

Random Feistel Schemes: security in $m \ll 2^{3n/4}$ for ≥ 6 rounds

Jacques Patarin

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

Note: This paper is the extended version of the paper “About Feistel Schemes with Six (or more) Rounds” published at FSE’98, except that all the results about homogenous generator are now in an another specific paper (called “Homogenous Permutations. Random Feistel schemes are never homogenous”).

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 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]).

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, \dots, f_k be k functions of F_n . Then by definition:

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

(When f_1, \dots, 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:

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

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, \dots, f_6) of F_n^6 such that:

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

satisfies:

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

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 ??, 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.

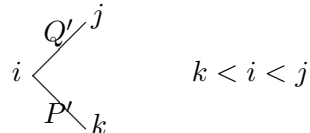
Finally, the new values Q' will be defined such that if $P'_i = P'_j$ and $i < j$ and $P_i^* \neq P_j^*$, and $\forall \alpha < i, P'_i \neq P'_\alpha, Q'_j = Q'_i \oplus X'_i \oplus X'_j$. (We do not give a complete definition of Λ since in this section we just want to show an idea of possible improvement).

We have: $R \rightarrow X', S \rightarrow Y', X' \rightarrow P^*, (P^*, Y') \rightarrow Q^*, (Q^*, X') \rightarrow P'$ and $P' \rightarrow Q'$, where “ $A \rightarrow B$ ” 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



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 , $i \neq j$, $1 \leq i \leq m$, $1 \leq j \leq m$, 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 $H_{\mathcal{F}} = \sum_{\substack{(X,Y,P,Q) \\ \text{satisfying (c) and } \mathcal{F}}} 2^{n(x+y+p+q+r+s)}$.

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.

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

Thus

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

And

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

Finally using 1. we obtain the desired result:

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

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.

5 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 is 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 has been completely answered only in 2004/2005 and is given in the paper “Security of Random Feistel Schemes with 5 or more Rounds”). 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.

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:

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

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 ?? 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 $\Lambda : D \rightarrow I_n^4$ 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

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

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

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

Thus, from lemma 1:

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

Therefore, from lemma 2:

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

i.e.

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

Finally, from lemma 3:

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

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 $\frac{m^2}{2^n} = \frac{2^{1.4n}}{2^n} = 2^{0.4n}$.

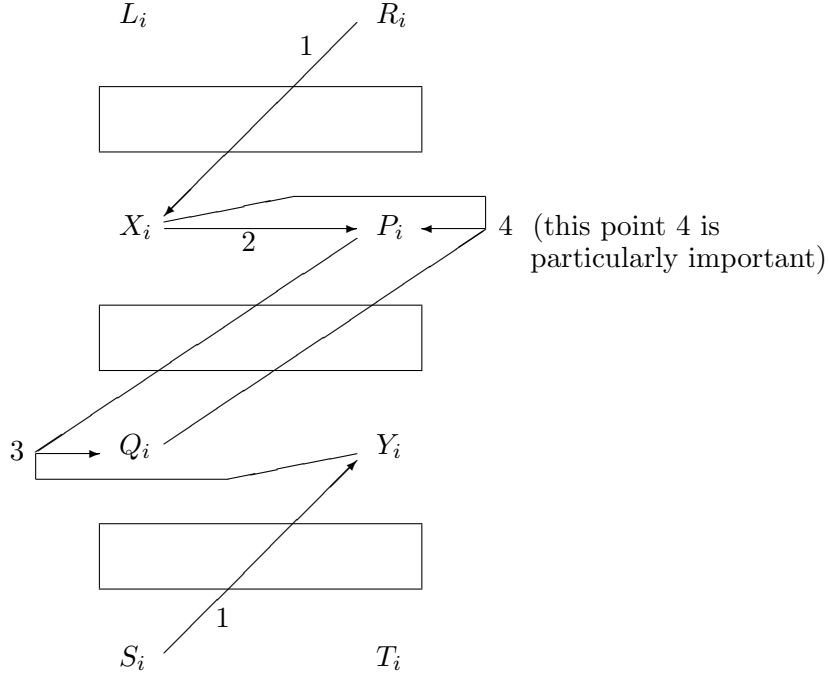


Figure 1: General view of the construction of Λ .

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 $X = (X_1, \dots, X_m)$ 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 $X' = (X'_1, \dots, X'_m)$ 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, $Y' = (Y'_1, \dots, Y'_m)$ 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 $P^* = (P_1^*, \dots, P_m^*)$ 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:

$$\left\{ \begin{array}{l} Y'_{i_1} = Y'_{i_2} \\ P_{i_2}^* = P_{i_3}^* \\ \vdots \\ Y'_{i_{\ell-1}} = Y'_{i_\ell} \\ P_{i_\ell}^* = P_{i_1}^* \end{array} \right.$$

where i_1, i_2, \dots, 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: $\forall i, 1 \leq i \leq m, Q'_i = Q_{\min_{Q^*}(i)} \oplus g(i, S, X')$. (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 “lastDchain”.

LastDchain: Let i be an index, $1 \leq i \leq m$. Then, by definition, $lastDchain(i)$ 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 $(P_\varepsilon^* = P_\zeta^*)$ 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 $i, 1 \leq i \leq m, P'_i$ is now defined in 8 cases:

Case 1: There is no equality of the type $Q'_\alpha = Q'_\beta$, with α and β in $lastDchain(i)$ and $\alpha \neq \beta$. 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: $\forall k, 1 \leq k \leq m, k \neq j, P_i^* \oplus Y'_i \oplus Y'_j \neq P_k^*$.

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

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

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

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 not 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 . Or, 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 $(X'_k = X'_\ell)$.

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

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

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 $(Q'_i = Q'_k)$.

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

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 $(Q'_i = Q'_k)$.

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

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

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

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

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

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 not 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 only 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 $i, j, k, \ell, i \neq j, i \neq k, k \neq \ell$, 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 5.1 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 5.2 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 5.3 At most $\frac{m^4}{2 \cdot 2^{3n}} \cdot 2^{4nm}$ values (X, Y, P, Q) do not satisfy rule 3.

(Easy.)

Theorem 5.4 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 5.5 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 5.6 If (X, Y, P, Q) satisfies the previous rules, then, if i, j, k are three different indices, we have:

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

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 5.7 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:

$$\begin{cases} P_i^* = P_j^* \\ Q'_i = Q'_j \\ X'_k = X'_\ell \end{cases} \text{ or } \begin{cases} P_i^* = P_j^* \\ X'_i = X'_k \\ Q'_k = Q'_\ell \end{cases} \text{ or } \begin{cases} X'_i = X'_j \\ P_i^* = P_k^* \\ Q'_k = Q'_\ell \end{cases} \text{ or } \begin{cases} X'_i = X'_j \\ Q'_i = Q'_k \\ P_i^* = P_\ell^* \end{cases}.$$

i, j, k are pairwise distinct.

Theorem 5.8 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 5.9 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:

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

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

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

Theorem 5.10 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 5.11 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 5.12 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 $i, j, k, \ell, i \neq j, i \neq k, k \neq \ell$, such that:

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

i, j, k are pairwise distinct.

Theorem 5.13 At most $\frac{4m^4}{2^3} \cdot 2^{4nm}$ 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 5.14 *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 5.15 *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 $j_0, 1 \leq j_0 \leq m$, 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 5.16 *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 5.17 *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 5.18 *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.