A Proof of Security in $O(2^n)$ for the Benes Scheme

Jacques Patarin
Université de Versailles
45 avenue des Etats-Unis, 78035 Versailles Cedex, France
jacques.patarin@prism.uvsq.fr

Abstract. In [1], W. Aiello and R. Venkatesan have shown how to construct pseudorandom functions of $2^n$ bits $\rightarrow 2^n$ bits from pseudorandom 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). This result may have many applications in Cryptography (cf [1,19,18] for example). However, as pointed out in [18] a complete proof of this result is not given in [1] since one of the assertions in [1] is wrong. It is not easy to fix the proof and in [18], only a weaker result was proved, i.e. that in the Benes Schemes we have security when $m \ll f(\epsilon) \cdot 2^{n-\epsilon}$, where $f$ is a function such that $\lim_{\epsilon \rightarrow 0} f(\epsilon) = +\infty$ ($f$ depends only of $\epsilon$, not of $n$). Nevertheless, no attack better than in $O(2^n)$ was found. In this paper we will in fact present a complete proof of security when $m \ll O(2^n)$ for the Benes Scheme, with an explicit $O$ function. Therefore it is possible to improve all the security bounds on the cryptographic constructions based on Benes (such as in [19]) by using our $O(2^n)$ instead of $f(\epsilon) \cdot 2^{n-\epsilon}$ of [18].

Keywords: Pseudorandom function, unconditional security, information-theoretic primitive, design of keyed hash functions, security above the birthday bound.

1 Introduction

In this paper we will study again the “Benes” Schemes of [1] and [18]. (The definition of the “Benes” Schemes will be given in Section 2). More precisely, the aim of this paper is to present a complete proof of security for the Benes schemes when $m \ll O(2^n)$ where $m$ denotes the number of queries in an Adaptive Chosen Plaintext Attack (CPA-2) with an explicit $O$ function. With this security result we will obtain a proof for the result claimed in [1] and this will also solve an open problem of [18], since in [18] only a weaker result was proved (security when $m \ll f(\epsilon) \cdot 2^{n-\epsilon}$ where $f$ is a function such that $\lim_{\epsilon \rightarrow 0} f(\epsilon) = +\infty$). It is important to get precise security results for these schemes, since they may have many applications in Cryptography, for example in order to design keyed hash functions (cf [1]) or in order to design Information-theoretic schemes (cf [18]).
Here we will prove security “above the birthday bound”, i.e. here we will prove security when \( m \ll 2^n \) instead of the “birthday bound” \( m \ll \sqrt{2^n} \) where \( m \) denotes the number of queries in an Adaptive Chosen Plaintext Attack (CPA-2). \( \sqrt{2^n} \) is called the ‘birthday bound’ since when \( m \ll \sqrt{2^n} \), if we have \( m \) random strings of \( n \) bits, the probability that two strings are equal is negligible. \( 2^n \) is sometimes called the ‘Information bound’ since security when \( m \ll 2^n \) is the best possible security against an adversary that can have access to infinite computing power. In fact, in [18], it is shown that Benes schemes can be broken with \( m = O(2^n) \) and with \( O(2^n) \) computations. Therefore security when \( m \ll O(2^n) \) is really the best security result that we can have with Benes schemes.

In [2], Bellare, Goldreich and Krawczyk present a similar construction that provides length-doubling for the input. However their construction is secure only against random queries and not against adaptively chosen queries. Benes schemes, in contrast, produce pseudorandom functions secure against adaptively chosen queries.

It is interesting to notice that there are many similarities between this problem and the security of Feistel schemes built with random round functions (also called Luby-Rackoff constructions), or the security of the Xor of two random permutations (in order to build a pseudorandom function from two pseudorandom permutations). The security of random Feistel schemes above the birthday bound has been studied for example in [13], [15], [17], and the security of the Xor of two random permutations above the birthday bound has been studied for example in [3], [8]. However the analysis of the security of the Benes schemes requires a specific analysis and the proof strategy used for Benes schemes is significantly different than for Feistel or the Xor of random permutations. In fact, our proof of security for Benes schemes in \( m \ll O(2^n) \) is more simple than the proofs of security in \( m \ll O(2^n) \) for Feistel schemes or the Xor of random permutations, since we will be able, as we will see, to use a special property of Benes schemes.

2 Notation

We will use the same notation as in [18].

- \( I_n = \{0,1\}^n \) 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 \( |F_n| = 2^{2n} \).
- 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 \textbf{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:

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