations. This result may be surprising, since it shows that – whatever the number of rounds of the L-R construction may be – there are still some "non-random places" in the resulting permutations (however, after a few rounds, the enemy is not able to choose the cleartexts or ciphertexts of his attack in order to be in one of these places: the scheme is pseudorandom).

We have finally given a few still open questions about Luby-Rackoff-like analysis of Feistel schemes.

References

1. W. Aiello, R. Venkatesan, *Foiling birthday attacks in length-doubling transformations*, EUROCRYPT'96, Springer-Verlag, pp. 307-320.
2. M. Luby, C. Rackoff, *How to construct pseudorandom permutations from pseudorandom functions*, SIAM Journal on Computing, vol. 17, n. 2, pp. 373-386, April 1988.
3. M. Naor, O. Reingold, *On the Construction of Pseudo-Random Permutations: Luby-Rackoff revisited*, Electronic Colloquium on Computational Complexity (ECCC), Report TR 97-005. Preliminary version in: Proc. 29th Ann. ACM Symp. on Theory of Computing, 1997, pp. 189-199. To appear in the Journal of Cryptology.
4. U. Maurer, *A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators*, EUROCRYPT'92, Springer-Verlag, pp. 239-255.
5. U. Maurer, J.Massey, *Local randomness in pseudorandom sequences*, Journal of Cryptology, vol. 4, pp. 135-149, 1991.
6. J. Patarin, *Pseudorandom Permutations based on the DES Scheme*, EUROCODE'90, LNCS 514, Springer-Verlag, pp. 193-204.
7. J. Patarin, *New results on pseudorandom permutation generators based on the DES scheme*, CRYPTO'91, Springer-Verlag, pp. 301-312.
8. J. Patarin, *Étude des Générateurs de Permutations Pseudo-aléatoires basés sur le schéma du DES*, Ph.D. Thesis, Université Paris VI, November 1991.

9. J. Patarin, *Improved security bounds for pseudorandom permutations*, 4th ACM Conference on Computer and Communications Security, April 1-4, 1997, pp. 142-150.
10. J. Pieprzyk, *How to construct pseudorandom permutations from single pseudorandom functions*, EUROCRYPT'90, Springer-Verlag, pp. 140-150.
11. S. Vaudenay, *La Sécurité des Primitives Cryptographiques*, Ph.D. Thesis, École Normale Supérieure, April 1995, section II.8: "Les multipermutations".