Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography

Jacques Patarin

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

Abstract. In this paper we will first study two closely related problems:
1. The problem of distinguishing $f(x\|0) \oplus f(x\|1)$ where f is a random permutation on n bits. This problem was first studied by Bellare and Implaglliazzo in [3].
2. The so-called "Theorem $P_i \oplus P_j$" of Patarin (cf [24]). Then, we will see many variants and generalizations of this "Theorem $P_i \oplus P_j$" useful in Cryptography. In fact all these results can be seen as part of the theory that analyzes the number of solutions of systems of linear equalities and linear non equalities in finite groups. We have nicknamed these analysis "Mirror Theory" due to the multiples induction properties that we have in it.

Key words: Xor of random permutations, Systems of linear Equalities and Linear non Equalities in finite groups, Security proofs beyond the Birthday Bound.

1 Introduction

Solving systems of linear equations in many variables are maybe the main tasks done by computers today. We have to do this for meteorology previsions, neutronics, many other physic simulations, last steps of factoring algorithms, light simulations, etc. This is generally done by Gaussian reductions algorithms, or improved versions of it, and the evaluation of the number of solutions on finite groups is based on the analysis of the number of independent linear equations that we have. The algorithms are polynomial. With degree two (or larger degrees), instead of degree one, the situation is very different, and much more complex, since, for example, the multivariate quadratic problem (MQ) is known to be NP complete on any finite field. In this paper, we will keep the degree to be one. However, we will not only consider linear equalities, but also linear non equalities in the variables (for example: $P_1 \oplus P_2 = \lambda_1$, $P_2 \oplus P_3 = \lambda_2$, $P_1 \neq P_3$). Our motivation comes from cryptographic security proofs, since many proofs of security "beyond the birthday proof" are linked to these problems, as we will see.

Since speaking about the theory that deals about "the number of solutions of linear systems of equalities and linear non equalities in finite groups" is a bit long, we will use a nickname: Mirror theory. This nickname comes from the multiple induction properties that we will have. The paper is organized as follows. First we will consider the cryptographic problem of distinguishing $f(x\|0) \oplus f(x\|1)$, where f is a random permutation, from a random function from n bits to n bits. This problem was already studied by Bellare and Implagliazzo [3] with a proof of security in $O(\frac{q}{2^n})$ where q is the number of queries. However no precise O function was given in [3]. In this paper we will prove that if $q \leq \frac{2^n}{67}$ then the advantage for any distinguisher for this problem satisfies: $Adv \leq \frac{q}{2^n}$. This result looks simple, but the proof of it is not. To obtain this result, we will prove a theorem, called "Theorem $P_i \oplus P_j$ with $\xi_{max} = 2$ that is part of the Mirror theory. Then, we will show that many generalizations if this "Theorem $P_i \oplus P_j$" exist.

2 Notation and $f(x\|0) \oplus f(x\|1)$ when $f \in_R B_n$

In all this paper, if n is an integer, we will denote $I_n = \{0,1\}^n$. F_n will be the set of all applications from I_n to I_n, and B_n will be the set of all permutations from I_n to I_n. Therefore, $|I_n| = 2^n$, $|F_n| = 2^{n \cdot 2^n}$, and $|B_n| = (2^n)!$. $x \in_R A$ means that s is randomly chosen in A with a uniform distribution. Our first aim in this paper will be to prove Theorem 1 below.

Theorem 1 *For all CPA-2 (Adaptive chosen plaintext attack) ϕ on a function G of F_n with q chosen plaintexts, we have: $Adv_\phi^{PRF} \leq O(\frac{q}{2^n})$ where Adv_ϕ^{PRF} denotes the the advantage to distinguish $f(x\|0) \oplus f(x\|1)$ with $f \in_R B_n$ from $g \in_R F_n$. Moreover instead of $Adv_\phi^{PRF} \leq O(\frac{q}{2^n})$ we will prove in this paper the precise bound: if $q \leq \frac{2^n}{67}$ then $Adv^{PRF} \leq \frac{q}{2^n}$.*

$\|$ denotes the concatenation function, and by "advantage" we mean here, as usual, for a distinguisher, the absolute value of the difference of the two probabilities to output 1. Here x has $n-1$ bits. Theorem 1 says that there is no way (even with infinite computing power) with an adaptive chosen plaintext attack to distinguish with a good probability $f(x\|0) \oplus f(x\|1)$ from $g \in_R F_n$ when the number q of queries satisfies $q \ll 2^n$. Since we know (for example from [3]) that there is an attack in $O(2^n)$, because $\oplus_{x \in I_{n-1}} f(x\|0) \oplus f(x\|1) = 0$, and also because $\forall x \in I_{n-1},\ f(x\|0) \oplus f(x\|1) \neq 0$, Theorem 1 says that $O(2^n)$ is the exact security for this problem. In fact, this problem for $f(x\|0) \oplus f(x\|1)$ was already considered in [3] but no explicit O function was given for the security. To prove Theorem 1, we will use this general Theorem:

Theorem 2 *Let α and β be real numbers, $\alpha > 0$, and $\beta > 0$. Let E be a subset of I_n^q such that $|E| \geq (1-\beta)2^{nq}$.*
If
1. For all sequences a_i, $1 \leq i \leq q$, of pairwise distinct elements of I_n and for all sequences b_i, (not necessary distinct), $1 \leq i \leq q$, of E we have $H \geq \frac{|B_n|}{2^{nq}}(1-\alpha)$.

Then
2. For every CPA-2 with q chosen plaintexts we have: $p \leq \alpha + \beta$ where $p = Adv_{\phi}^{PRF}$ denotes the advantage to distinguish $f(x\|0) \oplus f(x\|1)$ when $f \in_R B_n$ from a random function $g \in_R F_n$.

Proof of Theorem 2. It is not difficult to prove Theorem 2 with classical counting arguments. A complete proof of Theorem 2 can also be found in [28].
How to get Theorem 1 from theorem 2
In order to get Theorem 1 from Theorem 2, a sufficient condition is to prove that for "most" (since we need β small) sequences of values b_i, $1 \leq i \leq q$, $b_i \in I_n$, we have: the number H of $f \in B_n$ such that $\forall i,\ 1 \leq i \leq q,\ f(a_i\|0) \oplus f(a_i\|1) = b_i$ satisfies $H \geq \frac{|B_n|}{2^{nq}}(1-\alpha)$ for a small value α (more precisely with $\alpha \ll O(\frac{q}{2^n})$).This is what we will do in the next sections. We can assume that in E all the b_i values are $\neq 0$ because $(2^n-1)^q = 2^{nq}(1-\frac{1}{2^n})^q \geq 2^{nq}(1-\frac{q}{2^n})$ and the coefficient $\frac{q}{2^n}$ can be included in β.

3 Theorem "$P_i \oplus P_j$" when $\xi_{max} = 2$

Change of variables
Let N be the number of sequences P_i, $1 \leq i \leq 2q$, $P_i \in I_n$ such that:
1. The P_i are pairwise distinct, $1 \leq i \leq 2q$.
2. $\forall i$, $1 \leq i \leq q$, $P_{2i-1} \oplus P_{2i} = b_i$.
We see that $H = N \cdot \frac{|B_n|}{2^n(2^n-1)\ldots(2^n-2q+1)}$, since when the P_i are fixed, then f is fixed on exactly $2q$ pairwise distinct points by $\forall i,\ 1 \leq i \leq q,\ f(a_i\|0) = P_{2i-1}$ and $f(a_i\|1) = P_{2i}$. Therefore we see that to prove Theorem 1, we want to prove this property:
For "most" sequences of values b_i, $1 \leq i \leq q$, $b_i \in I_n$, $b_i \neq 0$, we have: the number N of sequences P_i, $1 \leq i \leq 2q$; $P_i \in I_n$ such that the P_i are pairwise distinct and $\forall i,\ 1 \leq i \leq q,\ P_{2i-1} \oplus P_{2i} = b_i$ satisfies: $N \geq \frac{2^n(2^n-1)\ldots(2^n-2q+1)}{2^{nq}}(1-\alpha)$ for a small value α $(*)$. The smallest α will be, the better our security bound will be. In fact, in this paper, we will prove a much stronger property that $(*)$: we will prove that $(*)$ holds not only for "most" b_i values, $b_i \neq 0$, but for all b_i values, $b_i \neq 0$, and moreover with $\alpha = 0$. This stronger property was called "Theorem $P_i \oplus P_j$ with $\xi_{max} = 2$" in [24]. We will improve the results of [24] by giving explicit security bounds.

Theorem 3 *("Theorem $P_i \oplus P_j$ with $\xi_{max} = 2$")*
Let (A) be a set of equations: $P_1 \oplus P_2 = \lambda_0$, $P_3 \oplus P_4 = \lambda_1, \ldots, P_{\alpha-1} \oplus P_\alpha = \lambda_{\alpha/2-1}$, where all the λ_i values are $\neq 0$. Then if $\alpha \ll 2^n$ (and more precisely this condition can be written with the explicit bound $\alpha \leq \frac{2^n}{67}$), the number h_α of $(P_1, \ldots, P_\alpha)$ solution of (A) such that all the P_i variables are pairwise distinct variables of I_n, $1 \leq i \leq \alpha$, satisfies: $h_\alpha \geq \frac{2^n(2^n-1)\ldots(2^n-\alpha+1)}{2^{na}}$ where $a = \alpha/2$ is the number of equations of (A).

Here $\xi_{max} = 2$ means that when we fix one variable P_i, then at most one other variable P_j is fixed from the equations (A). Later in this paper we will study more general (A) equations where ξ_{max} will not necessary be 2. We will denote by $J_\alpha = 2^n(2^n-1)\dots(2^n-\alpha+1)$. Therefore Theorem 3 means that $h_\alpha \geq \frac{J_\alpha}{2^{na}}$ if $\alpha \ll 2^n$. In this paper we want to find explicit bounds for α, not just $\alpha \ll 2^n$. $\frac{J_\alpha}{2^{na}}$ is the average number of solutions on all the 2^{na} values $\lambda_0, \lambda_1, \dots, \lambda_{\alpha/2-1}$ (including values $\lambda_i = 0$ where $h_\alpha = 0$). $\frac{J_\alpha}{(2^n-1)^a}$ is the average number of solutions on all the $(2^n-1)^a$ non zero values $\lambda_0, \lambda_1, \dots, \lambda_{\alpha/2-1}$. Theorem 3 means that when $\alpha \ll 2^n$, then the number of solutions when the λ_i values are compatible by linearity with the P_i pairwise distinct (i.e. $\lambda_i \neq 0$) is always greater that the average. It is like if, in a classroom all the students have either the grade 0, or a grade larger than the average grade. When $h_\alpha \neq 0$, and $\alpha \ll 2^n$, then $h_\alpha$is always larger than the average and sometimes is much larger than the average.

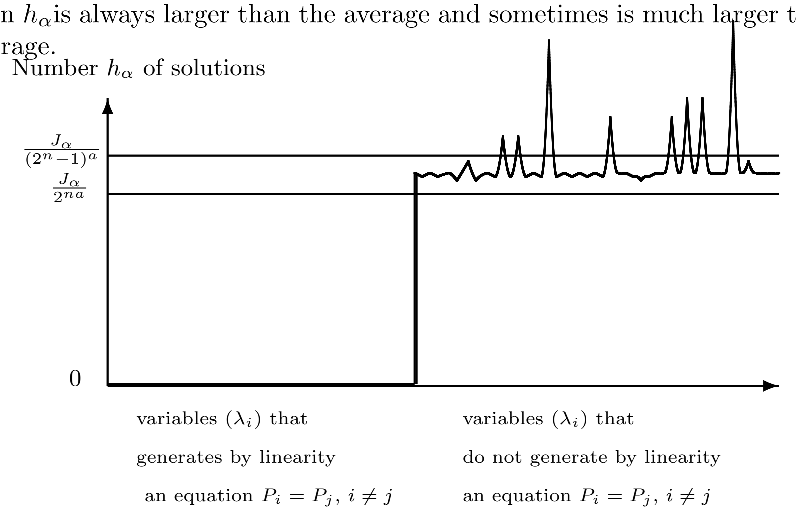

Number h_α of solutions
$\frac{J_\alpha}{(2^n-1)^a}$
$\frac{J_\alpha}{2^{na}}$
0
variables (λ_i) that
generates by linearity
an equation $P_i = P_j$, $i \neq j$
variables (λ_i) that
do not generate by linearity
an equation $P_i = P_j$, $i \neq j$

Fig. 1.

4 First results in the "Theorem $P_i \oplus P_j$" with $\xi_{max=2}$

Definition
We will denote $H_\alpha = 2^{na}h_\alpha$. Therefore $H_{\alpha+2} = 2^{n(a+1)}h_{\alpha+2}$.
In this section, we will illustrate the general proof strategy that we will follow in order to prove the "Theorem $P_i \oplus P_j$". We will prove that if $\alpha^2 \ll 2^n$, then $H_\alpha \geq J_\alpha$, and if $\alpha^3 \ll 2^{2n}$ then $H_\alpha \geq J_\alpha(1-\epsilon)$ where ϵ is very small, with explicit bounds. These bounds will then be improved later. (Remark: we follow here Patarin proof strategy given in [24], but we will present here an explicit bound instead of $H_\alpha \geq J_\alpha(1-O(\frac{\alpha^3}{2^{2n}})))$. We have $J_\alpha = 2^n(2^n-1)\dots(2^n-\alpha+1)$. Therefore, $J_{\alpha+2} = (2^n-\alpha)(2^n-\alpha-1)J_\alpha = (2^{2n}-2^n(2\alpha+1)+\alpha(\alpha+1))J_\alpha$ (1).

Lemma 1 *We have:* $(2^n-2\alpha)h_\alpha \leq h_{\alpha+2} \leq (2^n-\alpha)h_\alpha$

Proof. When $P_1, \dots, P_\alpha$ are fixed pairwise distinct, we look for solutions $P_{\alpha+1}, P_{\alpha+2}$ such that $P_{\alpha+1} \oplus P_{\alpha+2} = \lambda_{\alpha/2}$ and such that $P_1, \dots, P_\alpha, P_{\alpha+1}, P_{\alpha+2}$ are pairwise

distinct. So $P_{\alpha+2}$ is fixed when $P_{\alpha+1}$ is fixed and we want $P_{\alpha+1} \notin \{P_1, \ldots, P_\alpha, \lambda_{\alpha/2} \oplus P_1, \ldots, \lambda_{\alpha/2} \oplus P_\alpha\}$. Therefore for $(P_{\alpha+1}, P_{\alpha+2})$ we have between $2^n - 2\alpha$ and $2^n - \alpha$ solutions when $P_1, \ldots, P_\alpha$ are fixed, i.e. $(2^n - 2\alpha)h_\alpha \leq h_{\alpha+2} \leq (2^n - \alpha)h_\alpha$ as claimed.
Since $H_\alpha = 2^{na}h_\alpha$ and $H_{\alpha+2} = 2^{n(a+1)}h_{\alpha+2}$, we can write Lemma 1 like this:

$$2^n(2^n - 2\alpha)H_\alpha \leq H_{\alpha+2} \leq 2^n(2^n - \alpha)H_\alpha \quad (2)$$

Now from (1) and (2) we have:

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \frac{2^{2n} - 2\alpha \cdot 2^n}{2^{2n} - 2^n(2\alpha+1) + \alpha(\alpha+1)} \frac{H_\alpha}{J_\alpha}$$

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \big(1 + \frac{2^n - \alpha(\alpha+1)}{2^{2n} - 2^n(2\alpha+1) + \alpha(\alpha+1)}\big) \frac{H_\alpha}{J_\alpha} \quad (3)$$

We also have $H_2 > J_2$ since $H_2 = 2^{2n} > J_2 = 2^n(2^n - 1)$. Therefore, if $\alpha^2 \leq 2^n$, we have $H_\alpha \geq J_\alpha$ as claimed, by induction on α. Moreover, from (3):

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \big(1 + \frac{-\alpha(\alpha+1)}{2^{2n} - 2^n(2\alpha+1)}\big) \frac{H_\alpha}{J_\alpha}$$

Therefore we have:

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \big(1 + \frac{-\alpha(\alpha+1)}{2^{2n} - 2^n(2\alpha+1)}\big)^{\alpha/2} \frac{H_2}{J_2}$$

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq 1 - \frac{\alpha^2(\alpha+1)}{2(2^{2n} - 2^n(2\alpha+1))}$$

This gives:

$$H_\alpha \geq J_\alpha\big(1 - \frac{\alpha^3}{2 \cdot 2^{2n} - 4\alpha 2^n}\big) \quad (4)$$

Therefore, if $\alpha^3 \ll 2^{2n}$, $H_\alpha \geq J_\alpha(1 - \epsilon)$ where ϵ is very small, as claimed. (Moreover, from (4) we have an explicit bound).

5 General properties when $\xi_{max} = 2$

Here, since $\xi_{max} = 2$, our set of equations is:

$$(A) \begin{cases} P_2 = P_1 \oplus \lambda_0 \\ P_4 = P_3 \oplus \lambda_1 \\ \vdots \\ P_\alpha = P_{\alpha-1} \oplus \lambda_{\alpha/2-1} \end{cases}$$

h_α is by definition the number of $P_1, \cdots, P_\alpha$ pairwise distinct, elements of I_n, and solution of (A). We want to evaluate h_α by induction on α, i.e. we want to evaluate $h_{\alpha+2}$ from h_α. We will say that $(P_1, \cdots, P_\alpha)$ are solution of h_α, when

they are solution of (A). We will denote $\beta = \alpha/2 - 1$.
We will denote by $\lambda_{(i)}$ the coefficient λ in the equation (A) that involves P_i. For example: $\lambda_{(1)} = \lambda_{(2)} = \lambda_0$. $\lambda_{(\alpha)} = \lambda_{(\alpha-1)} = \lambda_{\alpha/2-1}$. We will say that two indices i and j "are in the same block", or "are in the same (A)-block" if $P_i \oplus P_j = \lambda_{(i)}$ is one of the equations (A). For $h_{\alpha+2}$ we have (A) and one more equation: $P_{\alpha+1} \oplus P_{\alpha+2} = \lambda_{\beta+1}$ (see figure 2)

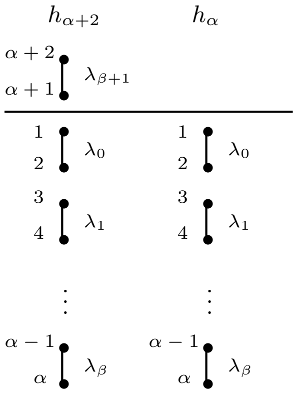


Fig. 2. We want to evaluate $h_{\alpha+2}$ from h_α.

Remark: We will evaluate here h_α for all the values λ_i, even the worse ones. However, in cryptographic applications we generally need h_α for most values of λ_i instead of all values λ_i.

We start from a solution $P_1, \cdots, P_\alpha$ of h_α and we want to complete it to get the solutions of $h_{\alpha+2}$. For this we have to choose $x = P_{\alpha+1} \oplus P_1$ such that x will not create a collision $P_j = P_{\alpha+1}$ or $P_j = P_{\alpha+2}$, $1 \leq j \leq \alpha$. This means $x \notin V$ with $V = V_1 \cup V_2$, with $V_1 = \{P_1 \oplus P_j, 1 \leq j \leq \alpha\}$ and $V_2 = \{\lambda_{\beta+1} \oplus P_1 \oplus P_j, 1 \leq j \leq \alpha\}$. We have $|V| = |V_1 \cup V_2| = |V_1| + |V_2| - |V_1 \cap V_2|$, and we have $|V_1| = \alpha$ and $|V_2| = \alpha$ (since the P_j values, $1 \leq j \leq \alpha$, are pairwise distinct). So

$$h_{\alpha+2} = \sum_{(P_1,\cdots,P_\alpha) \text{ solution of } h_\alpha} (2^n - |V|)$$

$$h_{\alpha+2} = \sum_{(P_1,\cdots,P_\alpha) \text{ solution of } h_\alpha} (2^n - 2\alpha + |V_1 \cap V_2|)$$

$$h_{\alpha+2} = (2^n - 2\alpha)h_\alpha + \sum_{(P_1,\cdots,P_\alpha) \text{ solution of } h_\alpha} |V_1 \cap V_2| \quad (1)$$

Approximation in $O(\frac{\alpha}{2^n})$.

Since $|V_1| = |V_2| = \alpha$ we obtain another proof for Lemma 1, that we will call here Theorem 4.

Theorem 4

$$(2^n - 2\alpha)h_\alpha \leq h_{\alpha+2} \leq (2^n - \alpha)h_\alpha$$

More Precise Approximation

The elements of V_1 are α pairwise distinct elements, and the elements of V_2 are α pairwise distinct elements, so from (1) we obtain:

$$h_{\alpha+2} = (2^n - 2\alpha)h_\alpha +$$

$$\sum_{(P_1,\cdots,P_\alpha) \text{ solution of } h_\alpha} \sum_{1\leq i\leq\alpha} \sum_{1\leq j\leq\alpha} [\text{ Number of Equations } P_i \oplus P_j = \lambda_{\beta+1}]$$

Therefore, by inverting the $\sum$:

$$h_{\alpha+2} = (2^n - 2\alpha)h_\alpha +$$

$$\sum_{1\leq i\leq\alpha} \sum_{1\leq j\leq\alpha} [\text{ Number of } P_1,\cdots,P_\alpha \text{ solution of } h_\alpha \text{ plus } P_i \oplus P_j = \lambda_{\beta+1}]$$

Now when we add the equality $\lambda_{\beta+1} = P_i \oplus P_j$ to the system of equation (A) of h_α, 3 cases can occur:

Case 1.

$\lambda_{\beta+1} = P_i \oplus P_j$ is a consequence of (A). Here this means that $\lambda_{\beta+1} = P_i \oplus P_j$ was already an equation of (A), and therefore $\lambda_{\beta+1} = \lambda_{(i)}$ for a value i, $1 \leq i \leq \alpha$. Remark: $\lambda_{\beta+1} = \lambda_{(i)}$ creates 2 collisions in $|V_1 \cap V_2|$: it creates $\lambda_{\beta+1} \oplus P_1 \oplus P_i = P_1 \oplus P_j$ and $\lambda_{\beta+1} \oplus P_1 \oplus P_j = P_1 \oplus P_i$.

Case 2.

$\lambda_{\beta+1} = P_i \oplus P_j$ is in contradiction with the equations of (A). If i and j are in the same block the contradiction comes from $i = j$ or from $i \neq j$ and $\lambda_{\beta+1} \neq \lambda_{(i)}$. If i and j are not in the same block, the contradiction comes from the fact that $\lambda_{\beta+1} = P_i \oplus P_j$ creates a collision; i.e. we have $\lambda_{\beta+1} = \lambda_{(i)}$, or $\lambda_{\beta+1} = \lambda_{(j)}$, or $\lambda_{\beta+1} = \lambda_{(i)} \oplus \lambda_{(j)}$ (cf Figure 3).

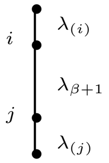


Fig. 3. Here $\lambda_{\beta+1} = \lambda_{(i)}$, $\lambda_{\beta+1} = \lambda_{(j)}$ and $\lambda_{\beta+1} = \lambda_{(i)} \oplus \lambda_{(j)}$ are impossible if the P_j are pairwise distinct.

Case 3.

The equation $\lambda_{\beta+1} = P_i \oplus P_j$ is not in contradiction with the equations of (A), and is not a consequence of the equations of (A). We will say that this case is the "generic" case.

From (1) and from the 3 cases above, we get immediately:

Theorem 5

$$\frac{h_{\alpha+2}}{2^n} = h_\alpha\big[1 - \frac{2\alpha}{2^n} + \frac{2 \textit{ Number of equations } \lambda_{\beta+1} = \lambda_i}{2^n}\big]$$

$$+\frac{1}{2^n}\sum_{(i,j)\in M} (\textit{ Number of } P_1, \cdots, P_\alpha \textit{ solution of } h_\alpha \textit{ plus } P_i \oplus P_j = \lambda_{\beta+1})$$

where

$$M = \{(i,j),, 1 \le i \le \alpha,\ 1 \le j \le \alpha, \textit{ such that } i \textit{ and } j \textit{ are not in the same block,}$$

$$\textit{and such that } \lambda_{\beta+1} \neq \lambda_{(i)}, \lambda_{\beta+1} \neq \lambda_{(j)}, \textit{ and } \lambda_{\beta+1} \neq \lambda_{(i)} \oplus \lambda_{(j)}\}$$

Now, in the Appendices B, C, E we explain how Theorem 3 (i.e. Theorem $P_i \oplus P_j$ with $\xi_{max} = 2$) can be proved from Theorem 5 with the explicit bound $\alpha \le \frac{2^n}{67}$, as claimed.

6 Theorem "$P_i \oplus P_j$" for any ξ_{max}

We will now present some generalizations of the Theorem "$P_i \oplus P_j$" that we have seen for $\xi_{max} = 2$. This generalization that we will see in Theorem 6 below was first introduced in [24]. In this paper we will obtain for it an explicit security bound. introduced

Definition 1 *Let (A) be a set of equations $P_i \oplus P_j = \lambda_k$, with $P_i, P_j \in I_n$. If by linearity from (A) we cannot generate an equation in only the λ_k, we will say that (A) has no "circle in P", or that the equations of (A) are "linearly independent in P".*

Let a be the number of equations in (A), and α be the number of variables P_i in (A). Therefore, we have parameters $\lambda_1, \lambda_2, \ldots, \lambda_a$ and $a + 1 \le \alpha \le 2a$

Definition 2 *We will say that two indices i and j are "in the same block" if by linearity from the equation of (A) we can obtain $P_i \oplus P_j =$ an expression in $\lambda_1, \lambda_2, \ldots, \lambda_a$.*

Definition 3 *We will denote by ξ_{max} the maximum number of indices that are in the same block.*

Example. If $A = \{P_1 \oplus P_2 = \lambda_1,\ P_1 \oplus P_3 = \lambda_2,\ P_4 \oplus P_5 = \lambda_3\}$, here we have two blocks of indices $\{1, 2, 3\}$ and $\{4, 5\}$ and $\xi_{max} = 3$.

Definition 4 *For such a system* (A)*, when* $\lambda_1, \lambda_2, \ldots, \lambda_a$ *are fixed, we will denote by* $h_\alpha(A)$ *the number of* $P_1, P_2, \ldots, P_\alpha$ *solutions of* (A) *such that:* $\forall i, j\ i \neq j \Rightarrow P_i \neq P_j$*. We will also denote* $H_\alpha(A) = 2^{na} h_\alpha(A)$*. We will generally denote* $H_\alpha(A)$ *simply by* H_α *and* $h_\alpha(A)$ *simply by* h_α*.* H_α *and* h_α *are simple concise notations, but for a given value* α*,* H_α *and* h_α *can have different values for different systems* (A)*.*

As above, we will denote by J_α the number of $P_1, P_2, \ldots, P_\alpha$ such that $\forall i, j\ i \neq j \Rightarrow P_i \neq P_j$. Therefore, $J_\alpha = 2^n(2^n - 1) \ldots (2^n - \alpha + 1)$.

Theorem 6 *("Theorem* $P_i \oplus P_j$*" for any* ξ_{max}*)*
let (A) *be a set of a equation* $P_i \oplus P_j = \lambda_k$ *with* α *variables such that:*
1. We have no circle in P *in the equations* (A)*.*
2. We have no more than ξ_{max} *indices in the same block.*
3. By linearity from (A) *we cannot generate an equation* $P_i = P_j$ *with* $i \neq j$*. (This means that if* i *and* j *are in the same block, then the expression in* $\lambda_1, \lambda_2, \ldots, \lambda_a$ *for* $P_i \oplus P_j$ *is* $\neq 0$*.*
Then: if $\xi_{max}^2 \alpha \ll 2^n$*, we have* $H_\alpha \geq J_\alpha$*. More precisely the fuzzy condition* $\xi_{max}^2 \alpha \ll 2^n$ *can be written with the explicit bound:* $(\xi_{max} - 1)\alpha \leq \frac{2^n}{67}$*.*

Proof. The proof of Theorem 6 is given in the Appendices.
Remark of 2017. A more complete and improved proof is available in [14] chapter 17 since 2017.
Remark. For cryptographic use, weaker version of this theorem will be enough. For example, instead of $H_\alpha \geq J_\alpha$, $H_\alpha \geq J_\alpha(1 - f(\frac{\xi_{max}}{2^n}))$ where f is a function such that $f(x) \to 0$ when $x \to 0$ is enough.
Various generalizations of Theorem $P_i \oplus P_j$
For balanced Feistel schemes Ψ^d, Theorem 6 will be enough. For unbalanced Feistel schemes, we will need a variant of it: Theorem 7

Theorem 7 *("Theorem* $P_i \oplus P_j$*" for* G_3^d *schemes)*
Let $\beta > 0$*. Let* (A) *be a set of equations with* α *variables* $P_i \oplus P_j = \lambda_k$*, with* $\lambda_k \neq 0$*. Let* (B) *be a set of non equalities of the form* $P_i \neq P_j$*, or of the form* $[P_i, P_j] \neq [P_k, P_l]$ *such that for all variable* i*, the number of* j *such that* $P_i \neq P_j$ *is in* (B) *is* $\leq \beta$*, and for all variables* (i, j)*, the number of* (k, l) *such that* $[P_i, P_j] \neq [P_k, P_l]$ *is in* (B) *is* $\leq \beta 2^n$*.*
‘ If
1. We have no circle in P *in the equations* (A)*.*
2. We have no more than ξ_{max} *indices in the same block.*
3. By linearity from (A) *we cannot generate an equation in contradiction with* (B)*.*
4. $\xi_{max}^2 \beta \leq \frac{2^n}{67}$*.*
Then $h_\alpha \geq \frac{Weight(B^+)}{2^{na}}$ *where* $Weight(B^+)$ *denotes the number of* $P_1, \ldots; P_\alpha$ *of* I_n^α *that satisfy the non equalities* (B) *plus for all equation* $P_i \oplus P_j = \lambda_k$ *of* (A)*,* $\lambda_k \neq 0$*, the non equalities:* $P_i \neq P_j$*.*

Proof. Proof of Theorem 7 can be done exactly as for Theorem 6, i.e. we proceed by induction on α, and the coefficient $\frac{1}{2^n}$ that comes from $P_\alpha \neq P_j$ for each equation in (A), i.e. in (B^+) when we deal with the index α, will be dominant for all the other terms. Notice that in Theorem 7 α can be much larger than 2^n (for G_3^d schemes we will have $\alpha \ll 2^{2n}$ or $\alpha \ll 2^{1.5n}$ and therefore $\alpha \geq 2^n$ in general): a product of terms ≥ 1 is always ≥ 1 whatever the number of terms.

Other generalizations

We will not need them in this paper, but many other generalizations of the "Theorem $P_i \oplus P_j$" exist. Here are some examples.

Generalization 1. The theorem is still true an any group G (instead of I_n). This is relatively easy to see since only the number of variables related with linear equalities are used in the proofs and never the specific nature of the group I_n. When G is not commutative, a special analysis might needed, however.

Generalization 2. The theorem $P_i \oplus P_j$ is still true if we change the condition $\xi_{max}\alpha \ll 2^n$ by $\xi_{average} \ll 2^n$.

Generalization 3. In Theorem 7 we can have more general non equalities in (B), such $[P_{i_1}, P_{j_1}, P_{k_1}] \neq [P_{i_2}, P_{j_2}, P_{k_2}]$ or more complex conditional non equalities.

Generalization 4. We can have equations $P_i \oplus P_j \oplus P_k = \lambda_{ijk}$ instead of $P_i \oplus P_j = \lambda_{ij}$. More generally we can have equations $P_{i_1} \oplus P_{i_2} \oplus \ldots \oplus P_{i_k} = \lambda_l$ with any number k of variables in each linear equation.

Generalization 5. We can also consider partial linear non equalities, for example on the first m bits, $m \leq n$, i.e. $\lceil P_i \rceil \neq \lceil P_J \rceil$ instead of $P_i \neq P_j$, where $\lceil P_i \rceil$ denotes the first m bits of P_i.

We do not claim to have proved all these 4 generalizations and we will not need them in this paper, but we believe that they will be relatively easy variants of the main Theorem 6 and Theorem 7

7 Conclusion

The starting point of this paper was Theorem 2, with a proof that if $q \leq \frac{2^n}{67}$, then $Adv^{PRF} \leq \frac{q}{2^n}$ for the problem of distinguishing $f(x\|0) \oplus f(x\|1)$ (with $f \in_R B_n$) from a random function. This result has its own interest, but, as we have seen the proof technique involved in this paper is very general and based on the evaluation of systems of linear equalities and linear non equalities on finite groups, i.e. Mirror Theory. We have proved in this paper many results on Mirror Theory with the group $(I_n, \oplus)$ and presented many possible generalizations. We believe that this paper can be seen as an introduction to Mirror Theory, and that many future results will come, with many cryptographic applications for proof of security "above the birthday bound" of various systems. At present at least 3 directions are under investigation: the security of unbalanced Feistel schemes, the generalizations of the "Theorem $P_i \oplus P_j$" presented in this paper and "Patarin Conjecture on the Xor of two random permutations". This conjecture says that for all functions f on n bits, if $\oplus_{x \in I_n} f(x) = 0$, then the number H of couples of permutations $(g, h) \in B_n^2$ such that $f = g \oplus h$ always satisfies: $H \geq \frac{|B_n|^2}{2^{2^n}}$. This is a rather extreme Mirror property since here we do not have $q \ll 2^n$ but

$q = 2^n - 1$ where q is the number of x involved. We do not need this conjecture in Cryptography, where proofs with $q \ll 2^n$ with precise bounds are generally enough, but it is a very challenging problem for Mirror Theory and it shows the diversity of the problems involved in this Mirror Theory.

References

1. William Aiello and Ramarathnam Venkatesan. Foiling Birthday Attacks in Length-Doubling Transformations - Benes: A Non-Reversible Alternative to Feistel. In Ueli M. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 307–320. Springer-Verlag, 1996.
2. Anonymous. Security of balanced and unbalanced Feistel Schemes with Linear Non Equalities. In *Paper submitted to Crypto 2010*, 2010.
3. Mihir Bellare and Russell 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.
4. Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In Kaisa Nyberg, editor, *Advances in cryptology – EUROCRYPT 1998*, volume 1403 of *Lecture Notes in Computer Science*, pages 266–280. Springer-Verlag, 1998.
5. Chris Hall, David Wagner, John Kelsey, and Bruce Schneier. Building PRFs from PRPs. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 370–389. Springer-Verlag, 1998.
6. Marshall Hall Jr. A Combinatorial Problem on Abelian Groups. *Proceedings of the Americal Mathematical Society*, 3(4):584–587, 1952.
7. Lars R. Knudsen. DEAL - A 128-bit Block Cipher. Technical Report 151, University of Bergen, Department of Informatics, Norway, february 1998.
8. Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.
9. Stefan Lucks. The Sum of PRPs Is a Secure PRF. In Bart Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 470–487. Springer-Verlag, 2000.
10. U. Maurer. A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators. In *Advances in Cryptology – EUROCRYPT '92*, Lecture Notes in Computer Science, pages 239–255. Springer-Verlag, 1992.
11. U. Maurer. Indistinguishability of Random Systems. In *Advances in Cryptology – EUROCRYPT '02*, volume 2332 of *Lecture Notes in Computer Science*, pages 100–132. Springer-Verlag, 2002.
12. Ueli Maurer and Krzysztof Pietrzak. The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 544–561. Springer-Verlag, 2003.
13. Valérie Nachef. Random Feistel Schemes for $m = 3$. *available from the author at: valerie.nachef@u-cergy.fr.*
14. Valérie Nachef, Jacques Patarin, and Emmanuel Volte. *Feistel Ciphers.* Springer Verlag, 2017.
15. Moni Naor and Omer Reingold. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *J. Cryptology*, 12(1):29–66, 1999.

16. Jacques Patarin. Pseudorandom Permutations based on the DES Scheme. In *Eurocode '91*, volume 514 of *Lecture Notes in Computer Science*, pages 193–204. Springer-Verlag, 1990.
17. Jacques Patarin. Etude de Générateurs de Permutations Basés sur les Schémas du DES. In *Ph. Thesis.* Inria, Domaine de Voluceau, France, 1991.
18. Jacques Patarin. New results on pseudorandom permutation generators based on the DES Scheme. In *Advances in Cryptology – CRYPTO 1991*, Lecture Notes in Computer Science, pages 301–312. Springer-Verlag, 1991.
19. Jacques Patarin. Improved Security Bounds for Pseudorandom Permutations. In *4th ACM Conference on Computer and Communication Security*, pages 142 – 150, 1997.
20. Jacques Patarin. About Feistel Schemes with 6 (or more) Rounds). In Serge Vaudenay, editor, *FSE 1998*, volume 1372 of *Lecture Notes in Computer Science*, pages 103 – 121. Springer-Verlag, 1998.
21. Jacques Patarin. Generic Attacks on Feistel Schemes. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 222–238. Springer-Verlag, 2001.
22. Jacques Patarin. Luby-Rackoff: 7 Rounds are Enough for $2^{n(1-\epsilon)}$ Security. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 513–529. Springer-Verlag, 2003.
23. Jacques Patarin. Security of Random Feistel Schemes with 5 or more rounds. In Matthew K. Franklin, editor, *Advances in Cryptology – CRYPTO' 04*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer-Verlag, 2004.
24. Jacques Patarin. On linear systems of equations with distinct variables and Small block size. In Dongho Wan and Seungjoo Kim, editors, *ICISC 2005*, volume 3935 of *Lecture Notes in Computer Science*, pages 299–321. Springer-Verlag, 2006.
25. Jacques Patarin. A proof of security in $O(2^n)$ for the Benes schemes. In Serge Vaudenay, editor, *Progress in Cryptology – AFRICACRYPT' 08*, volume 5023 of *Lecture Notes in Computer Science*, pages 209–220. Springer-Verlag, 2008.
26. Jacques Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations - Extended Version. *Cryptology ePrint archive: 2008/010: Listing for 2008*, 2008.
27. Jacques Patarin. Generic Attacks for the Xor of k Random Permutations. *Cryptology ePrint archive: 2008/009: Listing for 2008*, 2008.
28. Jacques Patarin. The coefficient H technique . In Roberto Avanzi, Liam Keliher, and Francesco Sica, editors, *SAC 2008*, volume 5381 of *Lecture Notes in Computer Science*, pages 66–81. Springer-Verlag, 2009.
29. Jacques Patarin, Valérie Nachef, and Côme Berbain. Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 396–411. Springer-Verlag, 2006.
30. F. Salzborn and G. Szekeres. A Problem in Combinatorial Group Theory. *Ars Combinatoria*, 7:3–5, 1979.
31. Bruce Schneier and John Kelsey. Unbalanced Feistel Networks and Block Cipher Design. In Dieter Gollmann, editor, *Fast Software Encrytion – FSE '96*, volume 1039 of *Lecture Notes in Computer Science*, pages 121–144. Springer-Verlag, 1996.
32. S. Vaudenay. Provable security for block ciphers by decorrelation. In *STACS '98*, volume 1373 of *Lecture Notes in Computer Science*, pages 249–275. Springer-Verlag, 1998.
33. Aaram Yun, Je Hong Park, and Jooyoung Lee. Lai-Massey Scheme and Quasi-Feistel Networks. *Cryptology ePrint archive: 2007/347: Listing for 2007.*

A Examples of h_α, h'_α and h''_α values for small α and $\xi_{max} = 2$

We present here quickly some examples of h_α, h'_α and h''_α values for $\alpha \leq 6$ and $\xi_{max=2}$. These values h_α have been defined in section 2. h'_α values are similar to h_α values but with one more linearly independent equation $P_i \oplus P_j = \lambda_{ij}$, and h''_α values are similar to h_α values but with two more linearly independent equations $P_i \oplus P_j = \lambda_{ij}$. These small examples illustrate the general results on the h_α values obtained in this paper.

A.1 Values with $\alpha = 2$

Here h_2 is the number of $P_1, P_2 \in I_n,\ P_1 \neq P_2$ such that $P_1 \oplus P_2 = \lambda_0$ with $\lambda_0 \neq 0$. Therefore $h_2 = 2^n$. (only one value for h_2).

A.2 Value with $\alpha = 4$

h_4 is the number of pairwise distinct P_1, P_2, P_3, P_4 such that: $P_1 \oplus P_2 = \lambda_0$ and $P_3 \oplus P_4 = \lambda_1$, with $\lambda_0 \neq 0$ and $\lambda_1 \neq 0$.
Case 1. $\lambda_0 \neq \lambda_1$. Then $h_4 = 2^n(2^n - 4)$.
Case 2. $\lambda_0 = \lambda_1$. Then $h_4 = 2^n(2^n - 2)$.
For h'_4 we have only one possible value: $h'_4 = 2^n$ for all the cases.

A.3 Examples with $\alpha = 6$

h_6 **values.**
h_6 is the number of pairwise distinct $P_1, P_2, P_3, P_4, P_5, P_6$ such that $P_1 \oplus P_2 = \lambda_0$, $P_3 \oplus P_4 = \lambda_1$, $P_5 \oplus P_6 = \lambda_2$, with with $\lambda_0 \neq 0$, $\lambda_1 \neq 0$ and $\lambda_2 \neq 0$. These values h_6 can be computed from the formulas that give the h_α values by induction, or directly and then we can check the formulas with these values.
Case 1. $\lambda_0, \lambda_1, \lambda_2$ are pairwise distinct and $\lambda_0 \oplus \lambda_1 \oplus \lambda_2 \neq 0$. Then $h_6 = 2^n(2^{2n} - 12 \cdot 2^n + 40)$.
Case 2. $\lambda_2 = \lambda_0 \neq \lambda_1$, or $\lambda_2 = \lambda_1 \neq \lambda_0$, or $\lambda_1 = \lambda_0 \neq \lambda_2$. Then $h_6 = 2^n(2^n - 4)(2^n - 6) = 2^n(2^{2n} - 10 \cdot 2^n + 24)$.
Case 3. $\lambda_0 \oplus \lambda_1 \oplus \lambda_2 = 0$. Then $h_6 = 2^n(2^{2n} - 12 \cdot 2^n + 32)$.
Case 4. $\lambda_0 = \lambda_1 = \lambda_2$. Then $h_6 = 2^n(2^n - 2)(2^n - 4)$.
Remark. If $n = 3$, then we are working in the group I_3 with 8 elements, and if $\lambda_0 \oplus \lambda_1 \oplus \lambda_2 = 0$ then $h_6 = h_8 = 0$. This shows that when α is very near 2^n we can have $h_\alpha = 0$. It also shows that the equations h_α can be linearly independent but not compatible when α is very near 2^n.
h'_6 **values.**

Let $P_2 \oplus P_3 = \lambda$ be the new equality in h'_6 that we did not have in h_6. We have $\lambda \notin \{0, \lambda_0, \lambda_1, \lambda_0 \oplus \lambda_1\}$ since this new equation must be linearly compatible with h_6. Then it is possible to prove that

$$h'_6 = 2^n(2^n - |\{0, \lambda_0, \lambda \oplus \lambda_0, \lambda_1 \oplus \lambda \oplus \lambda_0, \lambda_2, \lambda_2 \oplus \lambda_0, \lambda_2 \oplus \lambda \oplus \lambda_0, \lambda_2 \oplus \lambda_1 \oplus \lambda \oplus \lambda_0\}|)$$

We will now present some examples for the values $h'_6 - \frac{h_6}{2^n}$.
Example 1. If $\lambda_2 \notin \{\lambda_0, \lambda \oplus \lambda_0, \lambda_1 \oplus \lambda \oplus \lambda_0, \lambda, \lambda_1 \oplus \lambda, \lambda_1\}$ then $h'_6 = 2^n(2^n - 8)$. Moreover, if $\lambda_0, \lambda_1, \lambda_2$ are pairwise distinct and $\lambda_0 \oplus \lambda_1 \oplus \lambda_2 \neq 0$, and $\lambda \notin \{\lambda_0 \oplus \lambda_2, \lambda_0 \oplus \lambda_1 \oplus \lambda_2, \lambda_2, \lambda_1 \oplus \lambda_2\}$, then $h'_6 - \frac{h_6}{2^n} = 4 \cdot 2^n - 40$
Example 2. If $\lambda_0 \oplus \lambda_1 \oplus \lambda_2 = 0$, then $h'_6 = 2^n(2^n - 8)$. Here $h'_6 - \frac{h_6}{2^n} = 4 \cdot 2^n - 32$
Example 3. If $\lambda = \lambda_2$ and $\lambda_0, \lambda_1, \lambda_2$ are pairwise distinct and $\lambda_0 \oplus \lambda_1 \oplus \lambda_2 \neq 0$, then $h'_6 = 2^n(2^n - 6)$. Here $h'_6 - \frac{h_6}{2^n} = 6 \cdot 2^n - 40$
Example 4. If $\lambda = \lambda_2, \lambda_0 = \lambda_1$ and $\lambda_0 \neq \lambda_2$, then $h'_6 = 2^n(2^n - 4)$. Here $h'_6 - \frac{h_6}{2^n} = 6 \cdot 2^n - 24$
Example 5. If $\lambda_0 = \lambda_1 = \lambda_2$, then $h'_6 = 2^n(2^n - 4)$. Here $h'_6 - \frac{h_6}{2^n} = 2 \cdot 2^n - 8$
Example 6. If $\lambda_0 = \lambda_1$ is the only exceptional equation, then $h'_6 = 2^n(2^n - 8)$. Here $h'_6 - \frac{h_6}{2^n} = 2 \cdot 2^n - 24$
Example 7. If $\lambda_0 = \lambda_2$ is the only exceptional equation, then $h'_6 = 2^n(2^n - 6)$. Here $h'_6 - \frac{h_6}{2^n} = 4 \cdot 2^n - 24$
h''_α **values.**

In all cases $h''_6 = 2^n$

B Evaluation of $|M| =$ and introducing the h'_α values

B.1 Definitions

We will use the following notation.
• Let $\delta =$ the number of indices i, $0 \leq i \leq \beta$, such that $\lambda_{\beta+1} = \lambda_i$.
• Let $\varDelta = \sup_{0 \leq i \leq \beta+1}[$ Number of j, $0 \leq j \leq \beta + 1$, $j \neq i$, such that $\lambda_j = \lambda_i]$.
Then
$2\delta =$ Number of i, $1 \leq i \leq \alpha$, such that $\lambda_{\beta+1} = \lambda_i$.
Similarly $2\varDelta = \sup_{0 \leq i \leq \beta+1}[$ Number of j, $1 \leq j \leq \alpha + 2$, i and j are not in the same block, such that $\lambda_i = \lambda_{(j)}]$.

Lemma 2 *The number of indices j, $1 \leq j \leq \alpha+2$ such that $\lambda_{(j)} =$ a fixed value is $\leq 2\varDelta + 2$.*

Proof. If j_0 is a solution, then j'_0 such that j_0 and j'_0 are in the same block is also a solution. Now if j is another solution, j and j_0 not in the same block, we have $\lambda_{(j)} = \lambda_{(j_0)}$ and therefore at most $2\varDelta$ solutions for j, and $2\varDelta + 2$ solutions in total, including j_0 and j'_0.
$\varDelta$ is the maximum possible value for δ when we change the ordering of the indices. Moreover, we can always choose the ordering of the indices such that $\delta = \varDelta$. For this we just choose $\alpha + 1$ with a value $\lambda_{\alpha+1}$ that gives the larger δ.
• Let (F) be a system of linear equations in the P_i variables. Let E be a linear equation in the P_i variables. We will say that E is "locally independent from (F)", or is "linearly independent from (F)" if we cannot generate from (F) by linearity this equation E, and if from the equations (F) and the equation E we cannot generate by linearity an equation $P_i = P_j$ with $i \neq j$.

Remark. E can be linearly independent from (F), but A may have some solutions pairwise distinct, and $E+F$ may have no solutions pairwise distinct. (For example h_6 on $\{0,1\}^3$: cf Appendix A)

• We will denote by h'_α the number of pairwise distinct variables solutions of the system (A') where (A') denotes the system (A) seen in section 5 plus one linear equation of the type $P_k \oplus P_l = \lambda$ such that this new equation is linearly independent from (A). Since the set M seen in section 5 is precisely the number of (k,l) such that $\lambda_{\beta+1} = P_k \oplus P_l$ is linearly independent from (A), we can use these notations to write Theorem 4 like this:

Theorem 8

$$\frac{h_{\alpha+2}}{2^n} = h_\alpha\big(1 - \frac{2\alpha}{2^n} + \frac{2\delta}{2^n}\big) + \frac{1}{2^n}\sum_{(k,l)\in M} h'_\alpha(k,l)$$

Here $h'_\alpha(k,l)$ means that we have added the equation $\lambda_{\beta+1} = P_k \oplus P_l$. We will often write h'_α instead of $h'_\alpha(k,l)$ but we will have to remember that the values h'_α are generally different. In fact, to evaluate these values h'_α will be one of our aim.

Example. In Appendix A we give some examples of h_α and h'_α values where Theorem 8 can be illustrated.

B.2 Evaluation of $|M|$

Theorem 9 *The exact value of $|M|$ is:*

$$|M| = \alpha(\alpha-2) - 4\delta(\alpha-\delta-1) - [\textit{Number of } i,j,\ 1 \le i \le \alpha,\ 1 \le j \le \alpha,$$

$$\lambda_{\beta+1} = \lambda_{(i)} \oplus \lambda_{(j)}]$$

This is also:

$$|M| = \alpha(\alpha-2) - 4\delta(\alpha-\delta-1) - 8[\textit{Number of } i,j,\ 0 \le i < j \le \beta,$$

$$\lambda_{\beta+1} = \lambda_i \oplus \lambda_j]$$

Proof. If i and j are in the same (A)-block then $P_i \oplus P_j = \lambda_{\beta+1}$ cannot be linearly independent from (A). More precisely from Section 5, we have: $|M| = \alpha(\alpha-2) - [$ Number of (i,j), $1 \le i \le \alpha$,
$1 \le j \le \alpha$ such that i and j are not in the same block, and such that $\lambda_{\beta+1} = \lambda_{(i)}$, or $\lambda_{\beta+1} = \lambda_{(j)}$, or $\lambda_{\beta+1} = \lambda_{(i)} \oplus \lambda_{(j)}]$. We have seen that $2\delta =$ Number of i, $1 \le i \le \alpha$, such that $\lambda_{\beta+1} = \lambda_{(i)}$. Let D be the number of (i,j), $1 \le i \le \alpha$, $1 \le j \le \alpha$, such that i and j are not in the same block, and such that $(\lambda_{\beta+1} = \lambda_{(i)}$ or $\lambda_{\beta+1} = \lambda_{(j)})$. We have $D = (2\delta)(\alpha-2\delta) + (\alpha-2\delta)(2\delta) + 4\delta(\delta-1)$ because we have $2\delta(\alpha-2\delta)$ possibilities with $\lambda_{\beta+1} = \lambda_{(i)}$ and $\lambda_{\beta+1} \neq \lambda_{(j)}$, we have $(\alpha-2\delta)(2\delta)$ possibilities with $\lambda_{\beta+1} \neq \lambda_{(i)}$ and $\lambda_{\beta+1} = \lambda_{(j)}$, and we have $4\delta(\delta-1)$ possibilities with $\lambda_{\beta+1} = \lambda_{(i)} = \lambda_{(j)}$. Then $D = 4\delta(\alpha - 2\delta + \delta - 1) =$

$4\delta(\alpha-\delta-1)$, and $|M| = \alpha(\alpha-2) - 4\delta(\alpha-\delta-1) -$ [Number of i, j, $1 \le i \le \alpha$, $1 \le j \le \alpha$, $\lambda_{\beta+1} = \lambda_{(i)} \oplus \lambda_{(j)}$] as claimed. Let denote by i and i' two indices in the block of i and by j and j' two indices in the block of j. So $\lambda_{(i)} = \lambda_{(i')}$ and $\lambda_{(j)} = \lambda_{(j')}$. If i and j are not in the same block and if $\lambda_{\beta+1} = \lambda_{(i)} \oplus \lambda_{(j)}$, then (i,j), (i,j'), (i',j), (i',j'), (j,i), (j',i), (j,i'), (j',i') will also satisfy the equation. Therefore, we also have:
$|M| = \alpha(\alpha-2) - 4\delta(\alpha-\delta-1) - 8[$ Number of i, j, $0 \le i < j \le \beta$, $\lambda_{\beta+1} = \lambda_i \oplus \lambda_j]$, as claimed.

Theorem 10

$$\alpha^2 - 4\alpha - 2\Delta\alpha - 4\delta\alpha \le |M| \le \alpha(\alpha-2)$$

Proof. Let D' denote the number of i, j, $1 \le i \le \alpha$, $1 \le j \le \alpha$ such that $\lambda_{\beta+1} = \lambda_{(i)} \oplus \lambda_{(j)}$. We have $D' \le \alpha(2\Delta+2)$ because for i we have at most α solutions, and when i is fixed then $\lambda_{(j)}$ is fixed, so we have at most $2\Delta+2$ solutions for j. Therefore, from Theorem 9, we get

$$|M| \ge \alpha(\alpha-2) - 4\delta\alpha - \alpha(2\Delta+2)$$

$$|M| \ge \alpha^2 - 4\alpha - 2\Delta\alpha - 4\delta\alpha$$

Moreover $|M| \le \alpha(\alpha-2)$ is obvious since if $(i,j) \in M$, then i and j are not in the same block.

B.3 The "h'_α property"

As we will see now, in order to obtain our security results when $\alpha \ll 2^n$ and $\xi_{max} = 2$, a sufficient condition is to prove the property below.

h'_α property

We will say that the "h'_α property" is satisfied if we have found three fixed integers A, B and C such that for all $\alpha \ll 2^n$:

$$\sum_{(k,l)\in M} h'_\alpha(k,l) \ge \frac{h_\alpha}{2^n}|M|(1 - \frac{A}{2^n} - \frac{B\alpha}{2^{2n}} - \frac{C\Delta\alpha}{2^{2n}})$$

Of course, a sufficient condition to have this h'_α property is to have: $h'_\alpha(k,l) \ge \frac{h_\alpha}{2^n}(1 - \frac{A}{2^n} - \frac{B\alpha}{2^{2n}} - \frac{C\Delta\alpha}{2^{2n}})$.

Proof of $H_\alpha \ge J_\alpha$ from the h'_α property.

If we have the h'_α property, then from Theorem 5 and Theorem 10 we obtain:

$$\frac{h_{\alpha+2}}{2^n} \ge h_\alpha\big(1 - \frac{2\alpha}{2^n} + \frac{2\delta}{2^n} + \frac{\alpha^2 - 4\alpha - 2\Delta\alpha - 4\delta\alpha}{2^{2n}}(1 - \frac{A}{2^n} - \frac{B\alpha}{2^{2n}} - \frac{C\Delta\alpha}{2^{2n}})\big) \quad (\sharp)$$

Now since $J_{\alpha+2} = (2^{2n} - 2^n(2\alpha+1) + \alpha(\alpha+1))J_\alpha$ and $\frac{H_{\alpha+2}}{H_\alpha} = 2^n\frac{h_{\alpha+2}}{h_\alpha}$, we have

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} = \frac{2^n\frac{h_{\alpha+2}}{h_\alpha}}{(2^{2n} - 2^n(2\alpha+1) + \alpha(\alpha+1))}\frac{H_\alpha}{J_\alpha} \quad (\sharp\sharp)$$

Therefore from ($\sharp$)

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \frac{1-\frac{2\alpha}{2^n}+\frac{2\delta}{2^n}+\frac{\alpha^2-4\alpha-2\Delta\alpha-4\delta\alpha}{2^{2n}}(1-\frac{A}{2^n}-\frac{B\alpha}{2^{2n}}-\frac{C\Delta\alpha}{2^{2n}})}{1-\frac{2\alpha+1}{2^n}+\frac{\alpha(\alpha+1)}{2^{2n}}}\frac{H_\alpha}{J_\alpha}$$

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \big(1+\frac{\frac{1}{2^n}-\frac{5\alpha}{2^{2n}}+\frac{2\delta}{2^n}+\frac{-2\Delta\alpha-4\delta\alpha}{2^{2n}}-\frac{\alpha^2}{2^{2n}}(\frac{A}{2^n}+\frac{B\alpha}{2^{2n}}+\frac{C\Delta\alpha}{2^{2n}})}{1-\frac{2\alpha+1}{2^n}+\frac{\alpha^2+\alpha}{2^{2n}}}\big)\frac{H_\alpha}{J_\alpha} \quad (\sharp\sharp\sharp)$$

Now, as we have already said, we can choose the order of the indices such that $\delta = \Delta$. Then, a sufficient condition for $\frac{2\delta}{2^n} \geq \frac{2\Delta\alpha+4\delta\alpha}{2^{2n}} + \frac{C\Delta\alpha^3}{2^{4n}}$ when $\delta = \Delta$ is to have $\alpha \leq \frac{2\cdot 2^n}{6+C}$ (or $\delta = 0$) since $\alpha \leq 2^n$. We can assume that $\alpha \leq \frac{2\cdot 2^n}{6+C}$ since our aim is to obtain proofs for $\alpha \ll 2^n$. Then we see from ($\sharp\sharp\sharp$) that

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \frac{H_\alpha}{J_\alpha} \Leftrightarrow \frac{1}{2^n} \geq \frac{5\alpha}{2^{2n}} + \frac{\alpha^2}{2^{\ 2n}}(\frac{A}{2^n}+\frac{B\alpha}{2^{2n}}) \quad (\flat)$$

Since $\alpha \leq 2^n$, a sufficient condition for $\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \frac{H_\alpha}{J_\alpha}$ is therefore $\alpha \leq \frac{2^n}{5+A+B}$. Again, we can assume that $\alpha \leq \frac{2^n}{5+A+B}$. So we see why our aim (for $\xi_{max} = 2$) will be to prove the "h'_α property" above. This is what we have done in Appendix E with a proof that we can take $A = 0$, $B = 62$ and $C = 52$. For this we will have to evaluate the values h'_α.

Remark. The technical details must not hide the reason why we will have $H_\alpha \geq J_\alpha$. Fundamentally, $H_\alpha \geq J_\alpha$ comes from the fact that in ($\flat$), the coefficient $\frac{1}{2^n}$ is dominant from all other terms. This coefficient $\frac{1}{2^n}$ comes from $\frac{h_{\alpha+2}}{2^n} = h_\alpha(1-\frac{2\alpha}{2^n})+$ other terms and while $\frac{J_{\alpha+2}}{2^n} = J_\alpha(1-\frac{2\alpha+1}{2^n})+$ other terms. In $J_{\alpha+2}$ we had to impose $P_{\alpha+1} \notin \{P_1,\ldots,P_\alpha\}$ and $P_{\alpha+2} \notin \{P_1,\ldots,P_{\alpha+1}\}$ **including** the condition $P_{\alpha+1} \neq P_{\alpha+2}$, i.e. $2\alpha+2$ non equalities. For $H_{\alpha+2}$ however we **do not** have to consider the condition $P_{\alpha+1} \neq P_{\alpha+2}$ because $P_{\alpha+2} \oplus P_{\alpha+1} = \lambda_{\beta+1}$ with $\lambda_{\beta+1} \neq 0$, so $P_{\alpha+1} \neq P_{\alpha+2}$ is automatically imposed. This is why in $H_{\alpha+2}$ compared with H_α we have only 2α non equalities to consider (and not $2\alpha+1$). On the long term, this small deviation in $\frac{1}{2^n}$ due to $P_{\alpha+1} \neq P_{\alpha+2}$ automatic for $H_{\alpha+2}$ becomes dominant (as we will show in the proofs with all the technical details) and this is the deep reason that explains why $H_{\alpha+2} \geq J_{\alpha+2}$.

C Relations between $h'_{\alpha+2}$ and h_α when $\xi_{max} = 2$

Our aim is to prove that $h'_\alpha \geq \frac{h_\alpha}{2^n}(1+e_\alpha)$, with $|e_\alpha|$ as small as possible. For example, as we will see, $|e_\alpha| \leq O(\frac{\alpha}{2^n})$ will give security in $O(\frac{\alpha^4}{2^{3n}})$, and more generally, $|e_\alpha| \leq O((\frac{\alpha}{2^n})^k) + O(\frac{1}{2^n})$ will give security in $O(\frac{\alpha^{k+2}}{2^{(k+2)n}})$. We have various h'_α values from the same h_α, however since we will compare all these h'_α values from the same h_α, we can change the ordering of the indices without loosing generality. (In this paper we will never directly compose two values h'_α but compare them indirectly from the same h_α). Moreover, to illustrate more

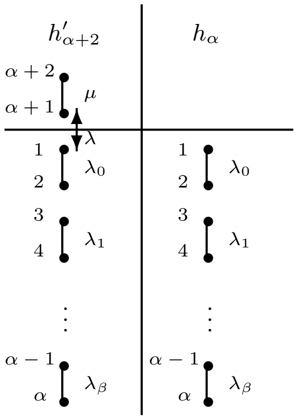


Fig. 4. We want to compare $h'_{\alpha+2}$ and $h_{\alpha+2}$. This figure illustrates that we will do this by evaluating $h'_{\alpha+2}$ from h_α.

easily the similarities between this section and the section where we have found the relations between $h_{\alpha+2}$ and h_α, we will evaluate here $h'_{\alpha+2}$ from $h_{\alpha+2}$ instead of h'_α from h_α. We will denote here by λ and μ the values $P_{\alpha+1} \oplus P_{\alpha+2} = \mu$ and $P_{\alpha+1} \oplus P_1 = \lambda$ (cf Figure 4), i.e. $P_{\alpha+1} \oplus P_1 = \lambda$ is here the new equation in $h'_{\alpha+2}$ that we did not have in $h_{\alpha+2}$. We have:

$$h'_{\alpha+2} = \sum_{(P_1,\cdots,P_\alpha) \text{ solution of } h_\alpha} [\text{ Number of } P_{\alpha+2}, P_{\alpha+1} \text{ values such that}$$

$$P_{\alpha+1} \oplus P_{\alpha+2} = \mu,\ P_{\alpha+1} \oplus P_1 = \lambda \text{ and these two equations}$$

$$\text{do not create a collision } P_{\alpha+1} = P_i, \text{ or } P_{\alpha+2} = P_i,\ 1 \le i \le \alpha]$$

We have $P_{\alpha+1} = P_1 \oplus \lambda$, $P_{\alpha+2} = P_1 \oplus \lambda \oplus \mu$, and we want no collision $P_1 = P_i \oplus \lambda$, or $P_1 \oplus \lambda \oplus \mu = P_i$, $1 \le i \le \alpha$. Here instead of $1 \le i \le \alpha$, we can write $3 \le i \le \alpha$, since by hypothesis $P_{\alpha+1} \oplus P_1 = \lambda$ is linearly compatible with h_α, i.e. $\lambda \ne 0$, $\lambda \ne \lambda_0$, $\lambda \ne \mu$ and $\lambda \ne \lambda_0 \oplus \mu$. Therefore:

$$h'_{\alpha+2} = \sum_{(P_1,\cdots,P_\alpha) \text{ solution of } h_\alpha} (1 - \delta(P_1, \ldots, P_\alpha))$$

with $\delta(P_1, \ldots, P_\alpha) = 0 \Leftrightarrow \forall i,\ 3 \le i \le \alpha,\ P_1 \ne P_i \oplus \lambda,$ and $P_1 \ne P_i \oplus \lambda \oplus \mu$.
$\delta(P_1, \ldots, P_\alpha) = 1 \Leftrightarrow \delta(P_1, \ldots, P_\alpha) \ne 0$
$\delta(P_1, \ldots, P_\alpha) = 1 \Leftrightarrow \exists i,\ 3 \le i \le \alpha,\ \ P_1 = P_i \oplus \lambda,$ and $P_1 = P_i \oplus \lambda \oplus \mu$.
$h'_{\alpha+2} = h_\alpha - \sum_{(P_1,\cdots,P_\alpha) \text{ solution of } h_\alpha} \delta(P_1, \ldots, P_\alpha)$.
Now when $P_1, \ldots, P_\alpha$ is a fixed solution of h_α we can have exactly 0 or 1 index i such that $P_1 = P_i \oplus \lambda$, and we can have exactly 0 or 1 index j such that $P_1 = P_j \oplus \lambda \oplus \mu$ (since the P_i values are pairwise distinct, $1 \le i \le \alpha$). Therefore,

$$h'_{\alpha+2} = h_\alpha - \sum_{(P_1,\cdots,P_\alpha) \text{ solution of } h_\alpha} \big([\text{ Number of } i,\ 3 \le i \le \alpha, \text{ such that} P_1 = P_i \oplus \lambda]$$

$$+[\text{ Number of } j,\, 3\leq j\leq \alpha,\ \text{ such that} P_1=P_j\oplus\lambda\oplus\mu]$$

$$-[\text{ Number of } i,j,\, 3\leq i\leq \alpha,\, 3\leq j\leq \alpha,\ \text{ such that} P_1=P_i\oplus\lambda=P_j\oplus\lambda\oplus\mu]\big)$$

$$h'_{\alpha+2}=h_\alpha-\sum_{(P_1,\cdots,P_\alpha)\text{ solution of }h_\alpha}\big([\sum_{i=3}^{\alpha}\text{ Number of equations } P_1=P_i\oplus\lambda]$$

$$+[\sum_{i=3}^{\alpha}\text{ Number of equations } P_1=P_i\oplus\lambda\oplus\mu]$$

$$-[\sum_{i=3}^{\alpha}\sum_{j=3}^{\alpha}\text{ Number of equations } P_1=P_i\oplus\lambda=P_j\oplus\lambda\oplus\mu]\big)$$

Thus by inverting the $\sum$:

$$h'_{\alpha+2}=h_\alpha-\sum_{i=3}^{\alpha}[\text{ Number of } (P_1,\dots P_\alpha) \text{ that satisfy } h_\alpha \text{ plus } P_1=P_i\oplus\lambda]$$

$$-\sum_{i=3}^{\alpha}[\text{ Number of } (P_1,\dots P_\alpha) \text{ that satisfy } h_\alpha \text{ plus } P_1=P_i\oplus\lambda\oplus\mu]$$

$$+\sum_{i=3}^{\alpha}\sum_{j=3}^{\alpha}[\text{ Number of } (P_1,\dots P_\alpha) \text{ that satisfy } h_\alpha \text{ plus } P_1=P_i\oplus\lambda=P_j\oplus\lambda\oplus\mu]\quad(\sharp)$$

Evaluation in $O(\frac{\alpha}{2^n})$
From ($\sharp$), we get immediately this evaluation in $O(\frac{\alpha}{2^n})$:

Theorem 11 $h_\alpha-2(\alpha-2)h'_\alpha\leq h'_{\alpha+2}\leq h_\alpha$.

Theorem 12 *(Approximation in $O(\frac{\alpha}{2^n})$ for $\frac{h'_\alpha}{h_\alpha}$)*

$$(1-\frac{2\alpha}{2^n-2\alpha})\frac{h_{\alpha+2}}{2^n}\leq h'_{\alpha+2}\leq\frac{h_{\alpha+2}}{2^n-2\alpha}$$

Therefore, we also have:

$$(1-\frac{2\alpha}{2^n-2\alpha})\frac{h_\alpha}{2^n}\leq h'_\alpha\leq\frac{h_\alpha}{2^n-2\alpha}$$

Proof. From theorem 11, $h_\alpha-2(\alpha-2)h'_\alpha\leq h'_{\alpha+2}\leq h_\alpha$ (1). From theorem 5, $(2^n-2\alpha)h_\alpha\leq h_{\alpha+2}\leq 2^nh_\alpha$ (2). From (1) and (2): $h'_\alpha\leq h_{\alpha-2}\leq\frac{h_\alpha}{2^n-2\alpha}$. Therefore, from (1) and (2) again: $(1-\frac{2\alpha}{2^n-2\alpha})\frac{h_{\alpha+2}}{2^n-2\alpha}\leq h'_{\alpha+2}\leq\frac{h_{\alpha+2}}{2^n-2\alpha}$ as claimed. We will now obtain a more precise evaluation of $h'_{\alpha+2}$. The number of $(P_1,\dots,P_\alpha)$ that satisfy h_α plus $P_1=P_i\oplus\lambda$ is a value h'_α except if $P_1=P_i\oplus\lambda$ is not compatible with $P_i\oplus P_{i'}=\lambda_{(i)}$, i.e. except if $\lambda_{(i)}=\lambda$, or $\lambda_{(i)}=\lambda\oplus\lambda_0$. Therefore we can write:

$$\sum_{i=3}^{\alpha}[\text{ Number of } (P_1,\dots P_\alpha) \text{ that satisfy } h_\alpha \text{ plus } P_1=P_i\oplus\lambda]$$

$$= (\alpha - 2 - [\text{ Number of } i,\ 3 \leq i \leq \alpha, \text{such that } \lambda_{(i)} = \lambda]$$
$$-[\text{ Number of } i,\ 3 \leq i \leq \alpha, \text{such that } \lambda_{(i)} = \lambda \oplus \lambda_0])h'_\alpha$$

We recall that this is a simple notation to denote a sum of such h'_α values, but these values h'_α can be different. Similarly,

$$\sum_{i=3}^{\alpha}[\text{ Number of } (P_1, \ldots P_\alpha) \text{ that satisfy } h_\alpha \text{ plus } P_1 = P_i \oplus \lambda \oplus \mu]$$
$$= (\alpha - 2 - [\text{ Number of } i,\ 3 \leq i \leq \alpha, \text{such that } \lambda_{(i)} = \lambda \oplus \mu]$$
$$-[\text{ Number of } i,\ 3 \leq i \leq \alpha, \text{such that } \lambda_{(i)} = \lambda \oplus \lambda_0 \oplus \mu])h'_\alpha$$

Now we have to evaluate

$$\sum_{i=3}^{\alpha}\sum_{j=3}^{\alpha}[\text{ Number of } (P_1, \ldots P_\alpha) \text{ that satisfy } h_\alpha \text{ plus } P_1 = P_i \oplus \lambda = P_j \oplus \lambda \oplus \mu] \quad (\sharp\sharp)$$

Case 1. i and j are in the same block

Then $P_i \oplus P_j = \lambda_{(i)}$, $P_1 = P_i \oplus \lambda$, and $P_i = P_j \oplus \lambda_{\beta+1}$. This is possible if and only if $\lambda_{(i)} = \lambda_{\beta+1}$, and then $\lambda \neq \lambda_{(i)}$ and $\lambda \neq \lambda_0 \oplus \lambda_{(i)}$, since by hypothesis $\lambda \neq \mu$ and $\lambda \oplus \lambda_0 \oplus \mu \neq 0$. Here when i is fixed then j is fixed since $i \neq j$ and i and j are in the same block. The contribution of these terms in $(\sharp\sharp)$ is therefore exactly: $[\text{ Number of } i,\ 3 \leq i \leq \alpha, \text{such that } \lambda_{(i)} = \mu] \cdot h'_\alpha$.

Case 2. i and j are not in the same block.

Then the equations h_α, $P_1 = P_i \oplus \lambda = P_j \oplus \lambda \oplus \mu$ create a block of 6 indices, with values $\leq \alpha$, linked with equalities. We denote by S the set of these indices, and by 1,2, i, i', j, j', these indices. Since they create a connection between P_i and P_j, the 2 equations $P_1 = P_i \oplus \lambda$ and $P_1 = P_j \oplus \lambda \oplus \mu$ cannot be a consequence by linearity of the equation (A), and $P_1 = P_i \oplus \lambda$ cannot be a consequence by linearity of (A) plus $P_1 = P_j \oplus \lambda \oplus \mu$. Therefore, the system will be linearly compatible, and we will be able to denote the number of solutions by a value h''_α, if and only if for these 6 indices of S, we did not create a collision.

The creation of a collision on the variables $(P_1, P_2, P_i, P_{i'}, P_j, P_{j'})$ means here one of these 7 equalities, since the other collisions are impossible due to the choice of $\lambda \neq \lambda_0$, $\lambda \neq \mu$, $\lambda \neq \lambda_0 \oplus \mu$. and all the λ_i values $\neq 0$. (cf Figure 5).

1. $\lambda_{(i)} = \lambda$ $(P_{i'} = P_1)$.
2. $\lambda_{(i)} = \lambda \oplus \lambda_0$ $(P_{i'} = P_2)$.
3. $\lambda_{(i)} = \mu$ $(P_{i'} = P_j)$.
4. $\lambda_{(j)} = \mu \oplus \lambda$ $(P_{j'} = P_1)$.
5. $\lambda_{(j)} = \mu \oplus \lambda \oplus \lambda_0$ $(P_{j'} = P_2)$.
6. $\lambda_{(j)} = \mu$ $(P_{j'} = P_i)$.
7. $\lambda_{(i)} \oplus \lambda_{(j)} = \mu$ $(P_{i'} = P_{j'})$.

We denote by $\mathcal{S}$ the set of these 7 equalities. Let

$$M' = \big\{(i,j),\ 3 \leq i \leq \alpha,\ 3 \leq j \leq \alpha, i \text{ and } j \text{ not in the same block,}$$
$$\text{such that none of the 7 equalities of } \mathcal{S} \text{ are satisfied } \big\}$$

Then, from all the cases above we can write:

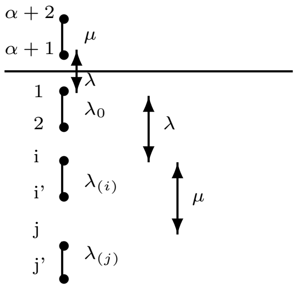


Fig. 5. The relations in S.

Theorem 13

$$h'_{\alpha+2} = h_\alpha + [-2\alpha + 4 + (\textit{ Number of } i,\ 3 \le i \le \alpha \textit{ such that } \lambda_{(i)} = \lambda)$$

$$+(\textit{ Number of } i,\ 3 \le i \le \alpha \textit{ such that } \lambda_{(i)} = \lambda \oplus \lambda_0)$$

$$+(\textit{ Number of } i,\ 3 \le i \le \alpha \textit{ such that } \lambda_{(i)} = \lambda \oplus \mu)$$

$$+(\textit{ Number of } i,\ 3 \le i \le \alpha \textit{ such that } \lambda_{(i)} = \lambda \oplus \mu \oplus \lambda_0)$$

$$+(\textit{ Number of } i,\ 3 \le i \le \alpha \textit{ such that } \lambda_{(i)} = \mu)]h'_\alpha + \sum_{(i,j)\in M'} h''_\alpha$$

Examples
We can verify with this theorem some of the h'_6 values give, in Appendix A. For example 3 of Appendix A (with $\lambda = \lambda_2$) we have $h'_6 = 2^n(2^n - 6)$, $h_4 = 2^n(2^n - 4)$, no h''_4 values exist, and Theorem 13 gives here: $h'_6 = h_4 + (-8 + 4 + 2) \cdot 2^n$ as expected. All the other examples of Appendix A can be verified similarly.
Evaluation of $|M'|$

$$|M'| = (\alpha-2)(\alpha-4) - \text{ Number of } (i,j),\ 3 \le i \le \alpha,\ 3 \le j \le \alpha, i \text{ and } j$$

$$\text{not in the same block, such that at least one of the 7 equalities of } \mathcal{S}$$

$$\text{is satisfied}$$

Now if $\lambda_{(i)}$ is fixed from one of the equation of $\mathcal{S}$, for i we have at most $2\Delta + 2$ possibilities, and for j when i is fixed at most $(\alpha - 4)$ possibilities. (Similarly when $\lambda_{(j)}$) is fixed. So $|M'| \ge (\alpha-2)(\alpha-4) - 7(2\Delta+2)(\alpha-4)$, and therefore:

Theorem 14 *$|M'| \ge \alpha^2 - 14\Delta\alpha - 20\alpha$.*

D Security when $\xi_{max} = 2$ and $\alpha^4 \ll 2^{3n}$

We have see that

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} = \frac{2^n \frac{h_{\alpha+2}}{h_\alpha}}{(2^{2n} - 2^n(2\alpha+1) + \alpha(\alpha+1))} \frac{H_\alpha}{J_\alpha} \quad (1)$$

(cf Property $(\sharp\sharp)$ of Appendix B.). From Theorem 8:

$$\frac{h_{\alpha+2}}{2^n} = h_\alpha(1 - \frac{2\alpha}{2^n} + \frac{2\delta}{2^n}) + \frac{1}{2^n} \sum_{(k,l)\in M} h'_\alpha(k,l) \quad (2)$$

From Theorem 10:

$$|M| \geq \alpha^2 - 4\alpha - 2\varDelta\alpha - 4\delta\alpha \quad (3)$$

From Theorem 13:

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

So if $\alpha \leq \frac{2^n}{4}$, we can write $\frac{h'_\alpha}{h_\alpha} - \frac{1}{2^n} \geq \frac{-4\alpha}{2^{2n}} \quad (4)$. Therefore from $(1), (2), (3), (4)$ we obtain:

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \frac{1 - \frac{2\alpha}{2^n} + \frac{2\delta}{2^n} + \frac{\alpha^2 - 4\alpha - 2\varDelta\alpha - 4\delta\alpha}{2^{2n}}(1 - \frac{4\alpha}{2^n})}{1 - \frac{2\alpha+1}{2^n} + \frac{\alpha^2+\alpha}{2^{2n}}} \frac{H_\alpha}{J_\alpha}$$

Now, as we have already mentioned, we can always choose the ordering of the indices such that $\delta = \varDelta$. For this we just choose $\alpha + 1$ with a value $\lambda_{(\alpha+1)}$ that gives the larger δ. Then, when $\delta = \varDelta$, $\frac{2\delta}{2^n} \geq \frac{2\varDelta\alpha + 4\delta\alpha}{2^{2n}} \Leftrightarrow \alpha \leq \frac{2^n}{3}$ (or $\delta = 0$), and we can assume $\alpha \leq \frac{2^n}{3}$. Then

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq (\frac{1 - \frac{2\alpha}{2^n} + \frac{\alpha^2 - 4\alpha}{2^{2n}} - \frac{4\alpha^3}{2^{3n}}}{1 + \frac{-2\alpha-1}{2^n} + \frac{\alpha^2+\alpha}{2^{2n}}}) \frac{H_\alpha}{J_\alpha}$$

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq (1 + \frac{\frac{1}{2^n} - \frac{5\alpha}{2^{2n}} - \frac{4\alpha^3}{2^{3n}}}{1 + \frac{-2\alpha-1}{2^n} + \frac{\alpha^2+\alpha}{2^{2n}}}) \frac{H_\alpha}{J_\alpha}$$

Therefore by induction on α we have:

$$\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \left(1 - \frac{4\alpha^3}{2^{3n}(1 - \frac{2\alpha}{2^n})} - o(\frac{\alpha^3}{2^{3n}})\right)^{\alpha/2} \frac{H_2}{J-2}$$

This shows that $\frac{H_{\alpha+2}}{J_{\alpha+2}} \geq \frac{H_\alpha}{J_\alpha}$ if $\alpha^3 \ll 2^{2n}$ and it shows that H_α is always very near J_α if $\alpha^4 \ll 2^{3n}$, i.e. it gives security when $\alpha^4 \ll 2^{3n}$.

E Relation between h'_α and h_α when $\xi_{max} = 2$

Theorem 15 $h'_{\alpha+2} = h_\alpha + (-2\alpha + T)h'_\alpha + \sum_{(i,j)\in M'} \leq h''_\alpha$
with $0 \leq T \leq 10\varDelta + 14$ *and* $\alpha^2 - 20\alpha - 14\varDelta\alpha \leq |M'|(\alpha-2)(\alpha-4)$.

Proof. This comes immediately from Theorem 13, since
(Number of i, $3 \leq i \leq \alpha$, $\lambda_{(i)} = \lambda) \leq 2\varDelta + 2$
(Number of i, $3 \leq i \leq \alpha$, $\lambda_{(i)} = \lambda \oplus \lambda_0) \leq 2\varDelta + 2$
(Number of i, $3 \leq i \leq \alpha$, $\lambda_{(i)} = \lambda \oplus \mu) \leq 2\varDelta + 2$
(Number of i, $3 \leq i \leq \alpha$, $\lambda_{(i)} = \lambda \oplus \mu \oplus \lambda_0) \leq 2\varDelta + 2$
and (Number of i, $3 \leq i \leq \alpha$, $\lambda_{(i)} = \mu) \leq 2\varDelta + 2$

Theorem 16 *("Central Theorem")*
If $\alpha \leq \frac{2^n}{8}$, *then*

$$\big|h'_{\alpha+2} - \frac{h_{\alpha+2}}{2^n}\big| \leq 2\alpha|h'_\alpha - \frac{h_\alpha}{2^n}| + \alpha^2|h''_\alpha - \frac{h'_\alpha}{2^n}| + h_{\alpha+2}(\frac{26\varDelta + 30}{2^{2n}})$$

Remark. We call this theorem the "Central Theorem" because from it, as we will see, we will be able to obtain evaluations of $|h'_\alpha - \frac{h_\alpha}{2^n}|$ in $O(\frac{\alpha^2}{2^{2n}})\frac{h_\alpha}{2^n}$, $O(\frac{\alpha^3}{2^{3n}})\frac{h_\alpha}{2^n}$ etc. $O(\frac{\alpha^k}{2^{kn}})\frac{h_\alpha}{2^n}$ for any integer k and it is the decisive step to obtain explicit security bounds in $O(\frac{\alpha}{2^n})$ for the Theorem $P_i \oplus P_j$.
Proof of Theorem 16 From Theorem 8 and Theorem 10 we have:

$$\frac{h_{\alpha+2}}{2^n} = h_\alpha(1 - \frac{2\alpha}{2^n} + \frac{2\delta}{2^n}) + \frac{1}{2^n}\sum_{(k,l)\in M} h'_\alpha$$

with $\alpha^2 - 4\alpha - 6\varDelta\alpha \leq |M| \leq \alpha(\alpha-2)$. Moreover, $M' \subset M$ since we have $\mu = \lambda_{\beta+1}$ and the 7 conditions $\mathcal{S}$ contain the 3 conditions: $\lambda_{(i)} = \mu$, $\lambda_{(j)} = \mu$ and $\lambda_{(i)} \oplus \lambda_{(j)} = \mu$.

$$M \setminus M' \subset \big\{(i,j),\ 3 \leq i \leq \alpha,\ 3 \leq j \leq \alpha,$$
$$i \text{ and } j \text{ not in the same block such that}$$
$$\lambda_{(i)} = \lambda,\ \text{or}\ \lambda_{(i)} = \lambda \oplus \lambda_0,\ \text{or}\ \lambda_{(j)} = \mu \oplus \lambda,\ \text{or}\ \lambda_{(j)} = \mu \oplus \lambda \oplus \lambda_0\big\}$$

Therefore, $|M \backslash M'| \leq (8\varDelta+8)(\alpha-2)$. From the Theorem 15 and these properties, we can write:

$$h'_{\alpha+2} - \frac{h_{\alpha+2}}{2^n} = -2\alpha(h'_\alpha - \frac{h_\alpha}{2^n}) + Th'_\alpha - \frac{2\delta}{2^n}h_\alpha$$
$$+ \sum_{(i,j)\in M'} (h''_\alpha - \frac{h'_\alpha}{2^n}) + \sum_{(k,l)\in M\backslash M'} \frac{h'_\alpha}{2^n}$$

Therefore

$$|h'_{\alpha+2} - \frac{h_{\alpha+2}}{2^n}| \leq 2\alpha|h'_\alpha - \frac{h_\alpha}{2^n}| + \alpha^2|h''_\alpha - \frac{h'_\alpha}{2^n}|$$

$$+(10\Delta+14)h'_\alpha+\frac{2\Delta}{2^n}h_\alpha+(8\Delta\alpha+8\alpha)\frac{h'_\alpha}{2^n}$$

Moreover, from Theorem 4: $h_\alpha \le \frac{h_{\alpha+2}}{2^n-2\alpha}$ and from Theorem 11: $h'_\alpha \le \frac{h_{\alpha+2}}{(2^n-2\alpha)^2}$. Now if $\alpha \le \frac{2^n}{8}$, $\frac{1}{(2^n-2\alpha)^2} \le \frac{2}{2^{2n}}$, and we obtain Theorem 16.

Theorem 17 *(Approximation in $O(\frac{\alpha^2}{2^{2n}})$)*
If $\alpha \le \frac{2^n}{8}$, then:

$$|h'_\alpha-\frac{h_\alpha}{2^n}| \le \big(\frac{5\alpha^2}{(2^n-2\alpha)^3}+\frac{26\Delta+30}{2^{2n}}\big)h_\alpha$$

Remark. Here the approximation is said to be in $O(\frac{\alpha^2}{2^{2n}})$, and not in $O(\frac{\alpha^2}{2^{3n}})$, because $\frac{h_\alpha}{2^n}$ is one of the term, and if we put $\frac{h_\alpha}{2^n}$ in factor we will have coefficients in $O(\frac{h_\alpha}{2^n})$.

Proof of Theorem 17. From Theorem 11 we have already found an approximation for $|h'_\alpha-\frac{h_\alpha}{2^n}|$ but only in $O(\frac{\alpha}{2^n})$: $|h'_\alpha-\frac{h_\alpha}{2^n}| \le \frac{2\alpha}{2^n-2\alpha}\cdot\frac{h_\alpha}{2^n}$. For $|h''_\alpha-\frac{h'_\alpha}{2^n}|$ we also have the approximation in $O(\frac{\alpha}{2^n})$: $|h''_\alpha-\frac{h'_\alpha}{2^n}| \le \frac{2\alpha}{2^n-2\alpha}\cdot\frac{h'_\alpha}{2^n}$. Here an even less precise approximation will be enough: $|h''_\alpha-\frac{h'_\alpha}{2^n}| \le \sup(h''_\alpha,\frac{h'_\alpha}{2^n})$. Now with $h_\alpha \le \frac{h_{\alpha+2}}{2^n-2\alpha}$ (cf Theorem 4), $h'_\alpha \le \frac{h_\alpha}{2^n-2\alpha} \le \frac{h_{\alpha+2}}{(2^n-2\alpha)^2}$ (cf Theorem 12) and similarly $h''_\alpha \le \frac{h_{\alpha+2}}{(2^n-2\alpha)^3}$. We obtain from Theorem 16 (i.e. "Central Theorem"):

$$|h'_{\alpha+2}-\frac{h_{\alpha+2}}{2^n}| \le 2\alpha\big(\frac{2\alpha}{(2^n-2\alpha)^2}\big)\frac{h_{\alpha+2}}{2^n}+\frac{\alpha^2 h_{\alpha+2}}{(2^n-2\alpha)^3}+h_{\alpha+2}\big(\frac{26\Delta+30}{2^{2n}}\big)$$

Therefore by changing $\alpha+2$ by α, we obtain Theorem 17.

Application. From an evaluation in $O(\frac{\alpha}{2^n})$ for h'_α/h_α, we have seen how to obtain $H_\alpha \ge J_\alpha$ for $\alpha^3 \ll 2^{2n}$, and security for $\alpha^4 \ll 2^{3n}$ (cf Appendix D). Similarly, from Theorem 17, i.e. an evaluation in $O(\frac{\alpha^2}{2^{2n}})$ for h'_α/h_α, we obtain $H_\alpha \ge J_\alpha$ for $\alpha^4 \ll 2^{3n}$, and security for $\alpha^5 \ll 2^{4n}$

More precise evaluation

We can continue this process to get security in $\alpha^6 \ll 2^{5n}$, $\alpha^7 \ll 2^{6n}$ etc. From our approximation in $O(\frac{\alpha^2}{2^{2n}})$ for h'_α/h_α given by Theorem 17 and the approximation in $O(\frac{\alpha}{2^n})$ for h''_α/h'_α given by

$$|h''_\alpha-\frac{h'_\alpha}{2^n}| \le \frac{2\alpha}{2^n-2\alpha}\frac{h'_\alpha}{2^n}$$

the central Theorem 16 will give us an approximation in $O(\frac{\alpha^3}{2^{3n}})$ for h'_α/h_α. More generally

$$|h^{[\mu]}_{\alpha+2}-\frac{h^{[\mu-1]}_{\alpha+2}}{2^n}| \le 2\alpha|h^{[\mu]}_\alpha-\frac{h^{[\mu-1]}_\alpha}{2^n}|+\alpha^2|h^{[\mu+1]}_\alpha-\frac{h^{[\mu]}_\alpha}{2^n}|+h_{\alpha+2}\big(\frac{26\Delta+30}{2^{2n}}\big) \quad (\sharp)$$

is valid for all μ as long as it remains some blocks with only 2 variables, i.e. as long as $\mu < \frac{\alpha}{2}$. We can generate like this approximations in $O(\frac{\alpha^k}{2^{kn}})$ for h'_α/h_α

with larger and larger k. Moreover, we need only to achieve a formula for $k = n$ since $\frac{\alpha^{k+1}}{2^{kn}} \leq \frac{\alpha}{2^n}$ for $k = n$ if $\alpha \leq \frac{2^n}{2}$. Therefore, the condition $\mu < \frac{\alpha}{2}$ is not a problem since $\alpha \geq \sqrt{2^n}$ and we only need $\mu \leq n$. More precisely, from the central Theorem 16 and its variants ($\sharp$) we obtain (from the geometric series in $\frac{\alpha}{2^n}$ and $\frac{\alpha^2}{2^{2n}}$):

Theorem 18 *$\forall k$, $1 \leq k \leq \frac{\alpha}{2} - 1$, if $\alpha \leq \frac{2^n}{8}$:*

$$|h'_\alpha - \frac{h_\alpha}{2^n}| \leq h_\alpha \Big(\frac{2^{2k}\alpha^k}{(2^n - 2\alpha)^{k+1}(1 - \frac{2\alpha}{2^n} - \frac{\alpha^2}{2^{2n}})} + \frac{26\Delta + 30}{2^{2n}(1 - \frac{2\alpha}{2^n} - \frac{\alpha^2}{2^{2n}})} \Big)$$

Therefore, if $\alpha \leq \frac{2^n}{32}$ and $k \geq n$

$$|h'_\alpha - \frac{h_\alpha}{2^n}| \leq \frac{h_\alpha}{2^n} \big(\frac{2\alpha}{2^{2n}} + \frac{52\Delta + 60}{2^n} \big)$$

Moreover, if we remember that $T \geq 0$, the terms in Δ can only be negative at the second stage, with terms in $\frac{\alpha}{2^n}$, and we have:

$$h'_\alpha \geq \frac{h_\alpha}{2^n}(1 - \frac{2\alpha}{2^{2n}} - \frac{52\Delta\alpha + 60\alpha}{2^{2n}})$$

$$h'_\alpha \geq \frac{h_\alpha}{2^n}(1 - \frac{62\alpha}{2^{2n}} - \frac{52\Delta\alpha}{2^{2n}})$$

Applications.
At last, we can now use the analysis done in Appendix B with the " h'_α property". We have obtained this h'_α property with $A = 0$, $B = 62$, and $C = 52$ (cf Theorem 16). Therefore, from section 6, we know that $H_\alpha \geq J_\alpha$ if $\alpha \leq \frac{2 \cdot 2^n}{6+C}$ and $\alpha \leq \frac{2^n}{5+A+B}$. This gives here: $\alpha \leq \frac{2^n}{67}$. We have finally proved Theorem 3 of Section 3 (i.e. Theorem $P_i \oplus P_j$ with $\xi_{max} = 2$) for $\alpha \leq \frac{2^n}{67}$. This is just the precise bound we were looking for, instead of just $\alpha \ll 2^n$.
Now for our initial problem for $f(x\|0) \oplus f(x\|1)$ with $f \in_R B_n$, we have proved Theorem 1 with $Avd_\phi^{PRF} \leq \frac{q}{2^n}$ if $q \leq \frac{2^n}{67}$. (Because if $q \leq \frac{2^n}{67}$, and all the b_i values are $\neq 0$, then $H \geq \frac{|B_n|}{2^{nq}}$ and we can apply Theorem 2 of section 2 with $\alpha = 0$ and $\beta = \frac{q}{2^n}$.)

F General properties for any ξ_{max}

h_α is by definition the number of $P_1, \cdots, P_\alpha$ pairwise distinct, elements of I_n, and solution of (A), where (a) is a system of equations $P_i \oplus P_j = \lambda_k$. We say that P_i and P_j are "in the same block" if when P_i is fixed, then P_j is fixed from the equations of (A). We denote by ξ_{max} the maximum number of P_i in the same block. The idea is to evaluate h_α by induction on the number of blocks, i.e. to evaluate $h_{\alpha+\xi}$ from h_α, where $h_{\alpha+\xi}$ is the number of $P_1, \cdots, P_\alpha, P_{\alpha+1}, \cdots, P_{\alpha+\xi}$ pairwise distinct, elements of I_n, solution of (A) and solution of this block of

$(\xi-1)$ equations $P_{\alpha+1},\cdots,P_{\alpha+\xi}$:
$P_{\alpha+2}=P_{\alpha+1}\oplus\lambda'_2$,
$P_{\alpha+3}=P_{\alpha+1}\oplus\lambda'_3$,
$\ldots$
$P_{\alpha+\xi}=P_{\alpha+1}\oplus\lambda'_\xi$
$(\xi\leq\xi_{max})$.
We will say that $P_1,\cdots,P_\alpha$ are solution of h_α when they are solution of (A). We start from a solution $P_1,\cdots,P_\alpha$ of (A) and we want to complete it to get the solution of $h_{\alpha+\xi}$. For this we have to choose $x=P_{\alpha+1}\oplus P_1$ such that x will not create a collision $P_j=P_{\alpha+1}$ or $P_j=P_{\alpha+2}$, $\cdots$, $P_j=P_{\alpha+\xi}$, $1\leq j\leq\alpha$. This means: $x\oplus P_1\neq P_j$, $x\oplus\lambda'_2\oplus P_1\neq P_j$, $\cdots$, $x\oplus\lambda'_\xi\oplus P_1\neq P_j$, $1\leq j\leq\alpha$. So this means $x\notin V$ with $V=\bigcup_{i=1}^{\xi}V_i$, with $V_i=\{P_1\oplus\lambda'_i\oplus P_j, 1\leq j\leq\alpha\}$ (by convention we define $\lambda'_1=0$). We have $\forall i$, $1\leq i\leq\xi$, $|V_i|=\alpha$ (since the P_j values, $1\leq j\leq\alpha$, are pairwise distinct).
$|V|=|\bigcup_{i=1}^{\xi}V_i|=\sum_{i=1}^{\xi}|V_i|-\sum_{i<j}^{\xi}|V_i\cap V_j|+\sum_{i<j<k}^{\xi}|V_i\cap V_j\cap V_k|+\cdots+(-1)^{\xi+1}|V_1\cap\cdots\cap V_\xi|$
So

$$h_{\alpha+\xi}=\sum_{(P_1,\cdots,P_\alpha)\text{ solution of }h_\alpha}(2^n-|V|)$$

So we have:
Theorem 19

$$h_{\alpha+\xi}=\sum_{(P_1,\cdots,P_\alpha)\ \textit{solution of}\ h_\alpha}(2^n-\xi\alpha+\sum_{i_1<i_2}^{\xi}|V_{i_1}\cap V_{i_2}|$$
$$-\sum_{i_1<i_2<i_3}^{\xi}|V_{i_1}\cap V_{i_2}\cap V_{i_3}|+\cdots+(-1)^{\xi}|V_1\cap\cdots\cap V_\xi|)$$

When i_1 and i_2 are fixed,

$$|V_{i_1}\cap V_{i_2}|=\sum_{1\leq j\leq\alpha,1\leq j'\leq\alpha}\text{Number of }P_1,\cdots,P_\alpha\text{ solution of }h_\alpha$$
$$\text{plus equation }P_j\oplus P_{j'}=\lambda'_{i_1}\oplus\lambda'_{i_2}$$

Now when we add to (A) the equality $P_j\oplus P_{j'}=\lambda'_{i_1}\oplus\lambda'_{i_2}$, 3 cases can occur:

Case 1 $\lambda'_{i_1}\oplus\lambda'_{i_2}=P_i\oplus P_j$ was already an equation of (A). Here this means $\lambda'_{i_1}\oplus\lambda'_{i_2}=\lambda_i$ for all value i, $1\leq i\leq\alpha$. Remark: $\lambda'_{i_1}\oplus\lambda'_{i_2}=\lambda_i$ creates 2 collisions in $V_{i_1}\cap V_{i_2}$: it creates $\lambda'_{i_1}\oplus P_1\oplus P_i=\lambda'_{i_2}\oplus P_1\oplus P_j$ and $\lambda'_{i_1}\oplus P_1\oplus P_j=\lambda'_{i_2}\oplus P_1\oplus P_i$.

Case 2 $\lambda'_{i_1}\oplus\lambda'_{i_2}=P_i\oplus P_j$ is in contradiction with the equations of (A). This can come from the fact that $P_i\oplus P_j=\lambda_k$ is in (A) and $\lambda_k\neq\lambda'_{i_1}\oplus\lambda'_{i_2}$. Or this can come from the fact that $P_i\oplus P_{i'}=\lambda_{i''}$ is in (A), $P_j\oplus P_{j'}=\lambda_{j''}$ is in (A), so from $P_i\oplus P_j=\lambda'_{i_1}\oplus\lambda'_{i_2}$ we get $P_{j'}=\lambda_{j''}\oplus\lambda'_{i_1}\oplus\lambda'_{i_2}\oplus P_i$, $P_{i'}=\lambda_{i''}\oplus\lambda'_{i_1}\oplus\lambda'_{i_2}\oplus P_j$, and $P_{i'}\oplus P_{j'}=\lambda_{i''}\oplus\lambda_{j''}\oplus\lambda'_{i_1}\oplus\lambda'_{i_2}$. This is impossible if $\lambda'_{i_1}\oplus\lambda'_{i_2}=\lambda_{j''}$, $\lambda'_{i_1}\oplus\lambda'_{i_2}=\lambda_{i''}$ or $\lambda'_{i_1}\oplus\lambda'_{i_2}=\lambda_{i''}\oplus\lambda_{j''}$, since the P_k values are pairwise distinct.

Case 3 The equation $\lambda'_{i_1} \oplus \lambda'_{i_2} = P_i \oplus P_j$ is not in contradiction with the equations of (A), and is not a consequence of the equations of (A). We will say that this case is the "generic" case, and we will denote by h'_α the number of $P_1, \cdots, P_\alpha$ solution of (A) and $\lambda'_{i_1} \oplus \lambda'_{i_2} = P_i \oplus P_j$ when we are in such "generic" case.

The value of h'_α is dependent on the λ_i values. We see from Theorem 19 that we can proceed for any ξ_{max} exactly as we did for $\xi_{max} = 2$, i.e. we can compute $h_{\alpha+\xi}$ from h_α and the h'_α values. The main difference, however, is that now all the blocks, except one: the block with the extra equations of h'_α, can have up to ξ_{max} variables instead of 2 variables. This is why in Theorem 6 the condition $(\xi_{max} - 1)\alpha \leq \frac{2^n}{67}$ will occur, instead of $\alpha \leq \frac{2^n}{67}$ for Theorem 3.

G Two examples for $h'_\alpha - \frac{h_\alpha}{2^n}$

Example 1
In this paper we proved that $H_\alpha \geq J_\alpha$ if $\xi_{max}\alpha \ll 2^n$. However, even for $\xi_{max} = 2$ we do not claim that $h'_\alpha \geq \frac{h_\alpha}{2^n}$ is always true. When Δ is very large and when the extra equation in h'_α has an exceptional λ (with $\delta = 0$ for this λ) then maybe $h'_\alpha < \frac{h_\alpha}{2^n}$ when $\alpha \geq O(\sqrt{2^n})$. For example, this is the case in Figure 6.

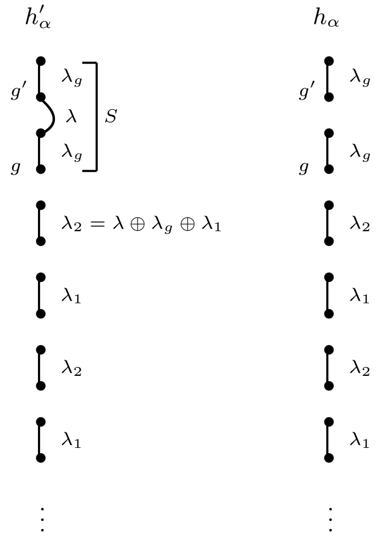
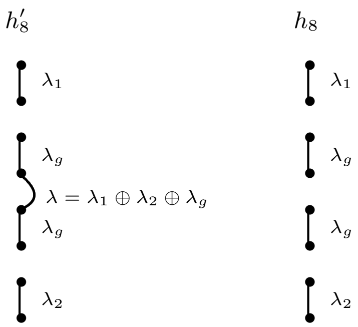


Fig. 6. An example where $h'_\alpha < \frac{h_\alpha}{2^n}$ may be possible.

In this example, λ is not present in h_α, and is present only once in λ'_α, with about 50% λ_1, about 50% λ_2, and only two λ_g. Here λ_1, λ_2, λ_g do not satisfy any special relation but λ is chosen such that $\lambda = \lambda_2 \oplus \lambda_g \oplus \lambda_1$. If we use the central theorem for $\xi_{max} = 2$ (cf Appendix D), with $P_{\alpha+2} \oplus P_{\alpha+1} = \lambda_1$, then in this example $\delta \simeq \frac{\beta}{2} \simeq \frac{\alpha}{2}$ and $|M \setminus M'|$ is in $O(\alpha)$. In fact, no connection in λ_1 can be made from the block S of h'_α so for $\alpha \geq \sqrt{2^n}$ we may have $h'_\alpha < \frac{h_\alpha}{2^n}$. If this is true, it would in a way explain why the analysis of systems of linear equalities and linear non equalities is so complex: a simple property such as $h'_\alpha \geq \frac{h_\alpha}{2^n}$ would be true on most, but not all cases.

Example 2

Let compute example 1 in the case of only 8 variables. (This will give us an example of what we did in the main body of this paper).



Computation of h_8 from $P_{\alpha+1} \oplus P_{\alpha+2} = \lambda_g$

Here $\alpha = 6$, $\delta = 1, |M| = 8$. $\frac{h_8}{2^n} = h_6(1 - \frac{12}{2^n} + \frac{2}{2^n}) + \frac{8}{2^n} h'_6$. With $h_6 = 2^n(2-6)$ and $h'_6 = 2^n(2^{2n} - 12 \cdot 2^n + 40)$ it gives: $\frac{h_8}{2^n} = 2^{3n} - 22 \cdot 2^{2n} + 168 \cdot 2^n - 448$.

Computation of h_8 from $P_{\alpha+1} \oplus P_{\alpha+2} = \lambda_1$

Here $\alpha = 6$, $\delta = 0, |M| = 24$. $\frac{h_8}{2^n} = h_6(1 - \frac{12}{2^n}) + \frac{8}{2^n} h_6^{'a} + \frac{16}{2^n} h_6^{'b}$. With $h_6 = 2^n(2^n - 4)(2^n - 6)$, $h_6^{'a} = 2^n(2^n - 8)$ and $h_6^{'b} = 2^n(2^n - 6)$. Therefore : $\frac{h_8}{2^n} = 2^{3n} - 22 \cdot 2^{2n} + 168 \cdot 2^n - 448$. We obtain the same value as above as expected.

Computation of h'_8

Here $\alpha = 6$, $\delta = 0$, $\delta' = 0$, $\mathit{\Delta} = 1$, $|M'| = 0$. Therefore $|M \setminus M'| = 24$. $\frac{h_8}{2^n} = h_6(1 - \frac{12}{2^n}) + 0$. Here "$+0''$ since it is not possible to connect two blocks in λ_1 (it would create a collision). $h'_6 = 2^n(2^n - 8)$ since in λ_2 we have no specific relation. $h'_8 = 2^{3n} - 20 \cdot 2^{2n} + 96 \cdot 2^n$. Therefore, in this example 2 we have:

$$h'_8 - \frac{h_8}{2^n} = 2 \cdot 2^{2n} - 72 \cdot 2^n + 448$$

and we here $h'_6 - \frac{h_6}{2^n} = 2 \cdot 2^n + 24$ (since $h_6 = 2^n(2^n-4)(2^n-6)$). We see that

$$h'_8 - \frac{h_8}{2^n} = 2^n(h'_6 - \frac{h_6}{2^n})(1 - \frac{24}{2^n} - \frac{64}{2^{2n}} + O(\frac{1}{2^{3n}}))$$

We can notice some interesting facts on this small example.
• The main term has kept the same coefficient (here 2) in $h'_8 - \frac{h_8}{2^n}$ and in $h'_6 - \frac{h_6}{2^n}$. This is conform with the central theorem for $\xi_{max} = 2$ since $\delta = 0$ and $\delta' = 0$.
• For the second term we had a modification of $\frac{-24}{2^n}$. This coefficient -24 comes from $-12 - 12$ where the first -12 comes from $\frac{-2\alpha}{2^n}$ (fixed), and the second -12 comes from $|M \setminus M'| = 24$ and here we divide this value 24 by 2 due to the fact that the first term of $h'_6 - \frac{h_6}{2^n}$ is a 2 as we have seen. For example 1, if this process continues, we may have $\frac{-2\alpha}{2^n}$ regularly and therefore when $\alpha \geq O(\sqrt{2^n})$ we may have $h'_\alpha < \frac{h_\alpha}{2^n}$ as we have said.

In the proof of our main theores in this paper we have avoided this problem by noticing that here Δ is large and the dominant term in δ has a good effect on $\frac{H_{\alpha+2}}{H_\alpha}$. Another possibility would have been to notice that in these examples 1 and 2, the value λ is used only once, while in our proofs the first connections in $\lambda_{\beta+1}$ are done for a $\lambda_{\beta+1}$ that has the maximum δ value. This property may be used to avoid the exceptional cases such as example 1 and example 2. (If $\delta' \neq 0$, then $\frac{\delta'}{2^n}$ dominates $\frac{|M \setminus M'|}{2^{2n}} \leq \frac{8(\alpha-2)}{2^{2n}}$.

Still another possibility would have been to notice that in our analysis of $h_{\alpha+2}$ we start from h_α and need only to compare $h_{\alpha+2}$ with $\sum_{(i,j)\in M} h'_\alpha$ for h'_α with an extra equation $P_{\alpha+1} \oplus P_{\alpha+2} = \lambda_{\beta+1}$, where $\lambda_{\beta+1}$ was a λ value of $h_{\alpha+2}$. In examples 1 and 2, if we start from h_α we will never get a $\lambda'_{\alpha-2}$ value with the exceptional value λ because λ was not in h_α.

H Some general properties of the J_α values

By definition, $J_\alpha = 2^n(2^n-1)(2^n-2)\dots(2^n-\alpha+1)$. In this Appendix we will see some properties of these J_α values. We will not need these properties in our cryptographic proofs but however they are interesting and they illustrate some of the complexities that we have to face.

Theorem 20

$$J_\alpha = 2^{\alpha n} - 2^{(\alpha-1)n}(\sum_{i=1}^{\alpha-1} i) + 2^{(\alpha-2)n}(\sum_{1\leq i<j<\alpha} ij)$$

$$-2^{(\alpha-3)n}(\sum_{1\leq i<j<k<\alpha} ijk) + \dots + (-1)^{\alpha-1}2^n(\alpha-1)!$$

We can also write this like that:

$$J_\alpha = \sum_{k=0}^{\alpha-1}(-1)^k 2^{(\alpha-k)n} j_k \quad \text{with} \quad j_k = \sum_{1\leq i_1<i_2<\dots<i_k<i_\alpha} i_1 i_2 \dots i_k$$

Proof. This comes immediately by developing J_α in powers of 2^n.

Theorem 21

$$j_1 = \frac{\alpha(\alpha-1)}{2} = \frac{\alpha^2}{2} - \frac{\alpha}{2}$$

$$j_2 = \frac{\alpha(\alpha-1)(\alpha-2)(3\alpha-1)}{24} = \frac{\alpha^4}{8} - \frac{5\alpha^3}{12} + \frac{3\alpha^2}{8} - \frac{\alpha}{12}$$

$$j_3 = \frac{\alpha^2(\alpha-1)^2(\alpha-2)(\alpha-3)}{48} = \frac{\alpha^6}{48} - \frac{7\alpha^5}{48} + \frac{17\alpha^4}{48} - \frac{17\alpha^3}{48} + \frac{\alpha^2}{8}$$

Proof. J_α is the number of $(P_1,\dots,P_\alpha) \in I_n^\alpha$ such that none of the $\frac{\alpha(\alpha-1)}{2}$ equalities $P_i = P_j$, $i < j$ is satisfied. Let $E_1, E_2, \dots, E_{\frac{\alpha(\alpha-1)}{2}}$ be these equalities. Let $\mu = \frac{\alpha(\alpha-1)}{2}$. $\forall i$, $1 \le i \le \mu$, $A_i = \{(P_1,\dots,P_\alpha) \in I_n^\alpha$, that satisfies $E_i\}$. We have: $J_\alpha = 2^{\alpha n} - |\cup_{i=1}^{\mu} A_i|$. Moreover

$$|\cup_{i=1}^{\mu} A_i| = \sum_{i=1}^{\mu} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k|$$

$$+ \dots + (-1)^{\mu+1} |A_1 \cap \dots \cap A_\mu|$$

Terms in $2^{n(\alpha-1)}$

$\forall i$, $1 \le i \le \mu$, $|A_i| = 2^{n(\alpha-1)}$ (because we fix one variable). Therefore, $\sum_{i=1}^{\mu} |A_i| = 2^{n(\alpha-1)}\mu$ and $j_1 = \mu = \frac{\alpha(\alpha-1)}{2}$.

Terms in $2^{n(\alpha-2)}$

Here we are looking for terms that gives exactly 2 independent equalities E_i. It could be equalities $\begin{cases} P_a = P_b \\ P_k = P_l \end{cases}$ with a, b, k, l pairwise distinct, or $P_a = P_b = P_k$ with a, b, k pairwise distinct. We have $\frac{\mu(\mu-1)}{2}$ terms that come from $\sum_{i<j} |A_i \cap A_j|$. Moreover we have to subtract to these values the systems of 3 equalities E_i with only 2 independent equalities, such as $P_1 = P_2,\ P_2 = P_3,\ P_1 = P_3$. We have $\frac{\alpha(\alpha-1)(\alpha-2)}{6}$ possibilities for these 3 equalities. Therefore $j_2 = \frac{\frac{\alpha(\alpha-1)}{2}\cdot(\frac{\alpha(\alpha-1)}{2}-1)}{2} - \frac{\alpha(\alpha-1)(\alpha-2)}{6}$. $j_2 = \frac{\alpha(\alpha-1)(\alpha-2)(3\alpha-1)}{24}$ as claimed. For j_3 we can proceed the same way, or use the well-known formulas for symmetrical expressions. We see that when $\alpha \ge \sqrt{2^n}$ we have:

Theorem 22 *When $\alpha \ge \sqrt{2^n}$, the first terms in Theorem 20, $2^{(\alpha-k)n} j_k$ are growing in $\frac{O(2^{2k})}{2^{kn}} \cdot 2^{\alpha n}$, i.e. all these first terms are much larger that J_α (in absolute value). This illustrated by Figure 7 below.*

Theorem 23

$$J_\alpha \sim_{\alpha\to+\infty} 2^{n\alpha} e^{-\frac{\alpha^3}{2\cdot 2^{2n}}}$$

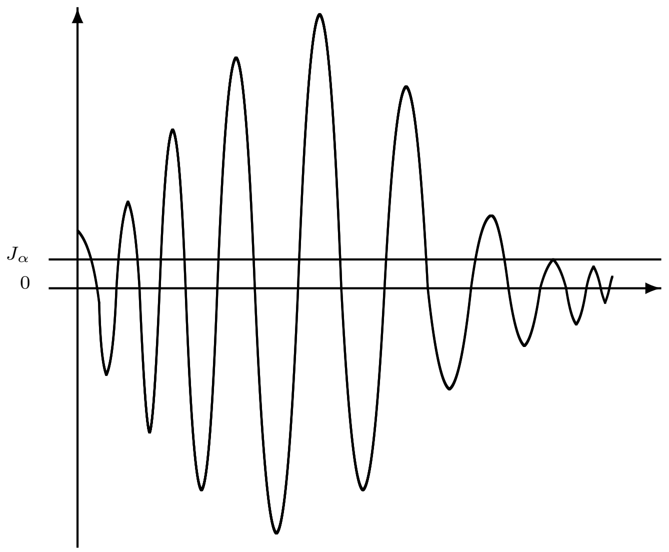


Fig. 7. The summation gives J_α but many terms are much larger than J_α

Proof. Let $X = 1 \cdot (1 - \frac{1}{2^n})(1 - \frac{2}{2^n}) \dots (1 - \frac{\alpha-1}{2^n})$. Therefore, $J_\alpha = 2^{n\alpha} X$. $\ln X = \sum_{i=0}^{\alpha} \ln(1 - \frac{i}{2^n})$. Let $a = 1 - \frac{1}{2^n},\ b = 1,\ f(x) = \ln(x)$.

$$\frac{1}{\alpha} \ln X = \frac{1}{\alpha} \sum_{i=0}^{\alpha} f(a + i(\frac{b-a}{\alpha}))$$

$$\frac{1}{\alpha} \ln X \sim_{\alpha \to +\infty} \int_{1-\frac{\alpha}{2^n}}^{1} \ln(t)\, dt$$

$(t \ln(t) - t)' = \ln t + 1 - 1 = \ln t$. Therefore

$$\frac{1}{\alpha} \ln X = \left[t \ln t - t \right]_{1-\frac{\alpha}{2^n}}^{1}$$

$$\frac{1}{\alpha} \ln X = -[(1 - \frac{\alpha}{2^n}) \ln(1 - \frac{\alpha}{2^n}) + \frac{\alpha}{2^n}]$$

Moreover, $\ln(1+\epsilon) = \epsilon - \frac{\epsilon^2}{2} + o(\epsilon^3)$.

$$-\frac{1}{\alpha} \ln X \simeq (1 - \frac{\alpha}{2^n})(-\frac{\alpha}{2^n} - \frac{\alpha^2}{2 \cdot 2^n} + \dots) + \frac{\alpha}{2^n}$$

$$\simeq \frac{\alpha^2}{2 \cdot 2^{2n}}$$

Therefore, $\ln X \simeq -\frac{\alpha^3}{2 \cdot 2^{2n}},\ X \simeq e^{-\frac{\alpha^3}{2 \cdot 2^{2n}}}$ and

$$J_\alpha \sim_{\alpha \to +\infty} 2^{n\alpha} e^{-\frac{\alpha^3}{2 \cdot 2^{2n}}}$$

as claimed.