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

Jacques Patarin, University of Versailles

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 [17]. 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.

An extended version of this paper is available from the author.

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 [10]). 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, 16, 17]. However in these papers the proven security is still $m \ll 2^{n/2}$. In [18], 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 [17], 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]).

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.

[1] In [19] such unbalanced Feistel schemes are studied under the angle of linear and differential cryptanalysis.

- For any $a, b \in I_n$, $[a, b]$ will be the string of length $2n$ of I_{2n} which is the concatenation of a and b.
- For $a, b \in I_n$, $a \oplus b$ stands for bit by bit exclusive or of a and b.
- Let f_1 be a function of F_n. Let L, R, S and T be four n-bit strings in I_n. Then by definition

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

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

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

The permutation 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 pseudorandom 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 31 (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 $[L_i, R_i], [S_i, T_i],\ 1 \le i \le m$ in input and outputs 0 or 1, we have that the expectation of $|P_1 - P_1^*|$ when the $[L_i, R_i],\ 1 \le i \le m$, are randomly chosen satisfy:

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

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 $i \ne j \Rightarrow L_i \ne L_j\ or R_i \ne R_j$, 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 31 is given in [15].
5. From this Theorem 31 we can prove that in order to attack Ψ^2 with KPA, we must have $m \ge$ about $2^{n/2}$ (see [15]).

Theorem 32 (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 $|E| \ge (1-\beta) \cdot 2^{2nm}$. If :
(1) For all sequences $[L_i, R_i], 1 \le i \le m$, of m pairwise distinct elements of I_{2n} and for all sequences $[S_i, T_i], 1 \le i \le m$, of E
we have: $H \ge \dfrac{|F_n|^p}{2^{2nm}}(1-\alpha)$

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

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

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 analyse the m values given by its oracle gates.
3. A proof of this Theorem 32 (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 32 (see [8], [10] or [15]), 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 33 (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: $H \geq \dfrac{|F_n|^p}{2^{2nm}}(1-\alpha)$

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

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

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 33 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 33 (see [8], [10] or [15]) we can prove that in order to attack Ψ^4 with CPCA we must have $m \geq$ about $2^{n/2}$.

Theorem 34 (Variant of Theorem 33, 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 34 can be found in [10] p. 38.
2. Theorem 33 is a special case of Theorem 34 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 34 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 31 for KPA on Ψ^4, Theorem 32 for CPA on Ψ^7 (and our result on Ψ^5), Theorem 33 for CPCA on Ψ^{10}, and Theorem 34 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 31, 32, 33 and 34 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 [15].

An exact formula for *H* for 4 rounds

Let P_i and Q_i, with $1 \le i \le m$, 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:

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

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

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 51 *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 $1 \le i < j \le m$.*

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

Definition 52 *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:

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

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

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

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

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 61 *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 62 *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 63 *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 64 *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 65 *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 66 *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. 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:

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

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 81 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) Analysing sets of equations $P_i \oplus P_j = \lambda_k$

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

b) Avoiding "circles" and "long lines"

Theorem 71 *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 [15] 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 [15]).

c) We can assume that the λ_k are generally random

Theorem 72 *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 $\lambda_k = L_i \oplus L_j$, or $\lambda_k = S_i \oplus S_j$, with no circle in the L or in the S variables that appear in the λ_k. Then if:*
(1a) The $[L_i, R_i, S_i, T_i]$ are random variables of I_n. or:
(1b)The $[S_i, T_i]$ are random variables of I_{2n} and the $[L_i, R_i]$ are obtained after a $\Psi^3(f_1, f_2, f_3)$ where f_1, f_2, f_3 are randomly chosen in F_n. or:
(1c)The $[L_i, R_i]$ are obtained after a $\Psi^3(f_1, f_2, f_3)$ and the $[S_i, T_i]$ are obtained after a $\Psi^3(g_1, g_2, g_3)$, where f_1, f_2, f_3, g_1, g_2, g_3 are randomly chosen in F_n. Then:
The probability to distinguish $\lambda_1, \lambda_2, \ldots, \lambda_a$ from a truly random values of I_n is $\leq 1 - \mathcal{O}(\frac{a^2}{2^{2n}})$ (with no limitation in the computing power).

Proof: See [15].

d) A general result of probability

Theorem 73 *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 [15].

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

Definition 81 *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 $\lambda_1, \lambda_2, \ldots, \lambda_a$ and $a+1 \leq \alpha \leq 2a$.

Definition 82 *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 $\lambda_1, \lambda_2, \ldots, \lambda_a$.*

Definition 83 *We will denote by ξ the maximum number of indices that are in the same block.*

Example. 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 84 *For such a system (A), when $\lambda_1, \lambda_2, \ldots, \lambda_a$ are fixed, we will denote by h_α the number of $P_1, P_2, \ldots, P_\alpha$ 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 85 *We will denote by J_α the number of $P_1, P_2, \ldots, P_\alpha$ in I_n such that: $\forall i, j,\ i \neq j \Rightarrow P_i \neq P_j$.*

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

Theorem 81 *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 $\lambda_1, \lambda_2, \ldots, \lambda_a$ 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 $\sigma \leq J_\alpha \cdot \mathcal{O}\left(\frac{\alpha\sqrt{\alpha}}{2^n\sqrt{2^n}}\right)$.

Proof: See [15]
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 $\lambda_1, \lambda_2, \ldots, \lambda_a$ is $\neq 0$. So this condition is in $1 - \mathcal{O}(\frac{\alpha}{2^n})$.
¿From Bienaymé-Tchébichef Theorem, we get :

Corollary 81 *For all $\lambda > 0$, with a probability $\geq 1 - \mathcal{O}(\frac{1}{\lambda^2}) - \mathcal{O}(\frac{\alpha}{2^n})$, 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 82 *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 $\lambda_1, \lambda_2, \ldots, \lambda_k$ 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 $\lambda_1, \lambda_2, \ldots, \lambda_a$ 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 [15]

Conjecture 81 *This Theorem 82 is still true when $\alpha \ll 2^n$ (instead of $\alpha^3 \ll 2^{2n}$).*

This conjecture 81 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 91 we get the following theorems on H (see [15] for the proofs).

Theorem 91 *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 distincts and the $[S_i, T_i]$ are pairwise distincts. 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 92 *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 distincts and the $[S_i, T_i]$ are pairwise distincts. Then for Ψ^7 we have:*
There is a subset E of I_{2n}^m with $|E| \geq (1 - \mathcal{O}(\frac{m}{2^n}) - \mathcal{O}(\frac{m^{\theta+1}}{2^{n\theta}}))$ 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 93 *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 distincts and the $[S_i, T_i]$ are pairwise distincts. Then for Ψ^{10} we have:*

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

Security results against cryptographic attacks
Finally our cryptographic results on 4,7 and 10 rounds are just a direct consequence of Theorem 91,92,93 and of Theorem 31, 32 and 33: 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 101 *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 [15] 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 $f_i \in I_{2n-1} \rightarrow I_1$. 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.

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.

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

References

1. William Aiollo, 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*, [RS]A'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. J. Patarin, *Luby-Rackoff: 7 Rounds are Enough for* $\mathbf{2^{n(1-\varepsilon)}}$ *Security*. Extended version of this paper. Available from the author.
16. S. Patel, Z. Ramzan and G. Sundaram, *Toward making Luby-Rackoff ciphers optimal and practical*, FSE'99, LNCS, Springer, 1999.
17. J. Pieprzyk, *How to construct pseudorandom permutations from Single Pseudorandom Functions*, Eurocrypt'90, LNCS 473, Springer, pp. 140-150.
18. Z. Ramzan, L. Reyzin, *On the Round Security of Symmetric-Key Cryptographic Primitives*, Crypto 2000, LNCS 1880, Springer, pp. 376-393.
19. B. Schneier and J. Kelsey, *Unbalanced Feistel Networks and Block Cipher Design*, FSE'96, LNCS 1039, Springer, pp. 121-144.

Appendix: Summary of the known results on $\boldsymbol{\Psi^k}$

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

	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 $\leq \mathcal{O}(2^{2n})$	$\geq \mathcal{O}(2^{\frac{n}{2}})$ and $\leq \mathcal{O}(2^{2n})$	$\geq \mathcal{O}(2^{n(1-\varepsilon)})$ and $\leq \mathcal{O}(2^{2n})$

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

Remark: The result $\lambda \leq \mathcal{O}(2^{2n})$ is obtained due to the fact that Ψ^k permutations 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].