About Feistel Schemes with six (or more) Rounds

Jacques Patarin

– Extended Version –

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 $\mathcal{O}\big(\frac{m^2}{2^n}\big)$ (for 3 or 4 rounds) to at most $\mathcal{O}\big(\frac{m^4}{2^{3n}}+\frac{m^2}{2^{2n}}\big)$. (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.

Note: This paper is the extended version of the paper with the same title published at FSE'98.

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 scheme (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 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 $\mathcal{O}(\frac{m^2}{2^n})$ for 3 or 4 rounds of a L-R construction, to at most $\mathcal{O}(\frac{m^3}{2^{2n}})$ 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 $\mathcal{O}(\frac{m^4}{2^{3n}}+\frac{m^2}{2^{2n}})$. 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:

$$\Psi(f_1)[L,R] = [S,T] \Leftrightarrow \begin{cases} S = R \\ \text{and} \\ T = L \oplus f_1(R). \end{cases}$$

- 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 3.1 (M. Luby and C. Rackoff, [2]) *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 (against chosen cleartext attacks) is guaranteed until $m = \mathcal{O}(2^{\frac{n}{2}})$.

Remark: It was shown in [7] that this security bound is tight: there is a way to distinguish Ψ^3 from a random permutation with about $\sqrt{2^n}$ chosen messages (chosen cleartext).

In [2], M. Luby and C. Rackoff also mentioned that it was possible to construct a strong pseudorandom permutation generator from a pseudorandom function generator. ("Strong pseudorandom" is also called "super pseudorandom"). They did not published their proof, but in 1990, I published a proof of this result. The result is based on the following theorem:

Theorem 3.2 (M. Luby and C. Rackoff, a proof is given in [6]) *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 are four independent functions randomly chosen in F_n, and $F = \Psi^4(f_1, f_2, f_3, f_4)$. Let P_1^{**} be the probability that $\phi(F) = 1$ when F is a permutation randomly chosen in B_{2n}. Then:

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

i.e. the security (against chosen cleartext and chosen ciphertext attacks) is guaranteed until $m = \mathcal{O}(2^{n/2})$.

Remark: It was shown in [7] that this security bound is tight: there is a way to distinguish Ψ^4 from a random permutation with about $\sqrt{2^n}$ chosen messages (chosen cleartext or chosen ciphertext).

In [9], we proved the following theorem:

Theorem 3.3 (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:*

$$|P_1 - P_1^{**}| \leq \frac{\frac{9}{2}m^3}{2^{2n}},$$

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 (J. Patarin, [7]): *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 3.4 (J. Patarin, in the present conference FSE'98) *Using the same notations as in theorem 3.2:*

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

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

To prove this theorem 3.4, we first prove this "H result":

"H 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 "H result": The proof of the "H result" is given in the appendix.

Proof of theorem 3.4: The proof of theorem 3.4 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 3.4 – 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 7, no general majoration of H exists near the value $\frac{|F_n|^6}{2^{2nm}}$.

4 Beyond $\mathcal{O}(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}})$

4.1 The problem

The next step in the direction of my conjecture of [7] would be to have a proof in $\mathcal{O}(\frac{m^5}{2^{4n}} + \frac{m^2}{2^{2n}})$ instead of $\mathcal{O}(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}})$. Then, we will have to handle the fact that three exceptional equations in X, P, Q or Y can occur between four given indices, and this creates problems in the proof. Typically, when we define Λ, from $P_1 = P_2$ we might want to modify a value Q_i^* or Q_j^*, but Q_i^* and Q_j^* might both create exceptional equations. So the way to improve our proof is not obvious: it is not clear yet if the proof can be improved in $\mathcal{O}(\frac{m^5}{2^{4n}} + \frac{m^2}{2^{2n}})$ or not. However, we will below give some hints that may lead to an improved result.

4.2 First example of possible improvement: with a new Λ.

New definition of Λ

In an extended definition of Λ (to improve the theorem) we can think about two strategies:

1. Now no equalities in P will create an equality in Q, and no equalities in Q will create an equality in P.
2. Or if we assume that no previously used equalities will be lost, but if we accept that an equality in Q (or Q^*, Q') can create an equality in P (or P^*, P'), we can maybe proceed like this.

The X', Y' and P^* are defined as before.

The values Q' defined before will now be denoted by Q^*.

The values P' are defined as before.

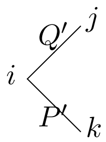
Finally, the new values Q' will be defined such that if $P'_i = P'_j$ and $i < j$ and $P^*_i \neq P^*_j$, and $\forall \alpha < i$, $P'_i \neq P'_\alpha$, $Q'_j = Q'_i \oplus X'_i \oplus X'_j$. (We do not give a complete definition of Λ since in this section we just want to show an idea of possible improvement).

We have: $R \to X'$, $S \to Y'$, $X' \to P^*$, $(P^*, Y') \to Q^*$, $(Q^*, X') \to P'$ and $P' \to Q'$, where "$A \to B$" denotes the fact that the values B are defined from the values A.

Now, the new $lastDchain(i)$ will be defined as 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 in X', Q^*, P' or Y'.

Here again, one of the key parts of the proof will be to prove that from a given $(P'_i, P'_j, P'_k, Q'_i, Q'_j, Q'_k)$, there are at most 2^{tn} possible values $(P_i, P_j, P_k, Q_i, Q_j, Q_k)$ such that Λ transforms the Q_i values into Q'_i values and the P_i values into P'_i values, and where t is the number of equalities in P' and Q'.

Example



$k < i < j$

Let assume that i, j, k are three indices, $k < i < j$, such that $(Q'_i = Q'_j)$ and $(P'_i = P'_k)$ are the only two equalities in X', Y', P', Q', linked with i, j and k.

How many possible values do we have for $(P_k, P_i, P_j, Q_k, Q_i, Q_j)$?

Case 1: We had $P^*_i = P^*_k$. So this created $Q'_i = Q_i \oplus X'_i \oplus X'_k$, but we had: $Q_i \oplus X'_i \oplus X'_k = Q_j$ (so it created $Q'_i = Q'_j$). Then $Q'_i = Q'_j$ created $P'_j = P'_i \oplus Y'_j \oplus Y'_i$.

This gives at most $1 \cdot 1 \cdot (2^n - \mu + 1) \cdot 1 \cdot 2^n \cdot 1 = 2^{2n} - \mu \cdot 2^n + 2^n$ possibilities for $(P_k, P_i, P_j, Q_k, Q_i, Q_j)$, where μ is the number of values P^*_λ, $\lambda \neq j$.

Case 2: We had $P^*_i \neq P^*_k$. So to create $P'_i = P'_k$, since $i < j$, we must have $Q^*_i = Q^*_j$ (so $Q_i = Q_j$), and $\exists \lambda$, $1 \leq \lambda \leq m$, $\lambda \neq j$, $P^*_i \oplus Y'_i \oplus Y'_j = P^*_\lambda$.

Then $\begin{cases} P'_i = P^*_j \oplus Y'_i \oplus Y'_j & \text{and this value was } P^*_k \\ P'_j = P^*_j \end{cases}$

Then Q^*_k has been modified in Q_k.

This gives at most $1 \cdot \mu \cdot 1 \cdot 2^n \cdot 1 \cdot 1 = \mu 2^n$ possibilities for $(P_k, P_i, P_j, Q_k, Q_i, Q_j)$.

So, by combining the two cases, we see that we have at most $2^{2n}(1 + \frac{1}{2^n})$ possibilities.

This kind of tricks can probably be generalized in order to have a proof in $\mathcal{O}(\frac{m^5}{2^{4n}} + \frac{m^2}{2^{2n}})$. Moreover, it may be possible to further generalize the proof in order to obtain a proof in $\mathcal{O}(\frac{m^{k+1}}{2^{kn}} + \frac{m^2}{2^{2n}})$ for all k. However, we will have to write a lot of technical details before being sure if these generalizations work or not.

4.3 Second example of possible improvement: the "framework and $H \geq$" technique.

We will call a "framework" any set $\mathcal{F}$ of equalities, such that for each equality of $\mathcal{F}$ there are two integers i and j, $\imath \neq j$, $1 \leq i \leq m$, $1 \leq j \leq m$, such that this equality is either $X_i = X_j$ or $Y_i = Y_j$, or $P_i = P_j$, or $Q_i = Q_j$.

Let $H_{\mathcal{F}} = \sum_{\substack{(X,Y,P,Q) \\ \text{satisfying } (C) \text{ and } \mathcal{F}}} 2^{n(x+y+p+q+r+s)}$.

Let E be a subset of the set of all (X, Y, P, Q).

Let $J_{\mathcal{F}\cap E}$ = the number of $(X, Y, P, Q) \in E$ satisfying $\mathcal{F}$.

If for all $k \in \mathbb{N}^*$ (or for $k \geq 4$) we can define a set E such that:

1. $|E| \;\geq\; 2^{4nm}(1 - o(\frac{m^{k+1}}{2^{nk}}))$
2. $\forall \mathcal{F},\;\; H_{\mathcal{F}} \;\geq\; J_{\mathcal{F}\cap E}(1 - o(\frac{m^{k+1}}{2^{nk}}))$

then we will improve the results of Ψ^6.

Proof: We know (cf. [9] p. 145 or [8] p.134) that the exact value of H is:

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

Therefore

$$H = \sum_{\text{all frameworks } \mathcal{F}} H_{\mathcal{F}} \frac{|F_n|^6}{2^{6mn}}.$$

Therefore from 2.

$$H \geq \sum_{\text{all frameworks } \mathcal{F}} J_{\mathcal{F}\cap E} \left(1 - o(\frac{m^{k+1}}{2^{nk}})\right) \frac{|F_n|^6}{2^{6mn}}.$$

Thus

$$H \geq \left(1 - o(\frac{m^{k+1}}{2^{nk}})\right) \sum_{\text{all frameworks } \mathcal{F}} (\text{Number of } (X,Y,P,Q) \text{ that satisfy } \mathcal{F}) \frac{|F_n|^6}{2^{6mn}}.$$

And

$$H \geq \left(1 - o(\frac{m^{k+1}}{2^{nk}})\right) \cdot |E| \cdot \frac{|F_n|^6}{2^{6mn}}.$$

Finally using 1. we obtain the desired result:

$$H \geq \frac{|F_n|^6}{2^{6mn}} \left(1 - o(\frac{m^{k+1}}{2^{nk}})\right)^2.$$

The proof technique will consist in finding such $\mathcal{E}$ for "most" of the inputs/outputs, and then by adding one or two rounds at the beginning and one or two rounds at the end by showing that we will obtain a general result.

This strategy of proof seems to be more simple and efficient than the strategy with a function Λ that we have used in this paper. So I will study this new strategy in future works.

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 1: 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 definition might look a bit complex but in fact 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 2: 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:

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

Remark: Roughly speaking, a permutation generator is "very strong" when for all set of m cleartext/ciphertext pairs, the number of possible keys (that send all the cleartexts on the ciphertexts) is always **at least** about the average number.

Theorem 5.1 *If G is a "homogeneous permutation generator", then G is a "very strong permutation generator".*

Theorem 5.2 *If G is a "very strong permutation generator", then G is a "strong permutation generator".*

Proof: Theorem 5.1 is an obvious consequence of the definitions. Theorem 5.2 corresponds to the technique of proof we used in part I. (This way of proving strong pseudorandomness was first explicitly 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.)

Remarks:

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

2. In some very special cases, this property of "homogeneity" may be useful and "strong pseudorandomness" 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. 309 (or in [1] p. 314), 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 $i = 1, 2, 3, 4$.

If $R_1 = R_3$, $R_2 = R_4 \neq R_1$, $S_1 = S_2$, $S_3 = S_4 \neq S_1$, $L_1 \oplus L_3 = L_2 \oplus L_4 = S_1 \oplus S_3 \neq 0$ and $T_1 \oplus T_2 = T_3 \oplus T_4 = R_1 \oplus R_2 \neq 0$, then we will see that H is at least about $2 \cdot \frac{|F_n|^6}{2^{8n}}$, instead of $\frac{|F_n|^6}{2^{8n}}$ as expected if it was homogenous. Therefore, Ψ^6 is not homogenous.

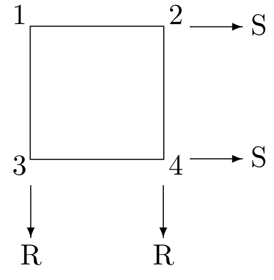


Figure 2: A representation of the equations $S_1 = S_2$, $S_3 = S_4$, $R_1 = R_3$ and $R_2 = R_4$.

Proof: We know (see [9] p.145 or [8] p.134) that the exact value of H is:

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

with (C) being the following set of conditions:

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

and with m being the number of independent equations $R_i = R_j$, $i \ne j$, s is the number of independent equations $S_i = S_j$, $i \ne j$, etc.. up to q being the number of independent equations $Q_i = Q_j$, $i \ne j$.

We will consider two special sets of values for (X, Y, P, Q).

First possible set.

Let X_1, Y_1, Q_1, P_1 have any value (thus we have 2^{4n} possible values here), and let $X_1 = X_2$, $X_3 = X_4 = X_1 \oplus L_1 \oplus L_3$, $Y_1 = Y_3$, $Y_2 = Y_4 = Y_1 \oplus T_1 \oplus T_2$, $Q_1 = Q_2$, $Q_3 = Q_4 = Q_1 \oplus S_1 \oplus S_3$, $P_1 \oplus P_3$ and $P_2 \oplus P_4 = P_1 \oplus R_1 \oplus R_2$.

It is easy to see that for these values all the conditions (C) are satisfied:

$$\begin{array}{llll} R_1 = R_3 & \Rightarrow & X_1 \oplus L_1 = X_3 \oplus L_3 & \text{(by definition of } X_3) \\ R_1 = R_3 & \Rightarrow & X_1 \oplus L_1 = X_3 \oplus L_3 & \text{(by definition of } X_3) \\ R_2 = R_4 & \Rightarrow & X_2 \oplus L_2 = X_4 \oplus L_4 & \text{(since } L_2 \oplus L_4 = L_1 \oplus L_3) \\ S_1 = S_2 & \Rightarrow & Y_1 \oplus T_1 = Y_2 \oplus T_2 & \text{(by definition of } Y_2) \\ S_3 = S_4 & \Rightarrow & Y_3 \oplus T_3 = Y_4 \oplus T_4 & \text{(since } T_1 \oplus T_2 = T_3 \oplus T_4) \\ X_1 = X_2 & \Rightarrow & P_1 \oplus R_1 = P_2 \oplus R_2 & \text{(by definition of } P_2) \\ X_3 = X_4 & \Rightarrow & P_3 \oplus R_3 = P_4 \oplus R_4 & \text{(since } R_1 \oplus R_2 = R_3 \oplus R_4) \\ Y_1 = Y_3 & \Rightarrow & Q_1 \oplus S_1 = Q_3 \oplus S_3 & \text{(by definition of } Q_3) \\ Y_2 = Y_4 & \Rightarrow & Q_2 \oplus S_2 = Q_4 \oplus S_4 & \text{(since } S_2 \oplus S_4 = S_1 \oplus S_3) \\ P_1 = P_3 & \Rightarrow & X_1 \oplus Q_1 = X_3 \oplus Q_3 & \text{(since } L_1 \oplus L_3 = S_1 \oplus S_3) \\ P_2 = P_4 & \Rightarrow & X_2 \oplus Q_2 = X_4 \oplus Q_4 & \text{(since } L_1 \oplus L3_= S_1 \oplus S_3) \\ Q_1 = Q_2 & \Rightarrow & P_1 \oplus Y_1 = P_2 \oplus Y_2 & \text{(since } R_1 \oplus R_2 = T_1 \oplus T_2) \\ Q_3 = Q_4 & \Rightarrow & P_3 \oplus Y_3 = P_4 \oplus Y_4 & \text{(since } R_1 \oplus R_2 = T_1 \oplus T_2). \end{array}$$

Only from these X, Y, P, Q we see that:

$$H \ge 2^{4n} \cdot \frac{|F_n|^6}{2^{24n}} \cdot 2^{n(2+2+2+2+2+2)} = \frac{|F_n|^6}{2^{8n}}.$$

Note. Here we have $r = 2$ equalities in R and $s = 2$ equalities in S, and we have found variables X, Y, P, Q that satisfy all the equations (C) by introducing only $\mu = 4$ equations with non-sero constants (i.e. $X_3 = X_1 \oplus L_1 \oplus L_3$, $Y_2 = Y_1 \oplus T_1 \oplus T_2$, $Q_3 = Q_1 \oplus S_1 \oplus S_3$ and $P_2 = P_1 \oplus R_1 \oplus R_2$). Since all the equations of (C) are satisfied with $\mu \leq r + s$ it will give a proof of non homogeneity.

Second possible set.

There is also the "usual" set, i.e. the values X, Y, P, Q that we have used in the proof that Ψ^6 is super-pseudo-random (these values introduce no equalities in the X, Y, P, Q variables, so this second set is entirely disjoint from the first set).

Here we have:

- X_1 has 2^n possibilities,
- X_2 has $(2^n - 2)$ possibilities (because $X_2 \neq X_1$ and $X_2 \neq X_1 \oplus L_1 \oplus L_3$ and since here $L_1 \oplus L_3 = L_2 \oplus L_4$ these two inequalities will imply $X_2 \oplus L_2 \oplus L_4 \neq X_1$ and $X_2 \oplus L_2 \oplus L_4 \neq X_1 \oplus L_1 \oplus L_3$),
- $X_3 = X_1 \oplus L_1 \oplus L_3$, $X_4 = X_2 \oplus L_2 \oplus L_4$,
- Y_1 has 2^n possibilities, $Y_2 = Y_1 \oplus T_1 \oplus T_2$,
- Y_3 has $(2^n - 2)$ possibilities (because $Y_3 \neq Y_1$ and $Y_3 \neq Y_1 \oplus T_1 \oplus T_2$ and since here we have $T_1 \oplus T_2 = T_3 \oplus T_4$ these two inequalities will imply $Y_3 \oplus T_3 \oplus T_4 \neq Y_1$ and $Y_3 \oplus T_3 \oplus T_4 \neq Y_1 \oplus T_1 \oplus T_2$).
- P_1 has 2^n possibilities, and P_2 has $2^n - 1$ possibilities (because $P_2 \neq P_1$). Similarly P_3 has $2^n - 2$ possibilities (because $P_3 \neq P_1$ and $P_3 \neq P_2$) and P_4 has $2^n - 3$ possibilities (because $P_4 \neq P_1$, and $P_4 \neq P_2$ and $P_4 \neq P_3$),
- For the same reason Q_1, Q_2, Q_3 and Q_4 have respectively $2^n, 2^n - 1, 2^n - 2$ and $2^n - 3$ possibilities.

Only from these X, Y, P, Q we see that

$$H \geq 2^{4n} \cdot (2^n - 1)^2 \cdot (2^n - 2)^4 \cdot (2^n - 3)^2 \cdot \frac{|F_n|^6}{2^{24n}} \cdot 2^{n(2+2)} \approx \frac{|F_n|^6}{2^{8n}}.$$

Therefore by combining the first and the second set, we have $H \geq$ about $2\frac{|F_n|^6}{2^{8n}}$, as claimed (instead of $H \approx \frac{|F_n|^6}{2^{8n}}$ if Ψ^6 was homogenous).

Remark 1.

Since $L_4 = L_1 \oplus L_2 \oplus L_3$ and $R_4 = R_2$, the index 4 is fixed the indices $1, 2$ and 3 are fixed.

In fact we have here 3 indices $1, 2$ and 3 and at least 4 equations on these indices that we cannot impose with a cleartext/ciphertext attack: $T_1 \oplus T_2 = R_1 \oplus R_2$, $L_1 \oplus L_3 = S_1 \oplus S_3$, $S_{4(1,2,3)} = S_3$, $T_{4(1,2,3)} = T_1 \oplus T_2 \oplus T_3$.

Thus, this example shows that Ψ^6 is not homogenous, but it does not give a cryptographic attack when $m < 2^n$.

Remark 2.

It is sometimes interesting to see if there is an attack when $2^n < m \ll 2^{2n}$, when this attack requires $\ll 2^{2n}$ computations.
However here when the index 1 is fixed (we have m possibilities for it), the index 2 is also "in a way" fixed, since $S_2 = S_1$ and $T_2 \oplus R_2 = T_1 \oplus R_1$ (because on average when 1 is fixed there will be about only one index 2 such that these two equations are satisfied). Similarly, when the index 1 is fixed, the index 3 is "in a way" fixed, since $R_3 = R_1$ and $S_3 \oplus L_3 = S_1 \oplus L_1$. So in fact, when 1 is fixed, 2, 3 and 4 are fixed. But there are still two exceptional equations: $S_{4(1)} = S_3$ and $T_{4(1)} = T_1 \oplus T_{2(1)} \oplus T_{3(1)}$, and when $m \ll 2^{2n}$ the probability that these equations occur is negligible. Therefore this example 1 does not give an attack even when $2^n < m \ll 2^{2n}$.

Example 2 (with $m = 9$):

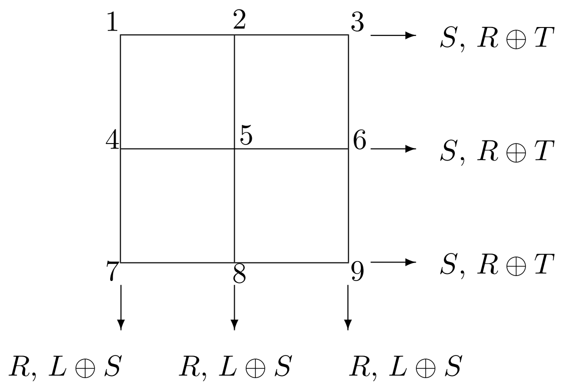


Figure 3: A representation of the 24 equations in S, L, R, T

Let $\Psi^6[L_i, R_i] = [S_i, T_i]$ for $1 \le i \le 9$. We study the values of H when

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

All these relations are represented on Figure 3. We also assume that $R_1 \neq R_2$, $R_1 \neq R_3$, $R_2 \neq R_3$, $S_1 \neq S_4$, $S_1 \neq S_7$ and $S_4 \neq S_7$.

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: Let $\alpha = R_1 \oplus R_2$, $\beta = R_1 \oplus R_3$, $\alpha' = S_1 \oplus S_4$ and $\beta' = S_1 \oplus S_7$ (by definition we have $\alpha \neq 0$, $\beta \neq 0$, $\alpha' \neq 0$ and $\beta' \neq 0$) We consider (X, Y, P, Q) values such that:

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

It is easy to verify that for there values all the conditions (C) are satisfied (these conditions were explicitly written for Ψ^6 in the section 6.3 above, Example 1):

$$\begin{array}{lcll}
R_1 = R_4 & \Rightarrow & X_1 \oplus L_1 = X_4 \oplus L_4 & (\text{because } \alpha' = L_1 \oplus L_4 = S_1 \oplus S_4) \\
R_1 = R_7 & \Rightarrow & X_1 \oplus L_1 = X_7 \oplus L_7 & (\text{because } \beta' = S_1 \oplus S_7 = L_1 \oplus L_7) \\
R_2 = R_5 & \Rightarrow & X_2 \oplus L_2 = X_5 \oplus L_5 & (\text{because } \alpha' = S_1 \oplus S_4 = S_2 \oplus S_5 = L_2 \oplus L_5) \\
R_2 = R_8 & \Rightarrow & X_2 \oplus L_2 = X_8 \oplus L_8 & (\text{because } \beta' = S_1 \oplus S_7 = S_2 \oplus S_8 = L_2 \oplus L_8) \\
R_3 = R_6 & \Rightarrow & X_3 \oplus L_3 = X_6 \oplus L_6 & (\text{because } \alpha' = S_1 \oplus S_4 = S_3 \oplus S_6 = L_3 \oplus L_6) \\
R_3 = R_9 & \Rightarrow & X_3 \oplus L_3 = X_9 \oplus L_9 & (\text{because } \beta' = S_1 \oplus S_7 = S_3 \oplus S_9 = L_3 \oplus L_9) \\
S_1 = S_2 & \Rightarrow & Y_1 \oplus T_1 = Y_2 \oplus T_2 & (\text{because } \alpha = R_1 \oplus R_2 = T_1 \oplus T_2) \\
S_1 = S_3 & \Rightarrow & Y_1 \oplus T_1 = Y_3 \oplus T_3 & (\text{because } \beta = R_1 \oplus R_3 = T_1 \oplus T_3) \\
S_4 = S_5 & \Rightarrow & Y_4 \oplus T_4 = Y_5 \oplus T_5 & (\text{because } \alpha = R_1 \oplus R_2 = R_4 \oplus R_5 = T_4 \oplus T_5) \\
S_4 = S_6 & \Rightarrow & Y_4 \oplus T_4 = Y_6 \oplus T_6 & (\text{because } \beta = R_1 \oplus R_3 = R_4 \oplus R_6 = T_4 \oplus T_6) \\
S_7 = S_8 & \Rightarrow & Y_7 \oplus T_7 = Y_8 \oplus T_8 & (\text{because } \alpha = R_1 \oplus R_2 = R_7 \oplus R_8 = T_7 \oplus T_8) \\
S_7 = S_9 & \Rightarrow & Y_7 \oplus T_7 = Y_9 \oplus T_9 & (\text{because } \beta = R_1 \oplus R_3 = R_7 \oplus R_9 = T_7 \oplus T_9) \\
X_1 = X_2 & \Rightarrow & P_1 \oplus R_1 = P_2 \oplus R_2 & (\text{because } \alpha = R_1 \oplus R_2) \\
X_1 = X_3 & \Rightarrow & P_1 \oplus R_1 = P_3 \oplus R_3 & (\text{because } \beta = R_1 \oplus R_3) \\
X_4 = X_5 & \Rightarrow & P_4 \oplus R_4 = P_5 \oplus R_5 & (\text{because } \alpha = R_1 \oplus R_2 = R_4 \oplus R_5) \\
X_4 = X_6 & \Rightarrow & P_4 \oplus R_4 = P_6 \oplus R_6 & (\text{because } \beta = R_1 \oplus R_3 = R_4 \oplus R_6) \\
X_7 = X_8 & \Rightarrow & P_7 \oplus R_7 = P_8 \oplus R_8 & (\text{because } \alpha = R_1 \oplus R_2 = R_7 \oplus R_8) \\
X_7 = X_9 & \Rightarrow & P_7 \oplus R_7 = P_9 \oplus R_9 & (\text{because } \beta = R_1 \oplus R_3 = R_7 \oplus R_9) \\
Y_1 = Y_4 & \Rightarrow & Q_1 \oplus S_1 = Q_4 \oplus S_4 & (\text{because } \alpha' = S_1 \oplus S_4) \\
Y_1 = Y_7 & \Rightarrow & Q_1 \oplus S_1 = Q_7 \oplus S_7 & (\text{because } \beta' = S_1 \oplus S_7) \\
Y_2 = Y_5 & \Rightarrow & Q_2 \oplus S_2 = Q_5 \oplus S_5 & (\text{because } \alpha' = S_1 \oplus S_4 = S_2 \oplus S_5) \\
Y_2 = Y_8 & \Rightarrow & Q_2 \oplus S_2 = Q_8 \oplus S_8 & (\text{because } \beta' = S_1 \oplus S_7 = S_2 \oplus S_8) \\
Y_3 = Y_6 & \Rightarrow & Q_3 \oplus S_3 = Q_6 \oplus S_6 & (\text{because } \alpha' = S_1 \oplus S_4 = S_3 \oplus S_6) \\
Y_3 = Y_9 & \Rightarrow & Q_3 \oplus S_3 = Q_9 \oplus S_9 & (\text{because } \beta' = S_1 \oplus S_7 = S_3 \oplus S_9) \\
Q_1 = Q_2 & \Rightarrow & P_1 \oplus Y_1 = P_2 \oplus Y_2 & (\text{because } P_1 \oplus P_2 = \alpha = Y_1 \oplus Y_2) \\
Q_1 = Q_3 & \Rightarrow & P_1 \oplus Y_1 = P_3 \oplus Y_3 & (\text{because } P_1 \oplus P_3 = \beta = Y_1 \oplus Y_3) \\
Q_4 = Q_5 & \Rightarrow & P_4 \oplus Y_4 = P_5 \oplus Y_5 & (\text{because } P_4 \oplus P_5 = \alpha = Y_4 \oplus Y_5) \\
Q_4 = Q_6 & \Rightarrow & P_4 \oplus Y_4 = P_6 \oplus Y_6 & (\text{because } P_4 \oplus P_6 = \beta = Y_4 \oplus Y_6) \\
Q_7 = Q_8 & \Rightarrow & P_7 \oplus Y_7 = P_8 \oplus Y_8 & (\text{because } P_7 \oplus P_8 = \alpha = Y_7 \oplus Y_8) \\
Q_7 = Q_9 & \Rightarrow & P_7 \oplus Y_7 = P_9 \oplus Y_9 & (\text{because } P_7 \oplus P_9 = \beta = Y_7 \oplus Y_9) \\
P_1 = P_4 & \Rightarrow & X_1 \oplus Q_1 = X_4 \oplus Q_4 & (\text{because } Q_1 \oplus Q_4 = \alpha' = X_1 \oplus X_4) \\
P_1 = P_7 & \Rightarrow & X_1 \oplus Q_1 = X_7 \oplus Q_7 & (\text{because } Q_1 \oplus Q_7 = \beta' = X_1 \oplus X_7) \\
P_2 = P_5 & \Rightarrow & X_2 \oplus Q_2 = X_5 \oplus Q_5 & (\text{because } Q_2 \oplus Q_5 = \alpha' = X_2 \oplus X_5) \\
P_2 = P_8 & \Rightarrow & X_2 \oplus Q_2 = X_8 \oplus Q_8 & (\text{because } Q_2 \oplus Q_8 = \beta' = X_2 \oplus X_8) \\
P_3 = P_6 & \Rightarrow & X_3 \oplus Q_3 = X_6 \oplus Q_6 & (\text{because } Q_3 \oplus Q_6 = \alpha' = X_3 \oplus X_6) \\
P_3 = P_9 & \Rightarrow & X_3 \oplus Q_3 = X_9 \oplus Q_9 & (\text{because } Q_3 \oplus Q_9 = \beta' = X_3 \oplus X_9)
\end{array}$$

Therefore, from the exact value of H (given in section 6.3), 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).

Note: Here we have $6 + 6 = 12$ equalities $R_i = R_j$ or $S_i = S_k$, and only 8 equalities with nonzero constants have been used to satisfy all the (C) conditions. So the deviation from the average is about $2^{(12-8)n}$.

Remark:
This attack shows that Ψ^6 is not homogenous as a generator of permutations. However for a specific permutation generated as a Ψ^6 this attack will not generally exist, since it requires more than 18 equations in only 9 indices and there are only 2^{2n} possible inputs.

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

Example 1 (with $m = (k/2)^2$)
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 $m = \lambda^2 (= \frac{k^2}{4})$.

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

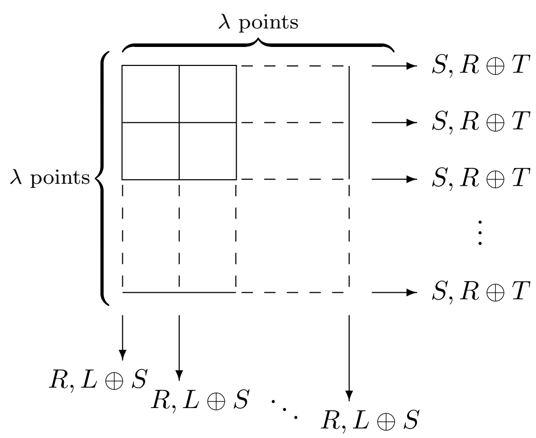


Figure 4: Modelling the $4 \cdot \lambda(\lambda-1)$ equations in S, L, R, T.

We will consider values $X^{(1)}, \dots, X^{(k-2)}$ such that:

1. In Figure 4 the $\oplus$ of two elements on the same line $= 0$ for $X^{(1)}, X^{(3)}, \dots, X^{(k-3)}$.
2. In Figure 4 the $\oplus$ of two elements on the same column $= 0$ for $X^{(2)}, X^{(4)}, \dots, X^{(k-2)}$.
3. We have the $(k-2)\cdot(\lambda-1)$ equalities with non zero constant needed to satisfy all the (C) conditions.

Then, in the exact formula given above for H, for these $X^{(1)}, \dots, X^{(k-2)}$ we have: $r = \lambda(\lambda-1)$, $s = \lambda(\lambda-1)$, $X^{(1)} = \lambda(\lambda-1)$, ... , $X^{(k-2)} = \lambda(\lambda-1)$. And we have $2^{(k-2)n}$ possibilities for $X^{(1)}, \dots, X^{(k-2)}$. Then:

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

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.

Note: Here we have $2\lambda(\lambda-1)$ equalities $R_i = R_j$ or $S_i = S_k$, and only $(k-2)(\lambda-1)$ equalities with nonzero constants have been used to satisfy all the conditions (C). So the deviation from the average is about $2^{(k-2)n}$.

Example 2 (with $m = (k/2-1)^2$)
If we take $\lambda = \frac{k}{2} - 1$ (instead of $\lambda = \frac{k}{2}$), then we will have still $2\lambda(\lambda-1)$ equalities in $S_i = S_j$ or $R_i = R_j$, $i \neq j$, and only $(k-2)(\lambda-1)$ equalities with nonzero constants to satisfy all the conditions (C). Here the obtained value of H will be about twice the average value. (This attack needs less points: $(\frac{k}{2}-1)^2$ instead of $(\frac{k}{2})^2$, but the deviation from the average is less important).

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 3.4 of section 3) are so difficult.

Remark 2: Here, in order to give an explicit construction with a non homogeneous property, we have taken $m = \mathcal{O}(k^2)$, 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).

Remark 3: These attacks show that Ψ^k is not homogenous as a generator of permutations. However on a specific permutation generated as a Ψ^k this attack will not generally exist when $k \geq 7$ since there are only 2^{2n} inputs and the probability that on some of these inputs all the needed equations appear, is then negligible (when the permutation Ψ^k is fixed).

In conclusion:

Ψ^k *is very strong pseudorandom* $\Leftrightarrow k \geq 4$.

Ψ^k *is never homogeneous* (this was a surprise for me).

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, 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, 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, pp. 193-204.

[7] J. Patarin, *New results on pseudorandom permutation generators based on the DES scheme*, CRYPTO'91, Springer, 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, pp. 140-150.

[11] S. Vaudenay, *La Sécurité des Primitives Cryptographiques*, Ph.D. Thesis, École Normale Supérieure, April 1995, section II.8: "Les multipermutations".

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

I. 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:

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

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 $R_i = R_j$, $i \neq j$,
- 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 $P_i = P_j$, $i \neq j$,
- and q is the number of independent equations $Q_i = Q_j$, $i \neq j$.

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.

II. Plan of the proof

To prove the "basic result", we proceed as follows: we define two sets E and D, $E \subset D \subset I_n^4$, and a function $\Lambda : D \to I_n^4$ such that the three lemmas below are satisfied. (D is the subset of I_n^4 on which Λ is defined, and E is the subset of D where we will proof the three lemmas).

Lemma 1 $\forall (X, Y, P, Q) \in E$, $\Lambda(X, Y, P, Q)$ *satisfies all the equations (C).*

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

Lemma 2 (This lemma will be the "heart" of the proof.) $\forall (X', Y', P', Q') \in \Lambda(E)$, *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 3

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

Then the "basic result" is just a consequence of these three lemmas, as follows. As we said in section 6.3,

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

Thus, from lemma 1:

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

Therefore, from lemma 2:

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

i.e.

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

Finally, from lemma 3:

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

as claimed.

We will now below define Λ and prove lemma 1, lemma 2 and lemma 3.

III. 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 3.2 given in [6] (about 2 pages), then to read the proof of theorem 3.3 (this proof, about 7 pages, can be found in the extended version of [9], available from the author) and then to read the proof of theorem 3.4 that we will give below (in the present paper, about 20 pages), because our proof of lemma 1, 2 and 3 below is essentially an improvement of the previous proofs.

Remark 2: After the definition of Λ (*i.e.* of X', Y', P', Q'), the proof is essentially done in two parts. First, we will analyze what the equalities in X', Y', P', Q' give in terms of equalities in X, Y, P, Q and so what kind of equalities in X', Y', P', Q' can be considered with a negligible probability to occur. This gives what we will call the "simplification rules". (This part is essentially "technical"). Then, we will use these "simplification rules" to prove the three lemmas, and especially lemma 2, which is the real heart of the proof.

Lemma 2 can be seen as a sort of "moving objects" trick: we must define $(X', Y', P', Q') = \Lambda(X, Y, P, Q)$ for almost all (X, Y, P, Q) in a way such that, for a given (X', Y', P', Q'), there are not too much possible pre-images (X, Y, P, Q).

Remark 3: 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 between three or four given indices (because $\frac{m^3}{2^{2n}}$ can be large). However, the probability that *three* exceptional equations occur between four given indices i, j, k, ℓ is assumed to be negligible (because our aim is to have a proof in $\mathcal{O}(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}})$ here so $\frac{m^4}{2^{3n}}$ can be assumed to be small). (In Luby-Rackoff proof of theorem 3.1, the probability that *one* exceptional equation occurs between the intermediate variables was negligible, but no more here. Similarly, in our previous proof of theorem 3.2, the probability that *two* exceptional equations occur between the intermediate variable was negligible, but no more here.)

Remark 4: At most *two* exceptional equations in X, P, Q or Y can occur between three or 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 $\frac{m^2}{2^n} = \frac{2^{1.4n}}{2^n} = 2^{0.4n}$.

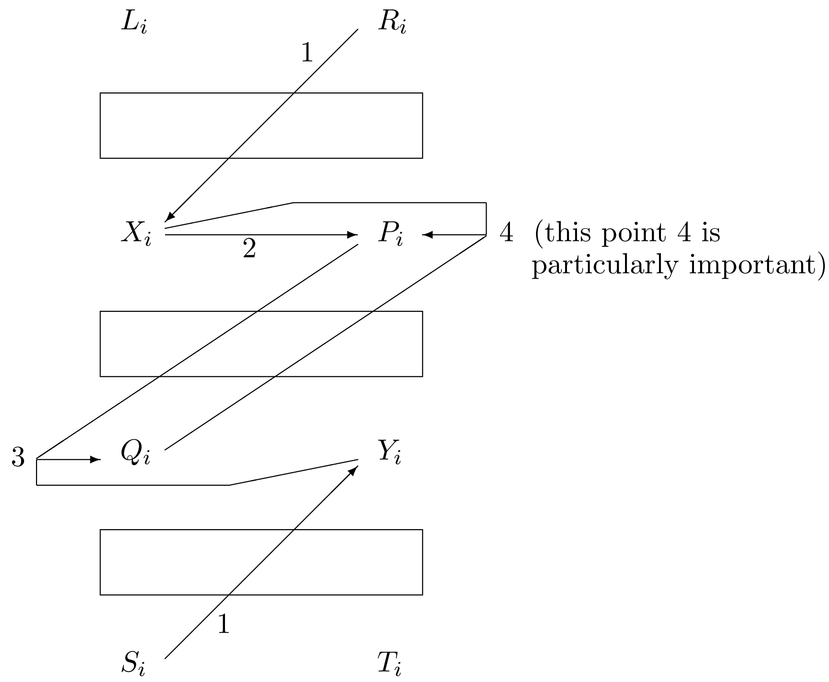


Figure 1: General view of the construction of Λ.

IV. 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 following type:

$$\begin{cases} Y'_{i_1} = Y'_{i_2} \\ P^*_{i_2} = P^*_{i_3} \\ \quad\vdots \\ Y'_{i_{\ell-1}} = Y'_{i_\ell} \\ P^*_{i_\ell} = P^*_{i_1} \end{cases}$$

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.* $(X, Y, P, Q) \notin D$). 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: $\forall i$, $1 \le i \le m$, $Q'_i = Q_{\min_{Q^*}(i)} \oplus g(i, S, X')$. (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 "lastDchain".

LastDchain: Let i be an index, $1 \le i \le m$. Then, by definition, $lastDchain(i)$ is the set of all indices j, $1 \le j \le m$, 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 $(P^*_\varepsilon = P^*_\zeta)$ or $(Y'_\eta = Y'_\theta)$.

Remark: The name $lastDchain(i)$ comes from the fact that P' is the last value to define before finishing the definition of Λ.

For an integer i, $1 \le i \le m$, 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 $lastDchain(i)$ and $\alpha \ne \beta$. Then (by definition) $P'_i = P^*_i$.

Remark: If i is the only index of $lastDchain(i)$, 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 $lastDchain(i)$, 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: $\forall k$, $1 \le k \le m$, $k \ne j$, $P^*_i \oplus Y'_i \oplus Y'_j \ne P^*_k$.

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

Subcase 2: $\exists k$, $1 \le k \le m$, $k \ne j$, $P^*_i \oplus Y'_i \oplus Y'_j = P^*_k$.

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

Remark 1: This case 2 was the most difficult case to handle to improve theorem 3.2 in order to obtain theorem 3.4. 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 2 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.

Remark 2: Most of the values (X, Y, P, Q) such that $\Lambda(X, Y, P, Q) = (X', Y', P', Q')$ with $(P'_i = P'_j)$ and $(Q'_i = Q'_k)$, $k < i < j$, should come from two equations in (X, Y, P, Q) (Because we want to have Lemma 2 in our proof).

Here, these two equations for "most" of the possible (X, Y, P, Q) have been chosen to be: $(P^*_i = P^*_j)$ and $(X'_i \oplus X'_j \oplus Q_i = Q_k)$. (Then $P^*_i = P^*_j$ will create $Q'_i = Q'_k$ and the, as we will decide in the Case 6, we will create $P'_k = P^*_i \oplus Y'_i \oplus Y'_k$).
Therefore most of the (X, Y, P, Q) such that $(P'_i = P'_j)$ and $Q'_i = Q'_k$ have been already chosen. In particular, most of the (X, Y, P, Q) such that $(Q_i = Q_k)$ and $(P_k \oplus Y'_i \oplus Y'_k = P_j)$ should <u>not</u> have a (P', Q') such that $(P'_i = P'_j$ and $(Q'_i = Q'_k)$.
This explains why, when $(Q_i = Q_k)$ and $P^*_k \oplus Y'_i \oplus Y'_k = P^*_j)$, we create a special subcase in the definition of Λ. 0r, to say it in another way, an equality in Q' should generally not create an equality in P'.

Case 3: There are exactly four distinct elements i, j, k, ℓ, in $lastDchain(i)$, and they are linked only by the following three equalities: $(Q'_i = Q'_k)$ and $(X'_i = X'_j)$ and $(X'_k = X'_\ell)$.

Then (by definition), if $i < k$: $\begin{cases} P'_i = P^*_i \\ P'_j = P^*_j \\ P'_k = P^*_i \oplus Y'_i \oplus Y'_k \\ P'_\ell = P^*_i \oplus Y'_i \oplus Y'_k \oplus R_k \oplus R_\ell \end{cases}$

and if $k < i$: $\begin{cases} P'_k = P^*_k \\ P'_\ell = P^*_\ell \\ P'_i = P^*_k \oplus Y'_i \oplus Y'_k \\ P'_j = P^*_k \oplus Y'_i \oplus Y'_k \oplus R_i \oplus R_j. \end{cases}$

Case 4: There are exactly three distinct elements i, j, k in $lastDchain(i)$, and they are linked only by the following two equalities: $(X'_i = X'_j)$ and $(Q'_i = Q'_k)$.

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

Case 5: There are exactly three distinct elements i, j and k in $lastDchain(i)$, 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 $lastDchain(i)$, and they are linked only by the following two equations: $(P^*_i = P^*_j)$ and $(Q'_i = Q'_k)$.

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

Case 7: There are exactly three distinct elements i, j, k in $lastDchain(i)$, 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 $lastDchain(i)$, 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.* $(X, Y, P, Q) \notin D$).

V. The simplification rules

In order to prove more easily lemmas 1, 2 and 3, we introduce more restrictions on the (X, Y, P, Q) that we consider, *i.e.* we will define E such that E will contain only values (X, Y, P, Q) for which the analysis is easier.

For this purpose, we now introduce what we call the "simplification rules". However, this must be done with caution: E must still be large enough to prove lemma 3. Roughly speaking, we can assume (by choosing E) that three independent exceptional equations in equations in X, P, Q or Y can never occur between four given indices. What about equations in X', Y', P^*, Q' or P' ? For some equations, we can assume (by choosing E) that they do not occur: this is the aim of the "simplification rules". However, for some special sets of three exceptional equations between four indices, we cannot assume that they cannot occur, and we will have to study them carefully.

Example: For example, if i, j, k, ℓ are four pairwise distinct indices, and if $R_i = R_k$, $R_j = R_\ell$, $L_i \oplus L_j \oplus L_k \oplus L_\ell = 0$ (so the index ℓ for example is fixed when i, j, k are given), then the probability that $\begin{cases} X'_i = X'_j \\ P^*_i = P^*_k \\ X'_k = X'_\ell \end{cases}$ might not be negligible, because this comes from only two equations over three indices in X, P (and <u>not</u> three equations over four indices).

Remark: Here a system of three equations (in X' or P^*) on four indices comes from a system of only two equations but over <u>only</u> three indices. This property (that a decrease in the number of equations is possible only with an at least similar decrease in the number of variables) can probably be generalized, and such a generalized property is probably useful for decreasing the $\mathcal{O}(\frac{m^4}{2^{3n}} + \frac{m^2}{2^{2n}})$ term in improved theorems.

Properties: *The following properties are always satisfied (proofs are easy). For all indices i and j such that $i \neq j$:*

$$(P1): \quad X'_i = X'_j \Leftrightarrow \begin{cases} X_{i_R} \oplus L_i \oplus L_{i_R} = X_{j_R} \oplus L_j \oplus L_{j_R} \\ i_R \neq j_R. \end{cases}$$

(Therefore $(R_i = R_j)$ and $(X'_i = X'_j)$ is impossible if $i \neq j$.)

$$(P2): \quad Y'_i = Y'_j \Leftrightarrow \begin{cases} Y_{i_S} \oplus T_i \oplus T_{i_S} = Y_{j_S} \oplus T_j \oplus T_{j_S} \\ i_S \neq j_S. \end{cases}$$

(Therefore $(S_i = S_j)$ and $(Y'_i = Y'_j)$ is impossible if $i \neq j$.)

$$(P3): \quad P^*_i = P^*_j \Leftrightarrow \begin{cases} P_{i_X} \oplus R_i \oplus R_{i_X} = P_{j_X} \oplus R_j \oplus R_{j_X} \\ i_X \neq j_X. \end{cases}$$

(Therefore $(P^*_i = P^*_j)$ and $(X'_i = X'_j)$ is impossible if $i \neq j$.)

$(P4):$ *There are no indices i, j, $i \neq j$, such that $(Q'_i = Q'_j)$ and $(Y'_i = Y'_j)$.*

$(P5):$ *There are no indices i, j, $i \neq j$, such that $(Q'_i = Q'_j)$ and $(P^*_i = P^*_j)$.*

$(P6):$ *There are no indices $i \neq j$, such that (P'_i and P'_j are defined) and $(P'_i = P'_j)$ and $(Q'_i = Q'_j)$.*

$(P7):$ *There are no indices $i \neq j$, such that (P'_i and P'_j are defined) and $(P'_i = P'_j)$ and $(X'_i = X'_j)$.*

Rules

We accept in E only values (X, Y, P, Q) satisfying all the following rules:

Rule 1: There are no indices i, j, k, ℓ, $i \neq j$, $i \neq k$, $k \neq \ell$, such that:

$$\begin{cases} X'_i = X'_j \\ P^*_i = P^*_k \\ Y'_\ell = Y'_k \end{cases} \text{or} \begin{cases} X'_i = X'_j \\ Y'_i = Y'_k \\ P^*_\ell = P^*_k \end{cases} \text{or} \begin{cases} X'_i = X'_\ell \\ Y'_i = Y'_k \\ P^*_i = P^*_j \\ i, j, k, \ell \text{ are pairwise distinct} \end{cases} \text{or} \begin{cases} X'_i = X'_k \\ Y'_i = Y'_j \\ P^*_k = P^*_\ell. \end{cases}$$

Theorem 8.1 *At most $\frac{4m^4}{2^{3n}} \cdot 2^{4mn}$ values (X, Y, P, Q) do not satisfy rule 1.*

(The proof is easy.)

Rule 2: There are no indices i and j, $i \neq j$, such that:

$$\begin{cases} X'_i = X'_j \\ Y'_i = Y'_j \end{cases} \text{or} \begin{cases} Y'_i = Y'_j \\ P^*_i = P^*_j \end{cases} \text{or} \begin{cases} X'_i = X'_j \\ Q'_i = Q'_j. \end{cases}$$

Theorem 8.2 *At most $\frac{3}{2} \cdot \frac{m(m-1)}{2^{2n}} \cdot 2^{4mn}$ values (X, Y, P, Q) do not satisfy rule 2.*

(Easy.)

Rule 3: There are no pairwise distinct indices i, j, k, ℓ such that:

$$(Y'_i = Y'_k) \text{ and } (P^*_k = P^*_\ell) \text{ and } (P^*_i = P^*_j).$$

Theorem 8.3 *At most* $\frac{m^4}{2\cdot 2^{3n}} \cdot 2^{4nm}$ *values* (X, Y, P, Q) *do not satisfy rule 3.*

(Easy.)

Theorem 8.4 *If* (X, Y, P, Q) *satisfies rules 1, 2 and 3, then it has no* Q^**-cycle.*

(Easy.)

Rule 4 (called the "Q' rule"): Let i and j be two indices, $i \neq j$. Then:

$$Q'_i = Q'_j \Leftrightarrow \begin{cases} Q_{\min_{Q^*}(i)} \oplus g(i, S, X') = Q_{\min_{Q^*}(j)} \oplus g(j, S, X') \\ \min_{Q^*}(i) \neq \min_{Q^*}(j). \end{cases}$$

Theorem 8.5 *At most* $(\frac{m^2}{2^{2n}} + \frac{m^3}{2^{3n}} + \frac{m^4}{2\cdot 2^{3n}}) \cdot 2^{4nm}$ *values* (X, Y, P, Q) *do not satisfy rule 4.*

Theorem 8.6 *If* (X, Y, P, Q) *satisfies the previous rules, then, if* i, j, k *are three different indices, we have:*

$$Q'_i = Q'_j = Q'_k \Leftrightarrow \begin{cases} Q_{\min_{Q^*}(i)} \oplus g(i, S, X') = Q_{\min_{Q^*}(j)} \oplus g(j, S, X') \\ \qquad = Q_{\min_{Q^*}(k)} \oplus g(k, S, X') \\ \min_{Q^*}(i),\ \min_{Q^*}(j) \textit{ and } \min_{Q^*}(k) \textit{ are pairwise distinct.} \end{cases}$$

Rule 5: There are no indices i, j, k, ℓ, $i \neq j$, $i \neq k$, $k \neq \ell$, such that:

$$\begin{cases} P^*_i = P^*_j \\ Q'_i = Q'_k \\ Y'_k = Y'_\ell \end{cases} \text{ or } \begin{cases} P^*_i = P^*_j \\ Y'_i = Y'_k \\ Q'_k = Q'_\ell \end{cases} \text{ or } \begin{cases} Y'_i = Y'_j \\ P^*_i = P^*_k \\ Q'_k = Q'_\ell. \end{cases}$$

Theorem 8.7 *At most* $\frac{4m^4}{2^{3n}} \cdot 2^{4nm}$ *values* (X, Y, P, Q) *do not satisfy rule 5.*

Rule 6: There are no indices i, j, k, ℓ, $i \neq j$, $i \neq k$, $k \neq \ell$, such that:

$$\begin{cases} P^*_i = P^*_j \\ Q'_i = Q'_j \\ X'_k = X'_\ell \end{cases} \text{ or } \begin{cases} P^*_i = P^*_j \\ X'_i = X'_k \\ Q'_k = Q'_\ell \end{cases} \text{ or } \begin{cases} X'_i = X'_j \\ P^*_i = P^*_k \\ Q'_k = Q'_\ell \end{cases} \text{ or } \begin{cases} X'_i = X'_j \\ Q'_i = Q'_k \\ P^*_i = P^*_\ell. \\ i, j, k \text{ are pairwise distinct.} \end{cases}$$

Theorem 8.8 *At most* $\frac{4m^4}{2^{3n}} \cdot 2^{4nm}$ *values* (X, Y, P, Q) *do not satisfy rule 6.*

Rule 7: There are no pairwise distinct indices i, j, k, ℓ such that:

$$\begin{cases} Q'_i = Q'_k \\ P^*_k = P^*_\ell \\ P^*_i = P^*_j. \end{cases}$$

Theorem 8.9 *At most* $\frac{m^4}{2\cdot 2^{3n}} \cdot 2^{4nm}$ *values* (X, Y, P, Q) *values satisfy the previous rules, but not rule 7.*

Rule 8 (called the "$2Q'$ rule"): If (X,Y,P,Q) satisfies the previous rules, and if i, j, k, ℓ are four pairwise distinct indices, then $\begin{cases} Q'_i = Q'_j \\ Q'_k = Q'_\ell \end{cases}$ if and only if one of the following three cases is satisfied:

$$(C1)\begin{cases} Q_{\min_{Q^*}(i)} \oplus g(i,S,X') = Q_{\min_{Q^*}(j)} \oplus g(j,S,X') \\ \min_{Q^*}(i) \neq \min_{Q^*}(j) \\ Q_{\min_{Q^*}(k)} \oplus g(k,S,X') = Q_{\min_{Q^*}(\ell)} \oplus g(\ell,S,X') \\ \min_{Q^*}(k) \neq \min_{Q^*}(\ell) \\ [(\min_{Q^*}(k) \neq \min_{Q^*}(i)) \text{ and } (\min_{Q^*}(k) \neq \min_{Q^*}(j))] \\ \qquad \text{or } [(\min_{Q^*}(\ell) \neq \min_{Q^*}(i)) \text{ and } (\min_{Q^*}(\ell) \neq \min_{Q^*}(j))]. \end{cases}$$

$$(C2)\begin{cases} S_i = S_j \\ S_k = S_\ell \\ T_i \oplus T_k \oplus T_j \oplus T_\ell = 0 \\ Y_{i_S} \oplus T_i \oplus T_{i_S} = Y_{k_S} \oplus T_k \oplus T_{k_S},\ i_S \neq k_S \\ Q_{\min_{Q^*}(i)} \oplus g(i,S,X') = Q_{\min_{Q^*}(j)} \oplus g(j,S,X') \\ \min_{Q^*}(i) \neq \min_{Q^*}(j). \end{cases}$$

$$(C3)\begin{cases} S_i = S_\ell \\ S_k = S_j \\ T_i \oplus T_k \oplus T_j \oplus T_\ell = 0 \\ Y_{i_S} \oplus T_i \oplus T_{i_S} = Y_{k_S} \oplus T_k \oplus T_{k_S},\ i_S \neq k_S \\ Q_{\min_{Q^*}(i)} \oplus g(i,S,X') = Q_{\min_{Q^*}(j)} \oplus g(j,S,X') \\ \min_{Q^*}(i) \neq \min_{Q^*}(j). \end{cases}$$

Theorem 8.10 *At most $\frac{m^4}{2\cdot 2^{3n}} \cdot 2^{4nm}$ values (X,Y,P,Q) do not satisfy rule 8.*

Rule 9: There are no four pairwise distinct indices i, j, k, ℓ such that:

$$\begin{cases} Q'_i = Q'_j \\ X'_j = X'_k = X'_\ell. \end{cases}$$

Theorem 8.11 *At most $\frac{m^4}{2\cdot 2^{3n}} \cdot 2^{4nm}$ values (X,Y,P,Q) satisfy the previous rules, but not rule 9.*

Rule 10: There are no four distinct indices i, j, k, ℓ such that:

$$\begin{cases} Q'_i = Q'_j \\ P^*_j = P^*_k = P^*_\ell. \end{cases}$$

Theorem 8.12 *At most $\frac{m^4}{2\cdot 2^{3n}} \cdot 2^{4nm}$ values (X,Y,P,Q) satisfy the previous rules, but not rule 10.*

Rule 11: There are no indices i, j, k, ℓ, $i \neq j$, $i \neq k$, $k \neq \ell$, such that:

$$\begin{cases} X'_i = X'_j \\ Q'_i = Q'_k \\ Y'_k = Y'_\ell \end{cases} \text{ or } \begin{cases} Q'_i = Q'_j \\ X'_i = X'_k \\ Y'_k = Y'_\ell \end{cases} \text{ or } \begin{cases} X'_i = X'_j \\ Y'_i = Y'_k \\ Q'_k = Q'_\ell \end{cases} \text{ or } \begin{cases} X'_i = X'_j \\ Q'_i = Q'_k \\ Y'_i = Y'_\ell. \\ i,j,k \text{ are pairwise distinct.} \end{cases}$$

Theorem 8.13 *At most $\frac{4m^4}{2^{3n}} \cdot 2^{4nm}$ values (X,Y,P,Q) do not satisfy rule 11.*

Rule 12: If i, j, k, ℓ are four pairwise distinct indices, and if $\begin{cases} Q'_i = Q'_k \\ X'_k = X'_\ell \\ X'_i = X'_j \end{cases}$, then we also have:

$$\begin{cases} R_i = R_k \\ R_\ell = R_j \\ L_i \oplus L_j \oplus L_k \oplus L_\ell = 0 \end{cases} \quad \text{or} \quad \begin{cases} R_i = R_\ell \\ R_j = R_k \\ L_i \oplus L_j \oplus L_k \oplus L_\ell = 0. \end{cases}$$

Theorem 8.14 *At most $\frac{m^4}{2 \cdot 2^{3n}} \cdot 2^{4nm}$ values (X, Y, P, Q) do not satisfy rule 12.*

Rule 13: There are no four pairwise distinct indices i, j, k, ℓ such that:

$$\begin{cases} Q'_i = Q'_j = Q'_k \\ Y'_k = Y'_\ell. \end{cases}$$

Theorem 8.15 *At most $\frac{m^4}{2 \cdot 2^{3n}} \cdot 2^{4nm}$ values (X, Y, P, Q) do not satisfy rule 13.*

VI. Proof of the three lemmas with two more rules (G1) and (G2)

For the proof of the three lemmas, we will introduce two more rules, denoted by (G1) and (G2). (These rules are put apart, because they involve P', so it look more time to prove them, since we will look all the different cases in the definition of P').

(G1): For all j_0, $1 \le j_0 \le m$, if $P'_{j_0} \neq P^*_{j_0}$, then:

$$\begin{cases} \forall \lambda_0 \neq j_0, \; P'_{j_0} \neq P^*_{\lambda_0} & \text{(G1a)} \\ \forall \lambda_0 \neq j_0, \; P'_{j_0} \neq P'_{\lambda_0} & \text{(G1b)} \end{cases}$$

Theorem 8.16 *At most $\frac{9m^4}{2^{3n}} \cdot 2^{4nm}$ values (X, Y, P, Q) satisfy the previous rules, but not rule (G1).*

(G2): For all defined (X', Y', P', Q'), there are at most $2^{n(x'+y'+p'+q')}$ possible values (X', Y', P, Q) (*i.e.* at most $2^{n(x'+y'+p'+q')}$ values (X', Y', P, Q) such that a (X, Y, P, Q) exists such that $\Lambda(X, Y, P, Q) = (X', Y', P', Q')$).

Theorem 8.17 *At most $(\frac{8m^4}{2^{3n}} + \frac{5m^2}{2^{2n}}) \cdot 2^{4nm}$ values (X, Y, P, Q) satisfy the previous rules, but not rule (G2).*

Theorem 8.18 *If (X, Y, P, Q) satisfies the previous rules, then it also satisfies lemma 1 and lemma 2. Moreover, with our definition of E, $|E|$ satisfies lemma 3.*

(This result is easy.)
Now we just have to prove (G1) and (G2) (this will be done below) and this will achieve the proof of the basic result.

Proof of (G1):

This part is not written yet.

Proof of (G2):

The proof of (G2) (*i.e.* of lemma 2) is the heart of the whole proof. This part is not written yet.