Luby - Rackoff: 5 Rounds are Enough for $2^{n-\epsilon}$ CPCA Security

Jacques Patarin
Université de Versailles
45 avenue des Etats-unis
78035 Versailles Cedex
France
Jacques.Patarin@prism.uvsq.fr

Abstract

We study adaptive chosen plaintext attacks (CPA) and adaptive chosen plaintext and chosen ciphertext attacks (CPCA) on random Feistel schemes.We denote by m the number of plaintext/ciphertext pairs, and by k the number of rounds.In their famous paper [2], M. Luby and C. Rackoff have completely solved the cases $m \ll 2^{n/2}$: the schemes are secure against all CPA attacks when $k \geq 3$ and against all CPCA attacks when $k \geq 4$.
In this paper we study the cases $m \ll 2^{n-\epsilon}$.We will show that in this case, $\forall \epsilon > 0$, the schemes are secure against all CPCA attacks when $k \geq 5$. This solves an open problem of [1], [8], and it improves the result of [8] where $2^{n(1-\epsilon)}$ security was proved for CPCA after 10 rounds (instead of 5 here). The number 5 of rounds is minimal since CPA attacks on 4 rounds are known when $m \geq o(2^{n/2})$ (see [1], [6]). Furthermore we have obtained an explicit and simple majoration for the distinguishing probability. Moreover for known plaintext attacks on 4 rounds, or for CPCA on 6 rounds, we also show that we have security when $m \ll \frac{2^n}{n}$ (instead of $2^{n-\epsilon}$).

1 Introduction

A "Luby - Rackoff construction with k rounds", which is also known as a "random Feistel cipher" is a Feistel cipher in which the round functions $f_1, \ldots, f_k$ are independently chosen as truly random functions (see section 2 for precise definitions).
Since the famous original paper [2] of M. Luby and C. Rackoff, these constructions have inspired a considerable amount of research. In [5] and [8] a summary of existing works on this topic is given.
We will denote by k the number of rounds and by n the integer such that the Feistel cipher is a permutation of $2n$ bits $\rightarrow 2n$ bits. In [2] it was proved that when $k \geq 3$ these Feistel ciphers are secure against all adaptative chosen plaintext attacks (CPA) when the number of queries (i.e. plaintext/ciphertext pairs obtained) is $m \ll 2^{n/2}$. Moreover when $k \geq 4$ they are secure against all adaptative chosen plaintext and chosen ciphertext attacks (CPCA) when the number of queries is $m \ll 2^{n/2}$.
These results are valid if the adversary has unbounded computing power as long as he does only m queries.
These results can be applied in two different ways: directly using k truly random functions $f_1, \ldots, f_k$ (that requires significant storage), or in a hybrid setting, in which instead of using k truly random functions $f_1, \ldots, f_k$, we use k pseudo-random functions. These two ways are both interesting for cryptography. The first way gives "locally random permutations" where we have proofs of security without any unproven hypothesis (but a lot of storage), and the second way gives constructions for block encryption schemes where the security can be relied on a pseudo-random number generator, or on any one-way function.
In this paper, we will study security when $m \ll 2^{n-\epsilon}$ where ϵ is any real number > 0 (instead of $m \ll 2^{n/2}$). For this we must have $k \geq 5$, since for $k \leq 4$ some CPA attacks when $m \geq o(2^{n/2})$ exist (see [1], [6]). Moreover the bound $m \ll 2^n$ is the larger bound that we can get, since an adversary with unlimited computing power can always distinguish a k-round random Feistel scheme from a random permutation with $o(k \cdot 2^n)$ queries and $o(2^{kn2^n})$ computations by simply guessing all the round functions (it is also possible to do less computing by using collisions, see [7]).
The bound $m \ll 2^{n/2}$ is called the 'birthday bound', i.e. it is about the square root of the optimal bound against an adversary with unbounded computing power. In [1] W. Aiello and R. Venkatesan have found a construction of locally random functions ('Benes') where the optimal bound ($m \ll 2^n$) is obtained instead of the birthday bound. However here the functions are not permutations. Similarly, in [3], U. Maurer has found some other construction of locally random functions (not permutations) where he can get as close as wanted to the optimal bound (i.e. $m \ll 2^{n(1-\epsilon)}$ and for all $\epsilon > 0$ we have a construction). In [5] the security of unbalanced Feistel schemes is studied. A security proof in $2^{n(1-\epsilon)}$ 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.
The main result of this paper will be that 5-round random Feistel schemes resist all CPCA attacks when $m \ll 2^n$. Here we have the optimal bound, and we have permutations. This solves an open problem of [1], [6]. It also improves the results of [4] in which the 2^n security is only obtained when the number of rounds tends to infinity, and the result of [8] where $2^{n(1-\epsilon)}$ security was proved for CPCA after 10 rounds (instead of 2^n security after 5 rounds here) and for CPA after 7 rounds (instead of 5 here). Moreover we will obtain in this paper an explicit and simple majoration for the distinguishing probability: the probability to distinguish a 5-round random Feistel scheme from a random permutation of $2n$ bits $\rightarrow 2n$ bits with a CPCA attack is

$$|P_1 - P_1^{**}| \leq \frac{m}{2^{2n}} + \frac{16m^3}{2^{3n}} \frac{1}{1 - \frac{4m}{2^n}}.$$

So when $m \ll 2^n$ this probability is negligible (to be compared with $|P_1 - P_1^*| \leq \frac{m^2}{2^n}$ of Luby and Rackoff where m must be $\ll 2^{n/2}$ in order to have $m^2/2^n$ negligible).

2 Notations

These notations are very similar to those of [4], [8] (we just introduce some specific notations for the internal values of 5-round Feistel schemes).

General 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 $\Psi^k(f_1, \ldots, f_k)$ is called a 'Feistel scheme with k rounds' or shortly Ψ^k. When $f_1, \ldots, f_k$ are randomly and independently chosen in F_n, then $\Psi^k(f_1, \ldots, f_k)$ is called a 'random Feistel scheme with k rounds' or a 'Luby-Rackoff construction with k rounds'.

Notations for 5 rounds

- We will denote by $[L_i, R_i]$, $1 \leq i \leq m$, the m cleartexts. These cleartexts can be assumed to be pairwise distinct, i.e. $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$.
- We call "index" any integer between 1 and m.
- $[R_i, X_i]$ is the output after one round, i.e.
$$\forall i, 1 \leq i \leq m, X_i = L_i \oplus f_1(R_i).$$
- $[X_i, Y_i]$ is the output after two rounds, i.e.
$$\forall i, 1 \leq i \leq m, Y_i = R_i \oplus f_2(X_i) = R_i \oplus f_2(L_i \oplus f_1(R_i)).$$
- $[Y_i, Z_i]$ is the output after three rounds, i.e.
$$\forall i, 1 \leq i \leq m, Z_i = X_i \oplus f_3(Y_i) = L_i \oplus f_1(R_i) \oplus f_3(Y_i)).$$
- $[Z_i, S_i]$ is the output after four rounds, i.e.
$$\forall i, 1 \leq i \leq m, S_i = Y_i \oplus f_4(Z_i).$$
- $[S_i, T_i]$ is the output after five rounds, i.e.
$$\forall i, 1 \leq i \leq m, T_i = Z_i \oplus f_5(S_i).$$

3 The proof strategy

Definition We will say that we have 'a circle in X, Y, Z' if there are k indices $i_1, \ldots, i_k$ with $k \geq 3$ and such that:

1. $i_k = i_1$ and $i_1 \neq i_2, \ldots, i_{k-1} \neq i_k$.
2. $\forall \lambda$, $1 \leq \lambda \leq k-2$ we have one of the three following conditions:
   - $X_{i_\lambda} = X_{i_{\lambda+1}}$ and ($Y_{i_{\lambda+1}} = Y_{i_{\lambda+2}}$ or $Z_{i_{\lambda+1}} = Z_{i_{\lambda+2}}$)
   - $Y_{i_\lambda} = Y_{i_{\lambda+1}}$ and ($X_{i_{\lambda+1}} = X_{i_{\lambda+2}}$ or $Z_{i_{\lambda+1}} = Z_{i_{\lambda+2}}$)
   - $Z_{i_\lambda} = Z_{i_{\lambda+1}}$ and ($X_{i_{\lambda+1}} = X_{i_{\lambda+2}}$ or $Y_{i_{\lambda+1}} = Y_{i_{\lambda+2}}$)

Example If $X_1 = X_2$ and $Y_1 = Y_2$, then we have a circle in X, Y, Z. If $X_1 = X_2$, $Y_2 = Y_3$, $Z_3 = Z_1$ and then we have a circle in X, Y, Z.

We will prove the following theorems.

Theorem 3.1 *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, f_2, f_3) such that we have a circle in X, Y, Z with at least one equation $Z_i = Z_j$ is less than*

$$|F_n|^3 \cdot \frac{2m^2}{2^{2n}} \cdot \frac{1}{1 - \frac{4m}{2^n}}.$$

Remark 1 This shows that when $m \ll 2^n$ and when f_1, f_2, f_3 are randomly chosen, the probability to have a circle in X, Y, Z is negligible.

Remark 2 In appendix B we will show that the condition 'with at least one equation $Z_i = Z_j$' is important: sometime we cannot avoid some circles in X, Y.

Theorem 3.2 *Let assume that we have two black boxes A and B.*
Black box A computes all the X_i, Y_i, Z_i values (from the $[L_i, R_i]$, $1 \leq i \leq m$ and from three functions f_1, f_2, f_3) and it outputs:

1. *all the (i, Z_i) values, $1 \leq i \leq m$.*
2. *for all i, j, $i < j$ such that $Z_i = Z_j$, it outputs $(i, j, Y_i \oplus Y_j)$.*

Black box B computes also all the X_i, Y_i, Z_i values (from the same $[L_i, R_i]$ and f_1, f_2, f_3) and it outputs:

1. *all the (i, Z_i) values, $1 \leq i \leq m$.*
2. *for all i, j, $i < j$ such that $Z_i = Z_j$, it randomly generates a value λ_k in $I_n - \{0\}$ and it outputs (i, j, λ_k).*

Then for all $[L_i, R_i]$, $1 \leq i \leq m$ (such that $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$), when (f_1, f_2, f_3) are randomly chosen in F_n, the probability to distinguish black box A from black box B is less than the probability to have a circle in X, Y, Z when (f_1, f_2, f_3) are randomly chosen in F_n.

Remark 1 Here all the $[L_i, R_i]$ values are always public. This theorem 3.2 shows that when $Z_i = Z_j$, then the $Y_i \oplus Y_j$ values are not distinguishable from truly random values of $I_n - \{0\}$, even if all the Z_i are given.

Remark 2 However we do not say that the Z_i values are not distinguishable from random values. We do not say either that the (i, j) such that $Z_i = Z_j$ do not have some special relations. This theorem is only on the $Y_i \oplus Y_j$ values and only when $Z_i = Z_j$.

Theorem 3.3 *Let assume that we have two black boxes C and D.*
Black box C computes all the X_i, Y_i, Z_i, S_i values and it outputs:

1. *all the (i, S_i) values, $1 \leq i \leq m$.*
2. *for all i, j, $i < j$ such that $S_i = S_j$, it outputs $(i, j, Z_i \oplus Z_j)$.*

Black box D computes also all the X_i, Y_i, Z_i, S_i values and it outputs:

1. *all the (i, S_i) values, $1 \leq i \leq m$.*
2. *for all i, j, $i < j$ such that $S_i = S_j$, it randomly generates a value λ_k in $I_n - \{0\}$ and it outputs (i, j, λ_k).*

Then for all $[L_i, R_i]$, $1 \leq i \leq m$ (such that $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$), when (f_1, f_2, f_3, f_4) are randomly chosen in F_n, the probability to distinguish black box C from black box D is less than the probability to have a circle in X, Y, Z when (f_1, f_2, f_3) are randomly chosen in F_n.

Remark This theorem 3.3 is exactly the same as theorem 3.2 but for one more round. From theorem 3.2 and theorem 3.3 we will prove:

Theorem 3.4 *For all $[L_i, R_i]$, $1 \leq i \leq m$ (such that $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$), when $(f_1, f_2, f_3, f_4, f_5)$ are randomly chosen in F_n, the probability to distinguish the m values obtained in a CPCA attack from values randomly chosen in I_{2n}, such that $i \neq j \Rightarrow (L_i \neq L_j$ or $R_i \neq R_j)$ and $(S_i \neq S_j$ or $T_i \neq T_j)$, is less than 2 times the probability to have a circle in X, Y, Z when (f_1, f_2, f_3) are randomly chosen in F_n.*
So, from theorem 3.1, this probability is less than

$$\frac{m^2}{2^{2n}} + \frac{16m^3}{2^{3n}} \cdot \frac{1}{1 - \frac{4m}{2^n}}$$

so when $m \ll o(2^n)$ this probability is negligible.

4 Lines of equalities in X

In order to prove theorem 3.1, we will first study some systems of equalities $X_i = X_j$, $i \neq j$.

Theorem 4.1 *For all integer $\theta \geq 1$, and for all pairwise distinct $[L_i, R_i]$, $1 \leq i \leq m$, when f_1 is randomly chosen in F_n, the probability P to have $\theta + 1$ indices $i_1 < i_2 < \ldots < i_{\theta+1}$ such that $X_{i_1} = X_{i_2} = \ldots = X_{i_{\theta+1}}$ satisfies*

$$P \leq \frac{m^{\theta+1}}{(\theta+1)!2^{n\theta}}.$$

Proof $X_i = X_j \Leftrightarrow L_i \oplus f_1(R_i) = L_j \oplus f_1(R_j)$. If $i \neq j$, this implies $R_i \neq R_j$ (because $R_i = R_j$ and $L_i = L_j \Rightarrow i = j$). So when i and j are fixed the number of functions f_1 that satisfy $X_i = X_j$ is 0 if $R_i = R_j$, and $\frac{|F_n|}{2^n}$ if $R_i \neq R_j$. So this number is always less than $\frac{|F_n|}{2^n}$. Now for (i, j), $i < j$, we have $\frac{m(m-1)}{2}$possibilities. Similarly, when $i_1, i_2, \ldots, i_{\theta+1}$ are fixed, $X_{i_1} = X_{i_2} = \ldots = X_{i_{\theta+1}} \Rightarrow R_{i_1}, R_{i_2}, \ldots, R_{i_{\theta+1}}$ have $\theta+1$ pairwise distinct values. So the number of functions f_1 that satisfy $X_{i_1} = X_{i_2} = \ldots = X_{i_{\theta+1}}$ is less than $\frac{|F_n|}{2^{n\theta}}$. Since we have at most $\frac{m^{\theta+1}}{(\theta+1)!}$ possibilities for $(i_1, \ldots, i_\theta)$, we see that we have at most $\frac{m^{\theta+1}}{(\theta+1)!2^{n\theta}}|F_n|$ functions f_1 such that there exist $i_1 < i_2 < \ldots < i_{\theta+1}$ such that $X_{i_1} = X_{i_2} = \ldots = X_{i_{\theta+1}}$.

Application We will fix such an integer θ (θ will be near n, or $log(m)$, at the end of this paper). So we can assume, with probability $\geq 1 - \frac{m^{\theta+1}}{(\theta+1)!2^{n\theta}}$, that when i is fixed, the number of indices j $j \neq i$ such that $X_i = X_j$, is always $\leq \theta$. When f_1 has this property we will say that f_1 has 'property X'.

5 Comparing the proof strategies of [8] and of this paper

The proof strategy of [8], to prove that Ψ^{10} resist all CPCA attacks when $m \ll o(2^{n-\epsilon})$, $\forall \epsilon > 0$, consists mainly of:

1. showing that for all pairwise distinct $[L_i, R_i]$, $1 \leq i \leq m$, for all pairwise distinct $[S_i, T_i]$, $1 \leq i \leq m$, and for all integer $\theta \geq 1$, the number H of $f_1, \ldots, f_{10} \in F_n$ such that$\forall i$, $1 \leq i \leq m$, $\Psi^{10}(f_1, \ldots, f_{10})[L_i, R_i] = [S_i, T_i]$ satisfies
$$H \geq \frac{|F_n|^{10}}{2^{2nm}} \left(1 - o\left(\frac{m}{2^n}\right) - o\left(\frac{m^{\theta+1}}{2^{n\theta}}\right)\right)$$
(cf theorem 9.3 of [8]).
2. To obtain this, the main tool of [8] is to study systems of equations $P_i \oplus P_j = \lambda_k$ where the λ_k are fixed, and where we look for pairwise distinct P_i solutions.

In this paper our proof strategy is different.

First, we do not show that for Ψ^5 the number H of $f_1, \ldots, f_5$ such that $\Psi^5(f_1, \ldots, f_5)[L_i, R_i] = [S_i, T_i]$, $\forall i$, $1 \leq i \leq m$, is
$$\geq \frac{|F_n|^5}{2^{2nm}} \left(1 - o\left(\frac{m}{2^n}\right) - o\left(\frac{m^{\theta+1}}{2^{n\theta}}\right)\right)$$
for all possible pairwise distinct $[L_i, R_i]$ and all possible pairwise distinct $[S_i, T_i]$. We will show that for all possible pairwise distinct $[L_i, R_i]$, the probability to distinguish the $[S_i, T_i]$ values, $1 \leq i \leq m$, from m pairwise distinct truly random values is negligible when $f_1, \ldots, f_5$ are randomly chosen. This is a less strong property, and it will be easier to prove, and it is exactly the property that we need to avoid the cryptographic attacks, as we show in this paper.

Second, we completely avoid the difficult analysis of the systems of equations $P_i \oplus P_j = \lambda_k$, where the P_i variables must be pairwise distinct. Instead we show that the probability to distinguish the $Y_i \oplus Y_j$ values (where the Y_i values are the values obtained after two rounds) from random values $\neq 0$ is negligible if we restrict the $Y_i \oplus Y_j$ given to indices (i,j) such that $Z_i = Z_j$ (where the Z_i values are the values obtained after three rounds).

Remark With the proof results of this paper we can obtain also another proof of theorem 9.3 of [8]. the general idea is that we will combine two Ψ^5 such that the inputs of first Ψ^5 are the pairwise distinct $[L_i, R_i]$, values the outputs of the second Ψ^5 are the pairwise distinct $[S_i, T_i]$ values. Moreover for the outputs of the first Ψ^5 which are equal with the inputs of the second Ψ^5, we will take any pairwise distinct $[A_i, B_i]$ values such that from these $[A_i, B_i]$ values the number H_1 of $f_1, \ldots, f_5$ such that $\Psi^5(f_1, \ldots, f_5)[L_i, R_i] = [A_i, B_i]$, $\forall i$, $1 \leq i \leq m$ and the number H_2 of $f_6, \ldots, f_{10}$ such that $\Psi^5(f_6, \ldots, f_{10})[A_i, B_i] = [S_i, T_i]$, satisfy

$$H_1 \geq \frac{|F_n|^5}{2^{2nm}} \cdot \left(1 - o\left(\frac{m^2}{2^{2n}}\right)\right) \text{ and } H_2 \geq \frac{|F_n|^5}{2^{2nm}} \cdot \left(1 - o\left(\frac{m^2}{2^{2n}}\right)\right).$$

For all pairwise distinct $[L_i, R_i]$ values, and for all pairwise distinct $[S_i, T_i]$ values, most of the $[A_i, B_i]$ values will satisfy these properties (i.e. we have more than $2^{2nm}\left(1 - o\left(\frac{m^2}{2^{2n}}\right)\right)$ possibilities for these $[A_i, B_i]$ values), so the number of $f_1, \ldots, f_{10}$ such that $\Psi^{10}[L_i, R_i] = [S_i, T_i]$, $1 \leq i \leq m$, is

$$\geq 2^{2nm}\left(1 - o\left(\frac{m^2}{2^{2n}}\right)\right) \cdot \frac{|F_n|^5}{2^{2nm}}\left(1 - o\left(\frac{m^2}{2^{2n}}\right)\right) \cdot \frac{|F_n|^5}{2^{2nm}}\left(1 - o\left(\frac{m^2}{2^{2n}}\right)\right)$$

$$\geq \frac{|F_n|^{10}}{2^{2nm}}\left(1 - o\left(\frac{m^2}{2^{2n}}\right)\right).$$

So we can obtain theorem 9.3 of [8] from our result (moreover with a better evaluation $o\left(\frac{m^2}{2^{2n}}\right)$ instead of $o\left(\frac{m}{2^n}\right) - o\left(\frac{m^{\theta+1}}{2^{n\theta}}\right)$, $\forall \theta$, and, if wanted, we can give an explicit function for the o). However, with our result, we need 10 rounds, as in [8], to have such a property valid <u>for all</u> (pairwise distinct) $[L_i, R_i]$ and (pairwise distinct) $[S_i, T_i]$.

6 Conclusion

In this paper we have solved an open problem of [1] and [8] about the properties of 5-round random Feistel schemes: 5-round random Feistel schemes can resist all interactive chosen plaintext and chosen ciphertext attacks when the number of queries is $m \ll 2^n$.
Moreover we have obtained a simple and explicit formula for the distinguishing probability (i.e. just an expression with a $o(2^n)$ or $(2^{n-\epsilon})$ as in [8] but an explicit formula).
We have also slightly improved the known results on 4-round random Feistel schemes with an explicit formula for the distinguishing probability against known plaintext attacks. Our proof strategy is very general and should be also efficient in the future to study different kinds of functions or permutation generators, such as, for example, Feistel scheme with a different group law than $\oplus$, or unbalanced Feistel schemes.

References

[1] W. Aiello and R. Venkatesan. Foiling Birthday Attacks in Length-Doubling Transformations-Benes: A Non-Reversible Alternative to Feistel. *EUROCRYPT '96* (Lecture Notes in Computer Science 1070), pp. 307–320, Springer-Verlag.

[2] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, vol. 17, n2, pp. 373–386, April 1988.

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

[4] U. Maurer and K. Pietrzak. he security of Many-Round Luby-Rackoff Pseudo-Random Permutations. *EUROCRYPT '03*, pp. –, Springer-Verlag.

[5] M. Naor and O. Reingold. On the Construction of pseudo-random perlutations: 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.

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

[7] J. Patarin. Generic Attacks on Feistel Schemes. *Asiacrypt '01* (Lecture Notes in Computer Science 2248), pp. 222–238, Springer-Verlag.

[8] J. Patarin. 7 Rounds are Enough for $2^{n(1-\epsilon)}$ Security. *Crypto '03* (Lecture Notes in Computer Science 2729), pp.513–529, Springer-Verlag.

[9] B. Schneier and J. Kelsey. Unbalanced Feistel Networks and Block Cipher Design. *FSE '96* (Lecture Notes in Computer Science 1039), pp. 121–144, Springer-Verlag.

A Summary of the known results on random Feistel schemes

KPA denotes known plaintext attacks. CPA denotes adaptive chosen plaintext attacks. CPCA denotes adaptive chosen plaintext and chosen ciphertext attacks.

A.1 Unbounded adversaries limited by m oracle queries

	Ψ	Ψ^2	Ψ^3	Ψ^4	$\Psi^k, k \geq 5$
KPA	1	$o(2^{n/2})$	$o(2^{n/2})$	$o(2^n)$	$o(2^n)$
CPA	1	2	$o(2^{n/2})$	$o(2^{n/2})$	$o(2^n)$
CPCA	1	2	3	$o(2^{n/2})$	$o(2^n)$

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

A.2 Adversaries bounded by λ computations (and also less than λ queries)

	Ψ	Ψ^2	Ψ^3	Ψ^4	Ψ^5	$\Psi^k, k \geq 6$
KPA	o(1)	$o(2^{n/2})$	$o(2^{n/2})$	$o(2^n)$	$\geq o(2^n)$ and $\leq o(2^{7n/4})$	$\geq o(2^n)$ and $\leq o(2^{2n})$
CPA	o(1)	o(1)	$o(2^{n/2})$	$o(2^{n/2})$	$\geq o(2^n)$ and $\leq o(2^{3n/2})$	$\geq o(2^n)$ and $\leq o(2^{2n})$
CPCA	o(1)	o(1)	o(1)	$o(2^{n/2})$	$\geq o(2^n)$ and $\leq o(2^{3n/2})$	$\geq o(2^n)$ and $\leq o(2^{2n})$

Figure 2: The minimum number λ of computations needed to distinguish Ψ^i from a random permutation of B_{2n}.

B A circle in X, Y that cannot be avoided

In this appendix B we will show that for some $[L_i, R_i]$, $1 \leq i \leq m$ (such that $i \neq j \Rightarrow L_i \neq L_j$ or $R_i \neq R_j$), when $m \ll 2^n$, when f_1, f_2, f_3 are randomly chosen in F_n, we will have with a very high probability some 4 pairwise distinct indices i, j, k, l such that:

$$(X_i = X_j) \text{ and } (X_k = X_l) \text{ and } (Y_i = Y_k) \text{ and } (Y_j = Y_l).$$

(This shows that in theorem 3.1 the condition 'with at least one equation $Z_i = Z_j$' is important: we cannot avoid some circle in X, Y for some $[L_i, R_i]$ values).
Here we want to evaluate the number of (f_1, f_2) such that

$$\begin{cases} L_i \oplus f_1(R_i) = L_j \oplus f_1(R_j) \\ L_k \oplus f_1(R_k) = L_l \oplus f_1(R_l) \\ R_i \oplus f_2(X_i) = R_k \oplus f_2(X_k) \\ R_i \oplus R_j \oplus R_k \oplus R_l = 0 \end{cases} \qquad (*)$$

(because, since $X_i = X_j$ and $X_k = X_l$ and $Y_i = Y_k$, $Y_j = Y_l$ is equivalent with $R_i \oplus R_j \oplus R_k \oplus R_l = 0$).
As an example, let assume that the chosen messages $[L_i, R_i]$, are all the possible messages such that: (here α is an integer parameter)

1. $R_i = R_1$ or $R_i = R_2$, where R_1 and R_2 are two values of I_n.
2. The first $n - \alpha$ bits of L_i are 0.

Then the number of pairwise distinct (i, j, k, l) such that $(R_i = R_k)$ and $(R_j = R_l \neq R_i)$ and $(L_i \oplus L_j \oplus L_k \oplus L_l = 0)$ is here $\simeq m \cdot \frac{m}{2} \cdot \frac{m}{2} \cdot 1$ (since for i we have m possibilities, then for j and k we have $\frac{m}{2}$ possibilities, and for l we have exactly one possibility: l is the index of the message such that $R_l = R_j$ and $L_l = L_i \oplus L_j \oplus L_k$). Now when (i, j, k, l) are fixed like this, $(*)$ is equivalent with:

$$\begin{cases} L_i \oplus f_1(R_i) = L_j \oplus f_1(R_j) \\ R_i \oplus f_2(X_i) = R_k \oplus f_2(X_k) \end{cases}.$$

So the number of (f_1, f_2) solution of $(*)$ is about $\frac{|F_n|^2}{2^{2n}}$. So when $\frac{m^3}{4} \gg 2^{2n}$, the probability to have such (f_1, f_2) solution of $(*)$ when (f_1, f_2) are randomly chosen is near 1 so with a high probability we will have a circle in X, Y.