Luby-Rackoff: 7 Rounds are Enough for $2^{n(1-\varepsilon)}$ Security

Jacques Patarin, University of Versailles, France

Abstract

In [3] M. Luby and C. Rackoff have proved that 3-round random Feistel schemes are secure against all adaptative chosen plaintext attacks when the number of queries is $m \ll 2^{n/2}$. Moreover, 4-round random Feistel schemes are also secure against all adaptative chosen plaintext and chosen ciphertext attacks when $m \ll 2^{n/2}$. It was shown later that these bounds are tight for 3 and 4 rounds (see [9] or [1]).

In this paper our main results are that for every $\varepsilon > 0$, when $m \ll 2^{n(1-\varepsilon)}$:

- for 4 rounds or more, a random Feistel scheme is secure against known plaintext attacks (KPA).
- for 7 rounds or more it is secure against all adaptative chosen plaintext attacks (CPA).
- for 10 rounds or more it is secure against all adaptative chosen plaintext and chosen ciphertext attacks (CPCA).

These results achieve the optimal value of m, since it is always possible to distinguish a random Feistel cipher from a truly random permutation with $\mathcal{O}(2^n)$ queries, given sufficient computing power.

This paper solves an open problem of [1, 9] and [16]. It significantly improves the results of [13] that proves the security against only $2^{\frac{3n}{4}}$ queries for 6 rounds, and the results of [6] in which the $2^{n(1-\varepsilon)}$ security is only obtained when the number of rounds tends to infinity. The proof technique used in this paper is also of independent interest and can be applied to other schemes.

This paper is the extended version of the paper with the same title published at Crypto 2003.

1 Introduction

In this paper we study the security proofs for random Feistel ciphers with k rounds, $k \in \mathbb{N}$, which is also known as "Luby-Rackoff construction with k rounds" or simply "L-R construction with k rounds" (see Section 2 for precise definitions). By definition a random Feistel cipher with k rounds, is a Feistel cipher in which the round functions $f_1, \ldots, f_k$ are independently chosen as truly random functions.

In their famous paper [3], M. Luby and C. Rackoff have shown that in an adaptative plaintext attack (CPA) with m queries to the encryption oracle, the probability to distinguish the 3-round L-R construction from a truly random permutation of $2n$ bits $\rightarrow 2n$ bits, is always $\leq m^2/2^n$. Therefore 3-round L-R constructions are secure against all chosen plaintext attacks when m is very small compared with $2^{n/2}$ (i.e. $m \ll 2^{n/2}$).

Moreover, in all adaptative chosen plaintext and chosen ciphertext attack (CPCA), the probability to distinguish the 4-round L-R construction from a truly random permutation of $2n$ bits $\rightarrow 2n$ bits, is also $\leq m^2/2^n$ (This result was mentioned in [3] and a proof published in [8]). Therefore 4-round L-R constructions are secure against CPCA when $m \ll 2^{n/2}$.

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

These results, as well the results of the present paper, can be applied in two different ways:

1. Directly, using k truly random functions $f_1, \ldots, f_k$ (that requires significant storage). Then we obtain an unconditionally secure cipher, that is secure even against adversaries that are not limited in their computing power, however they have to be limited in the number of known (plaintext, ciphertext) pairs.

2. In a hybrid setting, in which instead of using k truly random functions $f_1, \ldots, f_k$, we use k pseudo-random functions. If no adversary with limited computing power can distinguish these functions from truly random functions by any existing test, a fortiori he cannot achieve worse security for the hybrid cipher, than for the ideal version with truly random functions, and all the security results will hold.

The L-R construction inspired a considerable amount of research, see [7] for a summary of existing works on this topic. One direction of research is to use less than 4 different pseudo-random functions, or to use less than 4 calls to these functions in one encryption, see [7, 11, 15, 16]. However in these papers the proven security is still $m \ll 2^{n/2}$. In [17], the authors proved that even if the adversary has block-box access to the middle two functions of a 4 round $L - R$ construction the security proof is maintained.
Another direction of research, also followed in the present paper, is to improve the security bound $m \ll 2^{n/2}$. Then one may try to prove the security bound obtained is tight. Thus in [9] and independently in[1], it is shown that for the Luby-Rackoff theorems for 3 and 4 rounds, the bound $m \ll 2^{n/2}$ is optimal. Generic attacks exist, KPA for 3 rounds (with the notations that we will see below, just count the number of equalities $R_i \oplus S_i = R_j \oplus S_j$) and CPA for 4 rounds (take $R_i =$ constant and count the number of equalities $S_i \oplus L_i = S_j \oplus L_j$), that distinguish them from a random permutation for $m = \mathcal{O}(2^{n/2})$.
In order to improve this bound $m \ll 2^{n/2}$ we have the choice between two strategies: either to study the L-R constructions with 5 and more rounds (see for example [9, 13] and the present paper), or to design new constructions. For this second strategy the best results obtained so far are in [1] and [7]. In [1] the bound $m \ll 2^n$ could be achieved for a construction "Benes" that however is not a permutation. In [7] the security of unbalanced Feistel schemes[1] is studied. A security proof in $2^{n(1-\varepsilon)}$ is obtained, instead of $2^{n/2}$, but for much larger round functions (from $2n$ bits to ε bits, instead of n bits to n bits). This bound is basically again the birthday bound for these functions.
For the first strategy, the best security results obtained so far are in [13] and [6]. In [13] it is shown that when $m \ll 2^{\frac{3n}{4}}$ the L-R construction with 6 rounds (or more) is secure against CPCA. (In this paper, we will get $m \ll 2^{\frac{5n}{6}}$ for these conditions: 6 rounds and CPCA.) Recently in [6] it is shown that for L-R construction the security in $2^{n(1-\varepsilon)}$ can be achieved for all $\varepsilon > 0$, when the number of rounds $\to \infty$. In this paper we will show that when $m \ll 2^{n(1-\varepsilon)}$, $\varepsilon > 0$, 4 rounds are sufficient to achieve security against KPA, 7 rounds are sufficient to achieve security against CPA, and 10 rounds are sufficient for security against CPCA. Thus the number of rounds can in fact be fixed to a small value.
Thus we will solve an open problem described in [9], p. 310, as well as in [1], p. 319 and in [16], p. 149. This result also immediately improves the proven bound for one scheme of [2].
Our results are optimal with the regard of the number of queries, since an adversary with unlimited computing power can always distinguish a $k-$round L-R construction (i.e. a random Feistel cipher with k rounds) from a random permutation with $\mathcal{O}(k \cdot 2^n)$ queries and $\mathcal{O}(2^{kn2^n})$ computations by simply guessing all the round functions (this fact was already pointed out in [9] and in [14]).

[1] In [18] such unbalanced Feistel schemes are studied under the angle of linear and differential cryptanalysis.

Remark: It is conjectured but still unclear if 5 rounds are enough to avoid all CPCA attacks when $m \ll 2^{n(1-\varepsilon)}$. (See section 10).
In Appendix, we will summarize all the results proved so far for k rounds.

2 Notations

- $I_n = \{0,1\}^n$ denotes the set of the 2^n binary strings of length n. $|I_n| = 2^n$.
- The set of all functions from I_n to I_n is F_n. Thus $|F_n| = 2^{n \cdot 2^n}$.
- The set of all permutations from I_n to I_n is B_n. Thus $B_n \subset F_n$, and $|B_n| = (2^n)!$
- For any $f, g \in F_n$, $f \circ g$ denotes the usual composition of functions.
- For any $a, b \in I_n$, $[a, b]$ will be the string of length $2n$ of I_{2n} which is the concatenation of a and b.
- For $a, b \in I_n$, $a \oplus b$ stands for bit by bit exclusive or of a and b.
- Let f_1 be a function of F_n. Let L, R, S and T be four n-bit strings in I_n. Then by definition

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

- Let $f_1, f_2, \ldots, f_k$ be k functions of F_n. Then by definition:

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

The permutation function $\Psi^k(f_1, \ldots, f_k)$ is called "a Feistel scheme with k rounds" or shortly Ψ^k. When $f_1, f_2, \ldots, f_k$ are randomly and independently chosen functions in F_n, then $\Psi^k(f_1, \ldots, f_k)$ is called a "random Feistel scheme with k rounds", or a "L-R construction with k rounds".
We assume that the definitions of distinguishing circuits,and of normal and inverse (encrypting/decrypting) oracle gates are known. These standard definitions can be found in [3] and [7]. Let ϕ be a distinguishing circuit. We will denote by $\phi(F)$ it's output (1 or 0) when its oracle gates are implementing the encryption or decryption with the function F.

3 The "coefficients H technique"

We will formulate four theorems that we will use to prove our results. These theorems are the basis of a general proof technique, called the "coefficients H technique", that allows to prove security results for permutation generators (and thus applies for random and pseudo-random Feistel ciphers). This "coefficient H technique" was first described in [10].

Notations for this section
In this section, $f_1, \ldots f_p$ will denote p functions of F_n, and $\Lambda(f_1, \ldots, f_p)$ is a function of F_{2n} (Λ is derived from the $f_1, \ldots f_p$).
When $[L_i, R_i], [S_i, T_i], 1 \leq i \leq m$, is a given sequence of $2m$ values of I_{2n}, we will denote by $H(L, R, S, T)$ or in short by H, the number if $p - tuples$ of functions $(f_1, \ldots f_p)$ such that:

$$\forall i,\ 1 \leq i \leq m,\ \Lambda(f_1, \ldots, f_p)[L_i, R_i] = [S_i, T_i].$$

Theorem 3.1 (Coefficient H technique, sufficient condition for security against KPA) *Let α and β be real numbers, $\alpha > 0$ and $\beta > 0$.*
If :
(1) For random values $[L_i, R_i], [S_i, T_i], 1 \leq i \leq m$, such that $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$, with probability $\geq 1 - \beta$ we have: $H \geq \dfrac{|F_n|^p}{2^{2nm}}(1 - \alpha)$
Then:
(2) For all algorithm A (with no limitation in the number of computations) that takes the $[L_i, R_i], [S_i, T_i],\ 1 \leq i \leq m$ in input and outputs 0 or 1, we have that the expectation of $|P_1 - P_1^*|$ when the $[L_i, R_i],\ 1 \leq i \leq m$, are randomly chosen satisfy:

$$|E(P_1 - P_1^*)| \leq \alpha + \beta.$$

With P_1 being the probability that A outputs 1 when $[S_i, T_i] = \Lambda(f_1, \ldots, f_p)[L_i, R_i]$ and when $(f_1, \ldots, f_p)$ are p independent random functions chosen in F_n.
And with P_1^* being the probability that A outputs 1 when $[S_i, T_i] = F[L_i, R_i]$ and when F is randomly chosen in F_{2n}.

Remarks:

1. In this paper Λ will be the $L - R$ construction Ψ.
2. The condition $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$, is in $m(m-1)/2^{2n}$.
3. Here if $\alpha + \beta$ is negligible, $\Lambda(f_1, \ldots, f_p)$ will resist to all known plaintext attacks, i.e. an attack where m cleartext/ciphertext pairs are given and when the m cleartext have random values.
4. A proof of this Theorem 3.1 is given in Appendix C.
5. From this Theorem 3.1 we can prove that in order to attack Ψ^2 with KPA, we must have $m \geq$ about $2^{n/2}$ (see Appendix C).

Theorem 3.2 (Coefficient H technique sufficient condition for security against adaptative CPA)
Let α and β be real numbers, $\alpha > 0$ and $\beta > 0$.
Let E be a subset of I_{2n}^m such that $|E| \geq (1 - \beta) \cdot 2^{2nm}$. If :
(1) For all sequences $[L_i, R_i], 1 \leq i \leq m$, of m pairwise distinct elements of I_{2n} and for all sequences $[S_i, T_i], 1 \leq i \leq m$, of E
we have: $H \geq \dfrac{|F_n|^p}{2^{2nm}}(1 - \alpha)$

Then:
(2) For every distinguishing circuit ϕ with m oracle gates, we have :

$$\begin{cases} Adv_\phi^{PRF}(m,n) \stackrel{def}{=} |P_1 - P_1^*| \leq \alpha + \beta \\ Adv_\phi^{PRP}(m,n) \stackrel{def}{=} |P_1 - P_1^{**}| \leq \alpha + \beta + \frac{m(m-1)}{2.2^{2n}} \end{cases}$$

With P_1 being the probability that $\phi(F) = 1$ when $F = \Lambda(f_1, \ldots, f_p)$ and when $(f_1, \ldots, f_p)$ are p independent random functions chosen in F_n.
With P_1^{**} being the probability that $\phi(F) = 1$ when F is randomly chosen in B_{2n}. And with P_1^* being the probability that $\phi(F) = 1$ when F is randomly chosen in F_{2n}.

Remarks:

1. In all this paper, "pairwise distinct elements of I_{2n}" means here that $\forall i,\ 1 \leq i \leq m, (L_i \neq L_j)$ <u>or</u> $(R_i \neq R_j)$.

2. Note that there is no limitation in the number of computations that the distinguishing circuit can perform, in order to analyze the m values given by its oracle gates.

3. A proof of this Theorem 3.2 (and more general formulations of it) can be found in [10] page 27 (for P_1^*) and pages 27 and 40 (for P_1^{**}).

4. Note that when $m \ll 2^n$ the term $\frac{m(m-1)}{2 \cdot 2^{2n}}$ is negligible and this term will not be a problem.

5. Here if $Adv^{PRP} = |P_1 - P_1^{**}|$ is negligible, $\Lambda(f_1, \ldots, f_p)$ will resist to all chosen plaintext attacks (we have only encryption gates). This includes adaptive attacks: in the distinguishing circuit the query number i, $1 \leq i \leq m$ can depend on the results of the previous queries.

6. From this Theorem 3.2 (see [8], [10] or Appendix D), we obtain one way to prove the famous result of Luby and Rackoff: to attack Ψ^3 with CPA we must have $m \geq$ about $2^{n/2}$.

Theorem 3.3 (Coefficient H technique sufficient condition for security against adaptative CPCA)
Let $f_1, \ldots f_p$ be p functions in F_n, and let $\Lambda(f_1, \ldots, f_p) \in B_{2n}$. Let $\alpha > 0$.
If:
(1) For all sequences $[L_i, R_i], 1 \leq i \leq m$, of m distinct elements of I_{2n}, and for all sequences $[S_i, T_i], 1 \leq i \leq m$, of m distinct elements of I_{2n}
we have: $H \geq \frac{|F_n|^p}{2^{2nm}}(1 - \alpha)$

Then:
(2) For all super distinguishing circuit ϕ with m "super oracle gates" (normal/encryption or inverse/decryption gates), we have :

$$Adv_\phi^{SPRP}(m, n) \stackrel{def}{=} |P_1 - P_1^{**}| \leq \alpha + \frac{m(m-1)}{2 \cdot 2^{2n}}.$$

With P_1 being the probability that $\phi(F) = 1$ when $F = \Lambda(f_1, \ldots, f_p)$ and $(f_1, \ldots, f_p)$ are randomly (and independently) chosen in F_n.
And with P_1^{**} being the probability that $\phi(F) = 1$ when F is randomly chosen in B_{2n}.

Remarks:

1. This Theorem 3.3 can be found in [11], and in [10] p.40 where a proof is given.

2. Here if $Adv^{SPRP} = |P_1 - P_1^{**}|$ is negligible, $\Lambda(f_1, \ldots, f_p)$ will resist to all adaptive CPCA (we have both encryption and decryption oracle queries here).

3. From this Theorem 3.3 (see [8], [10] or Appendix D) we can prove that in order to attack Ψ^4 with CPCA we must have $m \geq$ about $2^{n/2}$.

Theorem 3.4 (Variant of Theorem 3.3, a bit more general)
With the same notations, let assume that

(1a) We have $H \geq \frac{|F_n|^p}{2^{2nm}}(1-\alpha)$ *for all* $[L,R,S,T] \in E$, *where* E *is a subset of* I_n^{4m}.

(1b) For all super distinguishing circuit ϕ *with* m *super oracle gates, the probability that* $[L,R,S,T](\phi) \in E$ *is* $\geq 1-\beta$, *when* ϕ *acts on a random permutation* f *of* B_{2n}. *(Here* $[L,R,S,T](\phi)$ *denotes the successive* $[S_i,T_i] = f[L_i,R_i]$ *or* $[L_i,R_i] = f^{-1}[S_i,T_i]$, $1 \leq i \leq m$, *that will appear.)*

Then $(2) : |P_1 - P_1^{**}| \leq \alpha + \beta + \frac{m(m-1)}{2 \cdot 2^{2n}}$.

Remarks:

1. This Theorem 3.4 can be found in [10] p. 38.
2. Theorem 3.3 is a special case of Theorem 3.4 where E is the set of all possible $[L,R,S,T]$ (with pairwise distinct $[L,R]$ and pairwise distinct $[S,T]$).
3. This Theorem 3.4 is sometime useful because it allows to study only cleartext/ciphertext pairs where we do not have too many equations that cannot be forced by CPCA attacks (for example like $R_i = S_i$, and unlike $L_i = R_i$).

In this paper we will use Theorem 3.1 for KPA on Ψ^4, Theorem 3.2 for CPA on Ψ^7 (and our result on Ψ^5), Theorem 3.3 for CPCA on Ψ^{10}, and Theorem 3.4 for our result for CPCA on Ψ^6.

4 An exact formula for H

Let $[L_i,R_i], 1 \leq i \leq m$ be m pairwise distinct elements of I_{2n}, and let $[S_i,T_i], 1 \leq i \leq m$ be some other m pairwise distinct elements of I_{2n}. We will note H the number of $(f_1,\ldots,f_k) \in F_n^k$ such that $\Psi^k(f_1,\ldots,f_k)[L_i,R_i] = [S_i,T_i]$.
This is the coefficient H that we need to apply Theorems 3.1, 3.2, 3.3 and 3.4 to k-round L-R construction Ψ^k. Fortunately it is possible to give an exact formula for H for every number of rounds k. Unfortunately when $k \geq 3$, the exact formula for H will involve a somewhat complex summation, and therefore it is not easy to use it. In this paper we will use the exact formula for H for 4 rounds. The proof of this formula (and formulas for $1, 2$, 3 rounds) can be found in [10], pages 132-136, or in Appendix D.

An exact formula for H for 4 rounds

Let P_i and Q_i, with $1 \leq i \leq m$, be the values such that $\Psi^2(f_1,f_2)[L_i,R_i] = [P_i,Q_i]$, i.e. the values after 2 rounds. Let $P = (P_1,\ldots P_m)$ and $Q = (Q_1,\ldots Q_m)$. Let (C) be the conditions:

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

Then

$$H = \sum_{(P,Q) \text{ satisfying } (C)} \frac{|F_n|^4}{2^{4mn}} \cdot 2^{n(r+s+p+q)},$$

with p being the number of linearly independent equations of the form $P_i = P_j$, $i \neq j$, and similarly with q,r and s being the number of linearly independent equations of the form respectively $Q_i = Q_j$, $i \neq j$, $R_i = R_j$, $i \neq j$ and $S_i = S_j$, $i \neq j$.

5 A formula for H for 4 rounds with "frameworks"

Most of the work in this paper is done for 4 rounds. Only at the end we will add some additional rounds to get the final results. From now on, we will use the same notations as in the formula for H for 4 rounds given in Section 4.

Definition 5.1 *We will call a "framework" a set $\mathcal{F}$ of equalities such that each equality of $\mathcal{F}$ is of one of the following forms: $P_i = P_j$ or $Q_i = Q_j$ with $1 \leq i < j \leq m$.*

Let (P, Q) be an element of $I_n^m \times I_n^m$.

Definition 5.2 *We will say that (P, Q) "satisfy" $\mathcal{F}$ if the set of all the equations of the form $P_i = P_j$ $i < j$ that are true in the sequence P, and all the equations of the form $Q_i = Q_j$ $i < j$ true in Q, is exactly $\mathcal{F}$.*
If it is so we will also say that $\mathcal{F}$ "is the framework of (P, Q)". (Each (P, Q) has one and only one framework).

Then from the exact formula given in Section 4 we have:

$$H = \sum_{\substack{\text{all frameworks} \\ \mathcal{F}}} \left[\sum_{\substack{(P,Q) \text{ satisfying} \\ (C) \text{ and } \mathcal{F}}} \frac{|F_n|^4}{2^{4mn}} \cdot 2^{n(r+s+p+q)} \right]$$

The set of conditions (C) was defined in Section 4. We observe that when $\mathcal{F}$ is fixed, from (C) we get a set of equations between the P values (and L and S values) or between the Q values (and T and R values), *i.e.* in these equations from (C), the P_i and the Q_i will never appear in the same equation.
We have:

$$H = \frac{|F_n|^4}{2^{4mn}} \sum_{\substack{\text{all frameworks} \\ \mathcal{F}}} \left[\sum_{P \text{ satisfying } (C1)} 2^{n(r+q)} \right] \cdot \left[\sum_{Q \text{ satisfying } (C2)} 2^{n(s+p)} \right]$$

With $(C1)$ and $(C2)$ being the sets of conditions defined as follows:

$$(C1): \begin{cases} \text{The equalities } P_i = P_j, i < j \text{ that are present in } \mathcal{F}, \\ \text{and no other equalities } P_i = P_j, i < j \\ R_i = R_j \Rightarrow P_i \oplus P_j = L_i \oplus L_j \\ \text{The equalities } P_i \oplus P_j = S_i \oplus S_j \text{ for all } (i,j) \text{ such that } Q_i = Q_j \text{ is in } \mathcal{F} \end{cases}$$

$$(C2): \begin{cases} \text{The equalities } Q_i = Q_j, i < j \text{ that are present in } \mathcal{F}, \\ \text{and no other equalities } Q_i = Q_j, i < j \\ S_i = S_j \Rightarrow Q_i \oplus Q_j = T_i \oplus T_j \\ \text{The equalities } Q_i \oplus Q_j = R_i \oplus R_j \text{ for all } (i,j) \text{ such that } P_i = P_j \text{ is in } \mathcal{F} \end{cases}$$

We have:

$$H = \frac{|F_n|^4}{2^{4mn}} \sum_{\substack{\text{all frameworks} \\ \mathcal{F}}} 2^{n(r+q)} \,[\text{Number of } P \text{ satisfying } (C1)] \cdot$$
$$\cdot\, 2^{n(s+p)} \,[\text{Number of } Q \text{ satisfying } (C2)]$$

For a fixed framework $\mathcal{F}$, let:

$H_{\mathcal{F}_1} = 2^{n(r+q)}$ [Number of $(P_1, \dots P_m)$ satisfying $(C1)$]

$H_{\mathcal{F}_2} = 2^{n(s+p)}$ [Number of $(Q_1, \dots Q_m)$ satisfying $(C2)$]

Then: $H = \frac{|F_n|^4}{2^{4mn}} \sum_{\substack{\text{all frameworks} \\ \mathcal{F}}} H_{\mathcal{F}_1} \cdot H_{\mathcal{F}_2}$.

Remark: When $\mathcal{F}$ is fixed, in $(C1)$ we have only conditions on P and in $(C2)$ we have only conditions on Q.

6 Some definitions on sets of equations and frameworks

Definition 6.1 *For a fixed framework $\mathcal{F}$,*
let $J_{\mathcal{F}_1}$ = Number of $(P_1, \dots P_m)$ such that the equalities $P_i = P_j$, $i < j$ are exactly those of $\mathcal{F}$.
let $J_{\mathcal{F}_2}$ = Number of $(Q_1, \dots Q_m)$ such that the equalities $Q_i = Q_j$, $i < j$ are exactly those of $\mathcal{F}$.

So we have: $J_{\mathcal{F}_1} = 2^n \cdot (2^n - 1) \cdot (2^n - 2) \cdot \ldots \cdot (2^n - m + 1 + p)$
and $J_{\mathcal{F}_2} = 2^n \cdot (2^n - 1) \cdot (2^n - 2) \cdot \ldots \cdot (2^n - m + 1 + q)$

Definition 6.2 *Let $\mathcal{F}$ be a framework. We will say that two indices i and j, $1 \leq i \leq m$ and $1 \leq j \leq m$ are "connected in P" if the equation $P_i = P_j$ is in $\mathcal{F}$. (Similar definition for "connected in Q"). We say that i and j are connected in R if we have $R_i = R_j$ (here it does not depend on $\mathcal{F}$).*

Definition 6.3 *Let $\mathcal{F}$ be a framework. We will say that $\mathcal{F}$ "has a circle in R, P, Q" if there are k indices $i_1, i_2, \dots, i_k$, with $k \geq 3$ and such that:*

1. *$i_k = i_1$ and $i_1 \neq i_2, i_2 \neq i_3, \dots, i_{k-1} \neq i_k$.*
2. *$\forall \lambda, 1 \leq \lambda \leq k-2$ we have one of the three following conditions:*
   - *i_λ and $i_{\lambda+1}$ are connected in R, and $i_{\lambda+1}$ and $i_{\lambda+2}$ are connected in P or in Q*
   - *i_λ and $i_{\lambda+1}$ are connected in P, and $i_{\lambda+1}$ and $i_{\lambda+2}$ are connected in R or in Q*
   - *i_λ and $i_{\lambda+1}$ are connected in Q, and $i_{\lambda+1}$ and $i_{\lambda+2}$ are connected in R or in P*

Examples.

- If $P_1 = P_2$ and $Q_1 = Q_2$ are in $\mathcal{F}$, then $\mathcal{F}$ has a circle in P, Q.
- If $\mathcal{F} = \{P_1 = P_2, P_2 = P_3\}$, then $\mathcal{F}$ has no circle in P, Q.

Definition 6.4 *Let $\mathcal{F}$ be a framework. We will say that (in $\mathcal{F}$) two indices i and j are connected by R, P, Q if there exist some indices i_1, i_2, ..., i_v such that $i = i_1$, $i_v = j$, and $\forall k$, $1 \leq k \leq v-1$, we have either $(R_{i_k} = R_{i_{k+1}})$, or $(P_{i_k} = P_{i_{k+1}}) \in \mathcal{F}$ or $(Q_{i_k} = Q_{i_{k+1}}) \in \mathcal{F}$.*

Definition 6.5 *Let $\mathcal{F}$ be a framework. We will say that $\mathcal{F}$ has "no more than θ equalities in R, P, Q in the same line" if for all set of $\theta + 1$ independent equations that are either of $\mathcal{F}$ or of the form $R_i = R_j$ (with $R_i = R_j$ true), there exist two indices i and j which are not connected by R, P, Q.(Similar definition for "no more than θ equalities in S, P, Q in the same line".)*

Definition 6.6 *Let $\mathcal{F}$ be a framework. Let $\mathcal{F}'$ be the set of all the following equations:*

- *$P_i = P_j$ such that $P_i = P_j$ is in $\mathcal{F}$.*
- *$P_i \oplus P_j = L_i \oplus L_j$ for all $i < j$ such that $R_i = R_j$.*
- *$P_i \oplus P_j = S_i \oplus S_j$ such that $Q_i = Q_j$ is in $\mathcal{F}$.*

If from these equations of $\mathcal{F}'$ we can generate by a linear combination an equation $P_i = P_j, i \neq j$, we say that $\mathcal{F}$ has a circle in $R, P, Q, [LS]$.
We define in the same way "$\mathcal{F}$ has a circle in S, P, Q, $[RT]$" (by interchanging R and S, P and Q, and L and T).

Example 6.1 *If $\mathcal{F} = \{Q_i = Q_k\}$ and we have $R_i = R_j$ and $L_i \oplus L_j = S_i \oplus S_k$ then $\mathcal{F}'$ contains $P_i \oplus P_j = L_i \oplus L_j$ and contains $P_i \oplus P_k = S_i \oplus S_k$, and then from $\mathcal{F}'$ we can generate $P_j = P_k$. Here $\mathcal{F}$ has a circle in $R, P, Q, [LS]$.*

7 The proof strategy

We recall that from the end of Section 5, for 4 rounds we have:
$H = \dfrac{|F_n|^4}{2^{4mn}} \sum_{\substack{\text{all frameworks} \\ \mathcal{F}}} H_{\mathcal{F}_1} \cdot H_{\mathcal{F}_2}$.
We will evaluate H with this formula, in order to get the results of section 9 below. For this, the general strategy is to study this summation "framework by framework", *i.e.* we will compare $H_{\mathcal{F}}$ and $J_{\mathcal{F}}$ for a fixed framework $\mathcal{F}$. We will do this by using mainly four ideas:

- We will see that when $m \ll 2^n$ we can avoid all the "circles" in the equalities in the variables, and when $m^{\theta+1} \ll 2^{n\theta}$ we can avoid all the $\theta + 1$ equalities of the variables in the same line.
- We will use a property (Theorem 8.1 given in section 8) on sets of equations $P_i \oplus P_j = \lambda_k$.
- We will see that we can assume that the λ_k are generally random (sometime by adding 3 rounds at the beginning or at the end).
- We will need a general result of probability (Theorem 73 below).

More precisely, we will prove the following theorems.

a) Analyzing sets of equations $P_i \oplus P_j = \lambda_k$

First we will prove Theorem 8.1 given in section 8. Conjecture 81 of section 8 is also of interest.

b) Avoiding "circles" and "long lines"

Theorem 7.1 *Let $\mathcal{M}$ be the set of all frameworks $\mathcal{F}$ such that:*

1. *$\mathcal{F}$ has no circle in R, P, Q*
2. *$\mathcal{F}$ has no circle in S, P, Q*
3. *$\mathcal{F}$ has no circle in $R, P, Q, [LS]$*
4. *$\mathcal{F}$ has no circle in $S, P, Q, [RT]$*
5. *$\mathcal{F}$ has no more than θ equalities in R, P, Q in the same line*
6. *$\mathcal{F}$ has no more than θ equalities in S, P, Q in the same line*

Let M be the number of (P, Q) such that the framework $\mathcal{F}$ of (P, Q) is in $\mathcal{M}$. Then, with probability $\geq p$, M satisfies:

$$M \geq 2^{2nm}\left(1 - \mathcal{O}\Big(\frac{m^2}{2^{2n}}\Big) - \mathcal{O}\Big(\frac{m^{\theta+1}}{2^{n\theta}}\Big)\right),$$

where p is near 1 when the big O in the expression above are small, and when the R, L, S, T variables have random values, or are the output of a two rounds (or more) random Feistel scheme.

See Appendix G for the exact value of p. A similar result, with a small restriction on the inputs/outputs also exist if we add only one round (see Appendix G).

c) We can assume that the λ_k are generally random

Theorem 7.2 *Let λ_k, $1 \leq k \leq a$, be some variables of I_n such that $\forall k$, $1 \leq k < a$, $\exists i, j$ such that ($\lambda_k = L'_i \oplus L'_j$ and $R'_i = R'_j$), where:*
(1a) The L'_i and R'_i variables are random variables of I_n. or:
(1b)$\forall i$, $1 \leq i \leq m$, $[L'_i, R'_i] = \Psi^3(f_1, f_2, f_3)[L_i, R_i]$, where f_1, f_2, f_3 are randomly chosen in F_n (and then when $R'_i = R'_j$ we can introduce a value $\lambda_k = L'_i \oplus L'_j$). Then:
The probability to distinguish λ_1, λ_2, ..., λ_a from a truly random values of I_n is $\leq 1 - \mathcal{O}\left(\frac{m}{2^n}\right)$.

Proof: See Appendix H.

d) A general result of probability

Theorem 7.3 *Let a_i and b_i, $1 \leq i \leq N$, be N variables $a_i \geq 0$, $b_i \geq 0$, such that: $\forall i, 1 \leq i \leq N, a_i \geq b_i$ with a probability $\geq 1 - \varepsilon$.*
Then: $\forall \lambda > 0$, the probability that $\sum_{i=1}^{N} a_i \geq \Big(\sum_{i=1}^{N} b_i\Big)(1 - \lambda\varepsilon)$ is $\geq 1 - \frac{1}{\lambda}$.

Proof: See Appendix I.

8 About sets of equations $P_i \oplus P_j = \lambda_k$

Definition 8.1 *Let (A) be a set of equations $P_i \oplus P_j = \lambda_k$. If by linearity from (A) we cannot generate an equation in only the λ_k, we will say that (A) has "no circle in P", or that the equations of (A) are "linearly independent in P".*

Let a be the number of equations in (A), and α be the number of variables P_i in (A). So we have parameters λ_1, λ_2, ..., λ_a and $a+1 \leq \alpha \leq 2a$.

Definition 8.2 *We will say that two indices i and j are "in the same block" if by linearity from the equations of (A) we can obtain $P_i \oplus P_j =$ an expression in λ_1, λ_2, ..., λ_a.*

Definition 8.3 *We will denote by ξ the maximum number of indices that are in the same block.*

Example 8.1 *If $A = \{P_1 \oplus P_2 = \lambda_1,\ P_1 \oplus P_3 = \lambda_2,\ P_4 \oplus P_5 = \lambda_3\}$, here we have two blocks of indices $\{1,2,3\}$ and $\{4,5\}$ and $\xi = 3$.*

Definition 8.4 *For such a system (A), when λ_1, λ_2, ..., λ_a are fixed, we will denote by h_α the number of P_1, P_2, ..., P_α solutions of (A) such that: $\forall i,j$, $i \neq j \Rightarrow P_i \neq P_j$.*
We will also denote $H_\alpha = 2^{na} h_\alpha$.

Definition 8.5 *We will denote by J_α the number of P_1, P_2, ..., P_α in I_n such that: $\forall i,j$, $i \neq j \Rightarrow P_i \neq P_j$.*

So $J_\alpha = 2^n \cdot (2^n - 1) \dots (2^n - \alpha + 1)$.

Theorem 8.1 *Let ξ be a fixed integer, $\xi \geq 2$.*
For all set (A) of equations $P_i \oplus P_j = \lambda_k$, with no circle in P, with no more than ξ indices in the same block, with α variables P_i and a equations in (A), with $\alpha \ll 2^n$ (and also $\xi\alpha \ll 2^n$ since ξ is a fixed integer), when λ_1, λ_2, ..., λ_a are randomly chosen in the subset D of I_n^a such that $H_\alpha \neq 0$, we have:
1) the average value of H_α is $\frac{2^{na}}{|D|} \cdot J_\alpha$ so is $\geq J_\alpha$.
2) the standard variation of H_α is $\sigma \leq J_\alpha \cdot \mathcal{O}\Big(\frac{\alpha\sqrt{\alpha}}{2^n\sqrt{2^n}}\Big)$.

Proof: See Appendix J.
The condition $H_\alpha \neq 0$ means that for all i and j in the same block, $i \neq j$, the expression of $P_i \oplus P_j$ in λ_1, λ_2, ..., λ_a is $\neq 0$. So this condition is in $1 - \mathcal{O}\big(\frac{\alpha}{2^n}\big)$.
From Bienaymé-Tchébichef Theorem, we get :

Corollary 8.1 *For all $\lambda > 0$, with a probability $\geq 1 - \mathcal{O}\big(\frac{1}{\lambda^2}\big) - \mathcal{O}\big(\frac{\alpha}{2^n}\big)$, we have:*

$$H_\alpha \geq J_\alpha\Big(1 - \frac{\lambda\alpha\sqrt{\alpha}}{2^n\sqrt{2^n}}\Big).$$

We will say that we have $H_\alpha \geq J_\alpha\Big(1 - \frac{\lambda\alpha\sqrt{\alpha}}{2^n\sqrt{2^n}}\Big)$ with a probability as near as 1 as we want.

Theorem 8.2 *Let ξ be a fixed integer, $\xi \geq 2$.*
Let (A) be a set of equations $P_i \oplus P_j = \lambda_k$ with no circle in P, with α variables P_i, such that:

1. $\alpha^3 \ll 2^{2n}$ *(and also* $\xi\alpha^3 \ll 2^{2n}$ *since* ξ *is here a fixed integer).*

2. *We have no more than* ξ *indices in the same block.*

3. *The* λ_1, λ_2, ..., λ_k *have any fixed values such that: for all* i *and* j *in the same block,* $i \neq j$, *the expression of* $P_i \oplus P_j$ *in* λ_1, λ_2, ..., λ_a *is* $\neq 0$ *(i.e. by linearity from* (A) *we cannot generate an equation* $P_i = P_j$ *with* $i \neq j$*).*

Then we have, for sufficiently large n: $H_\alpha \geq J_\alpha$.

Proof: See Appendix E.

Conjecture 8.1 *This Theorem 8.2 is still true when* $\alpha \ll 2^n$ *(instead of* $\alpha^3 \ll 2^{2n}$*).*

This Conjecture 8.1 is not yet proved in general.

9 Results for 4, 7 and 10 rounds in $\mathcal{O}(2^{n(1-\varepsilon)})$

From the theorems of Section 7 and Theorem 9.1 we get the following theorems on H (see Appendix K for the proofs).

Theorem 9.1 *Let* $[L_i, R_i]$, *and* $[S_i, T_i]$, $1 \leq i \leq m$, *be random values such that the* $[L_i, R_i]$ *are pairwise distinct and the* $[S_i, T_i]$ *are pairwise distinct. Then for* Ψ^4 *the probability* p *that :*

$$H \geq \frac{|F_n|^4}{2^{2nm}} \left(1 - \mathcal{O}\left(\frac{m}{2^n}\right) - \mathcal{O}\left(\frac{m^{\theta+1}}{2^{n\theta}}\right)\right).$$

satisfy:

$$p \geq 1 - \mathcal{O}\left(\frac{m}{2^n}\right)$$

Theorem 9.2 *Let* $[L_i, R_i]$, *and* $[S_i, T_i]$, $1 \leq i \leq m$, *be some values such that the* $[L_i, R_i]$ *are pairwise distinct and the* $[S_i, T_i]$ *are pairwise distinct. Then for* Ψ^7 *we have:*
There is a subset E *of* I_{2n}^m *with* $|E| \geq \left(1 - \mathcal{O}\left(\frac{m}{2^n}\right) - \mathcal{O}\left(\frac{m^{\theta+1}}{2^{n\theta}}\right)\right)$ *such that if the* $[S_i, T_i]$, $1 \leq i \leq m$ *are in* E *we have:*

$$H \geq \frac{|F_n|^7}{2^{2nm}} \left(1 - \mathcal{O}\left(\frac{m}{2^n}\right) - \mathcal{O}\left(\frac{m^{\theta+1}}{2^{n\theta}}\right)\right).$$

Theorem 9.3 *Let* $[L_i, R_i]$, *and* $[S_i, T_i]$, $1 \leq i \leq m$, *be some values such that the* $[L_i, R_i]$ *are pairwise distinct and the* $[S_i, T_i]$ *are pairwise distinct. Then for* Ψ^{10} *we have:*

$$\text{For all integer } \theta \geq 1 \quad H \geq \frac{|F_n|^{10}}{2^{2nm}} \left(1 - \mathcal{O}\left(\frac{m}{2^n}\right) - \mathcal{O}\left(\frac{m^{\theta+1}}{2^{n\theta}}\right)\right).$$

Security results against cryptographic attacks
Finally our cryptographic results on 4,7 and 10 rounds are just a direct consequence of Theorem 9.1,9.2,9.3 and of Theorem 3.1, 3.2 and 3.3: this is because θ can be any integer.

Remarks:

1. In these theorems when θ is fixed, we can get explicit values for all the coefficients that appear as $\mathcal{O}()$ in our theorems. Therefore our results are not only asymptotic (when $n \to \infty$), they can also be written as explicit concrete security bounds.

2. For Ψ^4 our security results are optimal both in term of m and in term of the number of computations to be performed. With $\mathcal{O}(2^n)$ messages and $\mathcal{O}(2^n)$ computations it is indeed possible to distinguish Ψ^4 from a truly random permutation with a KPA (count the number of (i, j, k) with $R_i = R_j$ and $S_i \oplus L_i = S_j \oplus L_j$).

10 Results for 5 or 6 rounds in $\mathcal{O}(2^{5n/6})$

Here we cannot assume that the λ_k are almost random. However, from Theorem 82 we can prove:

Theorem 10.1 *Ψ^5 resists all CPA when $m \ll \mathcal{O}(2^{5n/6})$. Ψ^6 resists all CPCA when $m \ll \mathcal{O}(2^{5n/6})$.*

(See the Appendix for the proofs. Hint: we will have $\alpha \simeq \frac{m^2}{2^n}$ and $\alpha^3 \ll 2^{2n}$, so $m \ll \mathcal{O}(2^{\frac{5n}{6}})$ will be our condition.)

Remark: If we can use Conjecture 81, then from it we can prove that Ψ^5 resists all CPA when $m \ll \mathcal{O}(2^{n(1-\varepsilon)})$ and Ψ^6 resists all CPCA when $m \ll \mathcal{O}(2^{n(1-\varepsilon)})$ since we will have to add only one or two rounds in addition of the central Ψ^4. However, Conjecture 81 is not yet proven in general.

11 Conclusion and further work

In this paper we were able to prove improved security bounds for random Feistel ciphers. It seems reasonable that our method can be extended, for example for 5 or 6 rounds. This method can also be used in various other directions. For example one can study Feistel schemes with a different group law than $\oplus$ (it has already been studied but only when $m \ll 2^{n/2}$). One can also study the Feistel schemes on digits/$GF(q)$/bytes etc. instead of bits. Finally one can study cryptographic constructions of different type.
It seems particularly interesting to study dissymmetric Feistel schemes, i.e. schemes in which a round is defined as $\Psi(f_i)[L, R] = [S, T] \overset{\text{def}}{\Leftrightarrow} S = R$ and $T = L \oplus f_1(R)$ but with L and T having only 1 bit, and S and R having $2n - 1$ bits, and with the f_i being single Boolean functions $f_i \in I_{2n-1} \to I_1$. It seems that in such schemes the methods of the present paper should give a security proof for $m \ll 2^{2n(1-\varepsilon)}$, even against unbounded adversaries [2]. (This will improve the $2^{n(1-\varepsilon)}$ result of [7] for such schemes). For comparison, the best possible result for classical Feistel schemes with the same block size $2n$ (and achieved in the present paper) is $m \ll 2^{n(1-\varepsilon)}$ and cannot be improved in the unbounded adversary model.
In conclusion we hope that the proof techniques given in this paper will be useful in future works, on one hand in the design of cryptographic schemes with optimal proofs of security, and on the other hand to detect flaws in existing designs and suggest some new attacks.

[2] The reason for this is that in the asymmetric Feistel scheme there are much more possible round functions.

12 Acknowledgement

I would like to thank the Stephan Banach Center of Warsaw where I was invited in January 2003 and where part of this work was done.

References

[1] William Aiello, Ramarathnam Venkatesan, *Foiling Birthday Attacks in Length-Doubling Transformations - Benes: A Non-Reversible Alternative to Feistel.* Eurocrypt 96, LNCS 1070, Springer, pp. 307-320.

[2] John Black, Philip Rogaway, *Ciphers with Arbitrary Finite Domains*, RSA'2002, pp. 114-130, Springer LNCS 2271, February 2002.

[3] 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.

[4] U. Maurer, *A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators*, Eurocrypt'92, Springer, pp. 239-255.

[5] U. Maurer: *Indistinguishability of Random Systems*, Eurocrypt 2002, LNCS 2332, Springer, pp. 110-132.

[6] U. Maurer, K. Pietrzak: *The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations*, Eurocrypt 2003, May 2003, Warsaw, Poland, LNCS, Springer.

[7] Moni Naor and Omer Reingold, *On the construction of pseudo-random permutations: Luby-Rackoff revisited*, Journal of Cryptology, vol 12, 1999, pp. 29-66. Extended abstract was published in: Proc. 29th Ann. ACM Symp. on Theory of Computing, 1997, pp. 189-199.

[8] J. Patarin, *Pseudorandom Permutations based on the DES Scheme*, Eurocode'90, LNCS 514, Springer, pp. 193-204.

[9] J. Patarin, *New results on pseudorandom permutation generators based on the DES scheme*, Crypto'91, Springer, pp. 301-312.

[10] J. Patarin, *Etude des générateurs de permutations basés sur le schéma du DES* . Ph. D. Thesis, Inria, Domaine de Voluceau, Le Chesnay, France, 1991.

[11] J. Patarin, *How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function.* Eurocrypt'92, Springer, pp. 256-266.

[12] J. Patarin, *Improved Security Bounds for Pseudorandom Permutations*, 4th ACM Conference on Computer and Communications Security April 2-4th 1997, Zurich, Switzerland, pp. 142-150.

[13] J. Patarin, *About Feistel Schemes with Six (or More) Rounds*, in Fast Software Encryption 1998, pp. 103-121.

[14] J. Patarin, *Generic Attacks on Feistel Schemes*, Asiacrypt 2001, LNCS 2248, Springer, pp. 222-238.

[15] S. Patel, Z. Ramzan and G. Sundaram, *Toward making Luby-Rackoff ciphers optimal and practical*, FSE'99, LNCS, Springer, 1999.

[16] J. Pieprzyk, *How to construct pseudorandom permutations from Single Pseudorandom Functions*, Eurocrypt'90, LNCS 473, Springer, pp. 140-150.

[17] Z. Ramzan, L. Reyzin, *On the Round Security of Symmetric-Key Cryptographic Primitives*, Crypto 2000, LNCS 1880, Springer, pp. 376-393.

[18] B. Schneier and J. Kelsey, *Unbalanced Feistel Networks and Block Cipher Design*, FSE'96, LNCS 1039, Springer, pp. 121-144.

A Appendix A: Summary of the main notations in this paper

A.1 Main paper

m: number of messages in the attack.

n: the Feistel schemes are from $2n$ bits $\rightarrow 2n$ bits

θ: We look for security in $\mathcal{O}\left(\frac{m^{\theta+1}}{2^{n\theta}}\right)$.

ε: we look for security when $m \ll 2^{n(1-\varepsilon)}$ so $\varepsilon = \frac{1}{\theta+1}$.

P_i, Q_i: Internal variables of the 4 rounds Feistel Scheme that we study.

A.2 Notations for Section 8

a: number of equations in systems of Section 8.

α: number of variables P_i in systems of Section 8.

ξ: maximum number of P_i variables that are fixed when one of them is fixed.

P_i: name of the variables in systems of Section 8.

λ_k: name of the fixed parameters in equations $P_i \oplus P_j = \lambda_k$ of Section 8.

J_α: $2^n(2^n-1)\dots(2^n-\alpha+1)$.

h_α: number of P_i, $1 \leq i \leq \alpha$, pairwise distinct and solution of a system of Section 8.

H_α: $2^{na}.h_\alpha$.

B Appendix B: Summary of the known results on random Feistel schemes

We denote the adaptive chosen plaintext attack by CPA, and CPCA is an adaptive chosen plaintext and chosen ciphertext attack.

Unbounded Adversaries limited by m oracle queries

	Ψ	Ψ^2	Ψ^3	Ψ^4	Ψ^5	Ψ^6	Ψ^7	$\Psi^k, k \geq 10$
KPA	1	$\mathcal{O}(2^{\frac{n}{2}})$	$\mathcal{O}(2^{\frac{n}{2}})$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^n)$
CPA	1	2	$\mathcal{O}(2^{\frac{n}{2}})$	$\mathcal{O}(2^{\frac{n}{2}})$	$\geq \mathcal{O}(2^{\frac{5n}{6}})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{\frac{5n}{6}})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^n)$
CPCA	1	2	3	$\mathcal{O}(2^{\frac{n}{2}})$	$\geq \mathcal{O}(2^{\frac{n}{2}})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{\frac{5n}{6}})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{\frac{n}{2}})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^n)$

Figure 2: The minimum number $\mathbf{m}$ *of queries needed to distinguish* Ψ^i *from a random permutation of* B_{2n}

Adversaries bounded by λ computations (and also $\leq \lambda$ queries)

	Ψ	Ψ^2	Ψ^3	Ψ^4	Ψ^5	Ψ^6	Ψ^7	$\Psi^k, k \geq 10$
KPA	$\mathcal{O}(1)$	$\mathcal{O}(2^{\frac{n}{2}})$	$\mathcal{O}(2^{\frac{n}{2}})$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^n)$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^{\frac{7n}{4}})$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^{2n})$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^{2n})$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^{2n})$
CPA	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(2^{\frac{n}{2}})$	$\mathcal{O}(2^{\frac{n}{2}})$	$\geq \mathcal{O}(2^{\frac{5n}{6}})$ and $\leq \mathcal{O}(2^{\frac{3n}{2}})$	$\geq \mathcal{O}(2^{\frac{5n}{6}})$ and $\leq \mathcal{O}(2^{2n})$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^{2n})$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^{2n})$
CPCA	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(1)$	$\mathcal{O}(2^{\frac{n}{2}})$	$\geq \mathcal{O}(2^{\frac{n}{2}})$ and $\leq \mathcal{O}(2^{\frac{3n}{2}})$	$\geq \mathcal{O}(2^{\frac{5n}{6}})$ and $\leq \mathcal{O}(2^{2n})$	$\geq \mathcal{O}(2^{\frac{5n}{6}})$ and $\leq \mathcal{O}(2^{2n})$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^{2n})$

Figure 3: The minimum number $\boldsymbol{\lambda}$ *of computations needed to distinguish* Ψ^i *from a random permutation of* B_{2n}

On Figure 1 we represented the known results about the best chosen plaintext attack and the best chosen plaintext/ciphertext attack in a model with infinite computing power and with only m queries to encryption/decryption oracles. The best attacks for $k = 1 \dots 5$ rounds given here come from [14]. We observe that:

- For 1, 2, 3 and 4 rounds, the situation is clear: the value of the minimum number m of queries necessary for the attacker is known.
- For 10 rounds or more, (and for 7 rounds for chosen plaintext attacks), on one hand the minimum number m of queries is $m \geq \mathcal{O}(2^{n(1-\varepsilon)})$ for any $\varepsilon > 0$. This is the main result of the present paper. On the other hand $m \leq \mathcal{O}(k \cdot 2^n)$ with k being the number of rounds (due to the brute force attack on all the round functions f_i). Therefore the situation is also clear here, and our result is near from optimal, both lower and upper bounds on m are $\mathcal{O}(2^n)$.
- For 5 rounds and 6 rounds the situation remains unclear (m is between $\mathcal{O}(2^{\frac{n}{2}})$ and $\mathcal{O}(2^n)$). However we have good hopes that the analysis given in this paper will help to bridge the gap and solve this remaining open problem.

On Figure 2 we represented the known results about the best chosen plaintext attack and the best chosen plaintext/ciphertext attack in a model with the adversary that is bounded by λ computations (and therefore also by λ queries, each of them requires at least 1 computation). In this second model there are still an important gap between the lower and upper bound on the minimum value of λ, so many open problems appear here.

Remark: Moreover the result $\lambda \leq \mathcal{O}(2^{2n})$ is obtained due to the fact that Ψ^k permutation always have an even signature: If we want to distinguish Ψ^k from random permutations with an even signature (instead of random permutations of the whole B_{2n}), or if we do not have exactly all the possible cleartext/ciphertext pairs, then we only know that (when k is even): $\lambda \leq \mathcal{O}(2^{n(k^2/2-4k+8)})$, see [14].

C Appendix C: Proof of Theorem 3.1 and an example for 2 rounds

C.1 Proof of Theorem 3.1

Let D be the set of all $[L_i, R_i]$, $1 \leq i \leq m$, such that $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$ (so $|D| \simeq 2^{2nm}(1 - \frac{m(m-1)}{2.2^{2n}})$). When the $[L_i, R_i]$, $1 \leq i \leq m$ are fixed, let $W(L, R)$ be the set of all $[S_1, T_1]$, $[S_2, T_2]$, ..., $[S_m, T_m]$ such that the algorithm A outputs 1 on the input $[L_i, R_i]$, $[S_i, T_i]$, $1 \leq i \leq m$.
When the $[L_i, R_i]$, $1 \leq i \leq m$ are fixed in D, then we have:

$$p_1^* = \frac{|W(L,R)|}{2^{2nm}} \qquad (1)$$

and

$$p_1 = \frac{1}{|F_n|^p} \sum_{[S,T] \in W(L,R)} [Number\ of\ (f_1, \ldots, f_p) / \forall i,\ 1 \leq i \leq m, \Lambda(f_1, \ldots, f_p)[L_i, R_i] = [S_i, T_i]]$$

so

$$p_1 = \frac{1}{|F_n|^p} \sum_{[S,T] \in W(L,R)} H(L, R, S, T) \qquad (2)$$

Moreover, by hypothesis we have that the number N of $[L, R, S, T]$ such that

$$H(L, R, S, T) \geq \frac{|F_n|^p}{2^{2nm}}(1 - \alpha) \text{ satisfy: } N \geq |D|.2^{2nm}(1 - \beta) \qquad (3)$$

When the $[L_i, R_i]$, $1 \leq i \leq m$ are fixed, let $N(L, R)$ be the set of all $[S, T]$ such that:

$$H(L, R, S, T) \geq \frac{|F_n|^p}{2^{2nm}}(1 - \alpha)$$

From (3) we have:

$$\sum_{[L,R] \in D} |N(L, R)| \geq |D|.2^{2nm}(1 - \beta) \qquad (4)$$

From (2) we have:

$$p_1 \geq \frac{1}{|F_n|^p} \sum_{[S,T] \in W(L,R) \cap N(L,R)|} H[L, R, S, T)$$

so

$$p_1 \geq \frac{(1 - \alpha)}{2^{2nm}} |W(L, R) \cap N(L, R)|$$

so

$$p_1 \geq \frac{(1 - \alpha)}{2^{2nm}} \ (W(L, R) - N'(L, R)) \qquad (5)$$

where $N'(L, R)$ is the set of all $[S, T]$ such that $[S, T] \notin N(L, R)$. $|N'(L, R)| = 2^{2nm} - |N(L, R)|$ so

$$\sum_{[L,R] \in D} |N'(L, R)| = |D| 2^{2nm} - \sum_{[L,R] \in D} |N(L, R)|$$

so from (4) we have:

$$\sum_{[L,R]\in D} |N'(L,R)| \leq \beta.|D|.2^{2nm}, \text{ so } E(|N'(L,R)|) \leq \beta.2^{2nm} \qquad (6)$$

(where the expectation is computed when the $[L_i, R_i]$, $1 \leq i \leq m$ are randomly chosen in D).
From (5) and (1) we have:

$$p_1 \geq (1-\alpha)(p_1^* - \frac{|N'(L,R)|}{2^{2nm}})$$

$$p_1 \geq (1-\alpha)p_1^* - \frac{|N'(L,R)|}{2^{2nm}}$$

so from (6) we get:

$$E(p_1) \geq (1-\alpha)E(p_1^*) - \beta$$

so

$$E(p_1) \geq E(p_1^*) - \alpha - \beta \qquad (7)$$

Now if we consider the algorithm A' that outputs 1 if and only if A outputs 0, we have $p_1' = 1 - p_1$ and $p_1^{*'} = 1 - p_1^*$ and from (7) we get:

$E(p_1') \geq E(p_1^{*'}) - \alpha - \beta$ (because (7) is true for all algorithm A, so it is true for A').

So

$$E(1-p_1) \geq E(1-p_1^*) - \alpha - \beta$$

so

$$E(p_1) - E(p_1^*) \leq \alpha + \beta \qquad (8)$$

From (7) and (8) we get: $|E(p_1 - p_1^*)| \leq \alpha + \beta$, as claimed.

C.2 Example for 2 rounds

For 2 rounds we have $S_i = L_i \oplus f_1(R_i)$ and $T_i = R_i \oplus f_2(S_i)$ (#)
For random values $[l_i, R_i]$, $[S_i, T_i]$, $1 \leq i \leq m$, (such that $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$) with probability $\geq 1 - m^2/2^n$ we have that all the R_i values are pairwise distinct and all the S_i values are pairwise distinct. Moreover, if this occurs, we have exactly $H = \frac{|F_n|^2}{2^{2nm}}$ (since (#) then fix f_1 exactly on m points and f_2 exactly on m points).
So from Theorem 3.1 (with $\alpha = 0$ and $\beta = m^2/2^n$) we get:

Theorem C.1 *For two rounds, and for all algorithm A that takes m cleartext/ciphertext pairs input, and outputs 0 or 1, we have:*

$$|E(p_1 - p_1^*)| \leq \frac{m^2}{2^n}$$

when the cleartexts are randomly chosen. So when $m \ll 2^{n/2}$, Ψ^2 will resist all known plaintext attacks.

Remark. This result is tight, since when m^2 becomes not negligible compared with 2^n, then by counting the number N of (i,j) / $S_i \oplus L_i = S_j \oplus L_j$ we will be able to distinguish Ψ^2 from a random permutation with a known plaintext attack.

D Appendix D: Exact Formulas for H, and examples for 3 and 4 rounds

D.1 Exact formulas for H

An exact formula for H for 1 round

Let (C) be the following set of conditions:

$$\forall(i,j),\ 1 \le i \le m, 1 \le j \le m, \begin{cases} R_i = S_i \\ R_i = R_j \end{cases} \Rightarrow \ T_i \oplus L_i = T_j \oplus L_j$$

If (C) is not satisfied, then $H = 0$ (it cannot be a Feistel scheme with 1 round).
If (C) is satisfied, then $H = \frac{|F_n|}{2^{mn}} \cdot 2^{nr}$, with r being the number of linearly independent equations $R_i = R_j$ with $i \neq j$.

An exact formula for H for 2 rounds

Let (C) be these conditions:

$$\forall(i,j),\ 1 \le i \le m, 1 \le j \le m, \begin{cases} R_i = R_j & \Rightarrow \ L_i \oplus S_i = L_j \oplus S_j \\ S_i = S_j & \Rightarrow \ R_i \oplus T_i = R_j \oplus T_j \end{cases}$$

If (C) is not satisfied, then $H = 0$.
If (C) is satisfied, then $H = \frac{|F_n|^2}{2^{2mn}} \cdot 2^{n(r+s)}$, with r being the number of linearly independent equations $R_i = R_j$ with $i \neq j$, and with s being the number of linearly independent equations $S_i = S_j$ with $i \neq j$.

An exact formula for H for 3 rounds

Let P_i, $1 \le i \le m$, be the values such that $\Psi(f_1)[L_i, R_i] = [R_i, P_i]$, i.e. the values after 1 round. Let $P = (P_1, \ldots P_m)$. Let (C) be the conditions:

$$\forall(i,j),\ 1 \le i \le m, 1 \le j \le m, \begin{cases} R_i = R_j & \Rightarrow \ L_i \oplus P_i = L_j \oplus P_j \\ S_i = S_j & \Rightarrow \ P_i \oplus T_i = P_j \oplus T_j \\ P_i = P_j & \Rightarrow \ R_i \oplus S_i = R_j \oplus S_j \end{cases}$$

Then

$$H = \sum_{P \text{ satisfying } (C)} \frac{|F_n|^3}{2^{3mn}} \cdot 2^{n(r+s+p)},$$

with r and s being defined as before, and similarly p being the number of linearly independent equations $P_i = P_j$ with $i \neq j$.

An exact formula for H for 4 rounds

It is given in Section 4 of this paper.

The formulas for H for 5 and more rounds

Obviously this method for computing H can be extended to any number of rounds, for example the formula for 6 rounds can be found in [12] and [13], but we will not need it in this paper. We will study 4 round schemes, and from their properties we will prove our theorems for more rounds.

D.2 Example with 3 rounds

We will now illustrate our general proof technique with 3 rounds. This section is just an example and is not needed to prove our new results.
Let E be the set of all $[S_i, T_i]$, $1 \leq i \leq m$ such that the S_i are pairwise distinct, i.e. $\forall (i,j),\ 1 \leq i \leq m, 1 \leq j \leq m, (i \neq j) \Rightarrow (S_i \neq S_j)$.
We have $|E| \geq 2^{2nm}\left(1 - \frac{m(m-1)}{2 \cdot 2^n})\right)$. This is true because if
$A_{ij} = \{[S_k, T_k], 1 \leq m | S_i = S_j\}$ we have $|A_{ij}| = \frac{2^{nm}}{2^n}$ and $E \subset I_{2n}^m - \bigcup_{1 \leq i < j \leq n} A_{ij}$.
If the S_i are pairwise distinct we have (from Section 4):

$$H = \sum_{P \text{ satisfying } (C)} \frac{|F_n|^3}{2^{3mn}} \cdot 2^{n(r+p)},$$

with (C) being the conditions:

$$\forall (i,j),\ 1 \leq i \leq m, 1 \leq j \leq m, \begin{cases} R_i = R_j & \Rightarrow \quad L_i \oplus P_i = L_j \oplus P_j \\ P_i = P_j & \Rightarrow \quad R_i \oplus S_i = R_j \oplus S_j \end{cases}$$

If we limit ourselves to solutions such that the P_i are also pairwise distinct, we get:

$$H \geq \frac{|F_n|^3}{2^{3mn}} \cdot 2^{nr} \cdot [\text{Number of } (P_1, \ldots P_m) \text{ satisfying (C)}] \quad (\#)$$

with $(C1)$ being the following: $(C1) \begin{cases} \text{The } P_i \text{ are pairwise distinct} \\ R_i = R_j \Rightarrow L_i \oplus P_i = L_j \oplus P_j \end{cases}$.
At this point we need the following theorem:

Theorem D.1 *Let $R = (R_1, \ldots, R_m)$ be any element of I_n^m. Let $L = (L_1, \ldots, L_m)$ be any element of I_n^m such that $\forall (i,j), 1 \leq i < j \leq m,\ \ (R_i = R_j) \Rightarrow (L_i \neq L_j)$. Let N be the number of $P = (P_1, \ldots, P_m)$ that satisfy $(C1)$. Then:*

$$2^{nr} \cdot N \geq \left(1 - \frac{m(m-1)}{2 \cdot 2^n}\right) \cdot 2^{mn}.$$

Proof of Theorem D.1. Let M be the number of functions f_1 of F_n such that the m values $f_1(R_i) \oplus L_i$, $1 \leq i \leq m$ are pairwise distinct. It is easy to see that $M = \frac{N}{2^{n(m-r)}} \cdot |F_n| \quad (D.2.1)$.
This is because we have N choices for the values $f_1(R_i) \oplus L_i = P_i$, and when these P_i are fixed we have exactly $\frac{|F_n|}{2^{n(m-r)}}$ solutions f_1.
Moreover $M \geq |F_n| - \frac{m(m-1)}{2 \cdot 2^n} |F_n| \quad (D.2.2)$.
This is because we have $m(m-1)/2$ choices for (i,j), $1 \leq i < j \leq m$ and at most $\frac{|F_n|}{2^n}$ functions f_1 such that $f_1(R_i) \oplus L_i = f_1(R_j) \oplus L_j$ when i and j are fixed, since $(R_i = R_j) \Rightarrow (L_i \neq L_j)$.
Therefore from (D.2.1) and (D.2.2) we get: $2^{nr} \cdot N \geq \left(1 - \frac{m(m-1)}{2 \cdot 2^n}\right) \cdot 2^{mn}$.

Remark: In the previous proof of Theorem D.1 we have just gone back to an expression in f_1 instead of P_i. Thus it was simpler to prove directly some results on (f_1, f_2, f_3) than to use our formula for H and come back to f_1. However there are also other ways to prove this theorem without going back to f_1, for example by a detailed analysis of a general system of pairwise distinct variables with fixed XOR. Later we will use this other approach, that is particularly useful for more than 3 rounds.
From (#) and from Theorem D.1 we get:

Theorem D.2 *For all $[L_i, R_i], 1 \leq i \leq m$ pairwise distinct in I_{2n}, and all $[S_i, T_i], 1 \leq i \leq m$, such that the S_i are pairwise distinct, we have:*

$$\text{For } \Psi^3 : \qquad H \geq \frac{|F_n|^3}{2^{3mn}} \cdot \left(1 - \frac{m(m-1)}{2 \cdot 2^n}\right)$$

Then since $|E| \geq 2^{2nm}\left(1 - \frac{m(m-1)}{2 \cdot 2^n}\right)$, and from Theorem D.2 and 3.1 we get exactly the Luby-Rackoff theorem:

Theorem D.3 (Luby-Rackoff) *For every distinguishing circuit ϕ with m encryption oracle gates, we have: $Adv_\phi^{PRF}(m,n) = |P_1 - P_1^*| \leq \frac{m(m-1)}{2 \cdot 2^n} + \frac{m(m-1)}{2 \cdot 2^n}$*
Therefore $Adv_\phi^{PRF}(m,n) = |P_1 - P_1^*| \leq \frac{m(m-1)}{2^n}$

This is exactly the main lemma of Luby and Rackoff from [3].

Remark: The proof we gave here is not the simplest proof known of their famous result, a simpler proof can be found for example in [10], [7] or [4]. However this proof illustrates the general proof technique we follow in the present paper: combination of the "coefficient H technique" with an exact formula for H that we computed in Section 4.

D.3 Example with 4 rounds

We will now illustrate our general proof technique with 4 rounds. This section is just an example and is not necessary to prove our new results.
In Section 4 we gave an exact formula for H with 4 rounds. If we limit ourselves to solutions such that the P_i are pairwise distinct and also the Q_i are pairwise distinct, we get:

$$H \geq \sum_{\substack{(P,Q) \text{ satisfying } (C) \\ \text{The } P_i \text{ and } Q_i \text{ are pairwise} \neq}} \frac{|F_n|^4}{2^{4mn}} \cdot 2^{n(r+s)},$$

with (C) being: $(C) : \left\{ \begin{array}{rcl} R_i = R_j & \Rightarrow & L_i \oplus P_i = L_j \oplus P_j \\ S_i = S_j & \Rightarrow & Q_i \oplus T_i = Q_j \oplus T_j \end{array} \right.$
Therefore

$$H \geq \frac{|F_n|^4}{2^{4mn}} \cdot 2^{n(r+s)} \cdot [\text{Number of } (P_1, \ldots P_m) \text{ satisfying (C1)}] \cdot \cdot [\text{Number of } (Q_1, \ldots Q_m) \text{ satisfying (C2)}].$$

with $(C1)$ and $(C2)$ being the following: $(C1) : \left\{ \begin{array}{l} \text{The } P_i \text{ are pairwise distinct} \\ R_i = R_j \Rightarrow L_i \oplus P_i = L_j \oplus P_j \end{array} \right.$ and with $(C2) : \left\{ \begin{array}{l} \text{The } Q_i \text{ are pairwise distinct} \\ S_i = S_j \Rightarrow Q_i \oplus T_i = Q_j \oplus T_j \end{array} \right.$.
From Theorem D.1 we get: For all sequences $[L_i, R_i],\ 1 \leq i \leq m$ of m distinct elements of I_{2n},
$2^{nr} \cdot [\text{Number of } (P_1, \ldots P_m) \text{ satisfying (C1)}] \geq \left(1 - \frac{m(m-1)}{2 \cdot 2^n})\right) \cdot 2^{mn}$.
Also from Theorem D.1 we get: For all sequences $[S_i, T_i],\ 1 \leq i \leq m$ of m distinct elements of I_{2n}, $2^{nr} \cdot [\text{Number of } (Q_1, \ldots Q_m) \text{ satisfying (C2)}] \geq \left(1 - \frac{m(m-1)}{2 \cdot 2^n})\right) \cdot 2^{mn}$.
Therefore for all $[L_i, R_i],\ 1 \leq i \leq m$ (pairwise distinct in I_{2n}) and all $[S_i, T_i],\ 1 \leq i \leq m$ (pairwise distinct in I_{2n}) we have:

$$\text{For } \Psi^4 \ : \qquad H \geq \frac{|F_n|^4}{2^{4mn}} \cdot \left(1 - \frac{m(m-1)}{2 \cdot 2^n}\right)^2 \cdot 2^{2nm}$$

$$H \geq \frac{|F_n|^4}{2^{2mn}} \cdot \left(1 - \frac{m(m-1)}{2^n}\right)$$

From Theorem 3.2 we have: for every super distinguishing circuit ϕ with m "super oracle gates" (normal/encryption or inverse/decryption gates) we have:
$Adv_{\phi}^{PRP}(m,n) = |P_1 - P_1^{**}| \leq \frac{m(m-1)}{2^n} + \frac{m(m-1)}{2.2^{2n}} \leq \frac{m^2}{2^n}$
Therefore we have obtained (as an example of the proof technique) a proof of the classical result on Ψ^4: $Adv_{\phi}^{PRP}(m,n) = |P_1 - P_1^{**}|$ is always $\leq \frac{m^2}{2^n}$, and therefore all the random Feistel ciphers are sure against adaptive chosen plaintext and chosen ciphertext attacks as long as $m \ll 2^{n/2}$.

E Appendix E: Proof of Theorem 8.2 when $\alpha^3 \ll 2^{2n}$, and proof $H > 0$, $\forall \alpha \ll 2^n$

E.1 Proof that $H_{\alpha+\xi} \geq 2^{(\xi-1)n}.(2^n - \xi\alpha)H_\alpha$

Let assume that $P_1, P_2, \ldots, P_\alpha$ are fixed. When we fix $P_{\alpha+1}$, we also fix $P_{\alpha+2}$, ..., $P_{\alpha+\xi}$ since: $P_{\alpha+2} = P_{\alpha+1} \oplus \lambda_{a+1}$, $P_{\alpha+3} = P_{\alpha+1} \oplus \lambda_{a+2}$, ..., $P_{\alpha+\xi} = P_{\alpha+1} \oplus \lambda_{a+\xi-1}$.

$$\begin{array}{rll} \text{So we want } P_{\alpha+1} \notin & \{ & P_1, P_2, \ldots, P_\alpha, \\ & & P_1 \oplus \lambda_{a+1}, P_2 \oplus \lambda_{a+1}, \ldots, P_\alpha \oplus \lambda_{a+1}, \\ & & \vdots \\ & & P_1 \oplus \lambda_{a+\xi-1}, P_2 \oplus \lambda_{a+\xi-1}, \ldots, P_\alpha \oplus \lambda_{a+\xi-1} \quad \}. \end{array}$$

So the number of possibilities for $P_{\alpha+1}$ is $\geq 2^n - \xi\alpha$.
So $h_{\alpha+\xi} \geq (2^n - \xi\alpha)h_\alpha$, and $H_{\alpha+\xi} \geq 2^{(\xi-1)n}(2^n - \xi\alpha)H_\alpha$, as claimed.

Corollary E.1 *When ξ is fixed and $\alpha \ll 2^n$, we will always have $H > 0$.*

E.2 Proof of Theorem 8.2 when $\alpha^3 \ll 2^{2n}$

We have: $H_{\alpha+\xi} \geq 2^{(\xi-1)n}(2^n - \xi\alpha)H_\alpha$
and $J_{\alpha+\xi} = (2^n - \alpha)(2^n - \alpha - 1)\ldots(2^n - \alpha - \xi + 1)J_\alpha$.
Moreover $(2^n - \alpha)(2^n - \alpha - 1)\ldots(2^n - \alpha - \xi + 1)$
$= \quad 2^{\xi n} \; + \; 2^{(\xi-1)n}(-\xi\alpha - \frac{\xi.(\xi-1)}{2}) \; + \; 2^{(\xi-2)n}(\frac{\xi.(\xi-1)}{2}\alpha^2 + \mathcal{O}(\alpha)) + \mathcal{O}(2^{(\xi-3)n}\alpha^3)$

So

$$\frac{H_{\alpha+\xi}}{J_{\alpha+\xi}} \geq \left[1 + \frac{2^{(\xi-1)n}\left(\frac{\xi(\xi-1)}{2}\right) + 2^{(\xi-2)n}\left(\frac{-\xi(\xi-1)}{2}\alpha^2 + \mathcal{O}(\alpha)\right) + \mathcal{O}\left(2^{(\xi-3)n}\alpha^3\right)}{2^{\xi n} + o(2^{\xi n})}\right]\frac{H_\alpha}{J_\alpha}$$

Moreover a sufficient condition to have $H_{\alpha+\xi} \geq J_{\alpha+\xi}$ is to have $\frac{H_{\alpha+\xi}}{J_{\alpha+\xi}} \geq \left[1 - o\left(\frac{1}{\alpha}\right)\right]\frac{H_\alpha}{J_\alpha}$.
So a sufficient condition to have $H_{\alpha+\xi} \geq J_{\alpha+\xi}$ (since then $\frac{H_{\alpha+\xi}}{J_{\alpha+\xi}} \geq \left[1 - o\left(\frac{1}{\alpha}\right)\right]^{\frac{\alpha}{\xi}}\frac{H_\xi}{J_\xi} \geq 1$ since $H_\xi = 2^{\xi n} > J_\xi = 2^n(2^n - 1)\cdots(2^n - \xi + 1)$) is to have:

$$-\alpha \cdot 2^{(\xi-1)n}\left(\frac{\xi(\xi-1)}{2}\right) + 2^{(\xi-2)n}\left(\frac{\xi(\xi-1)}{2}\alpha^3 + \mathcal{O}(\alpha^2)\right) + \mathcal{O}\left(2^{(\xi-3)n}\alpha^4\right) \ll 2^{\xi n}.$$

So a sufficient condition is: $2^{(\xi-2)n}\alpha^3 \ll 2^{\xi n}$, *i.e.* $\alpha^3 \ll 2^{2n}$.

F Appendix F: Some properties of randomness for one or two rounds

One round, evaluation with θ

F.1 After one round the number of simultaneous collisions can be assumed to be $\leq \theta$

Theorem F.1 *Let $[L_i, R_i]$, $1 \leq i \leq m$ be m pairwise distinct values in I_{2n} (i.e. $i \neq j \Rightarrow (L_i \neq L_j) or (R_i \neq R_j)$).*
Let θ be a fixed integer. Let f_1 be a function in F_n. For all i, $1 \leq i \leq m$, let $L'_i = R_i$ and $R'_i = L_i \oplus f_1(R_i)$.
Then the number N of functions f_1 in F_n such that it does not exist some pairwise distinct indices $i_1, \ldots, i_{\theta+1}$ (all between 1 and m) such that $R'_{i_1} = R'_{i_2} = \ldots = R'_{i_{\theta+1}}$ is:

$$N \geq |F_n| \left(1 - \frac{m^{\theta+1}}{2^{n\theta} \cdot (\theta+1)!}\right),$$

and therefore $N \geq |F_n| \left(1 - \mathcal{O}\left(\frac{m^{\theta+1}}{2^{n\theta}}\right)\right)$.

Proof of Theorem F.1
In order to choose the indices $i_1, \ldots, i_{\theta+1}$ we have exactly $\frac{m(m-1)\cdots(m-\theta)}{(\theta+1)!}$ possibilities, and therefore less than $\frac{m^{\theta+1}}{(\theta+1)!}$ possibilities.
Now when $i_1, \ldots, i_{\theta+1}$ are fixed (and pairwise distinct), the number M of functions f_1 of F_n such that

$$L_{i_1} \oplus f_1(R_{i_1}) = L_{i_2} \oplus f_1(R_{i_2}) = \ldots = L_{i_{\theta+1}} \oplus f_1(R_{i_{\theta+1}}) \quad (\#)$$

is $\leq \frac{|F_n|}{2^{n\theta}}$. This comes from the fact that if $\exists j, k$ with $j \neq k, 1 \leq j \leq \theta+1, 1 \leq k \leq \theta+1$ such that $R_{i_j} = R_{i_k}$, then $M = 0$ (because $L_{i_j} \neq L_{i_k}$ if $R_{i_j} = R_{i_k}$ and $j \neq k$).
And if the R_{i_j}, $1 \leq j \leq \theta+1$, are pairwise distinct, then $\#$ just fixes the value of f_1 on exactly θ points $R_{i_2}, \ldots, R_{i_{\theta+1}}$ (when $f(R_{i_1})$ is fixed to any value).
Conclusion: For any fixed value $\lambda \in I_n$, after just one round, we can assume that, when $m^{\theta+1} \ll 2^{n\theta}$, the number of indices i such that $R'_i = \lambda$ is $\leq \theta+1$.
Remark: This result, obtained after one round is also true for truly random values R'_i.

Corollary F.1 *$\forall \theta \in \mathbb{N}$, $\forall k < \theta$, when f_1 is randomly chosen in F_n, with a probability $\geq 1 - \frac{m^{\theta+1}}{2^{n\theta} \cdot (\theta+1)!}$, we have: the number of (i,j), such that $R'_i = R'_j$ is $\leq m\theta$, and the number of $(i_1, i_2, \ldots, i_{k+1})$ such that $R'_{i_1} = R'_{i_2} = \ldots = R'_{i_{k+1}}$ is $\leq m\frac{\theta^k}{k!}$.*
(Note: if $k \geq \theta$, this number is 0 with the same probability).

One round, evaluation with probability $2^{n\varepsilon}$

F.2 Number of 2-collisions after one round

We want to evaluate the number N of $(i,j), i < j / R'_i = R'_j$, with $R'_i = L_i \oplus f_1(R_i)$, for "most" of the functions f_1, (knowing however that the inputs $[L_i, R_i], 1 \leq i \leq m$ can be very special).

First evaluation From Theorem F.1, when j is fixed, we know that we can assume that when $m^{\theta+1} \ll 2^{n\theta}$, we have at most θ possibilities for $i \neq j$. Therefore $N \leq \theta m$.

Second evaluation

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

Proof of Theorem F.2

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

Corollary F.2 *Let $\lambda > 0$. Let M be the number of functions $f_1 \in F_n$ such that the number of $(i, j), i < j / R'_i \neq R'_j$, is $\geq \lambda \frac{m(m-1)}{2 \cdot 2^n}$.*
Then, $\forall \lambda > 0$ and for all (pairwise distinct) $[L_i, R_i], 1 \leq i \leq m$ we have $M \leq \frac{|F_n|}{\lambda}$

Proof: This follows immediately from Theorem F.2.

Corollary F.3 *With $\lambda = 2^{n\varepsilon}, \varepsilon > 0$ we get: the number M of functions f_1 such that [the number of $(i, j), i < j / R'_i = R'_j$ is $\geq \frac{m(m-1)}{2 \cdot 2^{n(1-\varepsilon)}}$] is $M \leq \frac{|F_n|}{2^{n\varepsilon}}$.*

Corollary F.4 *Therefore, when f_1 is chosen at random in F_n, we can assume (with probability $1 - \frac{1}{2^{n\varepsilon}}$) that the number N of $(i, j), i < j / R'_i \neq R'_j$, is $N \leq \frac{m(m-1)}{2 \cdot 2^{n(1-\varepsilon)}}$. (This improves $N \leq \theta m$ in our first evaluation.)*

Corollary F.5 *We can assume that (with probability $1 - \frac{1}{2^{n\varepsilon}}$) that the number of pairwise distinct R'_i values is $\geq m - \frac{m(m-1)}{2 \cdot 2^{n(1-\varepsilon)}}$.*

Example F.1 *If all the R_1 values are equal, then all the R'_i values are pairwise distinct, $1 \leq i \leq m$. Thus we will detect that the R'_i are not random when $m^2 \geq \mathcal{O}(2^n)$.*

Example F.2 *Let us consider the case where we have only two values for R_i: $R_i = R$ for $m/2$ cases, and $R_i = R'$ otherwise with $R' \neq R$. Assume that all the L_i values are chosen with v zeros at the end and with $n - v$ first bits that may be $\neq 0$.*
Then $f_1(R) \oplus f_1(R')$ has its v last bits (all) being 0 with probability $\frac{1}{2^v}$. If this occurs, then the number N of $(i, j), i < j / L_i \oplus f_1(R) = L_j \oplus f_1(R')$ will be about $\frac{m(m-1)}{2 \cdot 2^{n-v}}$. This shows that the bound for N obtained in Corollary F.4 is optimal.
In particular, it is not possible to assume after only one round that $N \approx \frac{m^2}{2 \cdot 2^n}$, since in this example, with probability 1/4 over f_1, we will have $N \approx \frac{2m^2}{2^n}$. Here again, when $m^2 = \mathcal{O}(2^n)$, we will distinguish with non-negligible probability the R'_i from a random sequence.

Remark:
In this example F.2, if we take m such that $m = 2 \cdot 2^{n-v}$, i.e. we use all the possible L_i having the v last bits at zero, then we get $N \approx \frac{m^2}{2 \cdot 2^{n-v}} \approx m$. Here N is of the same order of magnitude than m (instead of $\frac{m^2}{2 \cdot 2^n}$), but the probability for f_1 will be only about $\frac{1}{2^v} = \frac{m}{2 \cdot 2^n}$.

F.3 Number of multiple collisions after one round

We will generalize what we did in Section F.2 above , to multiple collisions.

Theorem F.3 *For all $k \in N^*$ and for all $[L_i, R_i]$, $1 \leq i \leq m$ (such that $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$) the number of $(f_1, i_1, i_2, \ldots, i_k)$ such that $R'_{i_1} = R'_{i_2} = \cdots = R'_{i_k}, i_1 < i_2 < \cdots < i_k$, is $\leq |F_n| \frac{m^k}{k! \cdot 2^{(k-1)n}}$.*

Proof of Theorem F.3
$R'_{i_1} = R'_{i_2} = \cdots = R'_{i_k}$ means $L_{i_1} \oplus f_1(R_{i_1}) = L_{i_2} \oplus f_1(R_{i_2}) = \cdots = L_{i_k} \oplus f_1(R_{i_k})$. This implies that $R_{i_1}, R_{i_2}, \ldots, R_{i_k}$ are pairwise distinct (because $L_i = L_j$ and $R_i = R_j \Rightarrow i = j$). Thus, when the k-tuple $(i_1, i_2, \ldots, i_k)$ is fixed, the number of f_1 such that $R'_{i_1} = R'_{i_2} = \cdots = R'_{i_k}$ is $\frac{|F_n|}{\cdot 2^{(k-1)n}}$. Therefore, since we have $\leq m^k/k!$ values $(i_1, i_2, \ldots, i_k)$ with $i_1 < i_2 < \cdots < i_k$, and such that the $R_{i_1}, R_{i_2}, \ldots, R_{i_k}$ are pairwise distinct, the total number of $(f_1, i_1, i_2, \ldots, i_k)$ is $\leq |F_n| \frac{m^k}{k! \cdot 2^{(k-1)n}}$ as claimed.

Corollary F.6 *Let $\lambda > 0$. Let M be the number of functions $f_1 \in F_n$ such that the number of $(i_1, i_2, \ldots, i_k)$ with $i_1 < i_2 < \cdots < i_k$ such that $R'_{i_1} = R'_{i_2} = \cdots = R'_{i_k}$ is $\geq \frac{\lambda m^k}{k! \cdot 2^{(k-1)n}}$.*
Then, $\forall \lambda > 0$ and for all (pairwise distinct) $[L_i, R_i], 1 \leq i \leq m$, we have $M \leq \frac{|F_n|}{\lambda}$

Proof: This follows immediately from Theorem F.3.

Corollary F.7 *With $\lambda = 2^{n\varepsilon}, \varepsilon > 0$ we get: the number M of of functions f_1 such that [the number of $(i_1, i_2, \ldots, i_k), i_1 < i_2 < \cdots < i_k$ such that $R'_{i_1} = R'_{i_2} = \cdots = R'_{i_k}$ is $\geq \frac{m^k}{k! 2^{(k-1-\varepsilon)n}}$] is $M \leq \frac{|F_n|}{2^{n\varepsilon}}$.*

Corollary F.8 *Therefore, when f_1 is chosen at random in F_n, we can assume (with probability $1 - \frac{1}{2^{n\varepsilon}}$) that the number N_k of $(i_1, i_2, \ldots, i_k), i_1 < i_2 < \cdots < i_k$ such that $R'_{i_1} = R'_{i_2} = \cdots = R'_{i_k}$ is $N_k \leq \frac{m^k}{k! 2^{(k-1-\varepsilon)n}}$.*

Corollary F.9 *For all fixed θ, and for all $\varepsilon > 0$, we can assume (with probability $\geq 1 - \frac{\theta}{2^{n\varepsilon}}$) that for all $k, 2 \leq k \leq \theta + 1$, we have:*

$$N_k \leq \frac{m^k}{k! 2^{(k-1-\varepsilon)n}}.$$

Two rounds

F.4 Number of multiple collisions after two rounds

Let $R''_i = R_i \oplus f_2(R'_i)$.
Let N_k be the number of $(i_1, i_2, \ldots, i_k), i_1 < i_2 < \cdots < i_k / R''_{i_1} = R''_{i_2} = \cdots = R''_{i_k}$. We want to evaluate N_k. From Corollary F.5 in Section F.2 above, we know that (with probability $1 - \frac{1}{2^{n\varepsilon}}$) the number of pairwise distinct R'_i values is $\geq m - \frac{m(m-1)}{2 \cdot 2^{n(1-\varepsilon)}}$.
Let us first consider all these pairwise distinct R'_i values. The R''_i values limited to such indices i are exactly a set of independent random variables of I_n (this is because when f_2 is randomly chosen in F_n, the $f_2(R'_i)$ are random if all the R'_i are pairwise distinct).

From these values we will get about

$$\frac{\left(m - \mathcal{O}\left(\frac{m^2}{2^{n(1-\varepsilon)}}\right)\right)^k}{k!2^{(k-1)n}}$$

k-collisions $R''_{i_1} = R''_{i_2} = \cdots = R''_{i_k}$, i.e.

$$\frac{m^k}{k!2^{(k-1)n}} - \mathcal{O}\left(\frac{m^{k+1}}{2^{(k-\varepsilon)n}}\right) + \mathcal{O}\left(\frac{m^{k/2}}{2^{(k-1)n/2}}\right)$$

collisions.
(Remark: the term $\mathcal{O}\left(\frac{m^{k/2}}{2^{(k-1)n/2}}\right)$ is the square root of the variance for random values).
We call these collisions "collisions of first case".
Now, when all the $f_2(R'_i)$ are fixed for all the independent R'_i values, this will also automatically generate some other k-collisions

$$R_{i_1} \oplus f_2(R'_{i_1}) = R_{i_2} \oplus f_2(R'_{i_2}) = \cdots = R_{i_k} \oplus f_2(R'_{i_k}),$$

these being due to the fact that $R'_{i_1} = R'_i, i \neq i_1$. For (i_1, i) such that $R'_{i_1} = R'_i, i \neq i_1$, we have $\mathcal{O}\left(\frac{m^2}{2^{n(1-\varepsilon)}}\right)$ possibilities (cf. Corollary F.4, with probability $1 - \mathcal{O}\left(\frac{1}{2^{n\varepsilon}}\right)$). For $i_2, i_3, \ldots, i_k$ we have at most m^{k-1} possibilities.
Now, when $i, i_1, i_2, \ldots, i_k$ are fixed, we have exactly $\frac{|F_n|}{2^{n(k-1)}}$ functions f_2 such that $R_{i_1} \oplus f_2(R'_{i_1}) = R_{i_2} \oplus f_2(R'_{i_2}) = \cdots = R_{i_k} \oplus f_2(R'_{i_k})$ (because we must have here all the R'_{i_l} pairwise distinct, $1 \leq l \leq k$). Therefore, the number of $(f_2, i_1, i_2, \ldots, i_k)$ such that we have a "k-collision of the second case" is $\leq \frac{|F_n|}{2^{n(k-1)}} \mathcal{O}\left(\frac{m^{k+1}}{2^{n(1-\varepsilon)}}\right)$.
Therefore, with probability $\geq 1 - \mathcal{O}\left(\frac{1}{2^{n\varepsilon}}\right)$ the function f_2 is such that the number of "k-collision of the second case" is $\leq \mathcal{O}\left(\frac{m^{k+1}}{2^{n(k-2\varepsilon)}}\right)$.
From here we get:

Theorem F.4 *$\forall k \geq 2$, for all $\varepsilon > 0$, with probability $\geq 1 - \mathcal{O}\left(\frac{1}{2^{n\varepsilon}}\right)$ the function f_2 is such that the number N_k of $R_{i_1} \oplus f_2(R'_{i_1}) = R_{i_2} \oplus f_2(R'_{i_2}) = \cdots = R_{i_k} \oplus f_2(R'_{i_k})$ (i.e. $R''_{i_1} = R''_{i_2} = \ldots = R''_{i_k}$) with $i_1 < i_2 < \cdots < i_k$, is*

$$N_k \leq \frac{m^k}{k!2^{(k-1)n}} + \mathcal{O}\left(\frac{m^{k+1}}{2^{(k-2\varepsilon)n}}\right) + \mathcal{O}\left(\frac{m^{k/2}}{2^{(k-1)n/2}}\right).$$

Remark: Here the dominant term is $\frac{m^k}{k!2^{(k-1)n}}$ and it is the same as for truly random values R''_i chosen in I_n.

Corollary F.10 *For all fixed θ, and for all $\varepsilon > 0$, we can assume that (with probability $\geq 1 - \mathcal{O}\left(\frac{1}{2^{n\varepsilon}}\right)$) that for all $k, 2 \leq k \leq \theta + 1$, we have: $N_k \leq \frac{m^k}{k!2^{(k-1)n}} + \mathcal{O}\left(\frac{m^{k+1}}{2^{(k-2\varepsilon)n}}\right) + \mathcal{O}\left(\frac{m^{k/2}}{2^{(k-1)n/2}}\right)$.*

F.5 Conclusion for Section F

1. After one round, $\forall \varepsilon > 0$ the R'_i values have at most $\frac{m^k}{k!2^{(k-1)n}} \cdot 2^{\varepsilon n}$ k-collisions with probability $1 - \frac{1}{2^{n\varepsilon}}$ (or $\forall \theta$, at most $m\theta^k$ k-collisions with probability $\geq 1 - \frac{m^{\theta+1}}{2^{n\theta}(\theta+1)!}$).

   However these values R'_i can be not random at all, for example if $R_i = C$ for some fixed constant C, then for all i, j we have $R'_i \oplus R'_j = L_i \oplus L_j$.

2. After two rounds, the R''_i values have a number of k-collisions that is very close to the number obtained for truly random variables. Here the deviation is at most by a factor of $1 + \mathcal{O}\left(\frac{m}{2^{(1-2\varepsilon)n}}\right)$ and with probability $1 - \mathcal{O}\left(\frac{1}{2^{n\varepsilon}}\right)$.

   Moreover, for two rounds, most of these values R''_j are indeed random, and most means that the proportion of non-random values is $\leq \frac{m}{2^{n(1-\varepsilon)}}$.

   However these values R''_i are not all random since the number of (i, j) such that $R''_i \oplus R_i = R''_j \oplus R_j$ is generally double compared with random R''_i values.

G Appendix G: Proof of Theorem 7.1

This part is not yet written.

H Appendix H: Proof of Theorem 7.2

This part is not yet written.

I Appendix I: Proof of Theorem 7.3

Let $a'_i = b_i$ if $a_i \geq b_i$ and $a'_i = 0$ if $a_i < b_i$. Then if we prove theorem 7.3 for a'_i instead of a_i, we will get it for a_i since $\forall i$, $1 \leq i \leq N$, $a_i \geq a'_i$ (because $a_i \geq 0$), so $\sum_{i=1}^N a_i \geq \sum_{i=1}^N a'_i$. Let $X = \sum_{i=1}^N a'_i$. We have $\forall i$, $1 \leq i \leq n$, $E(a'_i) \geq b_i(1-\varepsilon)$. So $E(X) \geq (\sum_{i=1}^N b_i)(1-\varepsilon)$ (1).

Let p be the probability that $X < (\sum_{i=1}^N b_i)(1-\lambda\varepsilon)$. So with probability $1-p$ we have: $X \geq (\sum_{i=1}^N b_i)(1-\lambda\varepsilon)$. However we always have (i.e. probability 1) that $X \leq \sum_{i=1}^N b_i$. So $E(X) \leq p \cdot (\sum_{i=1}^N b_i)(1-\lambda\varepsilon) + (1-p) \cdot \sum_{i=1}^N b_i$.

From (1) we get: $1 - \varepsilon \leq p \cdot (1-\lambda\varepsilon) + (1-p)$. So: $p \leq 1/\lambda$, as claimed in theorem 7.3.

Remark The hypothesis $a_i \geq 0$ is necessary in theorem 7.3. For example, let $N = 2$, $\varepsilon = 1/2$, $b_1 = b_2 = 1$,

$$\begin{cases} a_1 = b_1 \Leftrightarrow a_2 = -2 \text{ with probability } 1/2 \\ a_2 = b_2 \Leftrightarrow a_1 = -2 \text{ with probability } 1/2 \end{cases}$$

then $a_1 + a_2$ is always < 0 (since $a_1 + a_2 = -1$) and theorem 7.3 is not satisfied with $\lambda = 3/2$ for example.

J Appendix J: Proof of Theorem 8.1

This part is not yet written.

K Appendix K: Proof of the theorems of Section 9

This part is not yet written.