The Indistinguishability of the XOR of k permutations

Benoit Cogliati, Rodolphe Lampe, Jacques Patarin

University of Versailles, France

Abstract. Given k independent pseudorandom permutations $f_1, \ldots, f_k$ over $\{0,1\}^n$, it is natural to define a pseudorandom function by XORing the permutations: $f_1 \oplus \ldots \oplus f_k$. In [9] Stefan Lucks studied the security of this PRF. In this paper we improve the security bounds of [9] by using different proof techniques.

Keywords: Pseudorandom functions, pseudorandom permutations, security beyond the birthday bound, Luby-Rackoff backwards.

1 Introduction

Much research dealt with constructing cryptographic operations from other ones: Levin [6] got "pseudorandom bit generators" from "one-way functions", then Goldreich, Goldwasser and Micali [4] constructed pseudorandom functions (PRFs) from "pseudorandom bit generators". In [1], Aiello and Venkatesan studied how to construct PRFs from smaller PRFs. Luby and Rackoff [7] dealt with the problem of getting pseudorandom permutations (PRPs) from PRFs; further work about their construction can be found in [8, 11]. Our article focuses on the reverse problem of converting PRPs into PRFs named "Luby-Rackoff backwards" which was first considered in [3]. This problem is obvious if we are interested in an asymptotical polynomial versus non polynomial security model (since a PRP is then a PRF), but not if we are interested in achieving more optimal and concrete security bounds. More precisely, the loss of security when regarding a PRP as a PRF comes from the "birthday attack" which can distinguish a random permutation from a random function of n bits to n bits in $2^{\frac{n}{2}}$ operations and $2^{\frac{n}{2}}$ queries. Therefore different ways to build PRF from PRP with a security above $2^{\frac{n}{2}}$ and by performing very few computations have been suggested (see [2, 3, 5, 9]). One of the simplest way is to XOR k independent pseudorandom permutations with $k \geq 2$. In [9] (Theorem 2 p.474) Stefan Lucks proved, with a simple proof, that the XOR of k independant PRPs gives a PRF with security at least in $\mathcal{O}\left(2^{\frac{k}{k+1}n}\right)$. In [2] and [12] difficult analyses of $k = 2$ are given, with proofs that the security is good when the number of queries is lower than $\mathcal{O}\left(\frac{2^n}{n^{2/3}}\right)$ or $\mathcal{O}(2^n)$. For $k \geq 3$ there is a significant gap between the proven security of [9] and the best attacks of [13].

In this paper we reduce this gap by improving the proven security for the XOR of k permutations, $k \geq 3$. Constructions with $k \geq 3$ instead of $k = 2$

are interesting for various reasons. First, our proofs are much simpler than the proofs of [2] and [12]. Second, in many cryptographic applications the size n of the blocks cannot be chosen by the designer of the algorithm since it is imposed by the application. Then it is interesting to have another parameter to decrease the proven advantage of any adversary to a value as small as wanted with a simple construction. Our proof technique is based on the "coefficient H technique" of Patarin (cf [14]). However we only use the first steps (and not all the refinements) in order to keep very simple proofs with still better security results than previously known; we could achieve tighter bounds by using the full technique, but it would require more computations (such as [15]).

Related problems. In [10] the security of the XOR of two **public** permutations are studied (i.e. indifferentiability instead of indistinguishability).

Organisation of the paper. Section 2 presents the notations and basic definitions that are used in this paper. In section 3 and 4, two security bounds are shown with different techniques (respectively the "H_σ coefficient" technique and the "H coefficient" technique). Then both these results are compared to the one from [9] in the last section.

2 Preliminaries

We denote I_n the set of $n-$bits strings and J_n^q the subset of I_n^q of values $(x_i)_{1\leq i\leq q}$ satisfying $x_i \neq x_j, \forall i \neq j$. We denote F_n the set of functions from I_n to I_n and B_n the set of permutations of I_n. The notation $x \in_R E$ stands for "x is chosen randomly with a uniform distribution in E".

An adversary A trying to distinguish between $f_1 \oplus \ldots \oplus f_k$, where $f_i \in_R B_n$ for each $i \in \{1, \ldots, k\}$, from a random function $F \in_R F_n$ is considered to have access to an oracle Q. This oracle either simulates F or $f_1 \oplus \ldots \oplus f_k$. A chooses inputs $x \in \{0,1\}^n$; then Q responds $Q(x) \in \{0,1\}^n$. After at most q queries, A outputs $A(Q) \in \{0,1\}$. $A(Q)$ is then seen as a random variable over $\{0,1\}$. This is an adaptative chosen plaintext attack (cpa). To measure the pseudorandomness of the XOR of k permutations one must evaluate the advantage $\mathbf{Adv}^{\text{cpa}}_{A,f_1\oplus\ldots\oplus f_k}$ of an adversary A which is defined as

$$\mathbf{Adv}^{\text{cpa}}_{A,f_1\oplus\ldots\oplus f_k} = |Pr[A(f_1 \oplus \ldots \oplus f_k) = 1] - Pr[A(F) = 1]|.$$

We write $\mathbf{Adv}^{\text{cpa}}_{f_1\oplus\ldots\oplus f_k}$ for the maximal advantage any adversary can get when trying to distinguish the XOR of k random permutations from a random function.

3 Security Bound from the H_σ technique

3.1 Linking the advantage to a combinatorial problem

Let $k \geq 2$. We use theorem 3 from [14] :

Theorem 1. *Let $\alpha, \beta \in \mathbb{R}^+$ and $q \in \mathbb{N} \setminus \{0\}$. Let E be a subset of I_n^q such that $|E| \geq (1-\beta)2^{nq}$. Suppose that, for each sequence $(a_i)_{1\leq i\leq q}, (b_i)_{1\leq i\leq q} \in J_n^q$, with $(b_i)_{1\leq i\leq q} \in E$:*

$$H(a,b) \geq (1-\alpha)\frac{|B_n|^k}{2^{nq}},$$

with $H(a,b)$ the number of $(f_1,\ldots,f_k) \in B_n^k$ such that :

$$\forall i, 1 \leq i \leq q, (f_1 \oplus \ldots \oplus f_k)(a_i) = b_i \quad .$$

Then:

$$\mathbf{Adv}^{\text{cpa}}_{f_1\oplus\ldots\oplus f_k} \leq \alpha + \beta.$$

For every $b \in J_n^q$, let $h_q(b)$ be the number of sequences $x^1, x^2, \ldots, x^{k-1} \in J_n^q$ such that $x^1 \oplus \ldots \oplus x^{k-1} \oplus b \in J_n^q$ then

Lemma 1 *For all $a, b \in J_n^q$:*

$$H(a,b) = h_q(b)\frac{|B_n|^k}{\left(2^n \times \cdots \times (2^n - q + 1)\right)^k} \quad .$$

Proof. The number $H(a,b)$ can be seen as the sum, over the sequences $x^1, x^2, \ldots,$ $x^{k-1} \in J_n^q$ such that $x^1 \oplus \ldots \oplus x^{k-1} \oplus b \in J_n^q$, of the number of $f_1, \ldots, f_k \in B_n$ satisfying the equations $f_j(a_i) = x_i^j$ for all $j \leq k-1, i \leq q$ and $f_k(a_i) = x_i^1 \oplus \ldots \oplus x_i^{k-1} \oplus b_i, \forall i \leq q$. Then, for each choices of $x^1, \ldots, x^{k-1}$, each f_j is a uniformly random permutation fixed on q points so $H(a,b) = h_q(b)\left(\frac{|B_n|}{2^n \times \cdots \times (2^n - q+1)}\right)^k$, which also shows that $H(a,b)$ does not depend of a. □

We now see h_q as a random variable over $b \in_R I_n^q$. The security of the XOR of k permutations is closely related to the variance and the expectancy of this random variable:

Lemma 2 *The advantage satisfies:*

$$\mathbf{Adv}^{\text{cpa}}_{f_1\oplus\ldots\oplus f_k} \leq 2\left(\frac{\mathbb{V}\left[h_q\right]}{\mathbb{E}\left[h_q\right]^2}\right)^{1/3} \quad . \tag{1}$$

Proof. For all a, we define $H(a)$ the random variable over b equal to $H(a,b)$. The Bienayme-Chebyshev's inequality yields:

$$\forall \epsilon > 0, \Pr\left[|H(a) - \mathbb{E}\left[H(a)\right]| \leq \epsilon\right] \geq 1 - \frac{\mathbb{V}\left[H(a)\right]}{\epsilon^2}.$$

Taking $\epsilon = \alpha\mathbb{E}\left[H(a)\right]$:

$$\forall \alpha > 0, \Pr\left[|H(a) - \mathbb{E}\left[H(a)\right]| \leq \alpha\mathbb{E}\left[H(a)\right]\right] \geq 1 - \frac{\mathbb{V}\left[H(a)\right]}{\alpha^2\mathbb{E}\left[H(a)\right]^2} \quad .$$

Then

$$\forall \alpha > 0, \Pr\left[H(a) \geq (1-\alpha)\mathbb{E}\left[H(a)\right]\right] \geq 1 - \frac{\mathbb{V}\left[H(a)\right]}{\alpha^2 \mathbb{E}\left[H(a)\right]^2} \ .$$

Thus, defining $E = \{(b_i)_{1 \leq i \leq q} | H(a,b) \geq (1-\alpha)\mathbb{E}\left[H(a)\right]\}$, theorem 1 yields :

$$\forall \alpha > 0, \mathbf{Adv}^{\text{cpa}}_{f_1 \oplus \ldots \oplus f_k} \leq \alpha + \frac{\mathbb{V}\left[H(a)\right]}{\alpha^2 \mathbb{E}\left[H(a)\right]^2} \ .$$

Then, with $\alpha = \left(\frac{\mathbb{V}[H(a)]}{\mathbb{E}[H(a)]^2}\right)^{1/3}$:

$$\mathbf{Adv}^{\text{cpa}}_{f_1 \oplus \ldots \oplus f_k} \leq 2\left(\frac{\mathbb{V}\left[H(a)\right]}{\mathbb{E}\left[H(a)\right]^2}\right)^{1/3} = 2\left(\frac{\mathbb{V}\left[h_q\right]}{\mathbb{E}\left[h_q\right]^2}\right)^{1/3} \ .$$

□

Lemma 3 *The mean of h_q satisfies:*

$$\mathbb{E}\left[h_q\right] = \frac{\left[2^n(2^n-1)\ldots(2^n-q+1)\right]^k}{2^{nq}} \ .$$

Proof. This result generalizes a theorem found in [12]. We define δ_x, with $x = (x^1, \ldots, x^{k-1}) \in (J_n^q)^{k-1}$, a random variable over b such that $\delta_x = 1$ if $x^1, \ldots, x^{k-1}, b \oplus x^1 \oplus \cdots \oplus x^{k-1} \in J_n^q$ and $\delta_x = 0$ otherwise. It's clear that $h_q = \sum_{x \in (J_n^q)^{k-1}} \delta_x$, then

$$\begin{aligned}
\mathbb{E}\left[h_q\right] &= \sum_{x \in (J_n^q)^{k-1}} \mathbb{E}\left[\delta_x\right] \\
&= \sum_{x \in (J_n^q)^{k-1}} \Pr\left[\text{the } b_i \oplus x_i^1 \oplus \ldots \oplus x_i^{k-1} \text{ are pairwise distinct}\right] \\
&= \sum_{x \in (J_n^q)^{k-1}} \frac{2^n(2^n-1)\ldots(2^n-q+1)}{2^{nq}} \\
&= |J_n^q|^{k-1} \times \frac{2^n(2^n-1)\ldots(2^n-q+1)}{2^{nq}} \\
&= \frac{\left[2^n(2^n-1)\ldots(2^n-q+1)\right]^k}{2^{nq}} \ .
\end{aligned}$$

□

We now focus on the variance of h_q.

3.2 Study of $\mathbb{V}\left[h_q\right]$

We denote λ_q the number of sequences $g^1, \ldots, g^{2k} \in J_n^q$ such that $g^1 \oplus \cdots \oplus g^{2k} = 0$. These conditions will be referred to as the λ_q conditions. This is $2k$ sequences of q pairwise distinct elements and q equations so, we could expect λ_q to be close to

$$U_q := \frac{\left(2^n(2^n-1)(2^n-q+1)\right)^{2k}}{2^{2nq}} \quad .$$

We see in the next lemma that the problem of knowing how close λ_q is from U_q is at the core of the computation of the advantage.

Lemma 4 *The advantage satisfies:*

$$\mathbf{Adv}^{\mathrm{cpa}}_{f_1 \oplus \ldots \oplus f_k} \leq 2\left(\frac{\lambda_q}{U_q} - 1\right)^{1/3} \quad .$$

Proof. We know that $h_q = \sum_x \delta_x$ with the sum being over $x \in (J_n^q)^{k-1}$, so the linearity of the expected value operator yields:

$$\begin{aligned}
\mathbb{V}\left[h_q\right] &= \mathbb{E}\left[\left(\sum_x \delta_x - \mathbb{E}\left[h_q\right]\right)^2\right] \\
&= \mathbb{E}\left[\left(\sum_x \delta_x\right)^2 - 2\left(\sum_x \delta_x\right)\mathbb{E}\left[h_q\right] + \mathbb{E}\left[h_q\right]^2\right] \\
&= \mathbb{E}\left[\left(\sum_x \delta_x\right)\left(\sum_{x'} \delta_{x'}\right)\right] - 2\mathbb{E}\left[\sum_x \delta_x\right]\mathbb{E}\left[h_q\right] + \mathbb{E}\left[h_q\right]^2 \\
&= \mathbb{E}\left[\sum_{x,x'} \delta_x \delta_{x'}\right] - \mathbb{E}\left[h_q\right]^2,
\end{aligned}$$

the sum being over $x, x' \in (J_n^q)^{k-1}$. Then:

$$\mathbb{E}\left[\sum_{x,x'} \delta_x \delta_{x'}\right] = \frac{1}{2^{nq}} \sum_{b,x,x'} \delta_x(b)\delta_{x'}(b) \quad .$$

We know that $\delta_x(b)\delta_{x'}(b)$, with $x, x' \in (J_n^q)^{k-1}$, equals 1 if and only if $b \oplus x^1 \oplus \cdots \oplus x^{k-1} \in J_n^q$ and $b \oplus x'^1 \oplus \cdots \oplus x'^{k-1} \in J_n^q$. If we change variables like this: $g^i := x^i$ and $g^{i+k-1} := x'^i$ for all $1 \leq i \leq k-1$ and $g^{2k-1} := b \oplus x^1 \oplus \cdots \oplus x^{k-1}$, $g^{2k} := b \oplus x'^1 \oplus \cdots \oplus x'^{k-1}$, we see that $\sum_{b,x,x'} \delta_x(b)\delta_{x'}(b)$ is equal to λ_q. Then:

$$\begin{aligned}
\mathbb{V}\left[h_q\right] &= \frac{\lambda_q}{2^{nq}} - \mathbb{E}\left[h_q\right]^2 \\
&= \frac{\lambda_q - U_q}{2^{nq}} \text{ since } \mathbb{E}\left[h_q\right]^2 = \frac{U_q}{2^{nq}} \quad .
\end{aligned}$$

Moreover, using lemma 2:

$$\begin{aligned}\mathbf{Adv}^{\text{cpa}}_{f_1\oplus\ldots\oplus f_k} &\leq 2\left(\frac{\mathbb{V}\left[h_q\right]}{\mathbb{E}\left[h_q\right]^2}\right)^{1/3}\\ &\leq 2\left(\frac{\lambda_q-U_q}{U_q}\right)^{1/3}\\ &\leq 2\left(\frac{\lambda_q}{U_q}-1\right)^{1/3}\quad .\end{aligned}$$

□

The strategy we follow is to evaluate recursively, more and more accurately, the coefficients λ_α for $1 \leq \alpha \leq q$.

3.3 First evaluation of $\boldsymbol{\lambda_\alpha}$

By definition, $\lambda_{\alpha+1}$ is the number of tuples $g^1, \ldots, g^{2k} \in J_n^{\alpha+1}$ such that :

1. the λ_α conditions hold,
2. for all $1 \leq j \leq 2k$, $g^j_{\alpha+1} \notin \{g^j_i, 1 \leq i \leq \alpha\}$,
3. $g^1_{\alpha+1} \oplus \cdots \oplus g^{2k}_{\alpha+1} = 0$. $(E_{\alpha+1})$

Hence there are $2k\alpha$ equations that should not be verified. For $1 \leq i \leq 2k\alpha$, we denote β_i the i-th such equation. Let B_i be the set of tuples $(g^1, \ldots, g^{2k})$ which satisfy the λ_α conditions, the equation $(E_{\alpha+1})$ and the equation β_i, for $1 \leq i \leq 2k\alpha$. Then:

$$\lambda_{\alpha+1} = 2^{(2k-1)n}\lambda_\alpha - \left|\bigcup_{i=1}^{2k\alpha} B_i\right|.$$

Using the inclusion-exclusion principle:

$$\lambda_{\alpha+1} = 2^{(2k-1)n}\lambda_\alpha + \sum_{l=1}^{2k\alpha}(-1)^l \sum_{i_1<\ldots<i_l} |B_{i_1} \cap \ldots \cap B_{i_l}|.$$

When more than $2k+1$ equations β_i are considered, at least two of them use the same variable, for example $g^1_{\alpha+1} = g^1_1$ and $g^1_{\alpha+1} = g^1_2$, which is impossible according to the λ_α conditions. Thus:

$$\lambda_{\alpha+1} = 2^{(2k-1)n}\lambda_\alpha + \sum_{l=1}^{2k}(-1)^l \sum_{i_1<\ldots<i_l} |B_{i_1} \cap \ldots \cap B_{i_l}|. \tag{2}$$

Now, we study every kind of intersection.

- 1 **equation :**

The β_i equation fixes the value of one new variable, whereas the others are free, so:

$$|B_i| = 2^{(2k-2)n}\lambda_\alpha$$

and there exists $2k\alpha$ such sets.

- l **equations** $(2 \le l \le 2k-1)$:

Such an intersection is non-empty if every equation β_i uses a different new variable. In this case, l new variables are fixed and the others remain free. Thus,

$$|B_{i_1} \cap \ldots \cap B_{i_l}| = 2^{(2k-1-l)n}\lambda_\alpha$$

and there are $\binom{2k}{\ell}\alpha^k$ such non-empty intersections.

- $2k$ **equations :**

Like before, such a set is non-empty if every equation β_i uses a different new variable. In this case, the set $B_{i_1} \cap \ldots \cap B_{i_{2k}}$ is composed of tuples such that $g^1_{\alpha+1} = g^1_{i_1}, \ldots, g^{2k}_{\alpha+1} = g^{2k}_{i_{2k}}$ and the equation $(E_{\alpha+1})$ implies that:

$$g^1_{i_1} \oplus \cdots \oplus g^{2k}_{i_{2k}} = 0.$$

We denote X this equation and $\lambda'_\alpha(X)$ the size of $|B_{i_1} \cap \ldots \cap B_{i_{2k}}|$. There are 3 possible cases:

- If the $2k$ indexes in X are equal then X is always true. There are α possibilities and $\lambda'_\alpha(X) = \lambda_\alpha$.
- If $2k-1$ indexes are equal and the last is different, then $\lambda'_\alpha(X) = 0$ since X is in contradiction with λ_α. There are $2k\alpha(\alpha-1)$ possibilities.
- We denote S the set of equations X that are not of the previous types. We denote $\lambda'_\alpha = \max_S \lambda'_\alpha(X)$.

Hence, thanks to (2), one has:

$$\begin{aligned}
\lambda_{\alpha+1} &= 2^{(2k-1)n}\lambda_\alpha - 2k\alpha\lambda_\alpha + \sum_{\ell=2}^{2k-1}\binom{2k}{\ell}(-1)^l\alpha^l 2^{(2k-1-\ell)n}\lambda_\alpha + \sum_X \lambda'_\alpha(X) \\
&= \left(2^{2kn} - 2k\alpha 2^n + \sum_{\ell=2}^{2k-1}\binom{2k}{\ell}(-1)^l\alpha^l 2^{(2k-\ell)n}\right)\frac{\lambda_\alpha}{2^n} + \alpha\lambda_\alpha + \sum_{X\in S}\lambda'_\alpha(X) \\
&\le \frac{\left((2^n-\alpha)^{2k} - \alpha^{2k} + 2^n\alpha\right)\lambda_\alpha}{2^n} + \left(\alpha^{2k} - \alpha - 2k\alpha(\alpha-1)\right)\lambda'_\alpha
\end{aligned}$$

We denote $\epsilon_\alpha = \frac{2^n\lambda'_\alpha}{\lambda_\alpha} - 1$, so:

$$\begin{aligned}
\frac{2^n\lambda_{\alpha+1}}{\lambda_\alpha} &\le (2^n-\alpha)^{2k} - \alpha^{2k} + 2^n\alpha + \frac{2^n\lambda'_\alpha}{\lambda_\alpha} \times (\alpha^{2k} - \alpha - 2k\alpha(\alpha-1)) \\
&\le (2^n-\alpha)^{2k} + 2^n\alpha - \alpha - 2k\alpha(\alpha-1) + \epsilon_\alpha \times (\alpha^{2k} - \alpha - 2k\alpha(\alpha-1)) \\
&\le (2^n-\alpha)^{2k} - 2k\alpha^2 + \alpha(2^n+2k-1) + \epsilon_\alpha \times (\alpha^{2k} - 2k\alpha^2 + \alpha(2k-1))
\end{aligned}$$

3.4 Relation between the advantage and ϵ_α

Lemma 5 *For every $m \geq 1$, the advantage satisfies:*

$$\mathbf{Adv}^{\text{cpa}}_{f_1 \oplus \ldots \oplus f_k} \leq 2\left(\prod_{\alpha=1}^{m-1}\left(1+\frac{-2k\alpha^2+\alpha(2^n+2k-1)+\epsilon_\alpha\times(\alpha^{2k}-2k\alpha^2+\alpha(2k-1))}{(2^n-\alpha)^{2k}}\right)-1\right)^{1/3}.$$

Proof. We know that

$$\frac{2^n U_{\alpha+1}}{U_\alpha} = (2^n-\alpha)^{2k},$$

and the result of the previous section yields:

$$\begin{aligned}\frac{\lambda_{\alpha+1}}{U_{\alpha+1}} &\leq \frac{\lambda_\alpha}{U_\alpha}\left(\frac{(2^n-\alpha)^{2k}-2k\alpha^2+\alpha(2^n+2k-1)+\epsilon_\alpha\times(\alpha^{2k}-2k\alpha^2+\alpha(2k-1))}{(2^n-\alpha)^{2k}}\right)\\ &\leq \frac{\lambda_\alpha}{U_\alpha}\left(1+\frac{-2k\alpha^2+\alpha(2^n+2k-1)+\epsilon_\alpha\times(\alpha^{2k}-2k\alpha^2+\alpha(2k-1))}{(2^n-\alpha)^{2k}}\right)\end{aligned}$$

Since $U_1 = \lambda_1 = 2^{(2k-1)n}$:

$$\frac{\lambda_m}{U_m} \leq \prod_{\alpha=1}^{m-1}\left(1+\frac{-2k\alpha^2+\alpha(2^n+2k-1)+\epsilon_\alpha\times(\alpha^{2k}-2k\alpha^2+\alpha(2k-1))}{(2^n-\alpha)^{2k}}\right)$$

And Lemma 4 ends the proof. □

3.5 First approximation of ϵ_α

Before evaluating ϵ_α, we need a technical lemma:

Lemma 6 *For every $\alpha \in \{2, \ldots, m\}$, one has:*

$$1-\frac{2k\alpha}{2^n} \leq \frac{\lambda_\alpha}{2^{(2k-1)n}\lambda_{\alpha-1}} \leq 1. \tag{3}$$

Proof. We consider $g^1, \ldots, g^{2k} \in J_n^\alpha$ satisfying the conditions $\lambda_{\alpha-1}$. To satisfy the conditions λ_α, there are $(2^n-(\alpha-1))$ possibilities for each $g^1_\alpha, \ldots, g^{2k-2}_\alpha$ and there are $2(\alpha-1)$ non-equalities left: $g^{2k-1}_\alpha \neq g^{2k-1}_i$ and $g^{2k}_\alpha \neq g^{2k}_i$ for all $i \leq \alpha-1$. Since $g^{2k}_\alpha = g^1_\alpha \oplus \cdots \oplus g^{2k-1}_\alpha$, one sees these $2(\alpha-1)$ non-equalities as equations on g^{2k-1}_α. So, there are between $2^n-2(\alpha-1)$ and $2^n-(\alpha-1)$ possible choices for g^{2k-1}_α and 1 choice for g^{2k}_α. Then:

$$\lambda_{\alpha-1}(2^n-(\alpha-1))^{2k-2}(2^n-2(\alpha-1)) \leq \lambda_\alpha \leq \lambda_{\alpha-1}(2^n-(\alpha-1))^{2k-1}$$

which is equivalent to:

$$\left(1-\frac{\alpha-1}{2^n}\right)^{2k-2}\left(1-\frac{2(\alpha-1)}{2^n}\right) \leq \frac{\lambda_\alpha}{2^{(2k-1)n}\lambda_{\alpha-1}} \leq \left(1-\frac{\alpha-1}{2^n}\right)^{2k-1}.$$

Since the left term is bigger than $1-\frac{2k\alpha}{2^n}$ and the right term is inferior to 1, it ends the proof. □

Lemma 7 *Every value $\lambda'_\alpha(X)$ with $X \in S$ satisfies :*

$$\frac{2^n \lambda'_\alpha(X)}{\lambda_\alpha} \leq 1 + \frac{2k\alpha}{\left(1 - \frac{2k\alpha}{2^n}\right) 2^n}.$$

Proof. We now express λ'_α in terms of $\lambda_{\alpha-1}$. Without loss of generality, we suppose that X involves g^1_α, otherwise we can just reorder the variables. Let i be any index such that g^i_α is not involved in X (this is possible since $X \in S$). Let $g^1, \ldots, g^{2k} \in J^\alpha_n$ such that the $\lambda_{\alpha-1}$ conditions are satisfied. We now count $\lambda'_\alpha(X)$. There are at most $2^n - (\alpha-1)$ possible choices for each $g^j_\alpha, j \neq 1, i$. After we made these choices, there are two variables left: g^1_α and g^i_α. Since g^i_α is not involved in X, there is only, at most, one possible choice for g^1_α and there is, at most, one possible choice for g^i_α using the equation $g^1_\alpha \oplus \cdots \oplus g^{2k}_\alpha = 0$. Then:

$$\lambda'_\alpha(X) \leq (2^n - (\alpha - 1))^{2k-2} \lambda_{\alpha-1}.$$

Applying lemma 6, one finds that:

$$\lambda'_\alpha(X) \leq (2^n - (\alpha - 1))^{2k-2} \left(\frac{1}{1 - \frac{2k\alpha}{2^n}} \right) \frac{\lambda_\alpha}{2^{(2k-1)n}}$$

Since $2^n - \alpha - 1 \leq 2^n$ and $\frac{1}{1-\frac{2k\alpha}{2^n}} = 1 + \frac{2k\alpha}{(1-\frac{2k\alpha}{2^n})2^n}$, this ends the proof. □

Remark: These two technical lemmas formalize the intuition that, when one equation is added to the system, one degree of freedom is lost and this divides the number of possible solutions by around 2^n.

Finally

$$\epsilon_\alpha \leq \frac{2k\alpha}{\left(1 - \frac{2k\alpha}{2^n}\right) 2^n}.$$

First notice that if $q \leq \frac{2^n}{2k}$, $-2k\alpha^2 + \alpha(2^n) \geq 0$. Then, from lemma 5,

$$\mathbf{Adv}^{\text{cpa}}_{f_1 \oplus \ldots \oplus f_k} \leq 2 \left(\prod_{\alpha=1}^{q-1} \left(1 + \frac{-2k\alpha^2 + \alpha(2^n + 2k - 1) + \epsilon_\alpha \times (\alpha^{2k} - 2k\alpha^2 + \alpha(2k-1))}{(2^n - \alpha)^{2k}} \right) - 1 \right)^{1/3}.$$

If $q \leq \frac{2^n}{2k}$, all the terms of the product are greater than 1 and

$$\begin{aligned}
\mathbf{Adv}^{\text{cpa}}_{f_1 \oplus \ldots \oplus f_k} &\leq 2 \left(\prod_{\alpha=1}^{q-1} \left(1 + \frac{-2k\alpha^2 + \alpha(2^n + 2k - 1)}{(2^n - \alpha)^{2k}} + \frac{2k\alpha \times (\alpha^{2k} - 2k\alpha^2 + \alpha(2k-1))}{\left(1 - \frac{2k\alpha}{2^n}\right) 2^n \times (2^n - \alpha)^{2k}} \right) - 1 \right)^{1/3} \\
&\leq 2 \left(\prod_{\alpha=1}^{q-1} \left(1 + \frac{\alpha 2^n}{(2^n - \alpha)^{2k}} + \frac{2k\alpha^{2k+1}}{\left(1 - \frac{2k\alpha}{2^n}\right) 2^n (2^n - \alpha)^{2k}} \right) - 1 \right)^{1/3} \\
&\leq 2 \left(\left(1 + \frac{q 2^n}{(2^n - q)^{2k}} + \frac{2kq^{2k+1}}{\left(1 - \frac{2kq}{2^n}\right) 2^n (2^n - q)^{2k}} \right)^q - 1 \right)^{1/3}.
\end{aligned}$$

Thus we have proven that :

Theorem 2 (Upper bound of the advantage using H_σ). *The maximal advantage an adversary can get using q queries, with $q \le \frac{2^n}{2k}$ verifies:*

$$\mathbf{Adv}^{\mathrm{cpa}}_{f_1\oplus\ldots\oplus f_k} \le 2\left(\left(1+\frac{q2^n}{(2^n-q)^{2k}}+\frac{2kq^{2k+1}}{\left(1-\frac{2kq}{2^n}\right)2^n(2^n-q)^{2k}}\right)^q-1\right)^{1/3}.$$

Notice that

$$\mathbf{Adv}^{\mathrm{cpa}}_{f_1\oplus\ldots\oplus f_k} \lesssim 2\left(\frac{q^2}{2^{(2k-1)n}(1-\frac{q}{2^n})^{2k}}+\frac{2kq^{2k+2}}{2^{(2k+1)n}(1-\frac{6kq}{2^n})}\right)^{1/3}.$$

Since $k \ge 3$ and $q \le 2^n$, the first term is negligible in front of 1. Moreover, when $q^{2k+2} \ll 2^{(2k+1)n}$, $\mathbf{Adv}^{\mathrm{cpa}}_{f_1\oplus\ldots\oplus f_k} \ll 1$. Hence we have proven that the XOR of k permutations is safe as long as $q \ll 2^{\frac{2k+1}{2k+2}n}$ with this first technique.

4 Security bound from the standard H technique

We now use the "standard H technique", i.e. proofs from the general result (the corollary 8) below. In this section, $\mathbb{E}[h_q]$ is noted $\tilde{h}_q$ to lighten the notations.

Corollary 8 *Let $\alpha > 0$. If, for every sequence $b = (b_i)_{1\le i\le q} \in I_n^q$*

$$h_q(b) \ge (1-\alpha)\tilde{h}_q,$$

then

$$\mathbf{Adv}^{\mathrm{cpa}}_{f_1\oplus\ldots\oplus f_k} \le \alpha.$$

Proof. This result comes immediately from theorem 1 with $\beta = 0$ and lemmas 1 and 3. □

4.1 First approximation

Let us study $\frac{h_\alpha}{\tilde{h}_\alpha}$.

One has:

$$\tilde{h}_{\alpha+1} = \tilde{h}_\alpha\frac{(2^n-\alpha)^k}{2^n}.$$

We now evaluate $h_{\alpha+1}$ from h_α. From the definition of h_α (see section 3.1), we see that $h_{\alpha+1}$ is the number of sequence $(P_i^j)_{1\le i\le m, 1\le j\le k}$ such that:

- the h_α conditions hold ;
- $P^1_{\alpha+1}\oplus\ldots\oplus P^k_{\alpha+1} = b_{\alpha+1}$, this equation will be called X ;
- $P^j_{\alpha+1} \ne P^j_i$ for every $1\le i\le\alpha$, $1\le j\le k$.

Let β_i, $1 \leq k\alpha$ be the $k\alpha$ equations which should be false. Let, for $1 \leq i \leq k\alpha$, B_i be the set of the $\left(P_i^j\right)_{1\leq i\leq \alpha+1, 1\leq j\leq k}$ for which the h_α conditions and the equation β_i hold.

From the inclusion-exclusion principle, we get:

$$\begin{aligned} h_{\alpha+1} &= 2^{(k-1)n} h_\alpha - |\cup_{i=1}^{k\alpha} B_i| \\ &= 2^{(k-1)n} h_\alpha + \sum_{1\leq l\leq k\alpha} (-1)^l \sum_{i_1<\ldots<i_l} |B_{i_1} \cap \ldots \cap B_{i_l}|. \end{aligned}$$

When $k+1$ sets are intersected, at least two equations will use the same $P_{\alpha+1}^j$ variable, which is in contradiction with h_α. Thus,

$$h_{\alpha+1} = 2^{(k-1)n} h_\alpha + \sum_{1\leq l\leq k} (-1)^l \sum_{i_1<\ldots<i_l} |B_{i_1} \cap \ldots \cap B_{i_l}|. \tag{4}$$

We study the number of possible messages in function of the number of sets in the intersection.

- **l equations, $1 \leq l \leq k-1$:**

If we want $|B_{i_1} \cap \ldots \cap B_{i_l}| \neq 0$, every new β_i equation should bring a new variable $P_{\alpha+1}^j$. In this case, X and β_i fix $l+1$ variables, the remaining ones are free, so $|B_{i_1} \cap \ldots \cap B_{i_l}| = 2^{(k-l-1)n} h_\alpha$ and

$$\sum_{i_1<\ldots<i_l} |B_{i_1} \cap \ldots \cap B_{i_l}| = \binom{k}{l} \alpha^l 2^{(k-l-1)n} h_\alpha$$

- **k equations:**

As well as above, in order to have $|B_{i_1} \cap \ldots \cap B_{i_k}| \neq 0$, there must be an equation in every new variable:

$$P_{\alpha+1}^j = P_{i_j}^j,\ 1 \leq j \leq k.$$

So the condition $P_{\alpha+1}^1 \oplus \ldots \oplus P_{\alpha+1}^k = b_{\alpha+1}$ becomes:

$$P_{i_1}^1 \oplus \ldots \oplus P_{i_k}^k = b_{\alpha+1}.$$

Let $h'_\alpha(b_1, \ldots, b_{\alpha+1})(i_1, \ldots, i_k)$ or $h'_\alpha(i_1, \ldots, i_k)$ the number of $(P_i^j)_{1\leq i\leq\alpha, 1\leq j\leq k} \in I_n^{k\alpha}$ such that:

- the conditions h_α hold,
- $P_{i_1}^1 \oplus \ldots \oplus P_{i_k}^k = b_{\alpha+1}$.

Let $Y(i_1, \ldots, i_k)$ be this equality. Thus

$$\sum_{i_1<\ldots<i_k} |B_{i_1} \cap \ldots \cap B_{i_k}| = \sum_{1\leq i_1,\ldots,i_k\leq\alpha} h'_\alpha(i_1, \ldots, i_k).$$

From (4), we have:

$$h_{\alpha+1} = \frac{(2^n-\alpha)^k - (-1)^k \alpha^k}{2^n} h_\alpha + (-1)^k \sum_{1\leq i_1,\ldots,i_k\leq\alpha} h'_\alpha(i_1, \ldots, i_k). \tag{5}$$

Remark: if k is even, one has:

$$h_{\alpha+1} \geq h_\alpha \left(\frac{(2^n-\alpha)^k - \alpha^k}{2^n} \right).$$

So

$$\frac{h_{\alpha+1}}{\tilde{h}_{\alpha+1}} \geq \frac{h_\alpha}{\tilde{h}_\alpha} \left(1 - \frac{\alpha^k}{(2^n-\alpha)^k} \right).$$

As $h_1 = \tilde{h}_1 = 2^{(k-1)n}$,

$$\begin{aligned} h_q &\geq \tilde{h}_q \left(1 - \frac{q^k}{(2^n-q)^k} \right)^q \\ &\geq \tilde{h}_q \left(1 - \frac{q^{k+1}}{(2^n-q)^k} \right) \end{aligned}$$

Then, using corollary 8,

$$\mathbf{Adv}^{\text{cpa}}_{f_1 \oplus \ldots \oplus f_k} \leq \frac{q^{k+1}}{(2^n-q)^k}.$$

The upper bound we get in this case is in the same order of magnitude as the one from [9]. If we study more closely h'_α, we will get a better inequality.

4.2 Second approximation

In this section, we suppose that $k \geq 3$.
Let $M = \{i,\, 1 \leq i \leq \alpha,\, b_i = b_{\alpha+1}\}$. If $i \in M$, we have $h'_\alpha(i, \ldots, i) = h_\alpha$ and if $i \notin M$, $h'_\alpha(i, \ldots, i) = 0$. Furthermore, in order to be compatible with h_α, if $i \in M$, for each $1 \leq j \leq \alpha$, $i \neq j$,
$h'_\alpha(j, i, \ldots, i) = h'_\alpha(i, j, \ldots, i) = \ldots = h'_\alpha(i, \ldots, i, j) = 0$. Let I be the set of the tuples that do not satisfy these requirements. Then $|I| = \alpha^k - \alpha - k|M|(\alpha - 1)$.
By applying (5), one gets:

$$h_{\alpha+1} = \frac{(2^n-\alpha)^k - (-1)^k \alpha^k + (-1)^k 2^n |M|}{2^n} h_\alpha + (-1)^k \sum_{(i_1,\ldots,i_k) \in I} h'_\alpha(i_1, \ldots, i_k). \tag{6}$$

We now need a technical lemma:

Lemma 9 *If $i = (i_1, \ldots, i_k) \in I$,*

$$1 - \frac{3\alpha}{(2^n-\alpha)(1-\frac{\alpha}{2^n})} \leq \frac{2^n h'_\alpha(i_1, \ldots, i_k)}{h_\alpha} \leq \frac{1}{1 - \frac{3\alpha}{2^n}}.$$

Proof. Without loss of generality, we can suppose that $i_1 = \alpha$ and $i_2 = \alpha - 1$ (because we can reorder the queries). Let us evaluate h'_α and h_α from $h_{\alpha-2}$. To get h_α from $h_{\alpha-2}$, we have $2k$ new variables $P^j_{\alpha-1}$ and P^j_α, $1 \leq j \leq k$, such that:

- $P_\alpha^1 \oplus \ldots \oplus P_\alpha^k = b_\alpha$,
- $P_{\alpha-1}^1 \oplus \ldots \oplus P_{\alpha-1}^k = b_{\alpha-1}$,
- $\forall j,\ 1 \le j \le k,\ \forall i,\ 1 \le i \le \alpha-2,\ P_{\alpha-1}^j \ne P_i^j$,
- $\forall j,\ 1 \le j \le k,\ \forall i,\ 1 \le i \le \alpha-1,\ P_\alpha^j \ne P_i^j$.

We decide that the first equation will fix $P_{\alpha-1}^1$ and the next one P_α^1. For $j \ge 3$, we have respectively $2^n-(\alpha-2)$ and $2^n-(\alpha-1)$ possibilities for $P_{\alpha-1}^j$ and P_α^j. When these messages have been chosen, only $P_{\alpha-1}^2$ and P_α^2 remain, and they must satisfy:

- $P_{\alpha-1}^2 \ne P_i^2$, $1 \le i \le \alpha-2$,
- $P_{\alpha-1}^2 \ne P_i^1 \oplus b_{\alpha-1} \oplus P_{\alpha-1}^3 \oplus \ldots \oplus P_{\alpha-1}^k$, $1 \le i \le \alpha-2$,
- $P_\alpha^2 \ne P_i^2$, $1 \le i \le \alpha-1$,
- $P_\alpha^2 \ne P_i^1 \oplus b_\alpha \oplus P_\alpha^3 \oplus \ldots \oplus P_\alpha^k$, $1 \le i \le \alpha-1$.

There are for $P_{\alpha-1}^2$ between $2^n-2(\alpha-2)$ and $2^n-(\alpha-2)$ choices and for $P_{\alpha-1}^2$ between $2^n-2(\alpha-1)$ and $2^n-(\alpha-1)$. Thus

$$(2^n-(\alpha-2))^{k-2}(2^n-(\alpha-1))^{k-2}(2^n-2(\alpha-2))(2^n-2(\alpha-1)) \le \tfrac{h_\alpha}{h_{\alpha-2}}, \quad (7)$$
$$\tfrac{h_\alpha}{h_{\alpha-2}} \le (2^n-(\alpha-2))^{k-1}(2^n-(\alpha-1))^{k-1}. \quad (8)$$

In order to go from $h_{\alpha-2}$ to h'_α, we also have $2k$ new variables $P_{\alpha-1}^j$ and P_α^j, $1 \le j \le k$, such that:

- $P_{\alpha-1}^1 \oplus \ldots \oplus P_{\alpha-1}^k = b_{\alpha-1}$,
- $P_\alpha^1 = b_{\alpha+1} \oplus P_{\alpha-1}^2 \oplus P_{i_3}^3 \oplus \ldots \oplus P_{i_k}^k$,
- $P_\alpha^1 \oplus \ldots \oplus P_\alpha^k = b_\alpha$,
- $\forall j,\ 1 \le j \le k,\ \forall i,\ 1 \le i \le \alpha-2,\ P_{\alpha-1}^j \ne P_i^j$,
- $\forall j,\ 1 \le j \le k,\ \forall i,\ 1 \le i \le \alpha-1,\ P_\alpha^j \ne P_i^j$.

We have, for $j \ge 4$, respectively $2^n-(\alpha-2)$ and $2^n-(\alpha-1)$ possibilities for $P_{\alpha-1}^j$ and P_α^j. From these 3 equalities, we can fix the following variables:

1. $P_{\alpha-1}^1 = b_{\alpha-1} \oplus P_{\alpha-1}^2 \oplus \ldots \oplus P_{\alpha-1}^k$,
2. $P_\alpha^1 = b_{\alpha+1} \oplus P_{\alpha-1}^2 \oplus P_{i_3}^3 \oplus \ldots \oplus P_{i_k}^k$,
3. $P_\alpha^2 = (b_{\alpha+1} \oplus b_\alpha) \oplus P_{\alpha-1}^2 \oplus (P_{i_3}^3 \oplus P_\alpha^3) \oplus \ldots \oplus (P_{i_k}^k \oplus P_\alpha^k)$.

Then

- the condition $\forall i, 1 \le i \le \alpha-2, P_{\alpha-1}^1 \ne P_i^1$ becomes:

$$\forall i, 1 \le i \le \alpha-2, P_{\alpha-1}^2 \ne P_i^1 \oplus b_{\alpha-1} \oplus P_{\alpha-1}^3 \oplus \ldots \oplus P_{\alpha-1}^k,$$

- $\forall i, 1 \le i \le \alpha-1, P_\alpha^1 \ne P_i^1$ becomes:

$$\forall i, 1 \le i \le \alpha-1, P_{\alpha-1}^2 \ne b_{\alpha+1} \oplus P_i^1 \oplus P_{i_3}^3 \oplus \ldots \oplus P_{i_k}^k,$$

- $\forall i, 1 \le i \le \alpha-2, P_\alpha^2 \ne P_i^1$ becomes:

$$\forall i, 1 \leq i \leq \alpha - 2,\ P^2_{\alpha-1} \neq (b_{\alpha+1} \oplus b_\alpha) \oplus P^2_i \oplus (P^3_{i_3} \oplus P^3_\alpha) \oplus \ldots \oplus (P^k_{i_k} \oplus P^k_\alpha)$$

For $P^2_\alpha \neq P^2_{\alpha-1}$, there are two cases. If $i_3 = \ldots = i_k = \alpha$, since $(i_1, \ldots, i_k) \in I$, we have $b_{\alpha+1} \neq b_\alpha$ and this non-equality is automatically verified. Else, this means that there is an index $3 \leq j \leq k$ such that $i_j \neq \alpha$, e.g. $j = 3$. Then $P^2_\alpha \neq P^2_{\alpha-1}$ becomes :

$$P^3_\alpha \neq (b_{\alpha+1} \oplus b_\alpha) \oplus P^3_{i_3} \oplus \ldots \oplus (P^k_{i_k} \oplus P^k_\alpha).$$

Thus, after the other messages have been chosen, there are between $2^n - \alpha$ and $2^n - (\alpha - 1)$ possibilities for P^3_α, $2^n - (\alpha - 2)$ possibilities for $P^3_{\alpha-1}$ and finally between $2^n - (4\alpha - 7)$ and $2^n - (\alpha - 2)$ possibilities for $P^2_{\alpha-1}$. Then

$$(2^n - (\alpha - 2))^{k-2}(2^n - (\alpha - 1))^{k-3}(2^n - \alpha)(2^n - (4\alpha - 7)) \leq \frac{h'_\alpha}{h_{\alpha-2}} \quad (9)$$

$$(2^n - (\alpha - 2))^{k-1}(2^n - (\alpha - 1))^{k-2} \geq \frac{h'_\alpha}{h_{\alpha-2}}\ . \quad (10)$$

From 7,9 we can deduce the following inequalities that allow us to get the result we want:

$$\frac{2^n h'_\alpha}{h_{\alpha-2}} \geq 2^n \frac{(2^n - 4\alpha + 7)(2^n - \alpha)}{(2^n - (\alpha - 2))(2^n - (\alpha - 1))^2},$$
$$\frac{2^n h'_\alpha}{h_{\alpha-2}} \leq 2^n \frac{2^n - (\alpha - 2)}{(2^n - 2(\alpha - 2))(2^n - 2(\alpha - 1)).}$$

□

Remark: if we suppose $\alpha < \frac{2^n}{12}$, we get

$$0 < 1 - \frac{12\alpha}{2^n} \leq \frac{2^n h'_\alpha(i_1, \ldots, i_k)}{h_\alpha} \leq 1 + \frac{3\alpha}{2^n - 3\alpha}. \quad (11)$$

One has:

$$\frac{h_{\alpha+1}}{\tilde{h}_{\alpha+1}} = \frac{h_\alpha}{\tilde{h}_\alpha}\left(1 + \frac{(-1)^{k+1}\alpha^k}{(2^n - \alpha)^k} + (-1)^k \frac{2^n|M|}{(2^n - \alpha)^k} + (-1)^k \frac{\sum \frac{2^n h'_\alpha}{h_\alpha}}{(2^n - \alpha)^k}\right) \quad (12)$$

$$= \frac{h_\alpha}{\tilde{h}_\alpha}(1 - A_\alpha) \quad (13)$$

where

$$A_\alpha := \frac{(-1)^k\alpha^k}{(2^n - \alpha)^k} - (-1)^k \frac{2^n|M|}{(2^n - \alpha)^k} - (-1)^k \frac{\sum \frac{2^n h'_\alpha}{h_\alpha}}{(2^n - \alpha)^k}.$$

Lemma 10 *If $q < \frac{2^n}{12}$,*

$$A_\alpha \leq \frac{k.2^n\alpha}{(2^n - \alpha)^k} + 12\frac{\alpha^{k+1}}{(2^n - 3\alpha)(2^n - \alpha)^k}\ .$$

Proof. We have to study A_α according to the parity of k.

- k **even:**

$$\begin{aligned} A_\alpha &\leq \frac{\alpha^k}{(2^n-\alpha)^k} - \frac{2^n|M|}{(2^n-\alpha)^k} - \frac{(\alpha^k-\alpha-k|M|(\alpha-1))(1-\frac{12\alpha}{2^n})}{(2^n-\alpha)^k} \\ &\leq -\frac{2^n|M|}{(2^n-\alpha)^k} + \frac{(\alpha+k|M|(\alpha-1))(1-\frac{12\alpha}{2^n})}{(2^n-\alpha)^k} + 12\frac{\alpha^{k+1}}{2^n(2^n-\alpha)^k} \\ &\leq \frac{k.\alpha^2}{(2^n-\alpha)^k} + 12\frac{\alpha^{k+1}}{2^n(2^n-\alpha)^k} \end{aligned}$$

- k **odd:**

$$\begin{aligned} A_\alpha &\leq -\frac{\alpha^k}{(2^n-\alpha)^k} + \frac{2^n|M|}{(2^n-\alpha)^k} + \frac{(\alpha^k-\alpha-k|M|(\alpha-1))(1+\frac{3\alpha}{2^n-3\alpha})}{(2^n-\alpha)^k} \\ &\leq \frac{2^n|M|}{(2^n-\alpha)^k} - \frac{(\alpha+k|M|(\alpha-1))(1+\frac{3\alpha}{2^n-3\alpha})}{(2^n-\alpha)^k} + \frac{3\alpha^{k+1}}{(2^n-\alpha)^k(2^n-3\alpha)} \\ &\leq \frac{2^n\alpha}{(2^n-\alpha)^k} + \frac{3\alpha^{k+1}}{(2^n-\alpha)^k(2^n-3\alpha)} \end{aligned}$$

So, in both cases,

$$A_\alpha \leq \frac{k.2^n\alpha}{(2^n-\alpha)^k} + 12\frac{\alpha^{k+1}}{(2^n-3\alpha)(2^n-\alpha)^k},$$

□

From this lemma and 12,

$$\frac{h_{\alpha+1}}{\tilde{h}_{\alpha+1}} \geq \frac{h_\alpha}{\tilde{h}_\alpha}\left(1 - \frac{k.2^n\alpha}{(2^n-\alpha)^k} - 12\frac{\alpha^{k+1}}{(2^n-3\alpha)(2^n-\alpha)^k}\right).$$

Since $h_1 = \tilde{h}_1$, we get:

$$\begin{aligned} \frac{h_q}{\tilde{h}_q} &\geq \left(1 - \frac{k2^nq}{(2^n-q)^k} - 12\frac{q^{k+1}}{(2^n-3q)(2^n-q)^k}\right)^q \\ &\geq 1 - \frac{kq^2.2^n}{(2^n-q)^k} - 12\frac{q^{k+2}}{(2^n-3q)(2^n-q)^k}. \end{aligned}$$

Thus, with corollary 8, we have proven that, when $q < \frac{2^n}{12}$:

$$\mathbf{Adv}^{\text{cpa}}_{f_1\oplus\ldots\oplus f_k} \leq \frac{kq^2.2^n}{(2^n-q)^k} + 12\frac{q^{k+2}}{(2^n-3q)(2^n-q)^k} \tag{14}$$

$$\leq \frac{kq^2}{2^{(k-1)n}(1-k\frac{q}{2^n})} + 12\frac{q^{k+2}}{2^{(k+1)n}(1-(k+3)\frac{q}{2^n})}. \tag{15}$$

Hence we get the following result:

Theorem 3 (upper bound for the advantage with the standard H technique). *Let $k \geq 3$ and $q < \frac{2^n}{12}$. The advantage to distinguish, with q queries, the XOR of k bijections from a fonction $f \in_R F_n$ satisfies:*

$$\mathbf{Adv}^{\text{cpa}}_{f_1\oplus\ldots\oplus f_k} \leq \frac{kq^2}{2^{(k-1)n}(1-k\frac{q}{2^n})} + 12\frac{q^{k+2}}{2^{(k+1)n}(1-(k+3)\frac{q}{2^n})}.$$

Since $k \geq 3$, the first term is negligible when $q \ll 2^n$. This theorem shows that the XOR of k bijections is indistinguishable when $q \ll 2^{\frac{k+1}{k+2}n}$. This upper bound on q is worse than the previous one, but if $q \ll 2^{\frac{k+2}{k+4}n}$ (i.e. for small values of q) this new upper bound on the advantage is actually better.

5 Conclusion

This table regroups our results and the previous one from S. Lucks in [9], with order of magnitudes for these bounds beyond the birthday bound :

technique	upper bound for $\mathbf{Adv}^{\text{cpa}}_{f_1\oplus\ldots\oplus f_k}$	order of magnitude
S. Lucks	$2^{-k(n-1)}\sum_{0\leq i<q} i^k$	$\mathcal{O}\left(\frac{q^{k+1}}{2^{k(n-1)}}\right)$
H	$\frac{kq^2}{2^{(k-1)n}(1-k\frac{q}{2^n})} + 12\frac{q^{k+2}}{2^{(k+1)n}(1-(k+3)\frac{q}{2^n})}$	$O\left(\frac{q^{k+2}}{2^{(k+1)n}}\right)$
H_σ	$2\left(\frac{q^2}{2^{(2k-1)n}(1-\frac{q}{2^n})^{2k}} + \frac{2kq^{2k+2}}{2^{(2k+1)n}(1-\frac{6kq}{2^n})}\right)^{1/3}$	$O\left(\left(k\frac{q^{2k+2}}{2^{(2k+1)n}}\right)^{1/3}\right)$

Table 1. Comparison of the bounds on the advantage from 3 techniques

The upper bound we got with the coefficients H technique is smaller than the one from [9] by a factor $\frac{q}{2^n}$. The one we proved with the coefficients H_σ technique allows us to have $\mathbf{Adv}^{\text{cpa}}_{f_1\oplus\ldots\oplus f_k} \ll 1$ when $q \ll 2^{\frac{2k+1}{2k+2}n}$ instead of $q \ll 2^{\frac{k}{k+1}n}$ for [9]. For example with $k=3$ we have proven that $\mathbf{Adv}^{\text{cpa}}_{f_1\oplus\ldots\oplus f_k} \ll 1$ when $q \ll 2^{\frac{7}{8}n}$ instead of $q \ll 2^{\frac{3}{4}n}$. However, when q is fixed and k increases, the upper bound from the H technique becomes better than the one from H_σ. This graph shows the evolution of the order of magnitude of these three upper bounds in function of the logarithm of q, with $k = 5$ and $n = 40$:

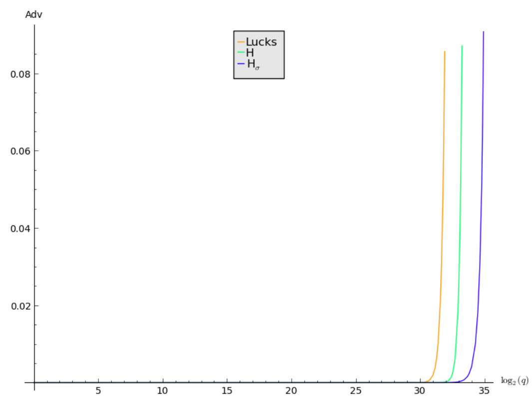

Table 2. Upper bound plotted versus the logarithm of q

Here is a more accurate view of the region where the curves from H and H_σ intersect:

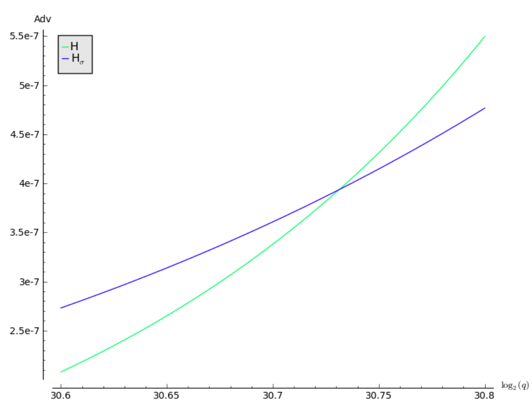

Table 3. Upper bound plotted versus the logarithm of q : comparison between H and H_σ

This illustrates that, depending on the value of q, our best bound can be the one from section 3 or the one from section 4. Moreover, the curve from [9] does not appear in this second graph because its values were much higher than ours (around $6 \cdot 10^{-4}$ whereas the bounds from this article are around $4 \cdot 10^{-7}$ in this graph). This shows why the two techniques studied in this paper are both useful.

References

[1] W. Aiello and R. Venkatesan. Foiling Birthday Attacks in Length Doubling Transformations. In *Advances in cryptology - EUROCRYPT 96*, pages 307–320. Springer-Verlag, 1996.

[2] M. Bellare and R. Impagliazzo. A Tool for Obtaining Tighter Security Analyses of Pseudorandom Function Based Constructions, with Applications to PRP to PRF Conversion. *ePrint Archive 1999/024: Listing for 1999*, 1999.

[3] M. Bellare, T. Krovetz, and P. Rogaway. Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In K. Nyberg, editor, *Advances in cryptology - EUROCRYPT 1998*, pages 266–280. Springer-Verlag, 1998.

[4] O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions. *Journal of the ACM*, 33(4):792–807, 1986.

[5] C. Hall, D. Wagner, J. Kelsey, and B. Schneier. Building PRFs from PRPs. In H. Krawcyk, editor, *Advances in cryptology - CRYPTO 1998*, pages 370–389. Springer-Verlag, 1998.

[6] L. Levin. One Way Functions and Pseudorandom Generators. *Combinatorica*, 7(4):357–363, 1987.

[7] M. Luby and C. Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[8] S. Lucks. Faster Luby-Rackoff Ciphers. In *Fast Software Encryption 1996*, pages 189–205. Springer-Verlag, 1996.

[9] S. Lucks. The Sum of PRPs Is a Secure PRF. In B. Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, pages 470–484. Springer-Verlag, 2000.

[10] A. Mandal, V. Nachef, and J. Patarin. Indifferentiability beyond the Birthday Bound for the Xor of Two Public Random Permutations. In *Progress in Cryptology - INDOCRYPT 2010*, pages 69–81, 2010.

[11] M. Naor and O. Reingold. On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited. *Journal of Cryptology*, 12(1):29–66, 1999.

[12] J. Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutation. In R. Safavi-Naini, editor, *ICITS 2008*, pages 328–345. Springer-Verlag, 2008.

[13] J. Patarin. Generic Attacks for the Xor of k Random Permutations. *Available on eprint*, 2008.

[14] J. Patarin. The "coefficients H" Technique. In *Selected Areas in Cryptography 2008*, pages 328–345. Springer-Verlag, 2008.

[15] J. Patarin. Security in $O(2^n)$ for the Xor of Two Random Permutations - Proof with the standard H technique -. *Available on eprint*, 2013.