Benes and Butterfly schemes revisited

Jacques Patarin, Audrey Montreuil
Université de Versailles
45 avenue des Etats-Unis
78035 Versailles Cedex - France

Abstract

In [1], W. Aiello and R. Venkatesan have shown how to construct pseudo-random functions of $2n$ bits $\rightarrow 2n$ bits from pseudo-random functions of n bits $\rightarrow n$ bits. They claimed that their construction, called "Benes", reaches the optimal bound ($m \ll 2^n$) of security against adversaries with unlimited computing power but limited by m queries in an adaptive chosen plaintext attack (CPA-2). However a complete proof of this result is not given in [1] since one of the assertions of [1] is wrong. Due to this, the proof given in [1] is valid for most attacks, but not for all the possible chosen plaintext attacks. In this paper we will in a way fix this problem since for all $\varepsilon > 0$, we will prove CPA-2 security when $m \ll 2^{n(1-\varepsilon)}$. However we will also see that the probability to distinguish Benes functions from random functions is sometime larger than the term in $\frac{m^2}{2^{2n}}$ given in [1]. One of the key idea in our proof will be to notice that, when $m \gg 2^{2n/3}$ and $m \ll 2^n$, for large number of variables linked with some critical equalities, the average number of solutions may be large (i.e. $\gg 1$) while, at the same time, the probability to have at least one such critical equalities is negligible (i.e. $\ll 1$).
Key Words: Pseudo-random functions, unconditional security, information-theoretic primitive, design of keyed hash functions.

1 Introduction

In [5], M. Luby and C. Rackoff have published their famous theorem: a 3-round Feistel scheme with three independent random round functions f_1, f_2, f_3 of n bits $\rightarrow n$ bits gives a pseudo-random function of $2n$ bits $\rightarrow 2n$ bits with security against all adaptive chosen plaintext attacks (CPA-2) when the number m of cleartext/ciphertext pairs chosen by the adversary satisfies $m \ll 2^{n/2}$ (even if the adversary has unbounded computing power). Since this paper [5], these constructions, or similar constructions, have inspired a considerable amount of research. In [10] a summary of existing works on this topic is given. 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 [11] and [1] it was proved that for 3 or 4-round Feistel schemes this bound $m \ll 2^{n/2}$ is the best we can get. One direction of research is to design or study various schemes where we have a better proved security than the birthday bound. This is what W. Aiello and R. Venkatesan have done in [1]: they have found a construction of locally random functions (called "Benes") where the optimal bound ($m \ll 2^n$) is obtained instead of the birthday bound. Here the functions are not permutations. Similarly, in [6] U. Maurer has found some other constructions of locally random functions (not permutations) where he can get as close as wanted to the optimal bound (i.e. $m \ll 2^{n(1-\varepsilon)}$ and for all $\varepsilon > 0$ he has a construction). In [10] the security of unbalanced Feistel schemes is studied and 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). However here this bound is basically again the birthday bound for this functions. In [14] J. Patarin obtained a security when $m \ll 2^n$ for 5-round Feistel scheme against all CPA-2 attacks.

In this paper we will study again the "Benes" schemes of [1]. First, we will notice that the proof of security given in [1] is valid for most chosen plaintext attacks, but is not valid for all chosen plaintext attacks. We will then in a way fix this problem. For known plaintext attacks, we will see that one Butterfly is enough to get security when $m \ll 2^n$ (Benes schemes and Butterfly schemes are defined in section 2). Then, for adaptive chosen plaintext attacks and for all $\varepsilon > 0$, we will prove CPA-2 security when $m \ll 2^{n(1-\varepsilon)}$ for sufficiently large n. However our proved security bound in this case will be larger than the term given in [1]. We will also mention what appears for a variant of Benes called "modified Benes", and we will give some examples of applications.

2 Notations

- $I_n = \{0,1\}^n$ is the set of the 2^n binary strings of length n.
- F_n is the set of all functions $f : I_n \to I_n$. Thus $|F_n| = 2^{n \cdot 2^n}$.
- For a, $b \in I_n$, $a \oplus b$ stands for bit by bit exclusive or of a and b.
- For a, $b \in I_n$, $a||b$ stands for the concatenation of a and b.
- For $a, b \in I_n$, we also denote by $[a, b]$ the concatenation $a||b$ of a and b.
- Given four functions from n bits to n bits, $f_1, \ldots, f_4$, we use them to define the **Butterfly transformation** (see [1]) from $2n$ bits to $2n$ bits. On input $[L_i, R_i]$, the output is given by $[X_i, Y_i]$, with:

$$X_i = f_1(L_i) \oplus f_2(R_i) \text{ and } Y_i = f_3(L_i) \oplus f_4(R_i).$$

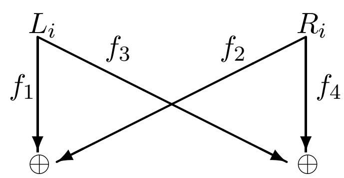

Figure 1: Butterfly transformation

- Given eight functions from n bits to n bits, $f_1, \ldots, f_8$, we use them to define the **Benes transformation** (see [1]) (back-to-back Butterfly) as the composition of two Butterfly transformations. On input $[L_i, R_i]$, the output is given by $[S_i, T_i]$, with:

$$S_i = f_5(f_1(L_i) \oplus f_2(R_i)) \oplus f_6(f_3(L_i) \oplus f_4(R_i)) = f_5(X_i) \oplus f_6(Y_i)$$
$$T_i = f_7(f_1(L_i) \oplus f_2(R_i)) \oplus f_8(f_3(L_i) \oplus f_4(R_i)) = f_7(X_i) \oplus f_8(Y_i).$$

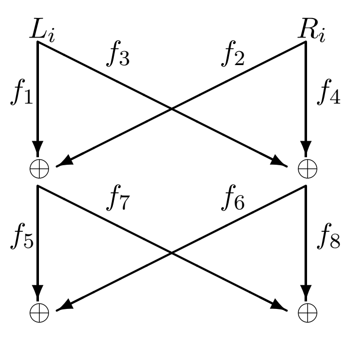

Figure 2: Benes transformation (back-to-back Butterfly)

3 A problem in the proof of [1]

Let $[L_1, R_1]$, $[L_2, R_2]$, $[L_3, R_3]$ and $[L_4, R_4]$ be four chosen inputs such that $L_1 = L_2$, $R_2 = R_3$, $L_3 = L_4$ and $R_4 = R_1$ (and $R_1 \neq R_2$ and $L_1 \neq L_3$). (Here we will say that we have "a circle in L, R" of length 4). Let p be the probability for these inputs to produce "a circle in X, Y" (or, in the language of [1], an "alternating cycle") after a Butterfly. In [1], page 318, it is claimed that "the probability that the top Butterfly produces an alternating cycle of length $2j$ is $\leq 2^{-2jn}$". So here this means $p \leq \frac{1}{2^{4n}}$. However we will see that $p \geq \frac{1}{2^{2n}}$. We have:

$$X_1 = f_1(L_1) \oplus f_2(R_1)$$

$$X_2 = f_1(L_2) \oplus f_2(R_2) = f_1(L_1) \oplus f_2(R_2)$$

$$X_3 = f_1(L_3) \oplus f_2(R_3) = f_1(L_3) \oplus f_2(R_2)$$

$$X_4 = f_1(L_4) \oplus f_2(R_4) = f_1(L_3) \oplus f_2(R_1)$$

$$Y_1 = f_3(L_1) \oplus f_4(R_1)$$

$$Y_2 = f_3(L_2) \oplus f_4(R_2) = f_3(L_1) \oplus f_4(R_2)$$

$$Y_3 = f_3(L_3) \oplus f_4(R_3) = f_3(L_3) \oplus f_4(R_2)$$

$$Y_4 = f_3(L_4) \oplus f_4(R_4) = f_3(L_3) \oplus f_4(R_1)$$

First possible circle in X, Y We will get the circle $X_1 = X_2$, $Y_2 = Y_3$, $X_3 = X_4$ and $Y_4 = Y_1$ if and only if $f_2(R_1) = f_2(R_2)$ and $f_3(L_1) = f_3(L_3)$ and the probability for this is exactly $\frac{1}{2^{2n}}$ (since $R_1 \neq R_2$ and $L_1 \neq L_3$).

Conclusion The probability p to have a circle in X, Y of length 4 (i.e. the probability that the top Butterfly produces an alternating cycle of length 4 in the language of [1]) is $\geq \frac{1}{2^{2n}}$, so it is not $\leq \frac{1}{2^{4n}}$ as claimed in [1].

As we will see in this paper, this problem is not easily solved: a precise analysis will be needed in order to prove the security result $m \ll 2^{n(1-\varepsilon)}$ for all $\varepsilon > 0$.

Remark It is possible to show that 6 different circles in X, Y are possible here, with a probability $\frac{1}{2^{2n}}$. So the probability p to have a circle in X, Y of length 4 will be between $\frac{1}{2^{2n}}$ and $\frac{6}{2^{2n}}$ here. One part of the work of this paper will be to see if $\frac{1}{2^{2n}}$ instead of $\frac{1}{2^{4n}}$ can create a problem or not, and another part of the work will be to evaluate the effect of the number of cases, 6 here, and the analysis will have to be done for circles of any length, not only length 4 as here.

4 One Butterfly: Proof of KPA security when $m \ll 2^n$

Here we will prove KPA security by using the "coefficient H technique" of [13] (more precisely theorem 3.1 p.516 of [13]). Let $[L_i, R_i]$, $1 \leq i \leq m$, be the inputs. With one round of Butterfly, the outputs are $[X_i, Y_i]$ with:

$$\forall i, 1 \leq i \leq m, \begin{cases} X_i = f_1(L_i) \oplus f_2(R_i) \\ Y_i = f_3(L_i) \oplus f_4(R_i) \end{cases} \qquad (\#)$$

Now when the values L_i, R_i, X_i, Y_i are given, $1 \leq i \leq m$, let H be the number of f_1, f_2, f_3, f_4 of F_n such that we have (#). If we have no circle in L, R then each new equation (#) fixes f_1 (or f_2) and f_3 (or f_4) in a new point. So if we have no circle in L, R we will have exactly: $H = \frac{|F_n|^4}{2^{2nm}}$. Moreover, since we are in KPA, with m random cleartext/ciphertext pairs, we will now see that we can indeed assume, when $m \ll 2^n$, that there are no circle in L, R.

1. Circle on 2 indices i, j, $i \neq j$, are impossible because $L_i = L_j$ and $R_i = R_j$ implies that $i = j$.

2. Without loosing generality, we can study only circles on r indices, with r even ($L_1 = L_2$, $L_2 = L_3$ and $R_3 = R_1$ for example gives the circle $L_1 = L_3$, $R_3 = R_1$). We will first study the case of circle on 4 indices. Here, we have some pairwise distinct indices i, j, k, l such that: $L_i = L_j$, $L_k = L_l$, $R_i = R_k$ and $R_j = R_l$. The probability to have such a circle, when the L_α, R_α are randomly chosen, is $\leq \frac{m^4}{4 \cdot 2^{4n}}$ (Proof: we have here $\frac{m^4}{4}$ possible choices for i, j, k, l since we can start the circle in i, j, k or l and each of the 4 equations have a probability $\frac{1}{2^n}$ to be satisfied if the L_α, R_α are randomly chosen).

3. More generally the probability to have a circle on r indices, when the L_i, R_i are randomly chosen, is $\leq \frac{m^r}{r \cdot 2^{nr}}$. So the probability p to have at least one circle in L, R, when the values L_α and R_α are randomly chosen satisfies: $p \leq \frac{1}{4} \sum_{i=2}^{\infty} \frac{m^{2i}}{2^{2in}} = \frac{1}{4} \cdot \frac{m^4}{2^{4n}} \cdot \frac{1}{1 - \frac{m^2}{2^{2n}}}$.

Conclusion By using theorem 3.1 p.516 of [13], we obtain (with $\alpha = 0$ and $\beta = \frac{1}{4} \cdot \frac{m^4}{2^{4n}} \cdot \frac{1}{1 - \frac{m^2}{2^{2n}}}$): for all algorithm A taking m values $[L_i, R_i]$ on input, $|E(P_1 - P_1^*)| \leq \frac{1}{4} \cdot \frac{m^4}{2^{4n}} \cdot \frac{1}{1 - \frac{m^2}{2^{2n}}}$ (where E is the expectancy on the $[L_i, R_i]$ randomly chosen).

So one Butterfly resist all KPA attacks when $m \ll 2^n$.

Remark 1 For Benes (i.e. two independent rounds of Butterfly), a similar KPA analysis would give security in $\mathcal{O}\left(\frac{m^2}{2^{2n}}\right)$ instead of $\mathcal{O}\left(\frac{m^4}{2^{4n}}\right)$ here for only one round of Butterfly. As we will see in appendix C for Benes, and more generally for λ rounds of Benes, $\lambda \geq 1$, the KPA security in $\mathcal{O}\left(\frac{m^2}{2^{2n}}\right)$ is tight: there is an explicit ciphertext only attack in $\mathcal{O}\left(\frac{m^2}{2^{2n}}\right)$. So for KPA security and for ciphertext only security one round of Butterfly is slightly better than two rounds (or λ rounds) when $m \ll 2^n$. This is due to the fact that for two rounds of Butterfly we can have $X_i = X_j$ and $Y_i = Y_j$ with $i < j$, and for one round we cannot have $L_i = L_j$ and $R_i = R_j$ with $i < j$ (two rounds of independent pseudo-random permutations cannot be less secure than one, but with pseudo-random functions, as here, it can be).

Remark 2 For CPA-1 security however, unlike KPA security or ciphertext only attacks, Benes (i.e. two independent rounds of Butterfly) is clearly much better than one. We will see that when $m \ll 2^{n(1-\varepsilon)}$, $\varepsilon > 0$, Benes is secure against all CPA-2 (so also CPA-1) attacks. For one round of Butterfly there is a CPA-1 attack with $m = 4$: just choose two values L_i and L_j, $L_i \neq L_j$ and two values R_i and R_j, $R_i \neq R_j$, and ask for the outputs of $[L_i, R_i]$, $[L_j, R_j]$, $[L_i, R_j]$ and $[L_j, R_i]$. With Benes we will have $X_1 \oplus X_2 \oplus X_3 \oplus X_4 = 0$ and $Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4 = 0$ with probability 1, and for random function this occurs with probability only $\frac{1}{2^{2n}}$.

5 Benes: First results on circles in X, Y

5.1 Circles in X, Y and CPA-2 security

With Benes, we have:

$$\forall i,\ 1 \leq i \leq m,\ Benes(f_1, \ldots, f_8)[L_i, R_i] = [S_i, T_i] \Leftrightarrow \left\{ \begin{array}{l} S_i = f_5(X_i) \oplus f_6(Y_i) \\ T_i = f_7(X_i) \oplus f_8(Y_i) \end{array} \right. \quad (1)$$

$$\text{with } \left\{ \begin{array}{l} X_i = f_1(L_i) \oplus f_2(R_i) \\ Y_i = f_3(L_i) \oplus f_4(R_i) \end{array} \right.$$

When some L_i, R_i, S_i, T_i values are given, $1 \leq i \leq m$, let H be the number of $f_1, \ldots, f_8$ such that: $\forall i$, $1 \leq i \leq m$, $Benes(f_1, \ldots, f_8)[L_i, R_i] = [S_i, T_i]$.

Definition 5.1

- *We will say that we have "a circle in X, Y of length k" if we have k pairwise distinct indices such that $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$,..., $X_{i_{k-1}} = X_{i_k}$, $Y_{i_k} = Y_{i_1}$.*
- *We will say that we have "a circle in X, Y" if there is an even integer k, $k \geq 2$, such that we have a circle in X, Y of length k.*

Theorem 5.1 *If the X_i and Y_i values are such that there are no "circles in X, Y" then the number of f_5, f_6, f_7, f_8 solution of (1) is exactly $\frac{|F_n|^4}{2^{2nm}}$.*

Proof Let $\mathcal{A}$ be a set of equations $S_i = f_5(X_i) \oplus f_6(Y_i)$. These equations are all independent, except if we have a subset of λ equations in $\mathcal{A}$ where all the X_i values and all the Y_i values are identical two by two (Proof: if this property does not occur we can associate a new variable $f_5(X_\alpha)$ or $f_6(Y_\beta)$ to each new equation $S_i = f_5(X_i) \oplus f_6(Y_i)$, where α and β are found by looking the equations where we have $f_5(X_i)$ or $f_6(Y_i)$). So, if the equations of $\mathcal{A}$ are not all independent, we will have some indices $i_1, \ldots, i_k$, k even, where all the X_i values and all the Y_i values are identical two by two, $i \in \{i_1, \ldots, i_k\}$. There is at least one index $j_2 \in \{i_1, \ldots, i_k\}$, $j_2 \neq i_1$, such that $X_{i_1} = X_{j_2}$. There is at least one index j_3, $j_3 \neq j_2$, such that $Y_{j_2} = Y_{j_3}$. If $j_3 = i_1$ we have a circle in X, Y. If not, we can continue: there is at least one index j_4, $j_4 \neq j_3$, such that $X_{j_4} = X_{j_3}$. If $j_4 \in \{i_1, j_2\}$ we have a circle in X, Y. If not, we can continue. Like this we will obtain a circle in X, Y of length $< k$, or at the end we have an index j_k, $j_k \neq j_{k-1}$, such that $Y_{j_k} = Y_{i_1}$ and this gives a circle in X, Y of length k. So, if we have no circle in X, Y, then all the equations $S_i = f_5(X_i) \oplus f_6(Y_i)$ of (1) are independent, so we have exactly $\frac{|F_n|^2}{2^{nm}}$ functions f_5, f_6 solution. Similarly, we have exactly $\frac{|F_n|^2}{2^{nm}}$ functions f_7, f_8 solution of the equation $T_i = f_7(X_i) \oplus f_8(Y_i)$ of (1). So if we have no circle in X, Y we have exactly $\frac{|F_n|^4}{2^{2nm}}$ functions f_5, f_6, f_7, f_8 solution of (1), as claimed.

Let p be the probability to get at least one circle in X, Y in a CPA-2 attack (when f_1, f_2, f_3, f_4 are randomly chosen). From theorem 5.1, we have $H \geq (1-p)\frac{|F_n|^8}{2^{2nm}}$. So with theorem 3.2 p.517 of [13] (with $\alpha = 0$ and $\beta = p$) we get:

Theorem 5.2 *The probability to distinguish Benes functions from random functions of $2n$ bits $\rightarrow$ $2n$ bits in a CPA-2 attack is always $\leq p$, when $f_1, \ldots, f_8$ are randomly and independently chosen in F_n, and where p is the probability to have a circle in X, Y.*

Remark 1 This result was already in [1], written in the language of "alternating cycles". In fact, this result can be obtained directly, without using theorem 3.2 of [13]: when there are no circles in X, Y in each equation (1), we have a new variable $f_5(X_i)$ or $f_6(Y_i)$, and a new variable $f_7(X_i)$ or $f_8(Y_i)$, so if f_5, f_6, f_7, f_8 are random functions, the outputs S_i and T_i are perfectly random and independent from the previous S_j, T_j, $i < j$.

Remark 2 In this paper we will evaluate p. One difficulty is the fact that in a CPA-2 attack we cannot assume that the variables X_i and Y_i are random, so we cannot use the same proof as we did in section 4 for KPA security. For example if we choose $L_1 = L_2$, $L_3 = L_4$, $R_1 = R_3$ and $R_2 = R_4$, then we will have: $X_4 = X_1 \oplus X_2 \oplus X_3$ and $Y_4 = Y_1 \oplus Y_2 \oplus Y_3$, so the X_i (and Y_i) variables are not independent random variables.

Remark 3 In this paper we will analyze when p is small, since p small is a sufficient condition for CPA-2 security. We can notice, however, that this is not a necessary condition. Let us assume that we can, with a non negligible probability p generate A circles in X, Y with k variables. For each such circles we will have: $S_{i_1} \oplus \dots S_{i_k} = 0$ and $T_{i_1} \oplus \dots T_{i_k} = 0$. (2)
For random functions, we will have about $\frac{m^k}{k! 2^{2n}}$ indices $i_1, \dots, i_k$ such (2), with a standard deviation of about $\sqrt{\frac{m^k}{k! 2^{2n}}}$ for this number. So even if p is not negligible, we may not be able to distinguish Benes functions from random functions if the probability to have $A \geq \sqrt{\frac{m^k}{k! 2^{2n}}}$ is negligible (instead of $A \neq 0$).

5.2 Circles in X, Y with $k = 2$

Theorem 5.3 *The probability p_2 to have a circle in X, Y of length 2, when f_1, f_2, f_3, f_4 are randomly chosen in F_n satisfies: $p_2 \leq \frac{m(m-1)}{2 \cdot 2^{2n}}$. So p_2 is negligible when $m \ll 2^n$.*

Proof Here we want $i < j$ such that:

$$\begin{cases} f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j) & (3) \\ f_3(L_i) \oplus f_4(R_i) = f_3(L_j) \oplus f_4(R_j) & (4) \end{cases}$$

First case: $R_i \neq R_j$**.** Then when f_1 is fixed, we have exactly $\frac{|F_n|}{2^n}$ functions f_2 such that (3) is satisfied, and when f_3 is fixed, we have exactly $\frac{|F_n|}{2^n}$ functions f_4 such that (4) is satisfied.

Second case: $R_i = R_j$**.** Then we have $L_i \neq L_j$ (since $i < j$ so $i \neq j$), so we have exactly $\frac{|F_n|}{2^n}$ functions f_1 such that (3) is satisfied and exactly $\frac{|F_n|}{2^n}$ functions f_3 such that (4) is satisfied.

Conclusion Whatever L_i, L_j, R_i, R_j are, when i and j are fixed, we have exactly $\frac{|F_n|^4}{2^{2n}}$ functions f_1, f_2, f_3, f_4 such that (3) and (4) are satisfied. So since we have $\frac{m(m-1)}{2}$ indices i, j, $i < j$, we have $p_2 \leq \frac{m(m-1)}{2 \cdot 2^{2n}}$, as claimed.

5.3 Circles in X, Y with $k = 4$

(As already said in section 4, without loosing generality we can study only circles with k even. $X_1 = X_2$, $X_2 = X_3$ and $Y_3 = Y_1$ for example gives the circle $X_1 = X_3$, $Y_3 = Y_1$ with $k = 2$).

Theorem 5.4 *The probability p_4 to have a circle in X, Y of length 4, when f_1, f_2, f_3, f_4 are randomly chosen in F_n satisfies: $p_4 \leq \frac{m^4}{4 \cdot 2^{4n}} + \frac{6m^2}{2^{2n}}$. So p_4 is negligible when $m \ll 2^n$.*

Proof Here we want 4 pairwise distinct i, j, k, l such that: $X_i = X_j$, $Y_j = Y_k$, $X_k = X_l$ and $Y_l = Y_i$, i.e. such that:

$$(5) \begin{cases} f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j) \\ f_1(L_k) \oplus f_2(R_k) = f_1(L_l) \oplus f_2(R_l) \\ f_3(L_j) \oplus f_4(R_j) = f_3(L_l) \oplus f_4(R_l) \\ f_3(L_i) \oplus f_4(R_i) = f_3(L_k) \oplus f_4(R_k) \end{cases}$$

For i, j, k, l, we have $\leq \frac{m(m-1)(m-2)(m-3)}{4}$ possibilities (since when i, j, k, l is a solution we can start the circle in X, Y with i, j, k or l).

- If in (5) the four equations are independent, the probability to obtain (5) will be $\leq \frac{m^4}{4 \cdot 2^{4n}}$.
- Now in (5), as we will see, there are $3 \times 2 = 6$ cases where the four equations are not independent (they come from only two independent equations). For example (case 1), if $L_i = L_j$, $L_k = L_l$, $R_i = R_k$ and $R_j = R_l$, then

  $$(5) \Leftrightarrow \begin{cases} f_2(R_i) = f_2(R_j) \\ f_3(L_i) = f_3(L_k) \end{cases}$$

  The equations number 1 and 3 of (5) are always independent , since f_3 and f_4 are randomly chosen independently from f_1 and f_2. However the equation number 2 can be equivalent with the equation number 1 if

  $$\begin{array}{r} L_i = L_j, L_k = L_l, R_i = R_k, R_j = R_l \\ \text{or } L_i = L_j, L_k = L_l, R_i = R_l, R_j = R_k \\ \text{or } L_i = L_k, L_j = L_l, R_i = R_j, R_k = R_l \\ \text{or } L_i = L_k, L_j = L_l, R_i = R_l, R_j = R_k \\ \text{or } L_i = L_l, L_j = L_k, R_i = R_j, R_k = R_l \\ \text{or } L_i = L_l, L_j = L_k, R_i = R_k, R_j = R_l \end{array}$$

  These 6 cases are also the conditions for the equations number 5 and 6 to be equivalent. However, in all of these 6 cases, 2 indices are fixed when two other indices are given. For example with case 1, if i and l are given, then j and k are fixed, since $L_j = L_i$ and $R_j = R_l$ (this fixes at most one j), and since $L_k = L_l$ and $R_k = R_i$ (this fixes at most one k).

Conclusion $p_4 \leq \frac{m(m-1)(m-2)(m-3)}{4 \cdot 2^{4n}} + \frac{6m(m-1)}{2^{2n}}$, so $p_4 \leq \frac{m^4}{4 \cdot 2^{4n}} + \frac{6m^2}{2^{2n}}$, as claimed.

5.4 Circles in X, Y, the general case

We will now consider the general case (Remark: in appendix F we study specifically $k = 6$ and we will get a more precise evaluation than the general evaluation. $k = 6$ is interesting since a large number, 128, appears and since a term in $\frac{m^\alpha}{2^{n\beta}}$ appears with $\alpha < \beta$).

Theorem 5.5 *Let k be an even integer. The probability p_k to have a circle in X, Y of length k, when f_1, f_2, f_3, f_4 are randomly chosen in F_n satisfies: $p_k \leq k^{2k} \frac{m^2}{2^{2n}}$.*

Proof We have a circle of length k in X, Y if and only if there are some pairwise distinct indices $i_1, \dots, i_k$ such that $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$, …, $Y_{i_k} = Y_{i_1}$, i.e. such that:

$$(8) \begin{cases} f_1(L_{i_1}) \oplus f_2(R_{i_1}) = f_1(L_{i_2}) \oplus f_2(R_{i_2}) \\ f_1(L_{i_3}) \oplus f_2(R_{i_3}) = f_1(L_{i_4}) \oplus f_2(R_{i_4}) \\ \vdots \\ f_1(L_{i_{k-1}}) \oplus f_2(R_{i_{k-1}}) = f_1(L_{i_k}) \oplus f_2(R_{i_k}) \end{cases} \quad \text{and } (9) \begin{cases} f_3(L_{i_2}) \oplus f_4(R_{i_2}) = f_3(L_{i_3}) \oplus f_4(R_{i_3}) \\ f_3(L_{i_4}) \oplus f_4(R_{i_4}) = f_3(L_{i_5}) \oplus f_4(R_{i_5}) \\ \vdots \\ f_3(L_{i_k}) \oplus f_4(R_{i_k}) = f_3(L_{i_1}) \oplus f_4(R_{i_1}) \end{cases}$$

For $\{i_1, \dots, i_k\}$ we have $\leq \frac{m^k}{k}$ possibilities (since we can start the circle with i_1, or i_2 ,…, or i_k). If in (8) and (9) the $\frac{k}{2} + \frac{k}{2} = k$ equations are independent, the probability to obtain (8) and (9) will be $\leq \frac{m^k}{k \cdot 2^{kn}}$. To study the general case, where the equations may be dependent, we will introduce the equations of the circle in X, Y one by one.

- The first equation is: $X_{i_1} = X_{i_2}$. Here we have $m(m-1)$ possible choices for i_1 and i_2, and when i_1 and i_2 are given, the probability to have $X_{i_1} = X_{i_2}$ is exactly $\frac{1}{2^n}$.
- The second equation is: $Y_{i_2} = Y_{i_3}$. Here, when i_1 and i_2 are given, we have $\leq m-2$ possible choices for i_3, and this equation $Y_{i_2} = Y_{i_3}$ is independent from the equation $X_{i_1} = X_{i_2}$ (since with Y we use f_3 and f_4 and with X we use f_1 and f_2), so the probability to have $Y_{i_2} = Y_{i_3}$ when $X_{i_1} = X_{i_2}$ and when i_1, i_2 and i_3 are given is exactly $\frac{1}{2^n}$.
- The equation number 3 is: $X_{i_3} = X_{i_4}$. Here, there are two cases.

  Case 1 $X_{i_3} = X_{i_4}$ is independent from $X_{i_1} = X_{i_2}$. Then for i_4 we have $m-3$ possible choices (when i_1, i_2 and i_3 are given), and the probability to have $X_{i_3} = X_{i_4}$ when $X_{i_1} = X_{i_2}$ and $Y_{i_2} = Y_{i_3}$ is $\frac{1}{2^n}$.

  Case 2 $X_{i_3} = X_{i_4}$ is dependent from $X_{i_1} = X_{i_2}$. Then the indices i_1, i_2, i_3 and i_4 can be associated two by two with equalities in R, and two by two with equalities in L (for example $L_{i_4} = L_{i_3}$, $L_{i_1} = L_{i_2}$, $R_{i_3} = R_{i_2}$, and $R_{i_4} = R_{i_1}$). So we have $L_{i_4} = L_{i_\alpha}$, $\alpha = 1, 2$ or 3, and $R_{i_4} = R_{i_\beta}$, $\beta = 1, 2$ or 3, and $\alpha \neq \beta$ (since $\alpha < 4$, and since $L_{i_4} = L_{i_\alpha}$ and $R_{i_4} = R_{i_\beta}$ would imply $i_4 = i_\alpha$ and $\alpha = 4$). So in this case 2, i_4 is fixed when i_1, i_2 and i_3 are fixed, and when the equalities in L and R are given. For these equalities in L and R we have here $\leq 3 \times 2 = 6$ possibilities (3 for α and 2 for β when α is fixed). We can continue like this for all the equations in X or Y, except the last one, that we will consider specifically.

- For equation number μ, $3 \leq \mu < k$, we have two cases.

  Case 1 This equation number μ is independent from the other equations. Then for $i_{\mu+1}$ we have $m - \mu$ possible choices (when i_1, i_2, …, i_μ are given), and the probability to have this equation number μ when the other equations are satisfied is $\frac{1}{2^n}$.

  Case 2 This equation number μ is dependent from the other equations. Then $\exists \alpha, \beta$, $\alpha \neq \beta$, $\alpha \leq \mu$, $\beta \leq \mu$, such that $L_{i_{\mu+1}} = L_{i_\alpha}$ and $R_{i_{\mu+1}} = R_{i_\beta}$. So (since the $[L_i, R_i]$, $1 \leq i \leq m$ are pairwise distinct), $i_{\mu+1}$ is fixed when i_1, i_2, …, i_μ are fixed, and when the equalities in L and R are given. For α and β we have $\leq \mu(\mu - 1)$ possibilities.

If equation number μ is the first in this case 2 If μ is the first integer such that equation number μ is in this case 2 (i.e. such that equation number μ is dependent from the other equations) then we will see now that not only one but at least two indices can be fixed from the other indices. Proof: since equation number μ is dependent from the previous equations, there is a subset S of the equations such that all the equations in S have a number $\leq \mu$, such that all the L_i variables in the equations of S can be associated two by two with equalities, and such that all the R_i variables in the equations of S can be associated two by two with equalities, and such that equation number μ is in S. So we have an index α, $\alpha \leq \mu$ such that $L_{i_{\mu+1}} = L_{i_\alpha}$ and an index β, $\beta \leq \mu$, $\alpha \neq \beta$, such that $R_{i_{\mu+1}} = R_{i_\beta}$, as said above, but we also have an index γ, $\gamma \leq \mu$, $\gamma \neq \alpha$ and an index δ, $\delta \leq \mu$, $\delta \neq \gamma$ such that $R_{i_\alpha} = R_{i_\gamma}$ and $L_{i_\gamma} = L_{i_\delta}$. Here we see that $i_{\mu+1}$ **and** i_γ can be fixed from the other indices $\leq \mu$ (since $L_{i_\gamma} = L_{i_\delta}$ and $R_{i_\gamma} = R_{i_\alpha}$, and $L_{i_{\mu+1}} = L_{i_\alpha}$ and $R_{i_{\mu+1}} = R_{i_\beta}$) and here for $\alpha, \beta, \gamma, \delta$, we have $\leq \mu(\mu-1)(\mu-1)^2$ possibilities.

Remark Alternatively it is also possible to show that since equation number μ is dependent from the previous equations, we will have one, or more than one circles in L, R (there is an index α_1 such that $L_{i_{\mu+1}} = L_{i_{\alpha_1}}$, and an index $\alpha_2 \neq \alpha_1$ such that $R_{i_{\alpha_1}} = R_{i_{\alpha_2}}$, and an index $\alpha_3 \neq \alpha_2$ such that $L_{i_{\alpha_2}} = L_{i_{\alpha_3}}$, etc. and since the number of indices is finite, we get like this a circle in L, R. If not all the indices of the dependencies are covered, we can continue to get some other circles in L, R). Since in a circle in L, R, 50% of the indices can be fixed from the other indices, and since a circle in L, R has a length ≥ 4 (since $L_i = L_j$ and $R_i = R_j$ imply $i = j$), we see again that at least 2 indices will be fixed with the first dependency. For the second dependency it may occur, however, that only one new index is fixed. For example if $L_1 = L_2 = L_3$, $L_4 = L_5 = L_6$, $R_1 = R_4$, $R_2 = R_5$ and $R_3 = R_6$, then $X_1 = X_4$ implies $X_2 = X_5$ (this fixes 2 indices) and $X_3 = X_6$ (this fixes only one more index).

- For equation number k, the last equation, it can be dependent or not from the previous equations, but here, unlike before, we do not introduce a new index (since we have a circle in the indices).

Conclusion for p_k If we have no dependencies in the equations, the probability to have all the equations is $\leq \frac{m^k}{k \cdot 2^{nk}}$. If we have a dependency, for equations number 1 and 2 and for indices i_1, i_2, i_3 we have a probability $\leq \frac{m^3}{2^{2n}}$. Then each new equation different from the last one, say equation number μ, $\mu < k$, either introduces a new index $i_{\mu+1}$ with a condition in $\frac{1}{2^n}$ (it gives a term $\leq \frac{m}{2^n}$) or we have less than $\mu(\mu-1)$ possibilities for this index $i_{\mu+1}$. Moreover, the first time that we have a dependency, say with equation number μ, $\mu < k$, then we can fix two indices, $i_{\mu+1}$ and i_α for $\alpha \leq \mu$, from the other indices i_β, $\beta \leq \mu$, and after less than $\mu(\mu-1)(\mu-1)^2$ possibilities for the equalities in L and R these two indices will be fixed. So we get: $p_k \leq \frac{m^k}{k \cdot 2^{nk}} + \frac{m^3}{2^{2n}} \frac{(k-1)^2}{m} \cdot (2 \cdot 3 + \frac{m}{2^n}) \cdot (4 \cdot 5 + \frac{m}{2^n}) \ldots ((k-2)(k-1) + \frac{m}{2^n})$. (Note: the term $\frac{(k-1)^2}{m}$ comes from the second fixed index when we get the first dependency). So if $m \leq 2^n$, $p_k \leq \frac{m^k}{k \cdot 2^{nk}} + \frac{m^2 (k-1)^2}{2^{2n}} \cdot (2 \cdot 3 + 1) \cdot (4 \cdot 5 + 1) \ldots ((k-2)(k-1) + 1)$, so $p_k \leq \frac{m^k}{k \cdot 2^{nk}} + \frac{m^2}{2^{2n}} \cdot (k-1)^2 (k^2)^{k-2}$, so since $\frac{m^k}{k \cdot 2^{nk}} \leq \frac{m^2}{k \cdot 2^{2n}}$ if $m \leq 2^n$ and $k \geq 2$, we get $p_k \leq k^{2k} \cdot \frac{m^2}{2^{2n}}$ as claimed.

Remark In appendix G we will show a slightly different way to prove this theorem 5.5 (by looking differently at all the possible equalities in L and R). In appendix G we will see that instead of the coefficient k^{2k}, we can get a coefficient near k^k. We can notice however that this coefficient can really be very large. For example, if we start from a fixed circle of length k in L, R:

- For equalities in X, Y such that we have a circle of length k in X, Y, we have potentially $(k-1)!$ possibilities.

- For equalities in X, Y such that all the indices can be associated two by two with equalities in X, and associated two by two with equalities in Y, we have potentially $(3 \cdot 5 \cdot 7 \ldots (k-1))^2$ possibilities (this is $\leq (k^{k/2})^2$).

6 Benes: Proof of CPA-2 security when $m \ll 2^{n(1-\varepsilon)}$

6.1 Security when $m \ll 2^{n/2}$

When f_1, f_2 are randomly and independently chosen in F_n, the probability q_1 to have i, j, $1 \le i < j \le m$, such that $X_i = X_j$ satisfies $q_1 \le \frac{m(m-1)}{2 \cdot 2^n}$. So the probability p to have a circle in X, Y (of any length) satisfies $p \le q_1 \le \frac{m(m-1)}{2 \cdot 2^n}$ (since in any circle in X, Y we will have $i < j$ such that $X_i = X_j$). So from theorem 5.2 we get:

Theorem 6.1 *The probability to distinguish Benes functions from random functions of $2n$ bits $\rightarrow 2n$ bits in any CPA-2 attack with m chosen messages is always $\le \frac{m(m-1)}{2 \cdot 2^n}$ (when $f_1, \ldots, f_8$ are randomly and independently chosen in F_n). This gives security when $m^2 \ll 2^n$, i.e. when $m \ll 2^{n/2}$.*

6.2 Security when $m \ll 2^{2n/3}$

When f_1, f_2, f_3, f_4 are randomly and independently chosen in F_n, the probability q_2 to have 3 pairwise distinct indices i, j, k, such that $X_i = X_j$ and $Y_j = Y_k$ satisfies $q_2 \le \frac{m(m-1)(m-2)}{2^{2n}}$ (Proof: when i, j, k are fixed $X_i = X_j$ is a condition with probability $\frac{1}{2^n}$ on f_1 and f_2 and $Y_j = Y_k$ is a condition with probability $\frac{1}{2^n}$ on f_3 and f_4, and f_1, f_2, f_3, f_4 are independently chosen). So the probability p to have a circle in X, Y (of any length) satisfies $p \le q_2 \le \frac{m^3}{2^{2n}}$. So from theorem 5.2 we get:

Theorem 6.2 *The probability to distinguish Benes functions from random functions of $2n$ bits $\rightarrow 2n$ bits in any CPA-2 attack with m chosen messages is always $\le \frac{m^3}{2^{2n}}$ (when $f_1, \ldots, f_8$ are randomly and independently chosen in F_n).*

6.3 Security when $m \ll 2^{3n/4}$

Theorem 6.3 *When f_1, f_2, f_3, f_4 are randomly and independently chosen in F_n, the probability q_3 to have 4 pairwise distinct indices i, j, k, l, such that $X_i = X_j$, $Y_j = Y_k$, $X_k = X_l$ satisfies $q_3 \le \frac{m^4}{2^{3n}} + \frac{6m^2}{2^{2n}}$.*

Proof If the two equations in X are independent, the probability to obtain these 3 independent equations on 4 indices is $\le \frac{m^4}{2^{3n}}$. If $f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j)$ and $f_1(L_k) \oplus f_2(R_k) = f_1(L_l) \oplus f_2(R_l)$ are dependent, then the values L_i, L_j, L_k, L_l can be linked two by two with equalities, and the values R_i, R_j, R_k, R_l can be linked two by two with equalities (for example: $L_i = L_j$, $L_k = L_l$, $R_i = R_k$ and $R_j = R_l$). These equations in L, R can be written as some circles of equalities in L, R (in the example above we have the circle: $L_i = L_j$, $R_j = R_l$, $L_l = L_k$, $R_k = R_i$). (Remark: here, with 2 equations in$X$, we can have only one circle, of length 4, since circles in L, R of length 2 cannot exist since $L_i = L_j$ and $R_i = R_j$ implies $i = j$). So two indices will be fixed from the two other indices from these equations in L, R of the circle (in the example above, j and k are fixed when i and l are given, since $L_j = L_i$, $R_j = R_l$, $L_k = L_l$ and $R_k = R_i$). Moreover, for the equalities in L and R we have here ≤ 6 possibilities (for α such that $R_k = R_\alpha$ we can take $\alpha = i, j$ or l, then for β such that $L_k = L_\beta$ we can take $\beta = i, j$ or l and we need $\alpha \neq \beta$).

Conclusion $q_3 \le \frac{m^4}{2^{3n}} + \frac{6m^2}{2^{2n}}$, as claimed.

Now from theorem 6.3 we get: the probability p to have a circle in X, Y (of any length) satisfies $p \le \frac{m^2}{2 \cdot 2^{2n}} + \frac{m^4}{2^{3n}} + \frac{6m^2}{2^{2n}}$.

Proof We have seen in section 5.2 that the probability to have a circle in X, Y of length 2 is $\leq \frac{m^2}{2 \cdot 2^{2n}}$, and circles in X, Y of length > 2 always have 4 pairwise distinct indices i, j, k, l such that $X_i = X_j$, $Y_j = Y_k$ and $X_k = X_l$.

Now from theorem 5.2 we get immediately the CPA-2 security of Benes schemes when $m \ll 2^{3n/4}$.

6.4 Security when $m \ll 2^{n(1-\varepsilon)}$

Let k be an integer, $k \geq 1$.

Definition 6.1 *If k is odd, we will say that we have "a line in X, Y of length k" if we have $k+1$ pairwise distinct indices such that $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$, $\ldots$, $Y_{i_{k-1}} = Y_{i_k}$, $X_{i_k} = X_{i_{k+1}}$. Similarly, if k is even, we will say that we have "a line in X, Y of length k" if we have $k+1$ pairwise distinct indices such that $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$, $\ldots$, $X_{i_{k-1}} = X_{i_k}$, $Y_{i_k} = Y_{i_{k+1}}$. So in a line in X, Y we have $k+1$ indices, and k equations, in X or in Y, and these equations can be written "in a line" from the indices.*

Theorem 6.4 *When f_1, f_2, f_3, f_4 are randomly and independently chosen in F_n, the probability q_k to have a line in X, Y of length k satisfies $q_k \leq \frac{m^{k+1}}{2^{nk}} + \frac{k^{2k} m^2}{2^{2n}}$, when $k \geq 4$ and $\frac{m^{k+1}}{2^{nk}} + \frac{k^{2k} m^4}{2^{4n}}$.*

Remark This minoration can be improved in different ways, for example if $k \geq 6$ we can get $\frac{k^{2k} m^4}{2^{4n}}$ instead of $\frac{k^{2k} m^2}{2^{2n}}$, and the value k^{2k} can be improved (see appendix G). However, this result will be enough to get security in $2^{n(1-\varepsilon)}$ for all fixed $\varepsilon > 0$.

Proof of theorem 6.4 The proof is exactly the same as the proof of theorem 5.5 of section 5.4. The proof is even slightly simpler here, since the last equation does not have to be treated differently from the other equations (each equation in X or Y introduces a new index and a new equation).

Theorem 6.5 *For all fixed integer k, $k \geq 1$, when $f_1, \ldots, f_8$ are randomly and independently chosen in F_n, the probability p to have a circle in X, Y (of any length) satisfies $p \leq \frac{m^2}{2 \cdot 2^{2n}} + \left(\frac{m^4}{4 \cdot 2^{4n}} + \frac{6m^2}{2^{2n}} \right) + \sum_{\lambda=6}^{k} \frac{\lambda^{2\lambda} m^2}{2^{2n}} + \left(\frac{m^{k+1}}{2^{nk}} + \frac{k^{2k} m^2}{2^{2n}} \right)$.*

Proof If we have a circle in X, Y, then we have a circle of length 2 (probability $\leq \frac{m^2}{2 \cdot 2^{2n}}$ from theorem 5.2), or a circle of length 4 (probability $\leq \frac{m^4}{4 \cdot 2^{4n}} + \frac{6m^2}{2^{2n}}$ from theorem 5.3), or we have a circle of length between 6 an k (probability $\leq \sum_{\lambda=6}^{k} \frac{\lambda^{2\lambda} m^2}{2^{2n}}$ from theorem 5.5), or we have a line in X, Y of length k (probability $\leq \frac{m^{k+1}}{2^{nk}} + \frac{k^{2k} m^2}{2^{2n}}$ from theorem 6.4).

Theorem 6.6 *For all fixed integer k, $k \geq 1$, the probability p to distinguish Benes functions from random functions of $2n$ bits $\to$ $2n$ bits in any CPA-2 attack with m chosen messages always satisfies $p \leq (6 + \frac{1}{2} + \sum_{\lambda=6}^{k} \lambda^{2\lambda} + k^{2k}) \frac{m^2}{2 \cdot 2^{2n}} + \frac{1}{4} \frac{m^4}{2^{4n}} + \frac{m^{k+1}}{2^{nk}}$ (when $f_1, \ldots, f_8$ are randomly and independently chosen in F_n). So if k is fixed, $n \to \infty$ and $m^{k+1} \ll 2^{nk}$, then p will be $\ll 1$. So, for any k, for sufficiently large n, $m \ll 2^{nk/(k+1)}$ gives CPA-2 security for Benes. So, for any $\varepsilon > 0$, for sufficiently large n, $m \ll 2^{n(1-\varepsilon)}$ gives CPA-2 security for Benes.*

Proof Theorem 6.6 follows immediately from theorem 6.5 and theorem 5.2.

7 Modified Benes, i.e. Benes with $f_2 = f_3 = Id$

7.1 First comments on modified Benes

If we take $f_2 = f_3 = Id$ in the Benes schemes, we obtain a scheme called "Modified Benes" (see [1]). Then we have: $X_i = f_1(L_i) \oplus R_i$, $Y_i = L_i \oplus f_4(R_i)$ and the output $[S_i, T_i]$ is such that: $S_i = f_5(X_i) \oplus f_6(Y_i)$ and $T_i = f_7(X_i) \oplus f_8(Y_i)$. In [1] it is said that the probability p to distinguish this modified Benes from a random function of $2n$ bits $\to 2n$ bits satisfies $p \leq \frac{m^2}{2^{2n}}$ since we can proceed as for Benes. This evaluation is too optimistic. First, we have at least the same attack with $p \simeq \frac{7m^2}{4 \cdot 2^{2n}}$ as done for Benes in appendix D. Second, modified Benes require a specific analysis since it behaves not exactly as Benes. For example, let us evaluate p_4, the probability to have a circle in X, Y of length 4 for modified Benes. We have: $X_i = X_j$ and $X_k = X_l$ if and only if $f_1(L_i) \oplus R_i = f_1(L_j) \oplus R_j$ and $f_1(L_k) \oplus R_k = f_1(L_l) \oplus R_l$. This can occur for example for $L_i = L_k$, $L_j = L_l$ and $R_i \oplus R_j \oplus R_k \oplus R_l = 0$. Here only one index is fixed (for example l) unlike for Benes where we have seen that at least two indices were fixed for the first dependency. So in p_4 we will get a term in $\frac{m^3}{2^{3n}}$ that did not exist in the original Benes. Similarly, if we consider the probability q_3 to have a line $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$, we will get $q_3 \leq \frac{m^4}{2^{3n}} + \frac{2m^3}{2^{2n}}$ (unlike $q_3 \leq \frac{m^4}{2^{3n}} + \frac{6m^2}{2^{2n}}$ for the original Benes). So here we have a term in $\frac{m^3}{2^{2n}}$, and therefore we will have to consider longer lines in X, Y to get a security in $m \ll 2^{3n/4}$ for modified Benes compared with the original Benes. As we will see below, it is however possible to prove that for modified Benes, when ε is fixed and $n \to \infty$, there are no CPA-2 attacks if $m \ll 2^{n(1-\varepsilon)}$. However the evaluation of the security parameter in k that we have obtained is larger for modified Benes compared with the original Benes schemes.

7.2 Ideas of the proof of security when $m \ll 2^{n(1-\varepsilon)}$ for modified Benes

We give here only the main ideas.

Theorem 7.1 *Let us consider a line of $\lambda + \alpha$ equations in X, Y such that the λ first equations may be dependent or independent, and the other α equations are all dependent from the λ first equations. Then we always have:*

$$\alpha \leq (\lambda + 1)^2.$$

Proof We have: $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$, ..., $Y_{i_\lambda} = Y_{i_{\lambda+1}}$ (and these λ equations (A) are dependent or independent), and we have: $X_{i_{\lambda+1}} = X_{i_{\lambda+2}}$, $Y_{i_{\lambda+2}} = Y_{i_{\lambda+3}}$, ..., $Y_{i_{\lambda+\alpha}} = Y_{i_{\lambda+\alpha+1}}$ (and these α equations (B) are dependent from the λ equations of (A)). If an equation $X_i = X_j$ is dependent from previous equations, then L_i and L_j are values that have appeared before, since $X_i = X_j \Leftrightarrow f_1(L_i) \oplus R_i = f_1(L_j) \oplus R_j$, and here we see that $i \neq j$ implies $L_i \neq L_j$. Similarly, if an equation $Y_k = Y_l$ is dependent from previous equations, then R_k and R_l are values that have appeared before, since $Y_k = Y_l \Leftrightarrow L_k \oplus f_4(R_k) = L_l \oplus f_4(R_l)$, and here we see that $k \neq l$ implies $R_k \neq R_l$. Now from the λ equations of (A) we have at most $\lambda + 1$ values L_i and $\lambda + 1$ values R_j, so at most $(\lambda + 1)^2$ values (L_i, R_j) are possible in (B).

Circles in X, Y In a circle (C) in X, Y, we can analyze the equations in X and in Y as we did with theorem 7.1 in a line, if we can put at the end an equation in X or Y which is independent from the others. If not, then this means that all the equations in X and Y are dependent from the other equations in X or Y. However in this case all index i of the circle (C) is such that there is an index j in (C), $j \neq i$ such that $L_i = L_j$ and similarly there is an index k in (C) such that $k \neq i$ and $R_i = R_k$. In this case we will have at least one circle in L, R (with indices from the circle (C) in X, Y) so at least 2 indices can be fixed from the other indices (as we have seen for the original Benes). So for the modified Benes, we will get a security in $m \ll 2^{n(1-\varepsilon)}$ as for the original Benes (but with slightly different security coefficients).

8 Examples of applications

Keyed hash functions In [1] it is explained how Benes schemes can be used for the design of keyed hash function. From an input $[L_i, R_i]$ of $2n$ bits, the Benes transformation gives a keyed hash function of n bits (the key is the functions f_1, f_2, f_3, f_4). By combining this construction with the scheme of [2] it is also possible to obtain a keyed hash function where the inputs can have any length and the outputs will have n bits.

Information-theoretic application Let us first describe a problem. Alice wants to send many encrypted messages to Bob (for example 1 million messages) with a stream cipher. Charlie is an adversary of Alice and Bob. He has "dynamic" access to m messages. "Dynamic" means that he can choose a message, get the corresponding ciphertext and then adaptively choose the next message and get the corresponding ciphertext, etc., m times. Moreover, Charlie has unlimited computing power: he has access to only m messages but he can perform an infinite number of computations. Alice and Bob know a secret K. We want to design an encryption function that will "resist" Charlie's attacks. "Resist" means that, even if Charlie uses the m cleartext/ciphertext pairs he has access to, he has no practical information on the other cleartexts. Benes functions offer a solution for these problems with a length of the key (i.e. the functions f_1, f_2, f_3, f_4) not far from the optimal. The idea is to use the Benes functions to create a stream cipher like this: the message number i, says m_i, will be encrypted as $c_i = Benes(i) \oplus m_i$ (since this is a stream cipher, we do not need here Benes to be invertible). Here i can be any value between 0 and $2^{2n} - 1$, so we can encrypt $N = 2^{2n}$ messages. So here Charlie can choose m values i between 0 and $2^{2n} - 1$ and he will get $Benes(i)$. The length of the key is here $K = 4 \cdot n \cdot 2^n$ bits and the scheme will be secure as long as $m \ll 2^{n(1-\varepsilon)}$ for any fixed ε and sufficiently large n.

9 Conclusion

William Aiello and Ramarathnam Venkatesan did a wonderful work by pointing out the great potentialities of the Benes schemes and by giving some very important parts of a possible proof. Unfortunately, the complete proof of security when $m \ll 2^n$ for CPA-2 is more complex than what they published in [1] due to some possible attacks with circles in L, R. However, a careful analysis of these attacks shows that $\forall \varepsilon > 0$, for large values n the probability p to distinguish Benes schemes from truly random functions satisfies for all CPA-2 attacks: $p \ll 1$ when $m \ll 2^{n(1-\varepsilon)}$ (but we do not have always $p \leq \frac{m^2}{2^{2n}}$ as claimed in [1]), so the final security is in a way similar, at least for large n. One of the key point in our proof was to notice the fact that the expectancy of the number of circles in X, Y may be large (when $m \gg 2^{2n/3}$) while the probability to have at least one such circle is generally negligible (when $m \ll 2^n$). The security bound in $m \ll 2^n$ is also the security bound for the complexity, since we have shown in this paper how to distinguish Benes (and more generally λ rounds of independent Benes schemes for all integer $\lambda \geq 1$) from random functions with a cyphertext only attack of about 2^n messages with about 2^n computations (for Feistel schemes we do not have a similar result).

References

[1] W. Aiello and R. Venkatesan, *Foiling Birthday Attacks in Lenght-Doubling Transformations - Benes: a non-reversible alternative to Feistel*, Eurocrypt '96, LNCS 1070, pp. 307–320, Springer.

[2] I. Damgård, *Design Principles of Hash Functions*, Crypto '89, Springer-Verlag.

[3] O. Goldreich, S. Goldwasser and S. Micali, *How to Construct Random Functions*, *JACM*, 33, pp 792–807, 1986.

[4] M. Luby. *Pseudorandomness and Its Cryptographic Applications, Princeton Computer Science Notes, Princeton University Press.*

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

[6] U. Maurer. *A simplified and Generalized Treatment of Luby-Rackoff Pseudorandom Permutation Generators, Eurocrypt '92*, Lecture Notes in Computer Science 658, pp. 239–255, Springer-Verlag.

[7] U. Maurer. *Information-Theoretic Cryptography, Crypto '99*, Lecture Notes in Computer Science 1666, pp. 47–64, Springer.

[8] U. Maurer. *Indistinguishability of Random Systems, Eurocrypt '02*, Lecture Notes in Computer Science 2332, pp. 110–132, Springer.

[9] U. Maurer and K. Pietrzak. *The security of Many-Round Luby-Rackoff Pseudo-Random Permutations,Eurocrypt '03*, pp. 544–561, Springer.

[10] M. Naor and O. 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 ACM Symp. on Theory of Computing*, 1997, pp. 189–199.

[11] J. Patarin, *New results on pseudo-random permutation generators based on the DES scheme, Crypto '91*, Lecture Notes in Computer Science 576, pp. 301–312, Springer-Verlag.

[12] J. Patarin, *Improved security bounds for pseudorandom permutations*, 4th ACM Conference on Computer and Communications Security, April 1-4, 1997, Zurich, ACM Press, pp. 142–150.

[13] J. Patarin, *Luby-Rackoff: 7 rounds are Enough for* $2^{n(1-\varepsilon)}$ *Security, Crypto '03*, Lecture Notes in Computer Science 2729, pp. 513–529, Springer.

[14] J. Patarin, *Security of Random Feistel Scemes with 5 or more rounds, Crypto '04*, Lecture Notes in Computer Science 3152, pp. 106–122, Springer.

Appendices

A Summary of the security results for Benes and Butterfly schemes

We summarize the security results on Benes and Butterfly schemes on figure 3 and figure 4 below. We also compare them with Feistel schemes. For large values of n the minimum number of computations is always $\geq m$, where m is the number of messages used in the attack.

	Random Ciphertext only attack	KPA	CPA-2
One round of Butterfly	2^n	2^n	4
Benes	2^n	2^n	$\geq 2^{n(1-\varepsilon)}$
λ rounds of Benes $\lambda \geq 1$	2^n	2^n	$\geq 2^{n(1-\varepsilon)}$
3 rounds of Feistel	Does not exist *	$2^{n/2}$ **	$2^{n/2}$ **
λ rounds of Feistel $\lambda \geq 6$	Does not exist *	2^n **	2^n **

Figure 3: Minimum number m of queries needed to distinguish the schemes from random functions of $2n$ bits $\rightarrow 2n$ bits (or from random permutations for Feistel schemes), even if we have access to unbounded computing power. For simplicity we denote 2^α for $\mathcal{O}(2^\alpha)$, i.e. we have security if $m \ll 2^\alpha$.

	Random Ciphertext only attack	KPA	CPA-2
One round of Butterfly	2^n	2^n	4
Benes	2^n	2^n	$\geq 2^{n(1-\varepsilon)} \leq 2^n$
λ rounds of Benes $\lambda \geq 1$	2^n	2^n	$\geq 2^{n(1-\varepsilon)} \leq 2^n$
3 rounds of Feistel	Does not exist *	$2^{n/2}$ **	$2^{n/2}$ **
λ rounds of Feistel $\lambda \geq 6$	Does not exist *	$\geq 2^n \leq 2^{(\lambda-4)n}$ **	$\geq 2^n \leq 2^{(\lambda-4)n}$ **

Figure 4: Minimum number of computations needed to distinguish the schemes from random functions of $2n$ bits $\rightarrow 2n$ bits (or from random permutations for Feistel schemes)

$\geq$: best proved security.
$\leq$: best known attack.
* Feistel schemes are permutations, so the ciphertext of m random messages gives m random values. So there are no ciphertext only attacks from random cleartexts.
**cf [14].

B Benes: Example of CPA-1 attack with $k = 2$ where $p \simeq \frac{m^2}{4 \cdot 2^{2n}}$

Here we will see a simple ciphertext only attack and simple CPA-1 attack with $m \simeq 2 \cdot 2^n$ messages, and about $2 \cdot 2^n$ computations. The CPA-1 attack is not better than the ciphertext only attack that we will see in appendix C, but we will improve this CPA-1 attack in appendix D with $k = 2$ and $k = 4$. These attacks illustrate the fact that for Benes the security with the number of computations is not larger than the security with the number of messages: these attacks are with $2 \cdot 2^n$ computations. These attacks will also illustrates a difference (by a factor only 2 here) between the expectancy of the number of critical "circles" and the probability that at least such circles exist.

- We choose m such that $\sqrt{m}$ is an integer.
- We choose a set L of $\sqrt{m}$ possible values for the L_i values.
- We choose a set R of $\sqrt{m}$ possible values for the R_i values.
- So our messages are all the $\sqrt{m} \times \sqrt{m} = m$ values $[L_i, R_i]$, where $L_i \in L$ and $R_i \in R$.

(This is a non adaptive chosen plaintext attack, i.e. CPA-1, with m messages). Now we count the number N of (i, j), $i < j$, such that: $S_i = S_j$ and $T_i = T_j$.

First case: random functions For random functions, the average value of N is $\frac{m(m-1)}{2 \cdot 2^{2n}}$, since we have $\frac{m(m-1)}{2}$ values (i, j), $i < j$, and when i and j are fixed, we have a probability $\frac{1}{2^{2n}}$ to have $S_i = S_j$ and $T_i = T_j$.

Remark: It can also be shown that the standard deviation from the average value is about $\sqrt{\frac{m(m-1)}{2 \cdot 2^{2n}}}$, i.e. about $\frac{m}{\sqrt{2} \cdot 2^n}$.

Second case: Benes functions For Benes functions,

$$\begin{cases} S_i = S_j \\ T_i = T_j \end{cases} \Leftrightarrow \begin{cases} f_5(X_i) \oplus f_6(Y_i) = f_5(X_j) \oplus f_6(Y_j) \\ f_7(X_i) \oplus f_8(Y_i) = f_7(X_j) \oplus f_8(Y_j) \end{cases} \qquad (1)$$

This can occur either if ($X_i \neq X_j$ or $Y_i \neq Y_j$) and (1) is satisfied with probability $\frac{1}{2^{2n}}$, or if ($X_i = X_j$) and ($Y_i = Y_j$), i.e. if

$$\begin{cases} f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j) \\ f_3(L_i) \oplus f_4(R_i) = f_3(L_j) \oplus f_4(R_j) \end{cases} \qquad (2)$$

since $i < j$, we have $L_i \neq L_j$ or $R_i \neq R_j$, so (2) occurs with probability $\frac{1}{2^{2n}}$.

So for Benes functions, the average value of N is about $2 \cdot \frac{m(m-1)}{2 \cdot 2^{2n}}$, instead of about $\frac{m(m-1)}{2 \cdot 2^{2n}}$ for random functions.

Probability to get at least one such value Now let i, j, $i < j$, be two indices such that $X_i = X_j$ and $Y_i = Y_j$.

Case a: $L_i \neq L_j$ **and** $R_i \neq R_j$**.** Then let i' be the index such that: $[L_{i'}, R_{i'}] = [L_i, R_j]$, and let j' be the index such that: $[L_{j'}, R_{j'}] = [L_j, R_i]$. Then $\{i', j'\} \neq \{i, j\}$ (because $L_i \neq L_j$ and $R_i \neq R_j$) and $X_{i'} = X_{j'}$, $Y_{i'} = Y_{j'}$ (this comes immediately from (2)), so we will have: $S_{i'} = S_{j'}$ and $T_{i'} = T_{j'}$. So, if (i, j), $i < j$, are such that $S_i = S_j$ and $T_i = T_j$ and $L_i \neq L_j$ and $R_i \neq R_j$, we will have $S_{i'} = S_{j'}$ and $T_{i'} = T_{j'}$ with probability about $\frac{1}{2}$ if we have a Benes function, and with probability $\frac{1}{2^{2n}}$ if we have a random function.

Case b: $L_i = L_j$ **(we can analyze similarly** $R_i = R_j$**).** Then (2) becomes:

$$\begin{cases} f_2(R_i) = f_2(R_j) \\ f_4(R_i) = f_4(R_j) \end{cases} \qquad (3)$$

Now, let i', j' be two indices such that $R_{i'} = R_i$ and $R_{j'} = R_j$. For i', j', we have m possibilities (since for $L_{i'}$ we have $\sqrt{m}$ choices and for $L_{j'}$ we have $\sqrt{m}$ choices).

From (3), we get $X_{i'} = X_{j'}$ and $Y_{i'} = Y_{j'}$, so $S_{i'} = S_{j'}$ and $T_{i'} = T_{j'}$. So if (i, j), $i < j$, is such that $S_i = S_j$ and $T_i = T_j$ and $L_i = L_j$, we will have $S_{i'} = S_{j'}$ and $T_{i'} = T_{j'}$ for all these (i', j') values with probability about $\frac{1}{2}$ if we have a Benes function, and with probability $\frac{1}{2^{2n}}$ for each (i', j') if we have a random function.

Conclusion While analyzing a Benes function, if we get two indices i, j, $i < j$ such that $X_i = X_j$ and $Y_i = Y_j$, we will easily be able to certify with a very high probability that we have a Benes function by testing the i' and j' inputs/outputs. We can notice that the probability to obtain such indices is $\leq \frac{m(m-1)}{4 \cdot 2^n}$ since each time we get one such index we have in fact immediately 2 or m such indices, and since the average number of such indices is exactly $\frac{m(m-1)}{2 \cdot 2^n}$ for Benes functions.

Remark For large values of m such that $m(m-1) < 4 \cdot 2^n$, the probability to obtain such indices can be as near as wanted to $\frac{m(m-1)}{4 \cdot 2^n}$, since for large values of m, the number of (i, j), $i < j$, such that $L_i = L_j$ or $R_i = R_j$ becomes negligible compared with the number of (i, j), $i < j$, such that $L_i \neq L_j$ and $R_i \neq R_j$ (i.e. $m\sqrt{m}$ becomes negligible compared with $\frac{m(m-1)}{2} - m\sqrt{m}$).

Conclusion With $k = 2$, we have obtained here an attack with a probability to distinguish Benes functions from random functions of about $\frac{m(m-1)}{4 \cdot 2^{2n}}$, and an average number of critical values i, j, $i < j$, with $X_i = X_j$ and $Y_i = Y_j$ (i.e. an average number of circles in X, Y of length 2) of about $\frac{m(m-1)}{2 \cdot 2^{2n}}$.

C Benes and λ rounds of Benes: Example of Ciphertext only attack with about $2 \cdot 2^n$ computations

Let $[L_i, R_i]$ be m random messages. Let N be the number of i, j, $i < j$, such that: $S_i = S_j$ and $T_i = T_j$. With a similar analysis as done in appendix B for the CPA-1 attack, we can easily show that for random functions $N \simeq \frac{m(m-1)}{2 \cdot 2^{2n}}$, and for Benes functions the average value of N is about $N \simeq 2 \cdot \frac{m(m-1)}{2 \cdot 2^{2n}}$ (since $S_i = S_j$ and $T_i = T_j$ can occur if $X_i = X_j$ and $Y_i = Y_j$ with probability $\simeq \frac{1}{2^{2n}}$, or if $X_i \neq X_j$ or $Y_i \neq Y_j$ with probability $\simeq \frac{1}{2^n}$, when i and j are fixed). The probability to distinguish Benes functions from random functions with this ciphertext only attack is about $\frac{m(m-1)}{2 \cdot 2^{2n}}$ (when this value is < 1). (So this ciphertext only attack is slightly better than the CPA-1 attack of appendix B. We have introduced the CPA-1 attack because it illustrates what we will do in appendix D).

Remark More generally, for all integer $\lambda \geq 1$, this ciphertext only attack (i.e. counting the number N of i, j such that $S_i = S_j$ and $T_i = T_j$) distinguishes λ independent rounds of Butterfly from random functions with about m random messages and about 2^n complexity. So, unlike what appears with Feistel schemes (see [14] or appendix A), the number of computations to be done to distinguish λ Butterfly from random functions with our best known attacks do not increase with λ. For some applications Benes schemes may therefore be less useful than Feistel schemes, even if the permutations are not required.

Complexity The number of computations needed in these attacks (KPA or CPA-1) is about $2 \cdot 2^n$ (with the same memory) since we can store the $[S_i, T_i]$ values and look for collisions.

Remark It is also possible to need only $\frac{2 \cdot 2^n}{\lambda}$ memory with $\lambda(2 \cdot 2^n)$ computations with the usual time/memory tradeoff algorithm (storing $\frac{2 \cdot 2^n}{\lambda}$ values $[S_i, T_i]$ at each time).

D Benes: Example of CPA-1 attack with $k = 2$ and $k = 4$ where $p \simeq \frac{7m^2}{4 \cdot 2^{2n}}$

Here we will see an attack where the probability p to distinguish a random function from a Benes function can be as near as wanted to $\frac{7m(m-1)}{4 \cdot 2^{2n}}$ (for large values m and when $\frac{7m(m-1)}{4 \cdot 2^{2n}}$ is < 1). This shows that the result claimed in [1] (page 318 it is written: $p \leq \frac{m^2}{2^{2n}}$) is not always true (since $\frac{7}{4} > 1$). Moreover this example illustrates with $k = 4$ many things that we consider in this paper for general values of k. The beginning of the attack is similar with the attack given in appendix B:

- We choose m such that $\sqrt{m}$ is an integer.
- We choose a set L of $\sqrt{m}$ possible values for the L_i values.
- We choose a set R of $\sqrt{m}$ possible values for the R_i values.
- Our messages are all the $\sqrt{m} \times \sqrt{m} = m$ values $[L_i, R_i]$, where $L_i \in L$ and $R_i \in R$.

(this is a CPA-1 attack with m messages).Now we count the number N of $\{i, j, k, l\}$, i, j, k, l pairwise distinct, such that: $L_i = L_j$, $L_k = L_l$, $R_i = R_k$, $R_j = R_l$, $S_i \oplus S_j \oplus S_k \oplus S_l = 0$, $T_i \oplus T_j \oplus T_k \oplus T_l = 0$ and such that we do not have two indices α and β, $\alpha \neq \beta$, such that $\alpha, \beta \in \{i, j, k, l\}$ and:

$$\begin{cases} S_\alpha = S_\beta \\ T_\alpha = T_\beta \end{cases} \qquad (*)$$

This extra condition $(*)$ is here to guarantee that this attack of appendix D is really different from the attack of appendix B. At the end we will be able, if we want, to combine the two attacks.

First case: random functions For random functions, the average value of N is about $\frac{A}{2^{2n}}$, where A is the number of circles in L, R of length 4, i.e. the number of $\{i, j, k, l\}$, i, j, k, l pairwise distinct, such that $L_i = L_j$, $L_k = L_l$, $R_i = R_k$, $R_j = R_l$. We can find the exact value of A: we have $A = \frac{m}{4}(\sqrt{m} - 1)^2$ (Proof: For i we have m possibilities.Then for j such that $L_i = L_j$ and $i \neq j$ we have $\sqrt{m} - 1$ possibilities. Then for k such that $R_k = R_i$ and $k \neq i$ (i.e. $L_k \neq L_i$) we have $\sqrt{m} - 1$ possibilities. Then for l such that $L_l = L_k$ and $R_l = R_j$ we have exactly one possibility when i, j, k are fixed. Like this we have counted all the circles exactly 4 times (we can start the circle with i, j, k or l), so $A = \frac{m}{4}(\sqrt{m} - 1)^2$as claimed).

Second case: Benes functions For Benes functions,

$$\begin{cases} S_i \oplus S_j \oplus S_k \oplus S_l = 0 \\ T_i \oplus T_j \oplus T_k \oplus T_l = 0 \end{cases} \Leftrightarrow$$

$$\begin{cases} f_5(X_i) \oplus f_5(X_j) \oplus f_5(X_k) \oplus f_5(X_l) = f_6(Y_i) \oplus f_6(Y_j) \oplus f_6(Y_k) \oplus f_6(Y_l) \\ f_7(X_i) \oplus f_7(X_j) \oplus f_7(X_k) \oplus f_7(X_l) = f_8(Y_i) \oplus f_8(Y_j) \oplus f_8(Y_k) \oplus f_8(Y_l) \end{cases} \qquad (1)$$

This can occur either if the X_i values and the Y_i values can be eliminated two by two (for example if $X_i = X_j$, $X_k = X_l$, $Y_i = Y_k$ and $Y_j = Y_l$), or with probability $\frac{1}{2^{2n}}$ when i, j, k, l are fixed if the X_i values and the Y_i values cannot be eliminated two by two. However we do not want to have two indices α and β, $\alpha \neq \beta$, such that $\alpha, \beta \in \{i, j, k, l\}$ and $X_\alpha = X_\beta$ and $Y_\alpha = Y_\beta$ because this would imply $S_\alpha = S_\beta$ and $T_\alpha = T_\beta$ in contradiction with the condition $(*)$ above. So the X_i values and the Y_i values can be eliminated two by two if and only if we have a circle in X, Y of length 4 (i.e. if we can chose i_1, i_2, i_3, i_4 pairwise distinct in $\{i, j, k, l\}$ with $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$ and $Y_{i_4} = Y_{i_1}$). We have here 6 possible circles:

1. $X_i = X_j$, $Y_j = Y_k$, $X_k = X_l$ and $Y_l = Y_i$
2. $X_i = X_j$, $Y_j = Y_l$, $X_l = X_k$ and $Y_k = Y_i$
3. $X_i = X_k$, $Y_k = Y_j$, $X_j = X_l$ and $Y_l = Y_i$
4. $X_i = X_k$, $Y_k = Y_l$, $X_l = X_j$ and $Y_j = Y_i$

5. $X_i = X_l$, $Y_l = Y_j$, $X_j = X_k$ and $Y_k = Y_i$
6. $X_i = X_l$, $Y_l = Y_k$, $X_k = X_j$ and $Y_j = Y_i$

Moreover, since we have $L_i = L_j$, $L_k = L_l$, $R_i = R_k$, $R_j = R_l$, we always have $X_i \oplus X_j \oplus X_k \oplus X_l = 0$ and $Y_i \oplus Y_j \oplus Y_k \oplus Y_l = 0$ (because $X_i \oplus X_j \oplus X_k \oplus X_l = f_1(L_i) \oplus f_2(R_i) \oplus f_1(L_j) \oplus f_2(R_j) \oplus f_1(L_k) \oplus f_2(R_k) \oplus f_1(L_l) \oplus f_2(R_l)$ and similarly for Y).
So each of the 6 possible circles have a probability $\frac{1}{2^{2n}}$ to be true when f_1, f_2, f_3, f_4 are randomly chosen (since 2 of the 4 equalities are implied by the 2 other equalities). For example, we have $X_i = X_j$, $Y_j = Y_k$, $X_k = X_l$, $Y_l = Y_i$ if and only if $f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j)$ and $f_3(L_j) \oplus f_4(R_j) = f_3(L_k) \oplus f_4(R_k)$ i.e. if and only if $f_2(R_i) = f_2(R_j)$ and $f_3(L_i) \oplus f_4(R_j) = f_3(L_k) \oplus f_4(R_i)$. So for Benes functions, the average value of N is about $\frac{7A}{2^{2n}}$, where A is the number of "4-circles in L, R" (7=6+1 since we have 6 possible circles and a probability $\frac{1}{2^{2n}}$ to have (1) if we have no such circles).

Remark Moreover unlike what appeared with $X_\alpha = X_\beta$ and $Y_\alpha = Y_\beta$ in appendix B, none of these 6 conditions is equivalent to another of these 6 conditions, so the probability that at least one of these conditions is satisfied is really near $\frac{6A}{2^{2n}}$ (for large values of m and when $\frac{6A}{2^{2n}} < 1$).

Conclusion With $k = 4$, we have obtained here an attack with a probability to distinguish Benes functions from random functions of about $\frac{6m^2}{4 \cdot 2^{2n}}$ and an average number of about also $\frac{6m^2}{4 \cdot 2^{2n}}$ critical values $\{i, j, k, l\}$. This attack can also be combined with the attack with $k = 2$ given in appendix B. Then we obtain an attack with a probability of success of about $\frac{7m^2}{4 \cdot 2^{2n}}$ (with an average number of $\frac{8m^2}{4 \cdot 22^n}$ critical values).

E Why fixing the proof of [1] was not easy when $m \gg 2^{2n/3}$

It may seem difficult to use the results of section 5 to get a security in $2^{n(1-\varepsilon)}$ for all $\varepsilon > 0$, since k can be (a priori) as large as m, and then $\frac{k^{2k} m^3}{2^{4n}}$ is not at all negligible when $m \ll 2^{n(1-\varepsilon)}$. Moreover, we can choose m as a square of an integer, and choose all the $[L_i, R_i]$, $1 \le i \le m$, such that $L_i \in L$ and $R_i \in R$ where L and R are sets of only $\sqrt{m}$ values. Then let A be the set of all the circles in L, R of length k that we can generate such that two different circles of A have at least one different index. If we consider one such circle C, the probability p that we will get a circle in X, Y between the indices of C can be evaluated as $p \ge$ about $\frac{(k-1)!}{2^{n(k-2)}}$, since we have potentially $(k-1)!$ possible circles in X, Y on the m indices, and since at least two equations (one in X and one in Y) are implied by the other equations in X and Y due to the circle in L, R. So the expectancy for the number of circles in X, Y of A that we will find can be evaluated as $\ge$ about $\frac{|A|(k-1)!}{2^{n(k-2)}}$. Moreover, with our very specific chosen values L_i and R_i, we can show that $|A|$ will be $\simeq \frac{m^{k/2}}{k}$ (for $k = 4$ the exact value is $|A| = \frac{m}{4} \cdot (\sqrt{m} - 1)^2 \simeq \frac{m^2}{4}$). Here, we can have $\frac{m^{k/2}}{k}(k-1)! \gg 2^{n(k-2)}$, with $m \ll 2^n$. For example, with $k = \frac{m}{2}$, it is possible to show that this may indeed happen when $m \gg 2^{2n/3}$. So the expectancy of the number N of circles in X, Y may be large. Nevertheless the probability to obtain at least one such circle will be always negligible when $m \ll 2^n$, as we have seen in section 6. One reason for this is that in a line of equations in X, Y (i.e. $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, …, $Y_{i_{k-1}} = Y_{i_k}$) the value k is not bounded by a fixed integer when $m \ll 2^n$, but the probability to have $k \ge \frac{2^n}{2}$ for example is negligible. We can also notice that all the circles of A are not independent, since we have about $\frac{m^{k/2}}{k}$ circles in A and they are all built from k points chosen in the same set of m points. The expectancy of N is the sum of the expectancies on all the elements of A (the expectancy of a sum is the sum of the expectancies, even if the variables are not independent). However the probability for N to be $\neq 0$ is not the sum on all the elements of A of the probability to be $\neq 0$ (they are not independent). So we cannot hope to fix the proof of [1] just by computing the expectancy of the number of circles of length k and by summing them. We need to introduce the probability to obtain a line of length k in X, Y. This is what we have done in section 6.

F Benes: Circles in X, Y with $k = 6$

(We give here another example, $k = 6$ since with $k \geq 6$ a term in $\gamma \cdot \frac{m^\alpha}{2^{\beta m}}$ will appear, with $\alpha < \beta$, but with a "large" γ, so $k = 6$ is a better example of the general case than $k = 2$ or $k = 4$).

Theorem F.1 *The probability p_6 to have a circle in X, Y of length 6, when f_1, f_2, f_3, f_4 are randomly chosen in F_n satisfies: $p_6 \leq \frac{m^6}{6 \cdot 2^{6n}} + \frac{36m^4}{2^{5n}} + \frac{128m^3}{2^{4n}}$.*

Proof Here we want 6 pairwise distinct $i_1, i_2, i_3, i_4, i_5, i_6$ such that:

$$(6) \begin{cases} f_1(L_{i_1}) \oplus f_2(R_{i_1}) = f_1(L_{i_2}) \oplus f_2(R_{i_2}) \\ f_1(L_{i_3}) \oplus f_2(R_{i_3}) = f_1(L_{i_4}) \oplus f_2(R_{i_4}) \\ f_1(L_{i_5}) \oplus f_2(R_{i_5}) = f_1(L_{i_6}) \oplus f_2(R_{i_6}) \end{cases} \text{ and } (7) \begin{cases} f_3(L_{i_2}) \oplus f_4(R_{i_2}) = f_3(L_{i_3}) \oplus f_4(R_{i_3}) \\ f_3(L_{i_4}) \oplus f_4(R_{i_4}) = f_3(L_{i_5}) \oplus f_4(R_{i_5}) \\ f_3(L_{i_6}) \oplus f_4(R_{i_6}) = f_3(L_{i_1}) \oplus f_4(R_{i_1}) \end{cases}$$

Case 1 In (6) and (7) the 6 equations are independent. Here the probability to obtain (6) and (7) will be $\leq \frac{m^6}{6 \cdot 2^{6n}}$.

Case 2 One equation is equivalent to another one and the 5 other equations are independent. Here we have 3 possibilities for the choice of these equalities (since we have 3 possibilities for the other equations of (6)), and when these equations are chosen, we have 6 cases for the L_i, R_i values with in each of these 6 cases, $\leq m^2$ possibilities for the indices in the two equations (as we have seen in section 5.3 with $k = 4$). We have the same property with the equations of (7) instead of (6). So we have $3 \times 6 \times 2 = 36$ possibilities for one equation equivalent to the other one. So the probability here is $\leq \frac{36m^4}{2^{5n}}$ (m^4 since two indices are fixed from the others, and 2^{5n} since 5 equations are independent).

Case 3 We have a circle C in L, R on the 6 indices $i_1, \dots, i_6$, and no other circle independent from C can generate a dependency between some equations of (6) and (7). Here we can associate two by two all the indices with equalities in R, and we can associate two by two all the indices with equalities in L. So the $\oplus$ of all the equations of (6) is 0, and similarly the $\oplus$ of all the equations of (7) is 0. Since (by hypothesis here) we have no other circle than (C) that can generate dependencies between the equations of (6) and (7), we have exactly $6 - 2 = 4$ independent equations her in (6) and (7). 3 of the 6 indices are fixed from the other 3 since we have a circle in L, R on the 6 indices. We have 5! possibilities for the circle in L, R ($L_{i_1} = L_\alpha$ with 5 possibilities for $\alpha \neq i_1$, then $R_\alpha = R_\beta$ with 4 possibilities for $\beta \neq \alpha$ and $\beta \neq i_1$ etc.). So the probability here is $\leq \frac{120m^3}{2^{4n}}$.

Case 4 We have $R_{i_1} = R_{i_2} = R_{i_3}$, $R_{i_4} = R_{i_5} = R_{i_6}$, $L_{i_1} = L_{i_6}$, $L_{i_2} = L_{i_5}$, $L_{i_3} = L_{i_4}$, or similarly the same conditions by changing R with L and L with R, or by changing i_1 by i_2, i_3 by $i_4 \dots i_6$ by i_1 (so we have here $2 \times 2 = 4$ possibilities). Here i_2, i_4, i_6 are fixed when i_1, i_3, i_5 are given (for example i_2 is fixed since $L_{i_2} = L_{i_5}$ and $R_{i_2} = R_{i_1}$). So we have $\leq m^3$ possibilities for the indices. Here 4 of the 6 equations of circle are independent (no more equalities in L, R are possible since it would create $L_i = L_j$ and $R_i = R_j$ with $i \neq j$). So the probability here is $\leq \frac{4m^3}{2^{4n}}$.

Remarks

1. Here we will have $X_{i_2} = X_{i_5}$ and $Y_{i_2} = Y_{i_5}$ in addition to the 6 relations in X, Y of the circle given by the equations of (6) and (7). So we have here a circle in X, Y of length 6, and at least one circle of length 2. So this condition 4 is useful for p_6 but not for p'_6.
2. Here all the L_i and R_i cannot be associated two by two (R_{i_1} can be associated with R_{i_2} but then R_{i_3} is alone) so the $\oplus$ of all the equations of (6) or (7) is not necessary 0.

Case 5 We have $R_{i_1} = R_{i_3} = R_{i_5}$, $R_{i_2} = R_{i_4} = R_{i_6}$, $L_{i_1} = L_{i_2}$, $L_{i_3} = L_{i_4}$,$L_{i_5} = L_{i_6}$, or similarly the same conditions by changing R with L and L with R, or by changing i_1 by i_2, i_3 by $i_4 \ldots i_6$ by i_1. Here i_2, i_3, i_6 are fixed when i_1, i_4, i_5 are given. So we have $\leq m^3$ possibilities for the indices. Here 4 of the 6 equations of circle are independent. So the probability here is $\leq \frac{4m^3}{2^{4n}}$.

Remark Here we will have $Y_{i_1} = Y_{i_4}$ in addition to the 6 relations in X, Y of the circle given by the equations of (6) and (7). So we have here a circle in X, Y of length 6, and at least one circle of length 4: $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$, $Y_{i_4} = Y_{i_1}$. So this condition 5 is useful for p_6 but not for p'_6.

Conclusion it is possible to check that for $k = 6$ we are always in one of these 5 cases. So $p_6 \leq \frac{m^6}{6 \cdot 2^{6n}} + \frac{36m^4}{2^{5n}} + \frac{128m^3}{2^{4n}}$, as claimed.

G Improvements of theorem 5.5

The value $|\mathcal{C}_k|$ Let $\mathcal{C}_k$ be the set of all possible non equivalent equalities in L and R between the indices $\{i_1, \ldots, i_k\}$. We have $|\mathcal{C}_k| \leq k^{2k}$. Proof: We can find all the equalities in L and R if we know all the $(l(i), r(i))$, $i \in \{i_1, \ldots, i_k\}$, where $l(i)$ is the smallest $j \leq i$ such that $L_j = L_i$ and $r(i)$ is the smallest $j \leq i$ such that $R_j = R_i$. Since we have $\leq k^2$ possibilities for $(l(i), r(i))$ we have immediately $|\mathcal{C}_k| \leq k^{2k}$. However more precise evaluations of $|\mathcal{C}_k|$ are possible. For example we can prove that $|\mathcal{C}_k| \leq \left(\sum_{\lambda=1}^{k/2} \frac{(\lambda+1)^k}{\lambda!}\right)^2$ and we can show that this value is near k^k instead of k^{2k} (the evaluation k^{2k} was enough for our theorems but the coefficient k^{2k} can be improved). Proof: we look first for the possibilities for the equations in L. Let $\mathcal{R}$ be the relation such that for $i, j \in \{i_1, \ldots, i_k\}$, $i\mathcal{R}j \Leftrightarrow L_i = L_j$. This is a relation of equivalence. Let λ be the number of equivalence classes with at least 2 different elements in the classes. We have $\lambda \leq k/2$. Now let B be a set of $\lambda + 1$ boxes, $B = \{B_0, \ldots, B_{\lambda+1}\}$. From an application f of $\{i_1, \ldots, i_k\} \to B$ we can associate equalities in L like this:
• if $f(i) \in B_0$ then there is no $j \neq i$ such that $L_i = L_j$.
• if $f(i) \in B_k$, $k \neq 0$ then the indices j such that $L_j = L_i$ will be exactly all the indices j such that $f(j) \in B_k$. We have $\leq (\lambda + 1)^k$ possibilities for f such that $\forall \alpha$, $1 \leq \alpha \leq \lambda + 1$, $\exists j \in \{i_1, \ldots, i_k\}$ / $f(j) \in B_\alpha$, and each set of possible equations in L can be associate with $\lambda!$ such functions f since we can permute $B_1, \ldots, B_\lambda$ (but not B_0). So the number of non equivalent possibilities for the equations in L is $\leq \sum_{\lambda=1}^{k/2} \frac{(\lambda+1)^k}{\lambda!}$ (the only case with $\lambda = 0$ can be included with $\lambda = 1$), and similarly for the equations in R. So for the equations in L and R we get $|\mathcal{C}_k| \leq \left(\sum_{\lambda=1}^{k/2} \frac{(\lambda+1)^k}{\lambda!}\right)^2$ as claimed.

Conclusion for p_k Let $A \in \mathcal{C}_k$. Let $\alpha(A)$ be the number of dependent equations of (8) and (9) when the equalities in L and R are those of A. Let $\beta(A)$ be the number of indices of $\{i_1, \ldots, i_k\}$ that we can fix from the other indices of $\{i_1, \ldots, i_k\}$ due to the equalities in L and R of A. Our analysis done in section 5.4 of the equalities of (8) and (9) taken one by one shows that we always have $\alpha(A) \leq \beta(A) + 1$ (the +1 comes

from the last equation). Moreover, if $\alpha(A) \neq 0$, then when we will consider the first equation of (8) or (9) that gives a dependency, this dependency comes from one or more than one circle in L, R between the indices (these circles are not necessary disjoints). Now a circle in L, R has always a length ≥ 4. Moreover in a circle in L, R we can fix at least 50% of the indices from the other indices (we just need to know one over two indices and recover the other with the equalities in L and R of the circle). So the first time where we will get a dependency in X or Y we will have at least 2 indices fixed from the others to get this first dependency. So we always have $\alpha(A) \leq \beta(A)$.
We have $p_k \leq \frac{m^k}{k \cdot 2^{nk}} + \sum_{A \in \mathcal{C}_k} \frac{m^{k-\beta(A)}}{2^{n(k-\alpha(A))}}$ since we have $k - \alpha(A)$ independent equations and $\leq m^{k-\beta(A)}$ possibilities for the indices. Since $\alpha(A) \leq \beta(A)$, we get $p_k \leq \frac{m^k}{k \cdot 2^{nk}} + |\mathcal{C}_k| \frac{m^2}{2^{2n}}$. Moreover if $k \geq 6$ it is possible to show that we will have at least 4 independent equations in a circle of length k in X, Y. Then we get : $p_k \leq \frac{m^k}{k \cdot 2^{nk}} + |\mathcal{C}_k| \frac{m^4}{2^{4n}}$, with $|\mathcal{C}_k| \leq (\sum_{\lambda=1}^{k/2} \frac{(\lambda+1)^k}{\lambda!})^2$ for example, when $k \geq 6$.

H An example for theorem 5.5

In the proof of theorem 5.5, terms in $\mathcal{O}\left(\frac{m^\alpha}{2^{n\alpha}}\right)$, for some values α, appear for independent equations of (8) and (9) (we then have a term in $\mathcal{O}\left(\frac{m^k}{2^{nk}}\right)$) or with dependent equations. For dependent equations, all the terms are $\leq \mathcal{O}\left(\frac{m^2}{2^{2n}}\right)$ when k is fixed, as proved in theorem 5.5. Is it really possible to have a term in $\mathcal{O}\left(\frac{m^\alpha}{2^{n\alpha}}\right)$ or is it possible to prove that all the terms are in $\mathcal{O}\left(\frac{m^{\alpha-1}}{2^{n\alpha}}\right)$ for some values α when we have at least one dependent equation? In fact, as we will see now, it is really possible to have a term in $\mathcal{O}\left(\frac{m^\alpha}{2^{n\alpha}}\right)$ with some dependent equations. We give such an example in figure 5, with $k = 8$ indices, 4 equations in X and 4 equations in Y. In this example the term is in $\mathcal{O}\left(\frac{m^4}{2^{4n}}\right)$.

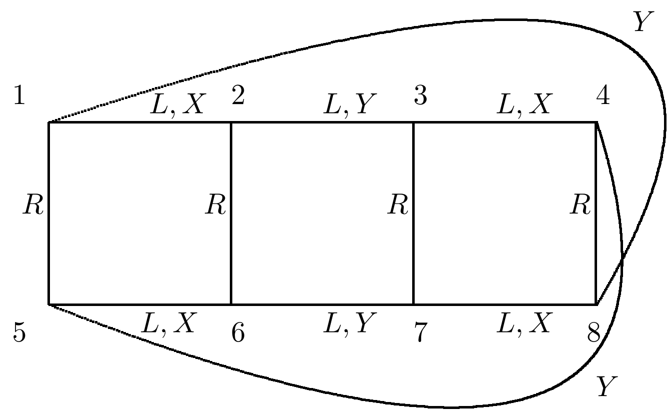

Figure 5: A line shows an equality between two indices. Here 4 indices can be fixed from the other 4 indices and 4 equations are dependent (2 in X and 2 in Y since the $\oplus$ of all the Y is 0, since the L_i variables are identical two by two and the R_i variables are identical two by two).