A Proof of security in $0(2^n)$ for the Benes Scheme

AFRICACRYPT 2008

Jacques PATARIN

Versailles University - France

⋆ Introduction

⋆ Butterfly transformation

⋆ Benes transformation

⋆ A problem in the proof of W. Aiello and R. Venkatesan

⋆ First ideas about our proof

⋆ Properties of“first dependency lines”

⋆ Security of the Benes Schemes

⋆ Open problem : Modified Benes

⋆ Conclusion

$\star$ Introduction

In 1996, W. Aiello and R. Venkatesan have shown how to construct pseudo-random functions of $2n$ bits $\longrightarrow$ $2n$ bits from pseudo-random functions of n bits $\longrightarrow n$ 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 their paper since one of their assertions is wrong.

In this conference (Africacrypt 2008), I will present a complete proof of this result : we have indeed security for Benes when $m \ll 2^n$.(12 years to fix the proof !).

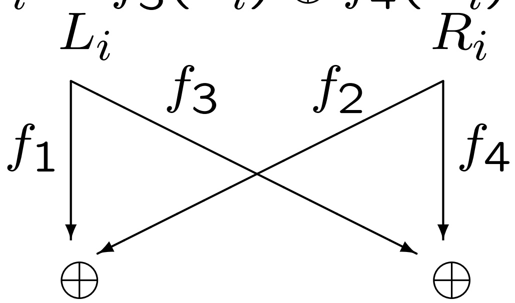
Remark : At ICISC'05, Jacques Patarin and Audrey Montreuil had only partially fixed this problem since for all $\epsilon > 0$, they have proved security when $m \ll f(\epsilon) \cdot 2^{n-\epsilon}$, where f is a function such that $\lim_{\epsilon \to 0} f(\epsilon) = +\infty$

⋆ Butterfly transformation

The f_k are randomly chosen in F_n, the set of all functions of n bits to n bits.

$$X_i = f_1(L_i) \oplus f_2(R_i)$$

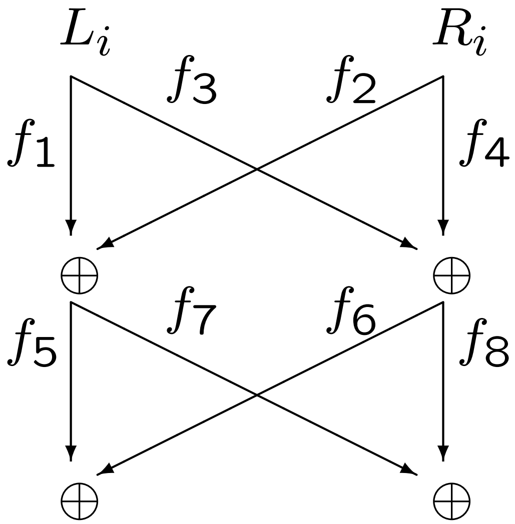
$$Y_i = f_3(L_i) \oplus f_4(R_i)$$



⋆ Benes transformation
(back-to-back Butterfly)

$$S_i = f_5(f_1(L_i) \oplus f_2(R_i)) \oplus f_6(f_3(L_i) \oplus f_4(R_i))$$

$$T_i = f_7(f_1(L_i) \oplus f_2(R_i)) \oplus f_8(f_3(L_i) \oplus f_4(R_i))$$

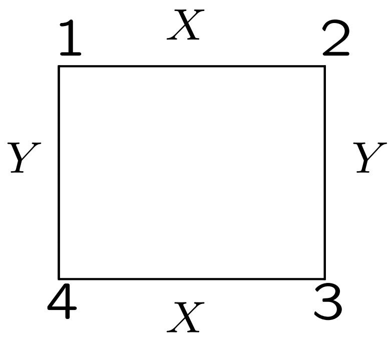


Definition

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.

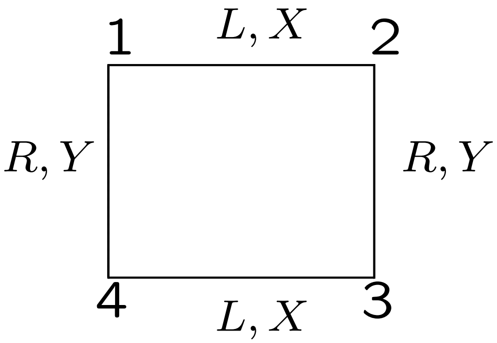
Example : A circle in X,Y of length 4



$\star$ A problem in the proof of Aiello and Venkatesan

Let $[L_1, R_1]$, $[L_2, R_2]$, $[L_3, R_3]$ and $[L_4, R_4]$ be four chosen inputs such that :$L_1 = L_2$, $R_2 = R_3$, $L_3 = L_4$, $R_4 = R_1$ (and $R_1 \neq R_2$ and $L_1 \neq L_3$). Here 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" after a Butterfly. In the paper of Aiello and Venkatesan, it is claimed that $p \leq \frac{1}{2^{4n}}$. However we will see that $p \geq \frac{1}{2^{2n}}$.



With $L_1 = L_2$, $R_2 = R_3$, $L_3 = L_4$ and $R_4 = R_1$, we have :

$$\begin{aligned}
X_1 &= f_1(L_1) \oplus f_2(R_1) \\
X_2 &= f_1(L_2) \oplus f_2(R_2) = f_1(L_1) \oplus f_2(R_2) \\
X_3 &= f_1(L_3) \oplus f_2(R_3) = f_1(L_3) \oplus f_2(R_2) \\
X_4 &= f_1(L_4) \oplus f_2(R_4) = f_1(L_3) \oplus f_2(R_1)
\end{aligned}$$

$$\begin{aligned}
Y_1 &= f_3(L_1) \oplus f_4(R_1) \\
Y_2 &= f_3(L_2) \oplus f_4(R_2) = f_3(L_1) \oplus f_4(R_2) \\
Y_3 &= f_3(L_3) \oplus f_4(R_3) = f_3(L_3) \oplus f_4(R_2) \\
Y_4 &= f_3(L_4) \oplus f_4(R_4) = f_3(L_3) \oplus f_4(R_1)
\end{aligned}$$

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 is $\geq \frac{1}{2^{2n}}$, so it is not $\leq \frac{1}{2^{4n}}$ as claimed in the paper of Aiello and Venkatesan.

This problem is not easily solved : a precise analysis will be needed in order to prove the security result $m \ll 2^n$.

$\star$ First ideas about our proof

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

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

Theorem 1

The probability to distinguish Benes functions from random functions of $2n$ bits → $2n$ bits in a CPA-2 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.

Proof of Theorem 1

With Benes, we have :

$$\forall i,\ 1 \leq i \leq m,\ Benes(f_1, \ldots, f_8)[L_i, R_i] = [S_i, T_i] \Leftrightarrow$$
$$\begin{cases} S_i = f_5(X_i) \oplus f_6(Y_i) \\ T_i = f_7(X_i) \oplus f_8(Y_i) \end{cases} \qquad (1)$$
$$\text{with } \begin{cases} X_i = f_1(L_i) \oplus f_2(R_i) \\ Y_i = f_3(L_i) \oplus f_4(R_i) \end{cases}$$

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, $i < j$.

Circles in X, Y with $k = 2$

Theorem

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 $X_i = X_j$ and $Y_j = Y_i$, i.e. such that :

$$\begin{cases} f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j) & (1) \\ f_3(L_i) \oplus f_4(R_i) = f_3(L_j) \oplus f_4(R_j) & (2) \end{cases}$$

$$\begin{cases} f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j) & (1) \\ f_3(L_i) \oplus f_4(R_i) = f_3(L_j) \oplus f_4(R_j) & (2) \end{cases}$$

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 (1) is satisfied, and when f_3 is fixed, we have exactly $\frac{|F_n|}{2^n}$ functions f_4 such that (2) is satisfied.

$$\begin{cases} f_1(L_i) \oplus f_2(R_i) = f_1(L_j) \oplus f_2(R_j) & (1) \\ f_3(L_i) \oplus f_4(R_i) = f_3(L_j) \oplus f_4(R_j) & (2) \end{cases}$$

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 (1) is satisfied and exactly $\frac{|F_n|}{2^n}$ functions f_3 such that (2) 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 (1) and (2) 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.

Theorem A [Patarin, Montreuil, ICISC'05]
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 : $p_k \leq k^{2k} \frac{m^2}{2^{2n}}$.

Definition

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 $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$, …, $Y_{i_{k-1}} = Y_{i_k}$, $X_{i_k} = X_{i_{k+1}}$.

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 $X_{i_1} = X_{i_2}$, $Y_{i_2} = Y_{i_3}$, $X_{i_3} = X_{i_4}$, …, $X_{i_{k-1}} = X_{i_k}$, $Y_{i_k} = Y_{i_{k+1}}$.

Theorem B [Patarin, Montreuil, ICISC'05]

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, when $k \geq 4$,

$$q_k \leq \frac{m^{k+1}}{2^{nk}} + \frac{k^{2k} m^2}{2^{2n}}$$

$\star$ First dependency lines

Definition A line in X, Y of length k will be called a "first dependency" line when all the equations in X, Y except the last one are independent and when the last one (i.e. the equation number k) is a consequence of the previous equations in X, Y.

Example : If $L_1 = L_3$, $L_2 = L_4$, $R_1 = R_2$, $R_3 = R_4$, then $(X_1 = X_2)$, $(Y_2 = Y_3)$, $(X_3 = X_4)$ is a "first dependency line", since $(X_1 = X_2)$ and $(Y_2 = Y_3)$ are independent, but $(X_3 = X_4)$ is a consequence of $(X_1 = X_2)$.

Definition A circle in X, Y will be called a " circle with one dependency" when all the equations in the circle, except one are independent from the others, and when exactly one is a consequence of the others equations in X, Y.

The key argument in our proof will be this (new) Theorem :

Theorem 2 When f_1, f_2, f_3, f_4 are randomly chosen in F_n, the probability q_k to have a "first dependency line" in X, Y of length k satisfies $q_k \leq k^5 \dfrac{m^{k-1}}{2^{(k-1)n}}$

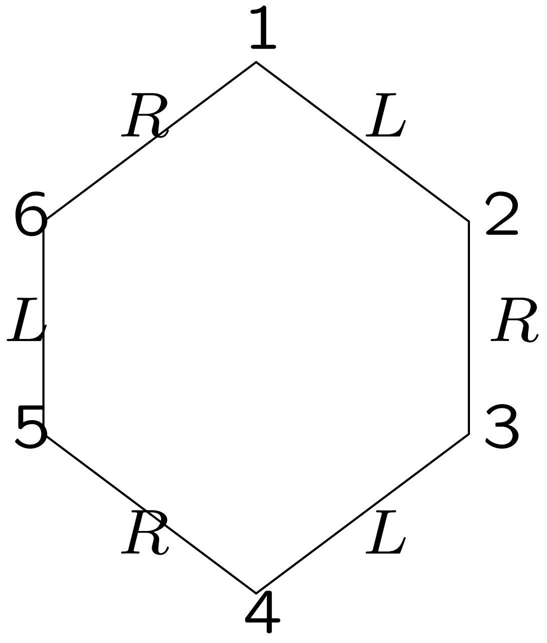
Proof of Theorem 2

a) Rough Evaluation

Since we have $(k-1)$ independent equations in X or Y, when all the indices are fixed the probability to have all these equations is $\frac{1}{2^{(k-1)n}}$. Now, in order to choose the $k+1$ indices of the messages, we have less than m^{k+1} possibilities. Therefore, $q_k \leq \frac{m^{k+1}}{2^{(k-1)n}}$. Moreover, the last equation (in X or Y) is a consequence of the previous equations in X, Y. However, a dependency in these equations implies the existence of a circle in L, R on a subset of the indices involved in the dependency. [The proof is exactly the same as for Theorem 1 except that here we use L, R instead of X, Y and X, Y instead of S, T].

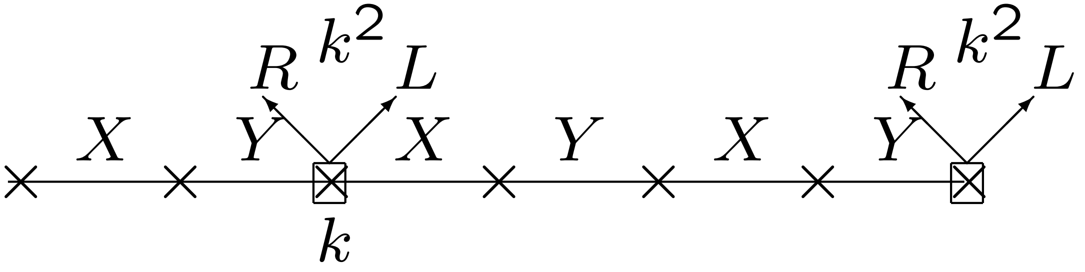
Now if we have a circle in L, R of length α, α even, we know that $\frac{\alpha}{2}$ of the messages in the circle come from the other $\frac{\alpha}{2}$ messages.

Example of a circle in L, R



For example, if $L_1 = L_2$, $R_2 = R_3$, $L_3 = L_4$, $R_4 = R_5$, $L_5 = L_6$, $R_6 = R_1$, we have a circle in L, R of length 6, and if we know the messages 1, 3, 5, then we know (L_1, R_1), (L_3, R_3), (L_5, R_5), and we can deduce (L_2, R_2), (L_4, R_4) and (L_6, R_6), since $(L_2, R_2) = (L_1, R_3)$, $(L_4, R_4) = (L_3, R_5)$ and $(L_6, R_6) = (L_5, R_1)$. In a circle in L, R of length α, we must have $\alpha \geq 4$, since $\alpha = 2$ gives $L_i = L_j$ and $R_i = R_j$, and therefore $i = j$. Therefore, if there is a circle in L, R we will be able to find $\frac{\alpha}{2}$ messages, $\frac{\alpha}{2} \geq 2$, from the other messages of the circle. So, in order to choose $k+1$ indices of the messages in a first dependency line, we will have $O(m^{k-1})$ possibilities (instead of m^{k+1} possibilities since at least 2 messages will be fixed from the others), and therefore $q^k \leq \frac{O(m^{(k-1)})}{2^{(k-1)n}}$. We will now evaluate the term $O(m^{(k-1)})$ more precisely.

b) More precise evaluation An example of line in X, Y



From a first dependency line in X, Y we have just seen that at least two messages of the line, let say messages $[L_a, R_a]$ and $[L_b, R_b]$ are such that $L_a = L_i$, $R_a = R_j$, $L_b = R_k$, $R_b = R_l$ with $i, j, k, l \notin \{a, b\}$.

Moreover, we can choose b to be the last message of the line (since between the two last messages we have a dependency in X or in Y from the other equations in X and Y). Now for a we have less than k possibilities, and for i, j, k, l we have less than $(k-1)^4$ possibilities. Therefore, for the choice of the $k+1$ messages of the line we have less than $k(k-1)^4\, m^{k-1}$ possibilities, which is less than $k^5\, m^{k-1}$. Therefore, $q_k \leq k^5 \frac{m^{k-1}}{2^{(k-1)n}}$ as claimed.

Theorem 3 When f_1, f_2, f_3, f_4 are randomly chosen in F_n, the probability q_k to have a "first dependency line" in X, Y of length k, or a "circle with one dependency" of length $k-1$ (k odd) satisfies : $q_k \leq k^5 \dfrac{m^{k-1}}{2^{(k-1)n}}$.

Proof of theorem 3

This is just a simple extension of Theorem 2. A circle of length $k-1$ with one dependency can be seen as a special line of length k with the first index equal to the index number k, and the proof given for Theorem 2 extended to the classical lines in X, Y and to these special lines gives immediately Theorem 3.

$\star$ Security of Benes Schemes

Theorem 4 When f_1, f_2, f_3, f_4 are randomly chosen in F_n, the probability p to have a circle in X, Y satisfies, if $m \leq \frac{2^n}{2}$

$$p \leq \frac{m^2}{2^{2n}}\left(\frac{1}{1-\frac{m^2}{2^{2n}}}\right) + \frac{m^2}{2^{2n}}\left(\sum_{k=3}^{+\infty} \frac{k^5}{2^{(k-3)}}\right)$$

and $\displaystyle\sum_{k=3}^{+\infty} \frac{k^5}{2^{(k-3)}} = 3^5 + \frac{4^5}{2} + \frac{5^5}{2^2} + \frac{6^5}{2^3} + \ldots$ converges to a finite value.

Therefore, when $m \ll 2^n$, $p \simeq 0$, as wanted.

Proof of theorem 4
For each circle in X, Y of length k, k even, we have three possibilities :

a) Either all the k equations in X, Y are independent. Then the probability to have a circle is less than or equal to $\frac{m^k}{2^{kn}}$.

b) Or there exists a first dependency line of length strictly less than k in the equations in X, Y of the circle.

c) Or the circle is a circle with exactly one dependency.

Now from Theorems 2 and 3, we get immediately :

$$p \leq \Big(\frac{m^2}{2^{2n}} + \frac{m^4}{2^{4n}} + \frac{m^6}{2^{6n}} + \frac{m^8}{2^{8n}} + \ldots\Big) + \sum_{k=3}^{+\infty} \frac{k^5\, m^{k-1}}{2^{(k-1)n}}$$

Therefore, if $m \leq \frac{2^n}{2}$,

$$p \leq \frac{m^2}{2^{2n}}\Big(\frac{1}{1-\frac{m^2}{2^{2n}}}\Big) + \frac{m^2}{2^{2n}}\Big(\sum_{k=3}^{+\infty} \frac{k^5}{2^{(k-3)}}\Big)$$

as claimed (since $\frac{m^{k-3}}{2^{(k-3)n}} \leq \frac{1}{2^{(k-3)}}$). Therefore, from Theorem 1, we see that we have proved the security of Benes when $m \ll O(2^n)$ against all CPA-2, with an explicit O function, as wanted.

$\star$ Open problem : Modified Benes, i.e. Benes with $f_2 = f_3 = \text{Id}$

If we take $f_2 = f_3 = \text{Id}$ in the Benes schemes, we obtain a scheme called "Modified Benes". 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 $T_i = f_7(X_i) \oplus f_8(Y_i)$. It is conjectured that the security for Modified Benes is also in $O(2^n)$ but so far we just have a proof of security in $O(2^{n-\epsilon})$ for all $\epsilon > 0$.

It is interesting to notice that the proof technique used in this paper for the regular Benes cannot be used for the Modified Benes, since, as we will see in the example below, for Modified Benes, unlike for regular Benes, the first 'dependent' equation can fix only one index instead of two.

Example :

If we have $L_1 = L_3$, $L_2 = L_4$, $R_1 \oplus R_2 \oplus R_3 \oplus R_4 = 0$, then we will get the 'line', $X_1 = X_2$, $Y_3 = Y_3$, $X_3 = X_4$ from only two independent equations in f, ($X_1 = X_2$ and $Y_2 = Y_3$), and the first 'dependent' equation, here $X_3 = X_4$, fixes only the index 4 from the previous indices (since $L_4 = L_2$ and $R_4 = R_1 \oplus R_2 \oplus R_3$).

Therefore, a proof of security in $O(2^n)$ for the Modified Benes will be different, and probably more complex than our proof of security on $O(2^n)$ for the regular Benes.

$\star$ Conclusion

W. Aiello and R. 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 their paper due to some possible attacks in L,R.

In this paper we have been able to solve this open problem by improving the analysis and the results of J.Patarin and A.Montreuil at ICISC'05. The key point in our improved proof was to analyse more precisely what happens just after the first 'dependent' equations in X,Y and to use the fact that in this case two 'indices' are fixed from the others.

Therefore we have obtained the optimal security bound (in $O(2^n)$) with an explicit O function. This automatically improves the proved security of many schemes based on Benes.

Thank you for your attention !