Mirror Theory: A simple proof of the $P_i \oplus P_j$ Theorem with $\xi_{\max} = 2$

Benoît Cogliati[1] and Jacques Patarin[2]

[1] CISPA Helmholtz Center for information security, Germany
[2] University of Versailles, France

Abstract. We provide a simple and complete proof of the famous $P_i \oplus P_j$ Theorem in the particular case where $\xi_{\max} = 2$. This Theorem gives a lower bound for the number of solutions of simple linear systems of equations in the case where all the variables have to be pairwise distinct. Such systems often occur in cryptographic proofs of security, and this particular Theorem can be used to prove that the function $x \mapsto P(0||x) \oplus P(1||x)$ is an optimally secure pseudorandom function when P is a uniformly random permutation.

Keywords: Mirror Theory, security proofs, optimal security

1 Introduction

1.1 Our Motivation

In general, the H coefficients technique [Pat08b] can always be used to turn a cryptographic problem involving block ciphers into a problem of counting the number of solutions of linear systems of equations under the constraint that some (or all) the variables are pairwise distinct. In some cases, it is possible to work around this difficulty by using another proof strategy, such as the Chi-Squared technique [DHT17]. However, if we are concerned with optimal security bounds, it is often necessary to solve the underlying combinatorial problem. The mathematical theory that focuses on such problems has been dubbed Mirror Theory by Patarin. A small number of results are already known, some of which have proofs whose credibility has recently been a subject of debate. Our goal in this work is to address some of this criticism by providing an updated and simplified proof of the following Theorem.

Theorem 1 ($P_i \oplus P_j$ **Theorem with** $\xi_{\max} = 2$)**.** *Let* $q \leq \frac{2^n}{72}$ *and* $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_q) \in (\{0,1\}^n \setminus \{0\})^q$. *Let* $\mathrm{h}_q(\boldsymbol{\lambda})$ *be the number of solutions of the system*

$$\begin{cases} P_1 \oplus P_2 = \lambda_1 \\ P_3 \oplus P_4 = \lambda_2 \\ \vdots \\ P_{2\alpha-1} \oplus P_{2\alpha} = \lambda_\alpha . \end{cases}$$

such that the P_is are also pairwise distinct. Then one has

$$\mathrm{h}_q(\boldsymbol{\lambda}) \geq \frac{(2^n)_{2q}}{2^{nq}},$$

where $(2^n)_{2q} = 2^n(2^{n-1}) \cdots (2^{n-2q+1})$.

Remark 1. It is easy to see that Theorem 1 is true for $q = 1, 2$.

1. When $q = 1$, since $\lambda_1 \neq 0$, $P_1 \neq P_2$ necessarily holds. Thus one has $\mathrm{h}_1(\boldsymbol{\lambda}) = 2^n \geq 2^n - 1$;
2. When $q = 2$, like in the previous case, P_1 can take any value. Finally, P_3 must be chosen such that $P_3 \neq P_1, P_2$ and $P_4 = \lambda_2 \oplus P_3 \neq P_1, P_2$. Thus one has $\mathrm{h}_2(\boldsymbol{\lambda}) \geq 2^n(2^n - 4) \geq \frac{(2^n)_4}{2^{2n}}$[3].

Hence, in our proof, we are going to focus on the case where $q \geq 3$.

1.2 Related Work

Theorem 1 has first been introduced in [Pat10a]. Patarin has given an alternative proof of this result in [Pat13]. Unfortunately, some intermediate results were stated without proof in all these articles. More recently, a complete proof has been given in [NPV17], but it has some flaws that make it difficult to verify. In this work, we incorporate the refinements that have been introduced throughout the years and we aim to provide a clear, concise and rigorous proof. Dutta et al. [DNS20] have done a similar work, using a slightly different strategy and presentation. We hope that the existence of two different proofs will help rebuild confidence in Mirror Theory, and will also serve as a good tutorial for this type of combinatorial proofs.

Several variants of Theorem 1 have also been studied, for example the $P_i \oplus P_j$ Theorem with any $\xi_{\max}$ [Pat03, Pat10b], or the $P_i \oplus Q_j$ Theorem, where only the P_is and Q_js have to be pairwise distinct [Pat08a, CLP14]. Several other security bounds have also been proved using different specialized Mirror Theory results (see e.g. [DDNY18, DNT19, BN18, DN20, JN20]).

2 Preliminaries

We adopt the general convention that tuples are **bold** variables and that, for any non-empty set S, any integer s, and any $\mathbf{x} = (x_1, \dots, x_s) \in S^s$, $\mathbf{x}||y = (x_1, \dots, x_s, y)$ for any $y \in S$. For any positive integers d and α such that $d > 1$, $\mathrm{Ind}_\alpha^{(d)}$ is the set of all tuples $(k_1, \dots, k_{d-1}) \in \{1, \dots, 2\alpha\}^d$ such that the values $\lceil k_l/2 \rceil$ are pairwise distinct for $l = 1, \dots, d-1$. Moreover, for any $\mathbf{x} \in S^\alpha$ and any $\boldsymbol{k} \in \mathrm{Ind}_\alpha^{(d)}$, we denote $\mathbf{x}_{\boldsymbol{k}} = (x_k)_{k \neq \lceil k_1/2 \rceil, \dots, \lceil k_{d-1}/2 \rceil}$ the tuple $\mathbf{x}$ where the coordinates at index $\lceil k_l/2 \rceil$ have been removed for $l = 1, \dots, d-1$.

[3] Note that for the case $q = 2$, the theorem only applies when $n \geq 8$, where this inequality also holds.

Let n be any positive integer. We denote by $\{0,1\}^n$ the set of all n-bit strings. For any $x, y \in \{0,1\}^n$, $x \oplus y$ denotes the bitwise XOR of x and y. As usual, we also denote $(a)_b$ the falling factorial, i.e. for any positive integers a, b such that $a \geq b$, one has $(a)_b = a(a-1)\cdots(a-b+1)$. By convention, we fix $(a)_0 = 1$.

3 Proof Strategy

3.1 Description of Mirror Systems

Let α, n be fixed integers such that $2\alpha \leq 2^n$. For any $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_\alpha) \in (\{0,1\}^n)^\alpha$, we denote by $(\mathrm{S}_\alpha(\boldsymbol{\lambda}))$ the following system of equations in 2α variables:

$$(\mathrm{S}_\alpha(\boldsymbol{\lambda}))\begin{cases} P_1 \oplus P_2 = \lambda_1 \\ P_3 \oplus P_4 = \lambda_2 \\ \vdots \\ P_{2\alpha-1} \oplus P_{2\alpha} = \lambda_\alpha. \end{cases}$$

In such a system, fixing the value of a variable implies fixing the value of exactly 2 variables. In this case, we say that these two variables are in the same block, and the maximum size of every block is $\xi_{\max} = 2$. Our goal is to find an accurate lower bound for the number $\mathrm{h}_\alpha(\boldsymbol{\lambda})$ of solutions of $(\mathrm{S}_\alpha(\boldsymbol{\lambda}))$ such that all the P_i variables are pairwise distinct variables of $\{0,1\}^n$, for all $1 \leq i \leq 2\alpha$.

As we are going to see in section 3.3, we will have to consider slightly more general systems. For any $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_\alpha) \in (\{0,1\}^n)^\alpha$, any integer d and any $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_{2d-1}) \in (\{0,1\}^n)^{2d-1}$, we denote by $\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})\right)$ the following system of equations in $2\alpha + 2d$ variables:

$$\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})\right)\begin{cases} P_1 \oplus P_2 = \lambda_1 \\ P_3 \oplus P_4 = \lambda_2 \\ \vdots \\ P_{2\alpha-1} \oplus P_{2\alpha} = \lambda_\alpha \\ P_{2\alpha+1} \oplus P_{2\alpha+2} = \mu_1 \\ P_{2\alpha+1} \oplus P_{2\alpha+3} = \mu_2 \\ \vdots \\ P_{2\alpha+1} \oplus P_{2\alpha+2d} = \mu_{2d-1}. \end{cases}$$

Such a system has α blocks of 2 variables and a final block of $2d$ variables. As in the previous case, we denote by $\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})$ the number of solutions of $\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})\right)$ such that all the P_i variables are pairwise distinct variables of $\{0,1\}^n$, for $1 \leq i \leq 2\alpha + 2d$. Note that for $\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})\right)$ to have solutions, the tuple $\boldsymbol{\mu}$ has to be chosen such that it does not trigger collisions in the last block. In more details, one needs $\mu_i \neq 0$ for $1 \leq i \leq 2d-1$, and $\mu_i \neq \mu_j$ for every $1 \leq i < j \leq 2d-1$. When this condition is fulfilled, we say that μ is *block compatible.*

In order to more easily navigate our systems of equations, we are going to add a few notations. For any $1 \leq i \leq 2\alpha$, we are going to denote by $P_i \oplus P_{\widehat{i}} = \lambda_{(i)}$ the (unique) equation in which the variable P_i is involved.[4] Moreover, for any $\theta \in \{0,1\}^n$, we denote by $\delta_{\boldsymbol{\lambda}}(\theta)$ the number of occurences of θ in $\boldsymbol{\lambda}$, and $\varDelta_{\boldsymbol{\lambda}} = \max_{\theta \in \{0,1\}^n} \{\delta_{\boldsymbol{\lambda}}(\theta)\}$.

3.2 Basic Properties

As we will see in section 3.3, most of our proof will revolve around the evaluation of the maximum difference between values of the type $\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})$ where α, d, $\boldsymbol{\lambda}$ and the first coordinate of $\boldsymbol{\mu}$ are fixed. As such, we introduce the following notation.

Definition 1. *Let α, d be integers such that $2\alpha + 2d \leq 2^n$, and let $\boldsymbol{\lambda} \in (\{0,1\}^n \setminus \{0\})^\alpha$ and $\theta \in \{0,1\}^n \setminus \{0\}$. We define the following quantities:*

- $\mathrm{BcT}^{(d)}_\theta$ *is the set of all block compatible tuples of the form $(\theta, \mu_2, \ldots, \mu_{2d-1})$;*
- $\left[\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}\right]$ *is the maximum over every $\boldsymbol{\mu} \in \mathrm{BcT}^{(d)}_\theta$ of $\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})$;*
- $\mathrm{Dist}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}$ *is the maximum over every $\boldsymbol{\mu}, \boldsymbol{\mu}' \in \mathrm{BcT}^{(d)}_\theta$ of $\left|\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu}) - \mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})\right|$;*
- $\mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}\right]$ *is the expectancy of $\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})$ when $\boldsymbol{\mu}$ is chosen uniformly at random in $\mathrm{BcT}^{(d)}_\theta$;*
- $\epsilon^{(d)}_{\alpha,\varDelta}$ *is the smallest value such that, for any $\boldsymbol{\lambda}$ such that $\varDelta_{\boldsymbol{\lambda}} \leq \varDelta$, any θ, and any $\boldsymbol{\mu}, \boldsymbol{\mu}' \in \mathrm{BcT}^{(d)}_\theta$, one has*

$$\mathrm{Dist}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta} \leq \mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}\right] \epsilon^{(d)}_{\alpha,\varDelta}.$$

In the case where $\alpha < 0$, by convention we define those quantities to be 0.

In the following Lemma, we present several basic properties of these quantities that will prove useful later. Its proof will also serve as a good warm-up for the other proofs in this paper.

Lemma 1. *Let α, β, d be positive integers such that $\alpha \leq \beta \leq 2^n/72$ and $\alpha + d \leq 2^n/72$. Let also $\theta \in \{0,1\}^n \setminus \{0\}$, $\boldsymbol{\lambda} \in (\{0,1\}^n \setminus \{0\})^\alpha$ and $\boldsymbol{\mu} \in (\{0,1\}^n \setminus \{0\})^\beta$ such that, for every $i \in \{1, \ldots, \alpha\}$, one has $\delta_{\boldsymbol{\lambda}}(\lambda_i) \leq \delta_{\boldsymbol{\mu}}(\lambda_i)$. One has*

1. $\left[\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}\right] \leq \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta)$,
2. $\mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}\right] \leq \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta)$,
3. $\mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}\right] \geq \left(\dfrac{35}{36}\right)^{2(d-1)} \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta)$,
4. $\dfrac{\mathrm{h}_\alpha(\boldsymbol{\lambda})}{\mathrm{h}_\beta(\boldsymbol{\mu})} \leq \dfrac{(18/17)^{\beta-\alpha}}{2^{n(\beta-\alpha)}}$.

Proof. The first inequality is obvious, since every solution of $\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})\right)$ for $\boldsymbol{\mu} \in \mathrm{BcT}^{(d)}_\theta$ yields a solution of $(\mathrm{S}_{\alpha+1}(\boldsymbol{\lambda}||\theta))$, and every solution of $\mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta)$

[4] Note that one has $(i) = \lceil i/2 \rceil$.

yields at most one solution of $\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})\right)$. The second inequality is also clearly a consequence of the first one. For the third inequality, we have to use the following two general remarks. First, by definition of $\mathrm{BcT}^{(d)}_{\theta}$, it is clear that $|\mathrm{BcT}^{(d)}_{\theta}| = (2^n - 2)_{2(d-1)}$. Indeed, this corresponds to the number of possible $\mu_2, \ldots, \mu_{2d-1}$ such that $0, \theta, \mu_2, \ldots, \mu_{2d-1}$ are pairwise disctinct. Second, one has

$$\sum_{\boldsymbol{\mu} \in \mathrm{BcT}^{(d)}_{\theta}} \mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu}) = (2^n - 2\alpha - 2)_{2(d-1)} \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta).$$

Indeed, this sum corresponds exactly to the number of $P_1, \ldots, P_{2\alpha+2d}$ that are pairwise distinct, and such that $P_1, \ldots, P_{2\alpha+2}$ is a solution of $(\mathrm{S}_{\alpha+1}(\boldsymbol{\lambda}||\theta))$. Hence, using the fact that $2\alpha + 2d \leq 2^n/36$, one has

$$\begin{aligned}
\mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}\right] &= \frac{(2^n - 2\alpha - 2)_{2(d-1)}}{(2^n - 2)_{2(d-1)}} \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta) \\
&\geq \frac{(2^n - 2\alpha - 2d)^{2(d-1)}}{2^{2n(d-1)}} \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta) \\
&\geq \left(\frac{35}{36}\right)^{2(d-1)} \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta).
\end{aligned}$$

The last inequality is obvious if $\alpha = \beta$. Thus, we assume that $\alpha < \beta$. We are now going to lower bound the number of $P_1, \ldots, P_{2\beta}$ that are pairwise distinct and solution of $(\mathrm{S}_\beta(\boldsymbol{\mu}))$. First, since reordering the equations does not change the number of solutions, we are going to reorder the equations of $(\mathrm{S}_\beta(\boldsymbol{\mu}))$ such that the α ones that are common between $(\mathrm{S}_\beta(\boldsymbol{\mu}))$ and $(\mathrm{S}_\alpha(\boldsymbol{\lambda}))$ appear first and in the same order (the fact that all the equations from $(\mathrm{S}_\alpha(\boldsymbol{\lambda}))$ are also in $(\mathrm{S}_\beta(\boldsymbol{\mu}))$ comes from our assumption that for every $i \in \{1, \ldots, \alpha\}$, one has $\delta_{\boldsymbol{\lambda}}(\lambda_i) \leq \delta_{\boldsymbol{\mu}}(\lambda_i)$). Let us fix $P_1, \ldots, P_{2\alpha}$ that are pairwise distinct and solution of the first α equations of $(\mathrm{S}_\beta(\boldsymbol{\mu}))$. By our choice of ordering for the equations, there are exactly $\mathrm{h}_\alpha(\boldsymbol{\lambda})$ possible choices. Now, we have to lower bound the number of possible choice for the remaining P_is. For $i = 1, \ldots, \beta - \alpha$, we have to choose $P_{2\alpha+2i-1}$ such that it is different from P_j and from $P_j \oplus \lambda_{\alpha+i}$ for $j < 2\alpha + 2i - 1$. Thus, there are at least $(2^n - 4\alpha)(2^n - 4\alpha - 4) \cdots (2^n - 4\beta + 4)$ possible choices for $P_{2\alpha+1}, \ldots, P_{2\beta}$. Overall, one has

$$\begin{aligned}
\frac{\mathrm{h}_\alpha(\boldsymbol{\lambda})}{\mathrm{h}_\beta(\boldsymbol{\mu})} &\leq \frac{1}{(2^n - 4\alpha)(2^n - 4\alpha - 4) \cdots (2^n - 4\beta + 4)} \\
&\leq \frac{1}{(2^n - 4\beta)^{\beta-\alpha}} \leq \frac{(18/17)^{\beta-\alpha}}{2^{n(\beta-\alpha)}}.
\end{aligned}$$

3.3 Orange Equation and Consequences

In this section, we are going to explain how systems of the type $\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})\right)$ for $d > 1$ come into play, and how they can be studied to derive Theorem 1. Namely, we prove the following classical Lemma.

Lemma 2 (Orange Equation). *Let* $\alpha > 0$, $\boldsymbol{\lambda} \in (\{0,1\}^n \setminus \{0\})^\alpha$ *and* $\mu \in \{0,1\}^n \setminus \{0\}$. *One has*

$$\mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\mu) = \mathrm{h}^{(1)}_{\alpha,\boldsymbol{\lambda}}(\mu) = (2^n - 4\alpha + 2\delta_{\boldsymbol{\lambda}}(\mu))\mathrm{h}_\alpha(\boldsymbol{\lambda}) + \sum_{(i,j)\in M_{\boldsymbol{\lambda}}(\mu)} \mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}(\boldsymbol{\mu}_{i,j}),$$

where

$$\begin{aligned}\boldsymbol{\lambda}_{i,j} =&(\lambda_k)_{k\neq(i),(j)},\\ \boldsymbol{\mu}_{i,j} =&(\mu, \lambda_{(i)}, \mu \oplus \lambda_{(j)}),\\ M_{\boldsymbol{\lambda}}(\mu) =&\{(i,j), 1 \le i,j \le 2\alpha, (i) \neq (j), \mu \neq \lambda_{(i)}, \mu \neq \lambda_{(j)}, \text{ and } \mu \neq \lambda_{(i)} \oplus \lambda_{(j)}\}.\end{aligned}$$

The proof of this Lemma can be found in Section 3.4. It links the number of solutions of the system $(\mathrm{S}_{\alpha+1}(\boldsymbol{\lambda}||\mu))$ in $\alpha+1$ blocks of 2 variables to:

- the number of solutions of the system $(\mathrm{S}_\alpha(\boldsymbol{\lambda}))$ that consists in α blocks of two variables;
- the number of solutions of the systems $\left(\mathrm{S}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}(\boldsymbol{\mu}_{i,j})\right)$ that consist in $\alpha-2$ blocks of two variables and one last block of 4 variables.

Recursively evaluating the number of solutions of a system of equations as a function of the number of solutions of new systems of equations that use a smaller number of blocks will be at the heart of our proof. Moreover, it highlights the need to study systems of the type $\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu})\right)$ for $d > 1$. The following Lemma will give us a sufficient condition for Theorem 1 to hold.

Lemma 3. *Let* $q \le \frac{2^n}{72}$ *and* $\boldsymbol{\lambda}_0 \in (\{0,1\}^n \setminus \{0\})^q$. *Let us assume that there there exists a constant* $C \le 100$ *such that* $\epsilon^{(2)}_{\alpha-2,\Delta_{\boldsymbol{\lambda}}} \le C\frac{\Delta_{\boldsymbol{\lambda}}}{2^n}$. *Then one has*

$$\mathrm{h}_q(\boldsymbol{\lambda}_0) \ge \frac{(2^n)_{2q}}{2^{nq}}.$$

Lemma 3 clearly states that, in order to prove Theorem 1, it is sufficient to focus our attention on the ratio between the deviation of the values $\mathrm{h}^{(2)}_{\alpha,\boldsymbol{\lambda}}(\mu)$ and their average value. In Section 4, we are actually going to prove that we can choose $C = 93$. Moreover, the proofs of Lemmas 2 and 3 can be found in Sections 3.4 and 3.5 respectively.

3.4 Proof of Lemma 2

The proof of this lemma is classical, and we state it for the sake of completeness.

In this proof, we want to evaluate the number of solutions of the system $(\mathrm{S}_{\alpha+1}(\boldsymbol{\lambda}||\mu))$ such that $P_1, \ldots, P_{2\alpha+2}$ are pairwise distinct.

Let us fix any integer α and any $\boldsymbol{\lambda} \in (\{0,1\}^n \setminus \{0\})^\alpha$. For $i = 1\ldots,4\alpha$, we denote with B_i the set of all $(P_1, \ldots, P_{2\alpha+2})$ such that:

- $P_1, \ldots, P_{2\alpha}$ are solutions to the $(\mathrm{S}_\alpha(\boldsymbol{\lambda}))$ system of equations,

- $P_1, \dots, P_{2\alpha}$ are pairwise distinct,
- $P_{2\alpha+1} \oplus P_{2\alpha+2} = \mu$,
- if $i \leq 2\alpha$, $P_{2\alpha+1} = P_i$, otherwise $P_{2\alpha+2} = P_{i-2\alpha}$.

One clearly has $|B_i| = \mathrm{h}_\alpha(\boldsymbol{\lambda})$. We also denote with B the set of all $(P_1, \dots, P_{2\alpha+2})$ such that:

- $P_1, \dots, P_{2\alpha}$ are solutions to the $(\mathrm{S}_\alpha(\boldsymbol{\lambda}))$ system of equations,
- $P_1, \dots, P_{2\alpha}$ are pairwise distinct,
- $P_{2\alpha+1} \oplus P_{2\alpha+2} = \mu$.

Then, it is clear that $|B| = 2^n \mathrm{h}_\alpha(\boldsymbol{\lambda})$, and

$$\mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\mu) = \left|B \setminus \left(\cup_{i=1}^{4\alpha} B_i\right)\right|.$$

It is also easy to see that, for any three pairwise distinct indexes i_1, i_2, i_3, then $B_{i_1} \cap B_{i_2} \cap B_{i_3} = \emptyset$. This is due to the fact that at least two B_i sets will involve $P_{2\alpha+1}$ or $P_{2\alpha+2}$, which implies an equality between two variables from $P_1, \dots, P_{2\alpha}$. Thus, the inclusion-exclusion principle yields:

$$\mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\mu) = (2^n - 4\alpha)\mathrm{h}_\alpha(\boldsymbol{\lambda}) + \sum_{i<j} |B_i \cap B_j|. \tag{1}$$

The last step of the proof is to evaluate $|B_i \cap B_j|$ for every $i < j$. Several cases can occur.

1. One has $i, j \leq 2\alpha$ or $i, j > 2\alpha$. In that case, there exists $i < j \leq 2\alpha$ such that $P_i = P_j$, which contradicts the requirement that $P_1, \dots, P_{2\alpha}$ are pairwise distinct. Hence, in that case, $|B_i \cap B_j| = 0$.
2. Otherwise, since $i < j$, one has $i \in \{1, \dots, \alpha\}$ and $j \in \{2\alpha + 1, \dots, 4\alpha\}$. This means that the equations added in $|B_i \cap B_j|$ imply a new equation $P_i \oplus P_{j-2\alpha} = \mu$. Let us denote $j' = j - 2\alpha$. We have to consider several subcases.
   (a) $j' = i$. One has

   $$\mu = P_{2\alpha+1} \oplus P_{2\alpha+2} = P_i \oplus P_i = 0,$$

   which is impossible since $\mu \neq 0$. Thus, in this case, one has $|B_i \cap B_j| = 0$.
   (b) $\{i, j'\} = \{2k - 1, 2k\}$ for $k \in \{1, \dots, \alpha\}$. This means that the constraints for the set $B_i \cap B_j$ contains the following equations:

   $$\begin{aligned} P_i \oplus P_{j'} =& \mu, \\ P_i \oplus P_{j'} =& \lambda_k. \end{aligned}$$

   Overall, if $\mu = \lambda_{(i)}$ (which can occur exactly $2\delta_{\boldsymbol{\lambda}}(\mu)$ times), then $|B_i \cap B_j| = \mathrm{h}_\alpha(\boldsymbol{\lambda})$. Otherwise, the set is empty.

(c) Otherwise, $B_i \cap B_j$ can be seen as the set of all $(P_1, \dots, P_{2\alpha})$ such that $P_1, \dots, P_{2\alpha}$ are pairwise distinct and solutions of the following system of equations:

$$\left\{\begin{array}{c} P_1 \oplus P_2 = \lambda_1 \\ \vdots \\ P_i \oplus P_{\widehat{i}} = \lambda_{(i)} \\ \vdots \\ P_{j'} \oplus P_{\widehat{j'}} = \lambda_{(j)} \\ \vdots \\ P_{2\alpha-1} \oplus P_{2\alpha} = \lambda_\alpha \\ P_i \oplus P_{j'} = \mu \end{array}\right. \iff \left\{\begin{array}{c} P_1 \oplus P_2 = \lambda_1 \\ \vdots \\ P_i \oplus P_{\widehat{i}} = \lambda_{(i)} \\ \vdots \\ P_i \oplus P_{\widehat{j}} = \mu \oplus \lambda_{(j)} \\ \vdots \\ P_{2\alpha-1} \oplus P_{2\alpha} = \lambda_\alpha \\ P_i \oplus P_{j'} = \mu \end{array}\right.$$

Up to a reordering of the unknowns, this is equivalent to the system $\left(\mathrm{S}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j'}}(\boldsymbol{\mu}_{i,j'})\right)$, where $\boldsymbol{\lambda}_{i,j'}$ and $\boldsymbol{\mu}_{i,j'}$ are as in Lemma 2. Two possible cases can occur: if $\mu = \lambda_{(i)}, \lambda_{(j')}$ or $\lambda_{(i)} \oplus \lambda_{(j')}$, then the system cannot have a solution such that $P_1, \dots, P_{2\alpha}$ are pairwise distinct. Otherwise, one has exactly $|B_i \cap B_j| = \mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j'}}(\boldsymbol{\mu}_{i,j'})$.

Overall, one has

$$\sum_{i<j} |B_i \cap B_j| = 2\delta_{\boldsymbol{\lambda}}(\mu)\mathrm{h}_\alpha(\boldsymbol{\lambda}) + \sum_{(i,j)\in M_{\boldsymbol{\lambda}}(\mu)} \mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}(\boldsymbol{\mu}_{i,j}). \qquad (2)$$

Combining Eqs (1) and (2) ends the proof of Lemma 2.

3.5 Proof of Lemma 3

Let $q \leq \frac{2^n}{72}$ and $\boldsymbol{\lambda}_0 \in (\{0,1\}^n)^q$. For $i = 1, \dots, q$, we write $\boldsymbol{\lambda}_{0,i} = (\lambda_{0,1}, \dots, \lambda_{0,i})$.

First step: reordering the equations

It is clear that reordering the equations (i.e. reordering the coefficients of $\boldsymbol{\lambda}_0$) does not change the value of $\mathrm{h}_q(\boldsymbol{\lambda}_0)$. Thus, we are now going to choose a specific ordering such that, for every $i = 1, \dots, q-1$, one has $\delta_{\boldsymbol{\lambda}_{0,i}}(\lambda_{0,i+1}) + 1 \geq \varDelta_{\boldsymbol{\lambda}_{0,i}}$. This can be done as follows. Let A_i denote the subset of all $\lambda_{0,j}$ values such that $\delta_{\boldsymbol{\lambda}_0}(\lambda_{0,j}) \geq i$ (i.e. values that appear at least i times in λ_0) for $i = 1, \dots, \varDelta_{\boldsymbol{\lambda}_0}$. We write $A_i = \{a_{i,1}, \dots, a_{i,a_i}\}$ using an arbitrary ordering of the elements of A_i. Then we are going to choose

$$\lambda_0 = (a_{1,1}, \dots, a_{1,a_1}, a_{2,1}, \dots, a_{2,a_2}, \dots, a_{\varDelta_{\boldsymbol{\lambda}_0},1}, \dots, a_{\varDelta_{\boldsymbol{\lambda}_0},a_{\varDelta_{\boldsymbol{\lambda}_0}}}).$$

It is easy to check that, in this case, one has $\delta_{\boldsymbol{\lambda}_{0,i}}(\lambda_{0,i+1}) + 1 = \varDelta_{\boldsymbol{\lambda}_{0,i}}$ as long as $i \neq \sum_{j=1}^k a_j$ for $k = 1, \dots, \varDelta_{\boldsymbol{\lambda}_0} - 1$, and $\delta_{\boldsymbol{\lambda}_{0,i}}(\lambda_{0,i+1}) = \varDelta_{\boldsymbol{\lambda}_{0,i}}$ otherwise.

Second step: relation between $\mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\mu)$ and $\mathrm{h}_\alpha(\boldsymbol{\lambda})$

Let $2 \leq \alpha \leq q$, $\boldsymbol{\lambda} \in (\{0,1\}^n)^\alpha$ and $\mu \neq 0^n$. From Lemma 2, one has

$$\begin{aligned} \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\mu) =& \mathrm{h}^{(1)}_{\alpha,\boldsymbol{\lambda}}(\mu) \\ =& (2^n - 4\alpha + 2\delta_{\boldsymbol{\lambda}}(\mu))\mathrm{h}_\alpha(\boldsymbol{\lambda}) \\ &+ \sum_{(i,j)\in M_{\boldsymbol{\lambda}}(\mu)} \mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}(\boldsymbol{\mu}_{i,j}), \end{aligned} \tag{3}$$

where

$$\boldsymbol{\mu}_{i,j} = (\mu, \lambda_{(i)}, \mu \oplus \lambda_{(j)}).$$

By definition of $M_{\boldsymbol{\lambda}}$, it is easy to see that, for every $\mu \neq 0$, one has

$$4\alpha^2 - 16\Delta_{\boldsymbol{\lambda}}\alpha \leq 4\alpha^2 - 4\alpha - 12\Delta_{\boldsymbol{\lambda}}\alpha \leq |M_{\boldsymbol{\lambda}}(\mu)| \leq 4\alpha^2 - 4\alpha \leq 4\alpha^2, \tag{4}$$

where $\Delta_{\boldsymbol{\lambda}} = \max_{\mu\neq 0}(\delta_{\boldsymbol{\lambda}}(\mu))$. Indeed, the number of (i,j) such that $1 \leq i,j \leq 2\alpha$ and $(i) \neq (j)$ is exactly $2\alpha(2\alpha-2)$. The number of possible values for i (resp. j) such that $\lambda_{(i)} = \mu$ (resp. $\lambda_{(j)} = \mu$) is at most $2\Delta_{\boldsymbol{\lambda}}$, and the number of possible values for (i,j) such that $\lambda_{(i)} \oplus \lambda_{(j)} = \mu$ is at most $4\alpha\Delta_{\boldsymbol{\lambda}}$.

Let us now denote $X(\mu) = \sum_{(i,j)\in M_{\boldsymbol{\lambda}}(\mu)} \mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}(\boldsymbol{\mu}_{i,j})$. We also denote with $S_{\boldsymbol{\lambda},i,j}$ the set of all $\boldsymbol{\mu} \in \{0,1\}^n \setminus \{0\}$ such that $(i,j) \in M_{\boldsymbol{\lambda}}(\mu)$ and $A_{\boldsymbol{\lambda},i,j}$ the average, when $\mu \in S_{\boldsymbol{\lambda},i,j}$, of $\mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}(\boldsymbol{\mu}_{i,j})$. Like in the proof of Lemma 1, it is easy to see that $\sum_{\mu\in S_{\boldsymbol{\lambda},i,j}} \mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}(\boldsymbol{\mu}_{i,j}) = \mathrm{h}_\alpha(\boldsymbol{\lambda})$ by definition of $\boldsymbol{\mu}_{i,j}$. Hence, since $2^n - 2 \geq |S_{i,j}| \geq 2^n - 4$, one has $\mathrm{h}_\alpha(\boldsymbol{\lambda})/(2^n-2) \leq A_{\boldsymbol{\lambda},i,j} \leq \mathrm{h}_\alpha(\boldsymbol{\lambda})/(2^n-4)$. Moreover, by definition of $\epsilon^{(2)}_{\alpha-2,\Delta_{\boldsymbol{\lambda}}}$, it is easy to see that

$$\mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}(\boldsymbol{\mu}_{i,j}) \geq A_{\boldsymbol{\lambda},i,j} - \epsilon^{(2)}_{\alpha-2,\Delta_{\boldsymbol{\lambda}}}\mathbb{E}\left[\mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}\right].$$

Using (4) and our hypothesis on $\epsilon^{(2)}_{\alpha-2,\Delta}$, one has

$$\begin{aligned} X(\mu) \geq& \sum_{(i,j)\in M_{\boldsymbol{\lambda}}(\mu)} \left(A_{\boldsymbol{\lambda},i,j} - \epsilon^{(2)}_{\alpha-2,\Delta_{\boldsymbol{\lambda}}}\mathbb{E}\left[\mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j}}\right]\right) \\ &\geq (4\alpha^2 - 16\Delta_{\boldsymbol{\lambda}}\alpha)\frac{\mathrm{h}_\alpha(\boldsymbol{\lambda})}{2^n} - 4\alpha^2\epsilon^{(2)}_{\alpha-2,\Delta_{\boldsymbol{\lambda}}} \max_{(i,j)\in M_{\boldsymbol{\lambda}}(\mu)} \mathbb{E}\left[\mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j},\lambda_{(i)}}\right] \\ &\geq (4\alpha^2 - 16\Delta_{\boldsymbol{\lambda}}\alpha)\frac{\mathrm{h}_\alpha(\boldsymbol{\lambda})}{2^n} - \frac{4C\alpha^2\Delta_{\boldsymbol{\lambda}}}{2^n} \max_{(i,j)\in M_{\boldsymbol{\lambda}}(\mu)} \mathbb{E}\left[\mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j},\lambda_{(i)}}\right]. \end{aligned} \tag{5}$$

The next step is to evaluate the value of $\max_{(i,j)\in M_{\boldsymbol{\lambda}}(\mu)} \mathbb{E}\left[\mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j},\lambda_{(i)}}\right]$. Let us fix any $(i,j) \in M_{\boldsymbol{\lambda}}(\mu)$. Using Lemma 1, one has, for every $(i,j) \in M_{\boldsymbol{\lambda}}(\mu)$,

$$\mathbb{E}\left[\mathrm{h}^{(2)}_{\alpha-2,\boldsymbol{\lambda}_{i,j},\lambda_{(i)}}\right] \leq \mathrm{h}_{\alpha-1}(\boldsymbol{\lambda}_{i,j}||\lambda_{(i)}) \leq \mathrm{h}_\alpha(\boldsymbol{\lambda})\frac{18/17}{2^n}. \tag{6}$$

Combining Eqs (3), (5), (6) and using the fact that

$$2^n - 4\alpha = \frac{(2^n-2\alpha)_2}{2^n-1} - \frac{4\alpha^2-2\alpha}{2^n-1} \geq \frac{(2^n-2\alpha)_2}{2^n-1} - \frac{4\alpha^2}{2^n-1},$$

one has

$$\frac{\mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\mu)}{\mathrm{h}_\alpha(\boldsymbol{\lambda})} \geq \frac{(2^n-2\alpha)_2}{2^n-1} - \frac{4\alpha^2}{2^n-1} + 2\delta_{\boldsymbol{\lambda}}(\mu) + \frac{4\alpha^2 - 16\varDelta_{\boldsymbol{\lambda}}\alpha}{2^n} - \frac{4.25C\alpha^2\varDelta_{\boldsymbol{\lambda}}}{2^{2n}}$$
$$\geq \frac{(2^n-2\alpha)_2}{2^n-1} + 2\delta_{\boldsymbol{\lambda}}(\mu) - \frac{16\varDelta_{\boldsymbol{\lambda}}\alpha}{2^n} - \frac{4.25C\alpha^2\varDelta_{\boldsymbol{\lambda}}}{2^{2n}}. \tag{7}$$

Third step: finalization

We can now apply formula (7) to $\boldsymbol{\lambda}_{0,\alpha}$ and $\lambda_{0,\alpha+1}$ for $\alpha = 1, \ldots, q-1$. Recall that one has $2 \leq \alpha \leq q$, $6q+4 \leq 8q \leq 2^n$ and

$$\varDelta_{\boldsymbol{\lambda}_{0,i}} \leq \delta_{\boldsymbol{\lambda}_{0,i}}(\lambda_{0,i+1}) + 1,$$

which gives

$$2\delta_{\boldsymbol{\lambda}}(\mu) - \frac{16\varDelta_{\boldsymbol{\lambda}}\alpha}{2^n} - \frac{4.25C\alpha^2\varDelta_{\boldsymbol{\lambda}}}{2^{2n}}$$
$$\geq \delta_{\boldsymbol{\lambda}}(\mu)\left(2 - 16\frac{\alpha}{2^n} - 4.25C\frac{\alpha^2}{2^{2n}}\right) - \frac{16\alpha}{2^n} - \frac{4.25C\alpha^2}{2^{2n}}$$
$$\geq -\frac{1}{3}.$$

The second inequality comes from the fact that $C \leq 100$ and $\alpha \leq q \leq 2^n/72$. Thus, one has

$$\frac{\mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}_{0,\alpha+1})}{\mathrm{h}_\alpha(\boldsymbol{\lambda}_{0,\alpha})} \geq \frac{(2^n-2\alpha)_2}{2^n-1} - \frac{1}{3}$$
$$\geq \frac{(2^n-2\alpha)_2}{2^n}\left(1 + \frac{1}{2^n-1} - \frac{2^n/3}{(2^n-2\alpha)_2}\right). \tag{8}$$

Since $q \leq \frac{2^n}{72}$, it is easy to see that $2\alpha+1 \leq 3q \leq \frac{2^n}{24}$. This yields

$$(2^n-2\alpha-1)^2 - 2^{2n}/3 \geq 2^{2n}\left(\frac{23^2}{24^2} - \frac{1}{3}\right) \geq 0,$$

and

$$\frac{\mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}_{0,\alpha+1})}{\mathrm{h}_\alpha(\boldsymbol{\lambda}_{0,\alpha})} \geq \frac{(2^n-2\alpha)_2}{2^n}. \tag{9}$$

Using (9) recursively and combining it with Remark 1, one gets

$$\mathrm{h}_q(\boldsymbol{\lambda}_0) = \mathrm{h}_2(\boldsymbol{\lambda}_{0,2}) \prod_{\alpha=2}^{q-1} \frac{\mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}_{0,\alpha}||\lambda_{\alpha+1})}{\mathrm{h}_\alpha(\boldsymbol{\lambda}_{0,\alpha})} \geq \frac{(2^n)_4}{2^{2n}} \prod_{\alpha=2}^{q-1} \frac{(2^n-2\alpha)_2}{2^n} = \frac{(2^n)_{2q}}{2^{qn}}. \tag{10}$$

4 General Purple Equations and their Consequence

4.1 Statement of the Results and Discussion

In this section, our goal is to compute an appropriate upper bound for $\epsilon^{(d)}_{\alpha,\Delta}$ in order to enable us to use Lemma 3. In a sense, this amounts to prove that the maximum deviation for $\mathrm{h}^{(d)}_{\alpha,\lambda}(()\boldsymbol{\mu})$ when $\boldsymbol{\mu}$ varies in $\mathrm{BcT}^{(d)}_{\theta}$ is small in front of its average value when $\boldsymbol{\mu}$ is chosen uniformly at random in $\mathrm{BcT}^{(d)}_{\theta}$. The first step of the proof is to upper bound this difference with a bound which involves mirror systems that have a *strictly smaller* number of blocks, which will allow us to conclude by induction on the number of blocks. One has the following result.

Lemma 4 (Differential General Purple Equation). *Let α, d be positive integers such that $\alpha + d \leq 2^n/72$. For any $\boldsymbol{\lambda} \in (\{0,1\}^n \setminus \{0\})^{\alpha}$ and any $\theta \in \{0,1\}^n \setminus \{0\}$, one has*

$$
\begin{aligned}
&\mathrm{Dist}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta} \\
&\leq 16(d-1)\Delta_{\boldsymbol{\lambda}} \max_{\boldsymbol{k}\in\mathrm{Ind}^{(2)}_{\alpha}} \left(\left[\mathrm{h}^{(2)}_{\alpha-1,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right]\right) + 4(d-1)\alpha \max_{\boldsymbol{k}\in\mathrm{Ind}^{(2)}_{\alpha}} \left(\mathrm{Dist}^{(2)}_{\alpha-1,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right) \\
&\quad + \sum_{\phi=2}^{2(d-1)} \binom{2(d-1)}{\phi} \cdot (2\alpha)^{\phi} \max_{\boldsymbol{k}\in\mathrm{Ind}^{(\phi+1)}_{\alpha}} \left(\mathrm{Dist}^{(\phi+1)}_{\alpha-\phi,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right) \\
&\quad + 2\sum_{\phi=2}^{2(d-1)} \binom{2(d-1)}{\phi} \cdot (2\alpha)^{\phi-1} \cdot 5\phi^2 \Delta_{\boldsymbol{\lambda}} \max_{\boldsymbol{k}\in\mathrm{Ind}^{(\phi+1)}_{\alpha}} \left(\left[\mathrm{h}^{(\phi+1)}_{\alpha-\phi,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right]\right) \\
&\quad + 2\sum_{\phi=2}^{2(d-1)} \sum_{m=1}^{\lfloor \phi/2 \rfloor} \binom{2(d-1)}{\phi} \binom{\phi-2}{m-1} \phi^2 \Delta_{\boldsymbol{\lambda}} (2\alpha)^{\phi-m-1} \\
&\qquad\qquad \times \max_{\boldsymbol{k}\in\mathrm{Ind}^{(\phi-m+1)}_{\alpha}} \left(\left[\mathrm{h}^{(\phi-m+1)}_{\alpha-\phi+m,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right]\right).
\end{aligned}
$$

Proof. The proof of this Lemma is deferred to Section 4.2.

Lemma 4 may seem complicated, but the intuition behind it as actually quite simple. Like in the proof of the orange equation, collisions between variables in the last block and the other variables will be added one by one, and we are going to consider the maximum difference between two coefficients of the type $\mathrm{h}^{(\phi)}_{\alpha,\boldsymbol{\lambda},\theta}(\mu)$. Several cases can occur:

- the variables that are involved in the collisions come from different blocks and no contradiction occur in either case: this is the source of the $\mathrm{Dist}^{(\phi+1)}_{\alpha-\phi,\boldsymbol{\lambda},\theta}$ terms in the bound;
- the variables that are involved in the collisions also come from different blocks but some contradiction occurs: in this case we simply upper bound the number of such cases, and introduce a term in $\left[\mathrm{h}^{(\phi+1)}_{\alpha-\phi,\boldsymbol{\lambda},\theta}\right]$;

- there exists collisions with variables from the same block, but no incompatibility occurs: this means that some equations are redundant and can be removed from the system; like in the previous case, we simply upper bound the number of such cases and introduce a term in $\left[\mathrm{h}^{(\phi-m+1)}_{\alpha-\phi+m,\boldsymbol{\lambda},\theta}\right]$, where m is the number of redundant equations.

As we will see, the last two types of terms can be shown to be negligible. This means that most of our efforts will be focused on the first type of terms. It is important to note that, while there are terms of the form $\mathrm{Dist}^{(d')}_{\alpha',\boldsymbol{\lambda}',\theta'}$ in both sides of the inequality, the ones that appear in the right hand side actually involve a number of blocks that is strictly smaller than the ones on the left hand side. This fact will allow us to derive an upper bound for $\epsilon^{(d)}_{\alpha,\Delta}$ by induction over the number of blocks that appear in a system of equations. Namely, we prove the following result.

Lemma 5. *Let α, d, Δ be positive integers such that $\alpha + d \leq 2^n/72$ and $\Delta \leq \alpha$. One has*

$$\epsilon^{(d)}_{\alpha,\Delta} \leq \left(\frac{36}{35}\right)^{2(d-1)} \frac{\Delta}{2^n}\left(c_1(d-1) + c_2 2^{2(d-1)}(d-1)^2\right),$$

where $c_1 = 23$ and $c_2 = 16$

Applying Lemma 5 to the case where $d = 2$ yields the following corollary which ends the proof of Theorem 1 when combined with Lemma 3.

Corollary 1. *Let α, Δ be positive integers such that $\alpha \leq 2^n/72$ and $\Delta \leq \alpha - 2$. One has*

$$\epsilon^{(2)}_{\alpha-2,\Delta} \leq 93\frac{\Delta}{2^n}.$$

The proof of this Lemma is deferred to Section 4.3.

4.2 Proof of Lemma 4

Let α, d be positive integers such that $\alpha + d \leq 2^n/72$. Let us fix any $\boldsymbol{\lambda} \in (\{0,1\}^n \setminus \{0\})^\alpha$, $\theta \in \{0,1\}^n \setminus \{0\}$, and any two block compatible $2d-1$-tuples $\boldsymbol{\mu}_1$ and $\boldsymbol{\mu}_2$ such that $\mu_{1,1} = \mu_{2,1} = \theta$. The goal of this proof is to upper bound the difference between the number of $(P_1, \dots, P_{2\alpha+2d})$ such that $P_1, \dots, P_{2\alpha+2d}$ are pairwise distinct, and are also solutions of the following system

$$\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu}_i)\right)\begin{cases} P_1 \oplus P_2 = \lambda_1 \\ \vdots \\ P_{2\alpha-1} \oplus P_{2\alpha} = \lambda_\alpha \\ P_{2\alpha+1} \oplus P_{2\alpha+2} = \mu_{i,1} = \theta \\ P_{2\alpha+1} \oplus P_{2\alpha+3} = \mu_{i,2} \\ \vdots \\ P_{2\alpha+1} \oplus P_{2\alpha+2d} = \mu_{i,2d-1} \end{cases}$$

for $i = 1, 2$.

We are going to proceed very similarly to the proof of Lemma 2, by using the inclusion-exclusion principle and then analysing every possible set intersection. For every $P_1, \ldots, P_{2\alpha+2d}$ that are pairwise distinct and solution of $\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu}_i)\right)$, the following facts hold:

- $P_1, \ldots, P_{2\alpha+2}$ are pairwise distinct and solution of $(\mathrm{S}_{\alpha+1}(\boldsymbol{\lambda}||\theta))$;
- for $i = 1, 2$ and $j = 3, \ldots, 2d$, $P_{2\alpha+j} = P_{2\alpha+1} \oplus \mu_{i,j-1} \neq P_k$ for $k \leq 2\alpha$[5].

Let us denote with B^i the set of all $P_1, \ldots, P_{2\alpha+2d}$ such that $P_1, \ldots, P_{2\alpha+2}$ are pairwise distinct and solution of $\left(\mathrm{S}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu}_i)\right)$ for $i = 1, 2$. We also denote with $B^i_{j,k}$ the subset of B^i that also satisfies $P_{2\alpha+j} = P_k$ for $j = 3, \ldots, 2d$ and $k = 1, \ldots, 2\alpha$. As usual, one has $B^i_{j,k_1} \cap B^i_{j,k_2} = \emptyset$ for any $i = 1, 2$, $j = 3, \ldots, 2d$ and any $1 \leq k_1 < k_2 \leq 2\alpha$, since this would imply an equality between P_{k_1} and P_{k_2}. Thus, using the inclusion-exclusion principle, the following holds for $i = 1, 2$:

$$\begin{aligned}
\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu}_i) =& \left| B^i \setminus \left(\bigcup_{3\leq j\leq 2d} \bigcup_{1\leq k\leq 2\alpha} B^i_{j,k} \right) \right| \\
=& \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta) - \left| \bigcup_{3\leq j\leq 2d} \bigcup_{1\leq k\leq 2\alpha} B^i_{j,k} \right| \\
=& \mathrm{h}_{\alpha+1}(\boldsymbol{\lambda}||\theta) - \sum_{\phi=1}^{2d-2} (-1)^{\phi+1} \sum_{\substack{3\leq j_1<\ldots<j_\phi\leq 2d \\ 1\leq k_1,\ldots,k_\phi\leq 2\alpha}} \left| \bigcap_{l=1}^{\phi} B^i_{j_l,k_l} \right| .
\end{aligned}$$

Finally, the triangular inequality yields

$$\left| \mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu}_1) - \mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda}}(\boldsymbol{\mu}_2) \right| \leq \sum_{\phi=1}^{2d-2} \sum_{\substack{3\leq j_1<\ldots<j_\phi\leq 2d \\ 1\leq k_1,\ldots,k_\phi\leq 2\alpha}} \left| \left| \bigcap_{l=1}^{\phi} B^1_{j_l,k_l} \right| - \left| \bigcap_{l=1}^{\phi} B^2_{j_l,k_l} \right| \right| . \qquad (11)$$

In order to conclude this proof, we have to consider the maximum variation between every possible intersection of $B^i_{j,k}$ sets.

Case $\boldsymbol{\phi = 1}$. In this case, there exists $j \in \{3, \ldots, 2d\}$ and $k \in \{1, \ldots, 2\alpha\}$ such that $P_{2\alpha+j} = P_k$. Recall that the only constraints we have on $P_{2\alpha+j'}$ for $j \neq j$ come from the equations $P_{2\alpha+j'} \oplus P_{2\alpha+1} = \mu_{i,j'-1}$. This means that $|B^i_{j,k}|$ is equal to the number of possible $P_1, \ldots, P_{2\alpha+2}$ that are pairwise distinct, satisfy

[5] Remark that once $P_{2\alpha+1}$ is fixed, then so is P_i for $i = 2\alpha+2, \ldots, 2\alpha+2d$. The fact that $\boldsymbol{\mu}_1$ and $\boldsymbol{\mu}_2$ are block compatible implies that the $P_{2\alpha+k}$ for $k = 1, \ldots, 2d$ are necessarily pairwise distinct.

the equations $P_l \oplus P_{\hat{l}} = \lambda_{(l)}$ when $(l) \neq (k)$ along with the following block of three equations:

$$\begin{aligned} P_{2\alpha+1} \oplus P_k =& \mu_{i,j-1} \\ P_{2\alpha+1} \oplus P_{\hat{k}} =& \lambda_{(k)} \oplus \mu_{i,j-1} \\ P_{2\alpha+1} \oplus P_{2\alpha+2} =& \theta. \end{aligned}$$

For this block to admit solutions, we need the following conditions to hold: $\mu_{i,j-1} \neq \lambda_{(k)}, \theta, \lambda_{(k)} \oplus \theta$. Since $\boldsymbol{\mu}_i$ is block compatible and $\mu_{i,1} = \theta$, we already know that $\mu_{i,j-1} \neq \theta$. Thus, as long as $\mu_{i,j-1} \neq \lambda_{(k)}, \theta \oplus \lambda_{(k)}$, we have:

$$|B^i_{j,k}| = \mathrm{h}^{(2)}_{\alpha-1,\boldsymbol{\lambda}_{(k)}}(\boldsymbol{\mu}_{i,j-1,k}) \leq \left[\mathrm{h}^{(2)}_{\alpha-1,\boldsymbol{\lambda}_{(k)},\theta}\right],$$

where $\boldsymbol{\lambda}_{(k)} = (\lambda_i)_{i \neq (k)}$ and $\boldsymbol{\mu}_{i,j-1,k} = (\mu_{i,j-1}, \theta, \mu_{i,j-1} \oplus \lambda_{(k)})$. If (j,k) is such that $\boldsymbol{\mu}_{i,j-1} = \lambda_{(k)}$ or $\boldsymbol{\mu}_{i,j-1} = \theta \oplus \lambda_{(k)}$, then $|B^i_{j,k}| = 0$. Note that this final case can occur at most $8(d-1)\Delta_{\boldsymbol{\lambda}}$ times for each value of i. Finally, one has

$$\begin{aligned} \sum_{\substack{3 \leq j \leq 2d \\ 1 \leq k \leq 2\alpha}} \left| |B^1_{j,k}| - |B^2_{j,k}| \right| \leq 16(d-1)\Delta_{\boldsymbol{\lambda}} \max_{\boldsymbol{k} \in \mathrm{Ind}^{(2)}_\alpha} \left(\left[\mathrm{h}^{(2)}_{\alpha-1,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right] \right) \\ + 4(d-1)\alpha \max_{\boldsymbol{k} \in \mathrm{Ind}^{(2)}_\alpha} \left(\mathrm{Dist}^{(2)}_{\alpha-1,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta} \right). \qquad (12) \end{aligned}$$

Case $\boldsymbol{1 < \phi \leq 2(d-1)}$. In this case, there exists $3 \leq j_1 < \cdots < j_\phi \leq 2d$ and $1 \leq k_1, \ldots, k_\phi \leq 2\alpha$ such that the k_l are pairwise distinct and $P_{2\alpha+j_l} = P_{k_l}$ for $l = 1, \ldots, \phi$. We denote $\boldsymbol{j} = (j_1, \ldots, j_\phi)$ and $\boldsymbol{k} = (k_1, \ldots, k_\phi)$.

Two different cases have to be considered. First, let us assume that the (k_l) values are pairwise distinct. As above, $|B^i_{j_1,k_1} \cap \cdots \cap B^i_{j_\phi,k_\phi}|$ is equal to the number of possible $P_1 \ldots, P_{2\alpha+2}$ that are pairwise distinct, satisfy the equations $P_l \oplus P_{\hat{l}} = \lambda_{(l)}$ when $(l) \neq (k_1), (k_2)$, along with the following block of $2\phi + 1$ equations:

$$\begin{aligned} P_{2\alpha+1} \oplus P_{2\alpha+2} &= \theta \\ P_{2\alpha+1} \oplus P_{k_1} &= \mu_{i,j_1-1} \\ P_{2\alpha+1} \oplus P_{\widehat{k_1}} &= \mu_{i,j_1-1} \oplus \lambda_{(k_1)} \\ &\vdots \\ P_{2\alpha+1} \oplus P_{k_\phi} &= \mu_{i,j_\phi-1} \\ P_{2\alpha+1} \oplus P_{\widehat{k_\phi}} &= \mu_{i,j_\phi-1} \oplus \lambda_{(k_\phi)}. \end{aligned}$$

As in the previous case, $|B^i_{j_1,k_1} \cap \cdots \cap B^i_{j_\phi,k_\phi}| = 0$ if one of the following conditions is fulfilled:

- there exist $l \in \{1, \ldots, \phi\}$ such that $\lambda_{(k_l)} = \mu_{i,j_l-1}$ or $\lambda_{k_l} = \mu_{i,j_l-1} \oplus \theta$,

– there exist $1 \leq l < l' \leq \phi$ such that $\lambda_{(k_l)} = \mu_{i,j_l-1} \oplus \mu_{i,j_{l'}-1}$, $\lambda_{(k_{l'})} = \mu_{i,j_l-1} \oplus \mu_{i,j_{l'}-1}$ or $\lambda_{(k_l)} \oplus \lambda_{(k_{l'})} = \mu_{i,j_l-1} \oplus \mu_{i,j_{l'}-1}$.

The first case can occur at most $2\begin{pmatrix} 2(d-1) \\ \phi \end{pmatrix} \cdot \phi \cdot (2\alpha)^{\phi-1} \cdot 2\Delta_{\boldsymbol{\lambda}}$ times for each value of i, while the second case can occur at most $3\begin{pmatrix} 2(d-1) \\ \phi \end{pmatrix} \cdot \begin{pmatrix} \phi \\ 2 \end{pmatrix} (2\alpha)^{\phi-1} \cdot 2\Delta_{\boldsymbol{\lambda}}$ times for each value of i. Overall, the intersection will be empty at most

$$\begin{pmatrix} 2(d-1) \\ \phi \end{pmatrix} \cdot (2\alpha)^{\phi-1} \cdot 5\phi^2 \Delta_{\boldsymbol{\lambda}}$$

times for each value of i. For the at most $\begin{pmatrix} 2(d-1) \\ \phi \end{pmatrix} (2\alpha)^{\phi}$ other cases, one simply has $|B^i_{j_1,k_1} \cap \cdots \cap B^i_{j_\phi,k_\phi}| = \mathrm{h}^{(\phi+1)}_{\alpha-\phi,\boldsymbol{\lambda_k}}(\boldsymbol{\mu}_{i,\boldsymbol{j},\boldsymbol{k}})$, where

$$\boldsymbol{\mu}_{i,\boldsymbol{j},\boldsymbol{k}} = (\theta, \mu_{i,j_1-1}, \mu_{i,j_1-1} \oplus \lambda_{(k_1)}, \ldots, \mu_{i,j_\phi-1}, \mu_{i,j_\phi-1} \oplus \lambda_{(k_\phi)})$$

is block compatible for $i = 1, 2$.

Second, let us consider the case where there exist collisions between the (k_l) values. Since one cannot have $P_{2\alpha+j_1} = P_{2\alpha+j_2}$ because of the block compatibility of $\boldsymbol{\mu}_i$, the only case we have to consider is the existence of colliding pairs, i.e. pairs of indices l_1 and l_2 such that $k_{l_1} = \widehat{k_{l_2}}$. In this case, the last block includes the following four equations:

$$\begin{aligned} P_{2\alpha+1} \oplus P_{k_{l_1}} &= \mu_{i,j_{l_1}-1} \\ P_{2\alpha+1} \oplus P_{\widehat{k_{l_1}}} &= \mu_{i,j_{l_1}-1} \oplus \lambda_{(k_{l_1})} \\ P_{2\alpha+1} \oplus P_{\widehat{k_{l_1}}} &= \mu_{i,j_{l_2}-1} \\ P_{2\alpha+1} \oplus P_{k_{l_1}} &= \mu_{i,j_{l_2}-1} \oplus \lambda_{(k_{l_1})}. \end{aligned}$$

This system only admits solutions if $\lambda_{(k_{l_1})} = \mu_{i,j_{l_1}-1} \oplus \mu_{i,j_{l_2}-1}$, and in this case we can simply eliminate the last two equations of the system. Let us now break the counting down depending on the number m of colliding pairs of indices. Let us fix $m \in \{1, \ldots, \lfloor \phi/2 \rfloor\}$ and one of the at most $\begin{pmatrix} 2(d-1) \\ \phi \end{pmatrix}$ possible choices for $\boldsymbol{j}$. We are first going to count the number of possible choices for the pairs of colliding indices $(l_1, l'_1), \ldots, (l_m, l'_m)$, along with the corresponding choice of k_{l_s} (knowing that in this case $k_{l'_s} = \widehat{k_{l_s}}$) for $s = 1, \ldots, m$. There are actually two ways of counting the number of such triples: we can either fix l_s and l'_s, and then choose k_s, or fix l_s and k_s, then choose l'_s. Both approaches yield different results, and we are going to use a mised strategy in order to get the desired bound. Let us first deal with the first pair. There are exactly $\phi(\phi-1)/2$ possible choice for l_1, l'_1, and then at most $2\Delta_{\boldsymbol{\lambda}}$ possible choices for k_{l_1} such that $\lambda_{(k_{l_1})} = \mu_{i,j_{l_1}-1} \oplus \mu_{i,j_{l'_1}-1}$. Let us now deal with the $m-1$ remaining pairs. There are $\begin{pmatrix} \phi-2 \\ m-1 \end{pmatrix}$ possible indices for $l_2, \dots, l_m$, and $(2\alpha)^{m-1}$ possible choices for the corresponding k_{l_s}. Recall that, for the system to admit solutions, we need $\lambda_{(k_{l_s})} = \mu_{i,j_{l_s}-1} \oplus \mu_{i,j_{l'_s}-1}$. Since $\boldsymbol{\mu}$ is block compatible, its components are pairwise distinct. Thus, once j_{l_s} and k_{l_s} are fixed, there is at most one possible choice for l'_s. For the remaining components of $\boldsymbol{k}$, there are as usual at most $(2\alpha)^{\phi-2m}$ possible choices. Once such a pair of tuples $(\boldsymbol{j}, \boldsymbol{k})$ is fixed, then one has

$$|B^i_{j_1,k_1} \cap \cdots \cap B^i_{j_\phi,k_\phi}| \leq \left[\mathrm{h}^{(\phi-m+1)}_{\alpha-\phi+m,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right]$$

since exactly $2m$ equations have been removed from the final block of $2\phi+2$ equations.

Overall, one has

$$\begin{aligned}
\sum_{\substack{3\leq j_1<\cdot<j_\phi\leq 2d\\ 1\leq k_1,\dots,k_\phi\leq 2\alpha}} &\Big||B^1_{j_1,k_1} \cap \cdots \cap B^1_{j_\phi,k_\phi}| - |B^2_{j_1,k_1} \cap \cdots \cap B^2_{j_\phi,k_\phi}|\Big| \\
&\leq \binom{2(d-1)}{\phi} \cdot (2\alpha)^\phi \max_{\boldsymbol{k}\in\mathrm{Ind}_\alpha^{(\phi+1)}} \left(\mathrm{Dist}^{(\phi+1)}_{\alpha-\phi,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right) \\
&\quad + 2\binom{2(d-1)}{\phi} \cdot (2\alpha)^{\phi-1} \cdot 5\phi^2 \mathit{\Delta}_{\boldsymbol{\lambda}} \max_{\boldsymbol{k}\in\mathrm{Ind}_\alpha^{(\phi+1)}} \left(\left[\mathrm{h}^{(\phi+1)}_{\alpha-\phi,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right]\right) \\
&\quad + 2\sum_{m=1}^{\lfloor\phi/2\rfloor} \binom{2(d-1)}{\phi}\binom{\phi-2}{m-1} \phi^2 \mathit{\Delta}_{\boldsymbol{\lambda}} (2\alpha)^{\phi-m-1} \\
&\qquad\qquad \times \max_{\boldsymbol{k}\in\mathrm{Ind}_\alpha^{(\phi-m+1)}} \left(\left[\mathrm{h}^{(\phi-m+1)}_{\alpha-\phi+m,\boldsymbol{\lambda}_{\boldsymbol{k}},\theta}\right]\right). \qquad (13)
\end{aligned}$$

Combining Eqs (11), (12) and (13) yields the result.

4.3 Proof of Lemma 5

We are going to prove this lemma using a recursion on the number of blocks.

For any d such that $d \leq 2^n/72$, and any block compatible $\boldsymbol{\mu}$ it is easy to see that $\mathrm{h}^{(d)}_{\alpha,()}(\boldsymbol{\mu}) = 2^n$. Indeed, once P_1 is fixed, all the other variables will be fixed and, thanks to the block compatibility of $\boldsymbol{\mu}$, they will be pairwise distinct. Hence, $\epsilon^{(d)}_{\alpha,0} = 0$.

Let us now assume that, for any $\alpha < \alpha_0$, any $\mathit{\Delta} \leq \alpha$ and any d such that $\alpha + d \leq 2^n/72$, one has

$$\epsilon^{(d)}_{\alpha,\mathit{\Delta}} \leq \left(\frac{36}{35}\right)^{2(d-1)} \frac{\mathit{\Delta}}{2^n}\left(c_1(d-1) + c_2 2^{2(d-1)}(d-1)^2\right).$$

Our goal is now to prove that this inequality also holds for $\epsilon^{(d)}_{\alpha_0,\mathit{\Delta}}$ for any $d \leq 2^n/72 - \alpha_0$.

Let us fix any $\boldsymbol{\lambda} \in (\{0,1\}^n \setminus \{0\})^{\alpha_0}$ such that $\varDelta_{\boldsymbol{\lambda}} \leq \varDelta$, any $\theta \in \{0,1\}^n \setminus \{0\}$, and any two block compatible $2d-1$-tuples $\boldsymbol{\mu}_1$ and $\boldsymbol{\mu}_2$ such that $\mu_{1,1} = \mu_{2,1} = \theta$. Using Lemma 1, for any $1 \leq \phi \leq 2(d-1)$ and any $\boldsymbol{k} \in \mathrm{Ind}_{\alpha_0}^{(\phi+1)}$, one has:

$$\frac{\left[\mathrm{h}^{(\phi+1)}_{\alpha_0-\phi,\boldsymbol{\lambda_k},\theta}\right]}{\mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha_0,\boldsymbol{\lambda},\theta}\right]} \leq \left(\frac{36}{35}\right)^{2(d-1)} \frac{\mathrm{h}_{\alpha_0-\phi+1}(\boldsymbol{\lambda_k}||\theta)}{\mathrm{h}_{\alpha_0+1}(\boldsymbol{\lambda}||\theta)} \leq \left(\frac{36}{35}\right)^{2(d-1)} \frac{(18/17)^{\phi}}{2^{n\phi}};$$

$$\begin{aligned}\frac{\mathrm{Dist}^{(\phi+1)}_{\alpha_0-\phi,\boldsymbol{\lambda_k},\theta}}{\mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha_0,\boldsymbol{\lambda},\theta}\right]} &\leq \epsilon^{(\phi+1)}_{\alpha_0-\phi,\varDelta} \frac{\mathbb{E}\left[\mathrm{h}^{(\phi+1)}_{\alpha_0-\phi,\boldsymbol{\lambda_k},\theta}\right]}{\mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha_0,\boldsymbol{\lambda},\theta}\right]} \leq \left(\frac{36}{35}\right)^{2(d-1)} \epsilon^{(\phi+1)}_{\alpha_0-\phi,\varDelta} \frac{\mathrm{h}_{\alpha_0-\phi+1}(\boldsymbol{\lambda_k}||\theta)}{\mathrm{h}_{\alpha_0+1}(\boldsymbol{\lambda}||\theta)} \\ &\leq \left(\frac{36}{35}\right)^{2(d-1)} \epsilon^{(\phi+1)}_{\alpha_0-\phi,\varDelta} \frac{(18/17)^{\phi}}{2^{n\phi}}.\end{aligned}$$

By combining Lemma 4 with those inequalities and the fact that $\binom{2(d-1)}{\phi} \leq 2^{2(d-1)}$ for every $0 \leq \phi \leq 2(d-1)$, one gets

$$\begin{aligned}&\left(\frac{36}{35}\right)^{-2(d-1)} \frac{\mathrm{Dist}^{(d)}_{\alpha_0,\boldsymbol{\lambda},\theta}}{\mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}\right]} \\ &\leq \frac{17(d-1)\varDelta}{2^n} + \frac{4.5(d-1)\alpha_0\epsilon^{(2)}_{\alpha_0-1,\varDelta}}{2^n} + 2^{2(d-1)} \sum_{\phi=2}^{2(d-1)} \epsilon^{(\phi+1)}_{\alpha_0-\phi,\varDelta} \left(\frac{2.25\alpha_0}{2^n}\right)^{\phi} \\ &\quad + 40\varDelta(d-1)^2 \cdot 2^{2(d-1)} \sum_{\phi=2}^{2(d-1)} (2\alpha_0)^{\phi-1} \frac{(18/17)^{\phi}}{2^{n\phi}} \\ &\quad + 2^{2d-1}\varDelta(d-1)^2 \sum_{\phi=2}^{2(d-1)} 2^{\phi} \sum_{m=1}^{\lfloor \phi/2 \rfloor} (2\alpha_0)^{\phi-m-1} \frac{(18/17)^{\phi-m}}{2^{n(\phi-m)}}. \qquad (14)\end{aligned}$$

Let us now upper bound each sum appearing in Eq (14) in turn. This step will be computationally heavy, but most of it will be centered around the use of the following classical inequality:

$$\sum_{i=0}^{n} x^i \leq \frac{1}{1-x} \qquad (15)$$

when $|x| < 1$. Since $\alpha \leq 2^n/72$, one has $\frac{2.25\alpha}{2^n} \leq \frac{1}{32}$. Moreover, $\alpha_0 - 1 < \alpha_0$ and, for $\phi = 2, \ldots, 2(d-1)$, $(\alpha_0 - \phi) + (\phi + 1) \leq \alpha_0 + d \leq 2^n/72$, which means that we can apply our induction hypothesis to all the $\epsilon^{(\phi+1)}_{\alpha_0-\phi,\varDelta}$ terms. Thus, one has

$$\begin{aligned}\frac{4.5(d-1)\alpha_0\epsilon^{(2)}_{\alpha_0-1,\varDelta}}{2^n} &\leq \frac{4.5(d-1)\alpha_0}{2^n} \left(\frac{36}{35}\right)^2 \frac{\varDelta}{2^n} (c_1 + 4c_2) \\ &\leq \frac{(c_1+4c_2)(d-1)}{15} \frac{\varDelta}{2^n}.\end{aligned}$$

Moreover, one has

$$\begin{aligned}
&\sum_{\phi=2}^{2(d-1)} \epsilon_{\alpha_0-\phi,\varDelta}^{(\phi+1)} \left(\frac{2.25\alpha_0}{2^n}\right)^{\phi} \\
&\quad \leq \sum_{\phi=2}^{2(d-1)} \left(\frac{36}{35}\right)^{2\phi} \frac{\varDelta}{2^n} \left(c_1\phi + c_2 2^{2\phi}\phi^2\right) \left(\frac{2.25\alpha_0}{2^n}\right)^{\phi} \\
&\quad \leq 2\left(\frac{36}{35}\right)^4 c_1(d-1)\frac{\varDelta}{2^n}\left(\frac{2.25\alpha_0}{2^n}\right)^2 \sum_{\phi=0}^{+\infty}\left(\frac{36}{35}\right)^{2\phi}\left(\frac{2.25\alpha_0}{2^n}\right)^{\phi} \\
&\qquad + 4\left(\frac{36}{35}\right)^4 c_2(d-1)^2\frac{\varDelta}{2^n}\left(\frac{2.25\alpha_0}{2^n}\right)^2 \sum_{\phi=0}^{+\infty}\left(\frac{36}{35}\right)^{2\phi} 2^{2\phi}\left(\frac{2.25\alpha_0}{2^n}\right)^{\phi}
\end{aligned}$$

Using Eq (15) yields

$$\begin{aligned}
&\sum_{\phi=2}^{2(d-1)} \epsilon_{\alpha_0-\phi,\varDelta}^{(\phi+1)} \left(\frac{2.25\alpha_0}{2^n}\right)^{\phi} \\
&\quad \leq 2\left(\frac{36}{35}\right)^4 c_1(d-1)\frac{\varDelta}{2^n}\left(\frac{2.25\alpha_0}{2^n}\right)^2 \sum_{\phi=0}^{+\infty}\left(\frac{3\alpha_0}{2^n}\right)^{\phi} \\
&\qquad + 4\left(\frac{36}{35}\right)^4 c_2(d-1)^2\frac{\varDelta}{2^n}\left(\frac{2.25\alpha_0}{2^n}\right)^2 \sum_{\phi=0}^{+\infty}\left(\frac{10\alpha_0}{2^n}\right)^{\phi} \\
&\quad \leq 2.5c_1(d-1)\frac{\varDelta}{2^n}\left(\frac{2.25\alpha_0}{2^n}\right)^2 + 6c_2(d-1)^2\frac{\varDelta}{2^n}\left(\frac{2.25\alpha_0}{2^n}\right)^2 \\
&\quad \leq \frac{2.5c_1+6c_2}{1024}(d-1)^2\frac{\varDelta}{2^n}.
\end{aligned}$$

Similarly, one has

$$\sum_{\phi=2}^{2(d-1)} (2\alpha_0)^{\phi-1}\frac{(18/17)^{\phi}}{2^{n\phi}} \leq \frac{2.25\alpha_0}{2^{2n}}\sum_{\phi=0}^{+\infty}\left(\frac{2.25\alpha_0}{2^n}\right)^{\phi} \leq \frac{2.25\alpha_0}{2^{2n}\left(1-\frac{2.25\alpha_0}{2^n}\right)} \leq \frac{2.5\alpha_0}{2^{2n}},$$

and

$$\begin{aligned}
&\sum_{\phi=2}^{2(d-1)} 2^{\phi} \sum_{m=1}^{\lfloor \phi/2 \rfloor} (2\alpha_0)^{\phi-m-1} \frac{(18/17)^{\phi-m}}{2^{n(\phi-m)}} \\
&\quad \leq \sum_{\phi=2}^{2(d-1)} 2^{\phi} \sum_{m=\lceil \phi/2 \rceil -1}^{+\infty} (2\alpha_0)^{m} \left(\frac{18/17}{2^n} \right)^{m+1} \\
&\quad \leq \sum_{\phi=2}^{2(d-1)} 2^{\phi} \left(\frac{2.25\alpha_0}{2^n} \right)^{\lceil \phi/2 \rceil -1} \frac{18/17}{2^n \left(1 - \frac{2.25\alpha_0}{2^n}\right)} \\
&\quad \leq \frac{1.1}{2^n} \sum_{\phi=2}^{2(d-1)} 2^{\phi} \left(\frac{2.25\alpha_0}{2^n} \right)^{\lceil \phi/2 \rceil -1} \leq \frac{4.4}{2^n} + \frac{2.2}{2^n} \sum_{\phi=1}^{+\infty} 2^{2\phi+3} \left(\frac{2.25\alpha_0}{2^n} \right)^{\phi} \\
&\quad \leq \frac{4.4}{2^n} + \frac{17.6}{2^n} \sum_{\phi=1}^{+\infty} \left(\frac{9\alpha_0}{2^n} \right)^{\phi} \leq \frac{4.4}{2^n} + \frac{161\alpha_0}{2^{2n}}.
\end{aligned}$$

Hence, Eq (14) yields

$$\begin{aligned}
&\left(\frac{36}{35}\right)^{-2(d-1)} \frac{\mathrm{Dist}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}}{\mathbb{E}\left[\mathrm{h}^{(d)}_{\alpha,\boldsymbol{\lambda},\theta}\right]} \\
&\leq \frac{17(d-1)\mathit{\Delta}}{2^n} + \frac{(c_1+4c_2)(d-1)}{15}\frac{\mathit{\Delta}}{2^n} + 2^{2(d-1)}\frac{2.5c_1+6c_2}{1024}(d-1)^2\frac{\mathit{\Delta}}{2^n} \\
&\qquad + \frac{2\mathit{\Delta}(d-1)^2 2^{2(d-1)}}{2^n} + 2\mathit{\Delta}(d-1)^2 2^{2(d-1)}\frac{4.4}{2^n} + 2\mathit{\Delta}(d-1)^2 2^{2(d-1)}\frac{161\alpha_0}{2^{2n}}.
\end{aligned}$$

This inequality holds regardless of our choice of $\boldsymbol{\lambda}$ and θ, which means that it also holds for $\epsilon^{(d)}_{\alpha_0,\mathit{\Delta}}$, and one has

$$\begin{aligned}
\epsilon^{(d)}_{\alpha_0,\mathit{\Delta}} \leq \left(\frac{36}{35}\right)^{2(d-1)} \frac{\mathit{\Delta}}{2^n} \Bigg(&\left(17 + \frac{c_1+4c_2}{15}\right)(d-1) \\
&+ \left(\frac{2.5c_1+6c_2}{1024} + 2 + 2 \times 4.4 + 2\frac{161\alpha_0}{2^n}\right) 2^{2(d-1)}(d-1)^2 \Bigg).
\end{aligned}$$

In order for our hypothesis to hold, we need the following inequalities:

$$17 + \frac{c_1+4c_2}{15} \leq c_1, \qquad \frac{2.5c_1+6c_2}{1024} + 10.8 + 2\frac{161\alpha_0}{2^n} \leq c_2.$$

Both inequalities hold if $c_1 = 23$, $c_2 = 16$ and $\alpha_0 \leq 2^n/72$.

References

[BN18] Srimanta Bhattacharya and Mridul Nandi. Revisiting variable output length XOR pseudorandom function. *IACR Trans. Symmetric Cryptol.*, 2018(1):314–335, 2018.

[CLP14] Benoit Cogliati, Rodolphe Lampe, and Jacques Patarin. The indistinguishability of the XOR of k permutations. In *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 285–302. Springer, 2014.

[DDNY18] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or decrypt? to make a single-key beyond birthday secure nonce-based MAC. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 631–661. Springer, 2018.

[DHT17] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 497–523. Springer, 2017.

[DN20] Avijit Dutta and Mridul Nandi. BBB secure nonce based MAC using public permutations. In *Progress in Cryptology - AFRICACRYPT 2020*, 2020.

[DNS20] Avijit Dutta, Mridul Nandi, and Abishanka Saha. Proof of mirror theory for $\xi_{\max} = 2$. Cryptology ePrint Archive, Report 2020/669, 2020. https://eprint.iacr.org/2020/669.

[DNT19] Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond birthday bound secure MAC in faulty nonce model. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 437–466. Springer, 2019.

[JN20] Ashwin Jha and Mridul Nandi. Tight security of cascaded LRW2. *Journal of Cryptology*, 33(3):1272–1317, 2020.

[NPV17] Valérie Nachef, Jacques Patarin, and Emmanuel Volte. *Feistel Ciphers - Security Proofs and Cryptanalysis*. Springer, 2017.

[Pat03] 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 *LNCS*, pages 513–529. Springer, 2003.

[Pat08a] Jacques Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations. In Reihaneh Safavi-Naini, editor, *Information Theoretic Security - ICITS 2008*, volume 5155 of *LNCS*, pages 232–248. Springer, 2008. Full version available at http://eprint.iacr.org/2008/010.

[Pat08b] Jacques Patarin. The "Coefficients H" Technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography - SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, 2008.

[Pat10a] Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. *IACR Cryptology ePrint Archive*, 2010:287, 2010.

[Pat10b] Jacques Patarin. Security of balanced and unbalanced Feistel Schemes with Linear Non Equalities. 2010. Available at http://eprint.iacr.org/2010/293.

[Pat13] Jacques Patarin. Security in $O(2^n)$ for the Xor of Two Random Permutations: Proof with the Standard H Technique. IACR Cryptology ePrint Archive, Report 2013/368, 2013. Available at http://eprint.iacr.org/2013/368.