Proof of Mirror Theory for $\xi_{\max} = 2$

Avijit Dutta[1] and Mridul Nandi[2] and Abishanka Saha[2]

Institute for Advancing Intelligence, TCG-CREST, Kolkata
Indian Statistical Institute, Kolkata

Abstract. In ICISC-05, and in the ePrint 2010/287, Patarin claimed a lower bound on the number of $2q$ tuples of n-bit strings $(P_1, \ldots, P_{2q}) \in (\{0,1\}^n)^{2q}$ satisfying $P_{2i-1} \oplus P_{2i} = \lambda_i$ for $1 \leq i \leq q$ such that $P_1, P_2, \ldots,$ P_{2q} are distinct and $\lambda_i \in \{0,1\}^n \setminus \{0^n\}$. This result is known as *Mirror theory* and widely used in cryptography. It stands as a powerful tool to provide a high-security guarantee for many block cipher-(or even ideal permutation-) based designs. In particular, Mirror theory has a direct application in the security of XOR of block ciphers. Unfortunately, the proof of Mirror theory contains some unverifiable gaps and several mistakes. This paper provides a simple and verifiable proof of Mirror theory.

Keywords: Mirror theory, Sum of Permutations, PRP, PRF, H-Coefficient Technique.

1 Introduction

Block ciphers, the workhorses of symmetric-key cryptography, are used in different modes of operations to provide solutions for data confidentiality, data integrity and authenticity etc. As most of the modes do not exploit the invertible property of the block cipher [2, 6, 23, 36], pseudo random function (or PRF) seems to be a more natural choice in such modes of operation. But unlike block ciphers, practical candidates for PRFs are rarely available. Although a block cipher is a good PRF, it can guarrantee only birthday bound security due to the PRF-PRP switching lemma [4, 7, 37]. To address the problem of converting a pseudorandom permutation (PRP) into a highly secure PRF, Bellare et al. [3] have designed several PRFs out of block ciphers in the name of *Luby-Rackoff backwards*. Among many such alternatives, xoring the outputs of two independent n-bit permutations, namely $\mathsf{XOR}_2(x) := \boldsymbol{\pi}(x) \oplus \boldsymbol{\pi}'(x)$, is one of them, where $\boldsymbol{\pi}$ and $\boldsymbol{\pi}'$ denote two n-bit independent random permutations, sampled uniformly and independently from the set of all permutations over the set $\{0,1\}^n$. Note that a random permutation is the ideal counter part of a block cipher, whereas a random function, (i.e., a function chosen randomly from the set of all functions over a finite domain and range), is the ideal counter part of a PRF. However, the authors of [3] did not give the security analysis of XOR_2 and its single-keyed variant $\mathsf{XOR}_1(x) := \boldsymbol{\pi}(0\|x) \oplus \boldsymbol{\pi}(1\|x)$. Popularity of these constructions have started gaining attention in the cryptographic community in the last few years due to their use in many important block cipher and tweakable block cipher-based designs that includes constructions like [11, 12, 15, 16, 18–21, 27, 28, 38–40].

History of XOR Function. In an unpublished work [1], Bellare et al. first showed that XOR_1 is a secure PRF up to $2^n/n$ queries. However, their analysis is incomplete and hard to verify. In [22], Lucks proved that XOR_2 achieves $2n/3$ bit PRF security. Afterwards, in a series of papers [33–35], Patarin claimed that XOR construction (i.e., both XOR_1 and XOR_2) is secured upto $O(2^n)$ queries. However, the correctness of the solutions proposed in [33–35] is debated in the community [10, 15]. In 2017, Dai et al. [10] have shown that XOR_1 and XOR_2 are optimally secure PRFs using the χ^2-method. In a related work, Cogliati et al. [8] have shown that XOR_k, i.e., xor of k independent permutations, for $k \geq 2$, achieves $kn/(k+1)$-bit PRF security.

Following Patarin's analysis, XOR_2 (resp. XOR_1) construction yields the following system of bivariate affine equations:

$$\mathbb{E}_\lambda = \{P_1 \oplus P_2 = \lambda_1, P_3 \oplus P_4 = \lambda_2, \ldots, P_{2q-1} \oplus P_{2q} = \lambda_q\},$$

where $q \geq 1$ and $\lambda := (\lambda_1, \ldots, \lambda_q)$ is a tuple of n-bit binary strings (for the XOR_1 construction, we additionally require that $\lambda_1, \ldots, \lambda_q$ are non-zero n-bit binary strings). The entire security analyses for both constructions stand on finding a good lower bound on the number of solutions $(P_1, \ldots, P_{2q})$ [1] to $\mathbb{E}_\lambda$ such that (i) for XOR_1 construction, we require that $P_i \neq P_j$ for $i \neq j$, while (ii) for XOR_2 construction, we require that (a) $P_i \neq P_j$ for $i \neq j$, where i, j both are odd, and (b) $P_x \neq P_y$ for $x \neq y$, where x and y both are even. Note that during the process of finding the solutions of $\mathbb{E}_\lambda$, assigning values to a variable P_i in $\mathbb{E}_\lambda$ fixes the value of exactly one variable (which is P_{i+1} if i is odd and P_{i-1} otherwise) in $\mathbb{E}_\lambda$. However, for a generic bivariate system of affine equations, one can see that assigning value to a single variable P_i might fix the values of more than just one other variable, say at most $k \geq 1$ variables in the set of equations. Patarin [34] named this notion the *block maximality* in a system of bivariate affine equations, denoted as $\xi_{\max}$. It is natural to see that the block maximality of the system of equations $\mathbb{E}_\lambda$ is 2 and thus the security analysis of the XOR construction is reduced to establish the following result.

"For a given system of bivariate affine equations over a finite group with non-equalities among the variables and $\xi_{\max} = 2$, the number of distinct solutions is always greater than the average number of solutions.".

Patarin named this result as **Theorem $P_i \oplus P_j$ for $\xi_{\max} = 2$** [30] (and later in [34], renamed it to *Mirror theory*). This theorem was stated as a conjecture in [29] and proved in [30]. However, in this paper, we refer to this result as **Mirror theory for $\xi_{\max} = 2$**. This result has been acknowledged in the community as a potential and a strong approach to establish the optimal security of XOR constructions (i.e., XOR_1 and XOR_2) [10].

[1] Abusing the notation, we use the same symbol to denote the variables and the solution of a given system of equations.

1.1 Mirror theory for $\xi_{\max} = 2$

Let $q \leq 2^n/134$ and $\lambda_1, \ldots, \lambda_q$ be non-zero n-bit strings. Patarin [34] showed that the number of solutions of distinct values to $P_1, \ldots, P_{2q}$ satisfying the bivariate affine equations $\mathbb{E}_\lambda$ is at least $\frac{(2^n)^{\underline{2q}}}{2^{nq}}$, where $a^{\underline{b}} := a(a-1)\cdots(a-b+1)$ for two positive integers $a \geq b$. Patarin [33] also showed that for any choice of n-bit strings $\lambda_1, \lambda_2, \ldots, \lambda_q$, the number of solutions to the system of bivariate affine equations $\mathbb{E}_\lambda$ such that $P_1, P_3, \ldots, P_{2q-1}$ are distinct and $P_2, P_4, \ldots, P_{2q}$ are distinct is at least

$$\frac{\left((2^n)^{\underline{q}}\right)^2}{2^{nq}} \times (1 - O(\frac{q}{2^n})).$$

Beside these two results, Patarin [30] also claimed the generic result for a general $\xi_{\max} > 2$, that the number of distinct solutions to a system of q bivariate affine equations with $\xi_{\max} > 2$ and with non-equality among the variables is always larger than the average number of solutions provided $q \leq 2^n/67 \cdot (\xi_{\max} - 1)$. Patarin named this result the "*Theorem $P_i \oplus P_j$ for any $\xi_{\max}$*". This result was stated as a conjecture (Conjecture 8.1 of [29]) in the context of analysing the security of the Feistel cipher. Only a couple of years later, this result was articulated in many follow-up works for analysing the security of the *xor of two permutations*, and it took a few articles [30, 33–35] for his result and security argument to evolve. Later, in 2017, this work culminated in a book [26] called *Feistel Ciphers: Security Proofs and Cryptanalysis* by Nachef et al. However, the proofs in most of these works are very sketchy, involve giants equations and are missing most of details.

1.2 Applications of Theorem $P_i \oplus P_j$ for any $\xi_{\max}$

Over the years, the Theorem $P_i \oplus P_j$ for any $\xi_{\max}$ has been proven to be a significant result in the context of analysing security bounds of numerous cryptographic designs. Apart from the stand-alone value of XOR_2 or XOR_1 constructions, they are used as a major component in many important block cipher and tweakable block cipher-based designs that includes [11,12,28,38–40]. However, the security proofs of most of these designs reveals the intermediate inputs of the construction to the distinguisher to get rid of the adaptive nature of the adversary. Hence the proof cannot use the fact that the sum function is a PRF. Instead, these security proofs require (by application of the H-Coefficient technique [31]) a good lower bound on the number of distinct solutions to a system of bivariate affine equations with a general $\xi_{\max}$ and therein comes the role of the result "Theorem $P_i \oplus P_j$ for any $\xi_{\max}$". It has also been used in proving the beyond birthday bound security of many nonce based MACs including [5,13–15,25]. Mennink [24] showed the optimal security bound of EWCDM using this result as the primary underlying tool, and Iwata et al. [17] also used it to show the optimal security bound of CENC. Despite the debate in the community regarding the correctness of the proof of "Theorem $P_i \oplus P_j$ for any $\xi_{\max}$" [30, 34], several authors have used this precarious result to derive an optimal bound for some constructions such as [17, 24, 41]. This triggers the need for a correct and verifiable proof of these two results, which will eventually help to correctly establish the security proof of the above constructions and improve their security.

Motivation. Bearing in mind the usefulness and the importance of this result in cryptography, this paper aims to fill in the gaps in the proof of *Mirror theory* (i.e., Theorem $P_i \oplus P_j$ for $\xi_{\max} = 2$), and thereby provide a complete proof. Although a verifiable proof for the Theorem $P_i \oplus P_j$ for any $\xi_{\max}$ would have been more useful in the cryptographic context, we believe that a correct proof for the Mirror theory will pave the way for a complete proof for general $\xi_{\max}$, which we leave as a future open problem. Recently, Cogliati and Patarin [9] have done a similar work. However, their approach and presentation is different from ours. We believe that two different proofs will help build confidence in the proof of Mirror theory.

1.3 H-Coefficient Technique

H-Coefficient technique serves as a "systematic" tool to upper bound the distinguishing advantage of any deterministic and computationally unbounded distinguisher $\mathscr{A}$ in distinguishing the real oracle $\mathscr{O}_1$ (construction of interest) from the ideal oracle $\mathscr{O}_0$ (idealized version). The collection of all the queries and responses that $\mathscr{A}$ made and received to and from the oracle, is called the *transcript* of $\mathscr{A}$, denoted as τ. Sometimes, we allow the oracle to release more internal information to $\mathscr{A}$ only after $\mathscr{A}$ completes all its queries and responses, but before it outputs its decision bit. We write $\mathscr{A}^{\mathscr{O}_1} \Rightarrow 1$ (resp. $\mathscr{A}^{\mathscr{O}_0} \Rightarrow 1$) to denote that $\mathscr{A}$ output decision bit 1 after it has completed its interaction with the oracle $\mathscr{O}_1$ (resp. $\mathscr{O}_0$). Note that, revealing extra informations will only increase the advantage of the distinguisher. We state the result of the H-Coefficient technique in upper bounding the PRF advantage of some keyed constructions, which will be used later in proving the PRF security of XOR_1 and XOR_2 constructions. Let $\mathscr{X}$ be any abirtrary countably infinite set and let $\mathsf{Func}(\mathscr{X}, \{0,1\}^n)$ be the set of all functions from $\mathscr{X}$ to $\{0,1\}^n$. We denote the real oracle $\mathscr{O}_1$ to be some family of keyed construction F from $\mathscr{X}$ to $\{0,1\}^n$ and $\mathscr{O}_0$ to be the random function RF uniformly sampled from $\mathsf{Func}(\mathscr{X}, \{0,1\}^n)$. Let X_{re} and X_{id} denote the transcript random variable induced by the interaction of $\mathscr{A}$ with the real oracle and the ideal oracle respectively. The probability of realizing a transcript τ in the ideal oracle (i.e., $\Pr[\mathsf{X}_{\mathrm{id}} = \tau]$) is called the *ideal interpolation probability*. Similarly, one can define the *real interpolation probability*. A transcript τ is said to be *attainable* with respect to $\mathscr{A}$ if the ideal interpolation probability is non-zero (i.e., $\Pr[\mathsf{X}_{\mathrm{id}} = \tau] > 0$). We denote the set of all attainable transcripts by Ω. Following these notations, we state the main result of H-Coefficient technique in Theorem 1. The proof of this theorem can be found in [32].

Theorem 1. *Suppose for some $\Omega_{\mathrm{bad}} \subseteq \Omega$, which we call the* bad *set of transcripts, the following conditions hold:*

1. $\mathsf{Pr}[\mathsf{X}_{\mathrm{id}} \in \Omega_{\mathrm{bad}}] \leq \epsilon_1$,

2. For any good transcript $\tau \in \Omega \backslash \Omega_{\text{bad}}$, *we have* $\mathsf{Pr}[\mathsf{X}_{\text{re}} = \tau] \geq (1-\epsilon_2) \cdot \mathsf{Pr}[\mathsf{X}_{\text{id}} = \tau]$.

Then, for any adversary $\mathscr{A}$, *we have*

$$\begin{aligned} \mathbf{Adv}_F^{\text{PRF}}(\mathscr{A}) &\overset{\text{def}}{=} |\mathsf{Pr}[\mathscr{A}^{F_K} \Rightarrow 1] - \mathsf{Pr}[\mathscr{A}^{\mathsf{RF}} \Rightarrow 1]| \\ &\leq \epsilon_1 + \epsilon_2, \end{aligned} \tag{1}$$

where the first probability is calculated over the randomness of $K \leftarrow_{\$} \mathscr{K}$ *and the second probability is calculated over the randomness of* $\mathsf{RF} \leftarrow_{\$} \mathsf{Func}(\mathscr{X}, \{0,1\}^n)$.

1.4 Our Contribution

The main contribution of this paper is to prove Mirror theory in a *simplified and verifiable* form. We prove two theorems of Mirror theory which are essentially restatements of its counting version in the terminology of probability. In the foregoing discussions, we assume that $\boldsymbol{\pi}$ and $\boldsymbol{\pi}'$ are two independently sampled n-bit uniform random permutations.

Theorem 2 (Single Permutation Mirror theory). *Let* $\gamma_1, \ldots, \gamma_q$ *be any non-zero n-bit strings and* $x_1, .x_2, \ldots, x_q$ *be distinct* $(n-1)$*-bit strings, where* $n \geq 12$ *and* $q \leq 2^n/58$. *Then the probability that*

$$\begin{cases} \boldsymbol{\pi}(x_1\|0) \oplus \boldsymbol{\pi}(x_1\|1) = \gamma_1 \\ \boldsymbol{\pi}(x_2\|0) \oplus \boldsymbol{\pi}(x_2\|1) = \gamma_2 \\ \vdots \quad \vdots \quad \vdots \\ \boldsymbol{\pi}(x_q\|0) \oplus \boldsymbol{\pi}(x_q\|1) = \gamma_q \end{cases}$$

holds is at least 2^{-nq}.

As an immediate application of the H-Coefficient technique [31] to the above theorem, one can see that the XOR_1 function behaves almost like a random function. For a distinguisher $\mathscr{A}$, the PRF advantage of a construction F, denoted as $\mathbf{Adv}_F^{\text{prf}}(\mathscr{A})$, denotes the distinguishing advantage from F to a function that returns random outputs on distinct queries.

Corollary 1. *For all* $q \leq 2^n/58$, $n \geq 12$ *and a distinguisher* $\mathscr{A}$ *making at most* q *queries, we have*

$$\mathbf{Adv}_{\mathsf{XOR}_1}^{\text{PRF}}(\mathscr{A}) \leq 1 - \left(1 - \frac{1}{2^n}\right)^q.$$

We defer the proof of the above corollary in Sect. 3.3, which actually gives a tight PRF bound $1-(1-2^{-n})^q$ of the XOR_1 construction. A simple distinguisher $\mathscr{A}$ returns 1 whenever it observes 0^n in any of the outputs. In the case of a random function, $\mathscr{A}$ returns 1 with probability exactly $1-(1-2^{-n})^q$, whereas $\mathscr{A}$ returns 1 with probability zero for the XOR_1 construction as the construction never returns 0.

As second contribution of the paper, we state the Mirror theory result for a pair of independent permutations as follows:

Theorem 3 (Independent Permutations Mirror theory). *Let $\gamma_1,, \ldots, \gamma_q$ be any non-zero n-bit strings and $x_1, \ldots, x_q$ be distinct n-bit strings where $n \geq 7$ and $q \leq 2^n/17$. Then the probability that*

$$\begin{cases} \boldsymbol{\pi}(x_1) \oplus \boldsymbol{\pi}'(x_1) = \gamma_1 \\ \boldsymbol{\pi}(x_1) \oplus \boldsymbol{\pi}'(x_1) = \gamma_1 \\ \vdots \quad \vdots \quad \vdots \\ \boldsymbol{\pi}(x_q) \oplus \boldsymbol{\pi}'(x_q) = \gamma_q \end{cases}$$

holds is at least $\left(1 - \frac{19q^2}{2^{2n}} - \frac{8n^3}{2^{2n}}\right) \frac{1}{2^{nq}}$.

As an application of H-Coefficient technique to Theorem 3, one can see that the XOR_2 function also behaves almost like a random function for all $q \leq 2^n/17$, where $n \geq 7$, as stated in the following corollary, proof of which is deferred in Sect. 6.2. This shows that the PRF advantage of the XOR_2 construction is at most $19q^2/2^{2n} + 8n^3/2^{2n}$.

Corollary 2. *For all $q \leq 2^n/17$, $n \geq 7$ and a distinguisher $\mathscr{A}$ making at most q queries, we have*

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{XOR}_2}(\mathscr{A}) \leq 19q^2/2^{2n} + 8n^3/2^{2n}.$$

Unlike the XOR_1 construction, we do not know of any tight matching attack for the XOR_2 construction. However, a simple distinguisher for XOR_2 (that makes 2^n distinct queries) returns 0 whenever it observes that the xor of the replies to its 2^n distinct queries is 0^n, and returns 1 otherwise.

Note that our proven PRF bound of XOR_2 is better than the existing bound already established in [33,35]. In fact, it also supersedes the bound $(q/2^n)^{1.5}, q \leq 2^n/16$, as proven by Dai et al. [10]. However, our bound is not yet proved tight because there is no known attack against XOR_2 that uses less than 2^n queries.

2 Recursive Inequality Lemma

For all positive integer j, $e^j \geq \frac{j^j}{j!}$ and so $1/j! \leq (e/j)^j$. Thus, for all $j \geq m/2$, we have

$$\binom{m}{j} \leq \frac{m^j}{j!} \leq (em/j)^j \leq (2e)^j. \tag{2}$$

Lemma 1 (Recursive Inequality Lemma).
Suppose $a_{d,\ell} \geq 0$ such that $a_{d,k} := 0$ for all $k < 0$ and for all $0 \leq d \leq 2n$ we have

$$a_{d,\ell} \leq \left(\frac{1}{4e}\right)^d \tag{3}$$

$$a_{d,\ell} \leq a_{d,\ell-1} + a_{d+1,\ell+1} + \frac{C}{2^n} \cdot \left(\frac{1}{4e}\right)^d \tag{4}$$

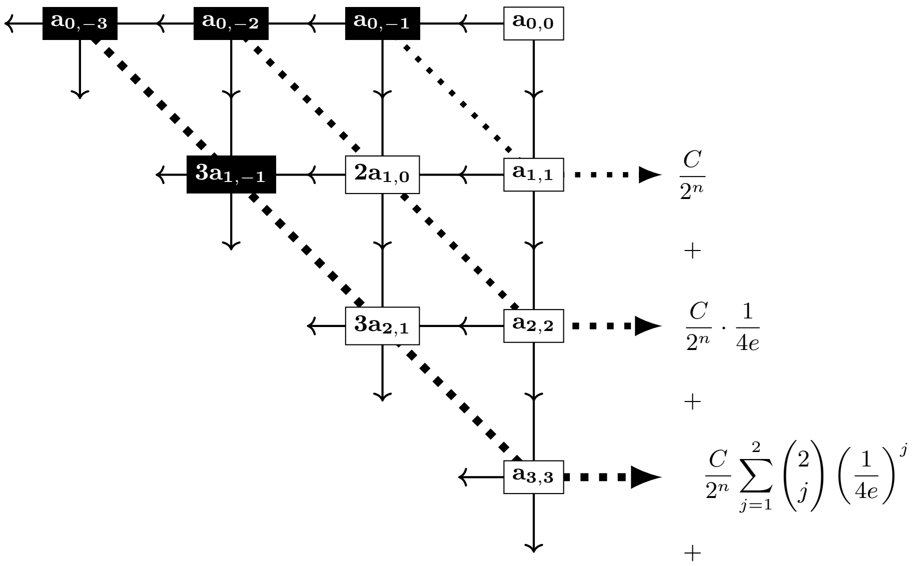

Fig. 2.1: The proof idea of the Recursive Inequality Lemma. The white terms in the black squares, in this pascal tree like structure are equal to zero. However, we keep them to achieve a compact coefficient $\binom{d_0}{i}$ due to our condition on the double sequence.

for some $C > 0$. Then

$$a_{0,0} \leq \frac{4C + 2}{2^n}.$$

<u>Proof Idea.</u> The *initial bound*, i.e., Eqn. (3) of $a_{d,\ell}$ says that $a_{0,0} \leq 1$. However, due to the *recursive inequality*, i.e., Eqn. (4), we show that $a_{0,0}$ has to be very small. The recursive inequality gives us $a_{0,0} = a_{1,1} + O(2^{-n})$. However, initial bound ensures $a_{1,1} \leq 1/4e$. Therefore, a single application of recursive inequality is not sufficient to conclude the desired bound. However, if we apply the recursive inequality twice before applying the initial bound, we have

$$\begin{aligned} a_{0,0} &= a_{1,0} + a_{2,2} + O(2^{-n}) \\ &= a_{2,1} + a_{2,2} + O(2^{-n}) = 2(1/4e)^2 + O(2^{-n}). \end{aligned}$$

So, we apply the recursive inequality several times before applying the bounds on a terms and we get an upper bound of $a_{0,0}$ of the form $M_d/(4e)^d + O(2^{-n})$ for some M_d. In the detailed proof we show that the constant term present in $O(2^{-n})$ do not blow up and the value of $M_d/(4e)^d = O(2^{-n})$ for $d = 2n$.

<u>Proof of Lemma 1.</u> We first state the following claim, which follows from iterated applications of the recursive inequality. A proof of the claim is deferred to the end of this section.

Claim 1. *For any* $0 \leq d_0 \leq 2n$*, we have*

$$a_{0,0} \leq \sum_{i=\lceil \frac{d_0}{2} \rceil}^{d_0} \binom{d_0}{i} a_{i,2i-d_0} + \frac{C}{2^n} \sum_{i=0}^{d_0-1} \sum_{j=\lceil \frac{i}{2} \rceil}^{i} \binom{i}{j} \left(\frac{1}{4e}\right)^j. \tag{5}$$

By plugging in the bound of each a-term from Eqn. (3) into the right hand side of Eqn. (5) and then using Eqn. (2) for each of the binomial coefficients, we get the following bound for all $d \leq 2n$.

$$a_{0,0} \leq \sum_{i=\lceil \frac{d}{2} \rceil}^{d} \left(2e \cdot \frac{1}{4e}\right)^i + \frac{C}{2^n} \sum_{i=0}^{d-1} \sum_{j=\lceil \frac{i}{2} \rceil}^{i} \left(2e \cdot \frac{1}{4e}\right)^j.$$

Now by using the inequality $\sum_{a \geq i} r^a \leq \frac{r^i}{1-r}$, we obtain

$$a_{0,0} \leq 2 \cdot 2^{-d/2} + \frac{2C}{2^n} \sum_{i=0}^{d-1} 2^{-i/2} \leq 2 \cdot 2^{-d/2} + \frac{4C}{2^n}.$$

By replacing $d = 2n$, we complete the proof of the lemma.
PROOF OF THE CLAIM : We prove the claim by induction on d_0. The result holds trivially for $d_0 = 1$ (by applying $d = \ell = 0$ in Eqn. (4)). Now we prove the statement for $d_0 + 1$, assuming it true for d_0. Therefore, we have

$$\begin{aligned} a_{0,0} &\leq \sum_{i=\lceil \frac{d_0}{2} \rceil}^{d_0} \binom{d_0}{i} a_{i,2i-d_0} + \frac{C}{2^n} \sum_{i=0}^{d_0-1} \sum_{j=\lceil \frac{i}{2} \rceil}^{i} \binom{i}{j} \left(\frac{1}{4e}\right)^j \\ &\leq \sum_{i=\lceil \frac{d_0}{2} \rceil}^{d_0} \binom{d_0}{i} \left(a_{i,2i-d_0-1} + a_{i+1,2i-d_0+1} + \frac{C}{2^n} \cdot \left(\frac{1}{4e}\right)^i \right) \\ &\quad + \frac{C}{2^n} \sum_{i=0}^{d_0-1} \sum_{j=\lceil \frac{i}{2} \rceil}^{i} \binom{i}{j} \left(\frac{1}{4e}\right)^j. \end{aligned} \tag{6}$$

For $i < \lceil (d_0+1)/2 \rceil$, $2i - (d_0+1) < 0$, and hence $a_{i,2i-(d_0+1)} = 0$. For $i > \lceil (d_0+1)/2 \rceil$, the coefficient of $a_{i,2i-(d_0+1)}$ in the above sum will be $\binom{d_0}{i-1} + \binom{d_0}{i}$, which is same as $\binom{d_0+1}{i}$ (see Fig. 2.1 for the recursive growth of coefficients). For $i = \lceil \frac{d_0+1}{2} \rceil$, the coefficient of $a_{i,2i-d_0-1}$ will be

$$\begin{cases} \binom{d_0}{i} & \text{if } d_0 \equiv 1 \pmod 2 \\ \binom{d_0}{i-1} + \binom{d_0}{i} & \text{if } d_0 \equiv 0 \pmod 2. \end{cases}$$

In both cases, the coefficient of $a_{i,2i-d_0-1}$ for $i = \lceil \frac{d_0+1}{2} \rceil$ is at most $\binom{d_0+1}{i}$. Using the above observation in Eqn. 6 the inductive step is proved.

Remark 1. The similar result is also achieved when the initial bound (i.e., Eqn. (3)) is replaced by $a_{d,\ell} \leq \beta^d$ for any constant $0 < \beta < 1$. However, we need that Eqn. (3) and Eqn. (4) hold for all $d \leq 2n/\log(\frac{1}{2e\beta})$.

3 Mirror theory for Single Permutation

In this section we prove Theorem 2. To do this, we first define a few notations, the notion of label and the probability of distinctness event. Followed by that, we state the main result of mirror theory for single permutation case (i.e., Lemma 2), which we used to prove Theorem 2. Finally, we conclude the section with a proof of Corollary 1.

NOTATIONS. For integers $a \le b$, the set $\{a, a+1, \cdots, b\}$ is denoted as $[a \ldots b]$ (or simply $[b]$, when $a = 0$ and $(b]$ when $a = 1$). We write $\mathsf{X} \leftarrow_{\$} S$ to mean that X is sampled uniformly from S and independent to all random variables defined so far. Similarly, we write $\mathsf{X}_1, \ldots, \mathsf{X}_s \leftarrow_{\$} S$ to mean that $\mathsf{X}_1, \ldots, \mathsf{X}_s$ are uniformly and independently distributed over S.

We write $\gamma^q := (\gamma_1, \ldots, \gamma_q)$ to denote a tuple of q elements and (γ_0, γ^q) to denote a tuple of $(q+1)$ elements respectively. For any tuple γ^q, we write $|\gamma^q| = q$ to denote its number of elements. For $i \in (q]$, we denote γ^q_{-i} to represent the tuple obtained after removing the i-th element γ_i from γ^q. Sometimes, we write a tuple simply as γ (instead of γ^q) without explicitly mentioning its number of elements. For two tuples γ, γ', we write $\gamma' \subseteq \gamma$ (we also call γ' is a sub-tuple of γ), if there are indices $i_1, i_2, \ldots, i_\beta$ with $1 \le i_1 < \cdots < i_\beta \le |\gamma|$ such that $\gamma' = (\gamma_{i_1}, \ldots, \gamma_{i_\beta})$.

3.1 Probability of Distinctness Event

Let $\mathscr{S} := \{\rho_1, \ldots, \rho_\ell\}$ be a set (possibly empty, i.e. $\ell = 0$) of non-zero n-bit strings and $\gamma^q = (\gamma_1, \ldots, \gamma_q)$ be a tuple of non-zero n-bit strings. We call the pair $\tau = (\gamma^q, \mathscr{S})$ *an (ℓ-linked) label.* The elements of γ^q will be called the *base elements* and that of $\mathscr{S}$ will be called the *linked elements.* Let $\mathsf{R}_0, \mathsf{R}_1, \ldots, \mathsf{R}_q \leftarrow_{\$} \{0,1\}^n$ and $\mathsf{R}'_i \overset{\text{def}}{=} \mathsf{R}_i \oplus \gamma_i$ for all $i \in (q]$. We now define the distinctness event $\mathsf{dist}(\tau)$ (or $\mathsf{dist}(\tau \mid (\mathsf{R}_0, \mathsf{R}^q))$ to emphasize the random source) corresponding to the label τ as follows:

1. **Case $\mathscr{S} \ne \varnothing$:** $\mathsf{dist}(\tau)$ is true if the following elements are distinct
$$\mathsf{R}_0, \ldots, \mathsf{R}_q, \mathsf{R}'_1, \ldots, \mathsf{R}'_q, \mathsf{R}_0 \oplus \rho_1, \ldots, \mathsf{R}_0 \oplus \rho_\ell.$$
2. **Case $\mathscr{S} = \varnothing$:** $\mathsf{dist}(\tau)$ is true if $\mathsf{R}_0, \ldots, \mathsf{R}_q, \mathsf{R}'_1, \ldots, \mathsf{R}'_q$ are distinct. Alternatively, we call $\tau = (\gamma^q, \varnothing)$ as a 0-*linked label.*

We write the probability of the distinctness event as follows:

$$\mathsf{P}(\tau) := \Pr(\mathsf{dist}(\tau \mid (\mathsf{R}_0, \mathsf{R}^q))).$$

1-LINKED LABEL. A 1-linked label $\tau = (\gamma^q, \mathscr{S} = \{\rho_1\})$ with q base elements is simply represented by a tuple $(\rho_1, \gamma_1, \ldots, \gamma_q)$. Similarly, a tuple γ^q can be equivalently viewed as a 1-linked label $\tau = (\gamma^q_{-1}, \{\gamma_1\})$. A tuple $\gamma^1 = (\gamma_1)$ is viewed as a 1-linked label $\tau = (\varnothing, \{\gamma_1\})$ consisting of zero base element and one link element γ_1. It is easy to see that the probability of distinctness $\mathsf{P}(\gamma^q, \mathscr{S})$ and

$\mathsf{P}(\gamma^q)$ (for 1-linked label) do not depend on the order of the tuple γ. Moreover, it is also to be noted that the distinctness event for a zero-linked label $(\gamma^q, \varnothing)$ and a 1-linked label γ^q are not same and thus the presence of the empty set is crucial. Having defined the notion of probability of distinctness and 1-linked label, we are now ready to state the main theorem of mirror theory for the single permutation case.

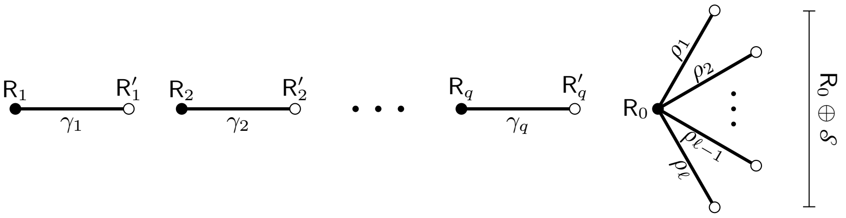

Fig. 3.1: Graphical representation of the distinctness event for an ℓ-linked label $\tau = (\gamma^q, \mathcal{S})$, where $\mathcal{S} = \{\rho_1, \cdots, \rho_\ell\}$. The vertices are the random variables and the label of edges are the base elements and link elements. The black vertices denote the n-bit numbers sampled independently and uniformly at random and the white vertices are the derived random variables. Thus, the graph actually represents $\mathsf{dist}(\tau)$ as all the vertices are distinct.

Lemma 2 (Main Result for Single Permutation). *For all* $1 \leq q \leq 2^n/58$, $n \geq 12$ *and 1-linked label* γ^q*, we have*

$$\mathsf{P}(\gamma^q) \geq \frac{(2^n)_{\underline{2q}}}{(2^n)^{2q}}. \tag{7}$$

3.2 Proof of Theorem 2

Using Lemma 2, we can now prove Theorem 2. Let $\gamma_1, \ldots, \gamma_q$ be any non-zero n-bit strings and $x_1, x_2, \ldots, x_q$ be distinct $(n-1)$ bits strings where $n \geq 12$ and $q \leq 2^n/58$. Let

$$\mathsf{P} := \mathsf{Pr}(\boldsymbol{\pi}(x_1\|0) \oplus \boldsymbol{\pi}(x_1\|1) = \gamma_1, \ldots, \boldsymbol{\pi}(x_q\|0) \oplus \boldsymbol{\pi}(x_q\|1) = \gamma_q),$$

where $\boldsymbol{\pi}$ denotes an n-bit random permutation. Let A be the set of all $\mathsf{z} := (z_1, \cdots, z_q) \in (\{0,1\}^n)^q$ such that $z_1, z_1 \oplus \gamma_1, \cdots, z_q, z_q \oplus \gamma_q$ are all distinct. Then we have $\mathsf{P} = \frac{|A|}{(2^n)_{\underline{2q}}}$. Moreover, we also have $\mathsf{P}(\gamma^q) = \frac{|A|}{2^{nq}}$. Combining these two, Theorem 2 immediately follows from Lemma 2.

3.3 Proof of Corollary 1

Let $\tau = \{(x_1, y_1), (x_2, y_2), \ldots, (x_q, y_q)\}$ be the transcript that result from the interaction between $\mathscr{A}$ and the corresponding oracle, where $x_i \in \{0,1\}^{n-1}$ is the

i-th query of $\mathscr{A}$ and y_i is the corresponding response. We call τ a *bad transcript* if there exists at least one $i \in [q]$ such that $y_i = 0^n$. Otherwise, τ is said to be a *good transcript.*

According to the H-Coefficient technique, we bound the probability of the occurence of bad transcripts in the ideal world. Let X_{re} (resp. X_{id}) be the random variable that takes the transcript induced by the real world (resp. ideal world) distribution. Let Ω_{bad} denotes the set of all bad transcripts. Then, we have

$$\begin{aligned}\mathsf{Pr}[\mathsf{X}_{\mathrm{id}} \in \Omega_{\mathrm{bad}}] &= \Pr[\exists i \text{ such that } y_i = 0^n] \\ &= 1 - \mathsf{Pr}[\forall i \text{ such that } y_i \neq 0^n] \\ &\overset{(1)}{=} 1 - (1 - 2^{-n})^q, \qquad (8)\end{aligned}$$

where (1) follows as the y_i's are independently and uniformly sampled in the ideal world. Therefore, for a good transcript τ, each y_i is a non-zero n-bit string. Therefore, for a good transcript $\tau = \{(x_1, y_1), (x_2, y_2), \ldots, (x_q, y_q)\}$, which is realized in the real world, we can write

$$\mathscr{E} = \begin{cases} \boldsymbol{\pi}(0\|x_1) \oplus \boldsymbol{\pi}(1\|x_1) = y_1 \\ \boldsymbol{\pi}(0\|x_2) \oplus \boldsymbol{\pi}(1\|x_2) = y_2 \\ \quad\vdots \quad\quad \vdots \quad\quad \vdots \quad\quad\quad \vdots \\ \boldsymbol{\pi}(0\|x_q) \oplus \boldsymbol{\pi}(1\|x_q) = y_q. \end{cases}$$

Computing the real interpolation probability for a good transcript τ, i.e., computing $\mathsf{Pr}[\mathsf{X}_{\mathrm{re}} = \tau]$, is equivalent to counting the number of permutations $\boldsymbol{\pi}$ satisfying $\mathscr{E}$. Note that, as τ is a good transcript, this number is at least $(2^n)_{2q}/2^{nq}$ that follows from our main theorem of the paper as we are dealing with $\xi_{\max} = 2$. Therefore,

$$\mathsf{Pr}[\mathsf{X}_{\mathrm{re}} = \tau] \geq \frac{1}{2^{nq}} = \mathsf{Pr}[\mathsf{X}_{\mathrm{id}} = \tau].$$

Thus, the ratio of real to ideal interpolation probability becomes at least 1. Hence, by the result of H-Coefficient technique,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XOR}_1}(\mathscr{A}) \leq 1 - (1 - 2^{-n})^q,$$

which proves the result.

4 Proof of Lemma 2

To complete the proof of the Mirror theory for the single permutation case, it now only remains to prove Lemma 2. To do this, we first establish the relationship between the probabilities of the distinctness event between related labels through Lemma 3 and Lemma 4. Followed by that, we introduce the notion of *"link-deletetion operation"* and the *"Link-Deletion Lemma"*(i.e., Lemma 5), which enables us to express the probability of the distinctness event of a ℓ-linked label in terms of the probability of the distinctness event of $(\ell - 1)$-linked label. These results together will suffice for stating the *"Core Lemma"*, which will be used to prove Lemma 2.

4.1 Probabilities of Distinctness for Related Labels

In this section, we establish the relationship of the probabilities of distinctness between a 0-linked label $(\gamma^q, \varnothing)$ and a 1-linked label γ^q. We also establish the relationship of the probabilities of distinctness between two 1-linked labels such that one is a sub-tuple of the other. Note that, for the 0-linked label, the distinctness event implies $\mathsf{R}_0, \mathsf{R}_1, \mathsf{R}_1 \oplus \gamma_1, \ldots, \mathsf{R}_q, \mathsf{R}_q \oplus \gamma_q$ are distinct, whereas for the 1-linked label γ^q, the distinctness event implies $\mathsf{R}_1, \mathsf{R}_1 \oplus \gamma_1, \ldots, \mathsf{R}_q, \mathsf{R}_q \oplus \gamma_q$ are distinct [2]. Thus, $\mathsf{dist}((\gamma^q, \varnothing) \mid (\mathsf{R}_0, \mathsf{R}^q))$ holds if and only if $\mathsf{dist}(\gamma^q \mid \mathsf{R}^q)$ and $\mathsf{R}_0 \notin \{\mathsf{R}_1, \mathsf{R}'_1, \ldots, \mathsf{R}_q, \mathsf{R}'_q\}$. By using the independence of R_0, the following result follows.

Lemma 3 (1-link-0-link). *Let $\tau = (\gamma^q, \varnothing)$ be a 0-linked label and γ^q be a 1-linked label. Then*

$$\mathsf{P}(\gamma^q, \varnothing) = \left(1 - \frac{2q}{2^n}\right) \cdot \mathsf{P}(\gamma^q).$$

Lemma 4 (1-link-1-link). *Let λ^q be a 1-linked label and let γ^{q-d} be a 1-linked label such that $\gamma^{q-d} \subseteq \lambda^q$. Then*

$$\mathsf{P}(\gamma^{q-d}) \leq \mathsf{P}(\lambda^q) / \left(1 - \frac{4q}{2^n}\right)^d. \tag{9}$$

Let $\tau = (\gamma^{q-d}, \mathcal{S})$ be a label such that there exists $x, y \in \mathcal{S}$ with $(\gamma_0, \gamma^{q-d}) \subseteq \lambda^q$ with $\gamma_0 = x \oplus y$. Then

$$\mathsf{P}(\gamma^{q-d}, \mathcal{S}) \leq \mathsf{P}(\lambda^q) / \left(1 - \frac{4q}{2^n}\right)^{d-1}. \tag{10}$$

Proof. If $d = 0$, the statement is trivial, because the tuple γ^q is a reordering of the tuple λ^q and hence we have $\mathsf{P}(\gamma^q) = \mathsf{P}(\lambda^q)$. For $d > 0$, we prove the statement as follows. Since $\gamma^{q-d} \subseteq \lambda^q$, there exists $1 \leq i_1 < i_2 < \cdots < i_{q-d} \leq q$, such that $\gamma^{q-d} = (\lambda_{i_1}, \cdots, \lambda_{i_{q-d}})$. We take any $z \in \lambda^q \setminus \gamma^{q-d}$, that is any $z = \lambda_i$ for $i \neq i_1, \cdots, i_{q-d}$. By setting $\gamma_0 = z$, we compare $\mathsf{P}(\gamma^{q-d})$ and $\mathsf{P}((\gamma_0, \gamma^{q-d}))$. Given that the event $\mathsf{dist}(\gamma^{q-d} \mid \mathsf{R}^{q-d})$ holds, the event $\mathsf{dist}((\gamma_0, \gamma^{q-d}) \mid (\mathsf{R}_0, \mathsf{R}^{q-d}))$ holds true if and only if both R_0 and $\mathsf{R}_0 \oplus \gamma_0$ are not the members of the set

$$\{\mathsf{R}_1, \mathsf{R}'_1, \ldots, \mathsf{R}_{q-d}, \mathsf{R}'_{q-d}\}.$$

[2] Note that as per the definition of an 1-linked label, γ^q is defined as $\gamma^q = ((\gamma_2, \gamma_3, \ldots, \gamma_q), \{\gamma_1\})$ and therefore $\mathsf{dist}(\gamma^q)$ is the event that $(\mathsf{R}_0, \mathsf{R}_1, \ldots, \mathsf{R}_{q-1}, \mathsf{R}_1 \oplus \gamma_2, \ldots, \mathsf{R}_{q-1} \oplus \gamma_{q-1}, \mathsf{R}_0 \oplus \gamma_1)$ are all distinct. Note that, this representation of the event $\mathsf{dist}(\gamma^q)$ is equivalent to the event defined here. We have sampled q random values $\mathsf{R}_1, \ldots, \mathsf{R}_q$ such that all of them are distinct and also $(\mathsf{R}_2 \oplus \gamma_2, \ldots, \mathsf{R}_q \oplus \gamma_q, \mathsf{R}_1 \oplus \gamma_1)$ are also distinct.

Therefore, for a given choice of values assigned to $\mathsf{R}_1, \ldots, \mathsf{R}_{q-d}$, the number of choices of value assigned to R_0 is at least $2^n - 4(q-d)$. Hence,

$$\begin{aligned} \mathsf{P}((\gamma_0, \gamma^{q-d})) &\geq \mathsf{P}(\gamma^{q-d}) \times \left(1 - \frac{4(q-d)}{2^n}\right) \\ &\geq \mathsf{P}(\gamma^{q-d}) \times \left(1 - \frac{4q}{2^n}\right). \end{aligned} \tag{11}$$

By inserting d elements of the tuple $\lambda^q \setminus \gamma^{q-d}$, one by one in the above manner, into γ^{q-d}, we obtain a re-ordered copy of λ^q, which has the same probability of distinctness as λ^q. Thus the first part of the lemma (i.e., Eqn. (9)) immediately follows from Eqn. (11) by applying it successively for d times.

To prove the second part of the lemma, we would like to note that

$$\mathsf{P}(\tau) \leq \mathsf{P}(\gamma^{q-d}, \{x, y\})) \leq \mathsf{P}(\gamma^{q-d}, \{x \oplus y\}). \tag{12}$$

If $\mathsf{R}_0, \mathsf{R}_1, \cdots, \mathsf{R}_{q-d}$ are uniformly and independently distributed over $\{0,1\}^n$, then for any $x \in \{0,1\}^n$, $\mathsf{R}_0 \oplus x, \mathsf{R}_1, \cdots, \mathsf{R}_{q-d}$ are also uniformly and independently distributed over $\{0,1\}^n$. Letting $\mathsf{R}_0^* := \mathsf{R}_0 \oplus x$, $\mathsf{dist}(\gamma^{q-d}, \{x, y\})$ is the event of distinctness of $\mathsf{R}_1, \mathsf{R}'_1, \cdots, \mathsf{R}_{q-d}, \mathsf{R}'_{q-d}, \mathsf{R}_0^*, \mathsf{R}_0^* \oplus x, \mathsf{R}_0^* \oplus x \oplus y$, while $\mathsf{dist}(\gamma^{q-d}, \{x \oplus y\})$ is the event of distinctness of $\mathsf{R}_1, \mathsf{R}'_1, \cdots, \mathsf{R}_{q-d}, \mathsf{R}'_{q-d}, \mathsf{R}_0^*, \mathsf{R}_0^* \oplus x \oplus y$. Thus, $\mathsf{dist}(\gamma^{q-d}, \{x, y\}) \subseteq \mathsf{dist}(\gamma^{q-d}, \{x \oplus y\})$. Hence, we have the second inequality of Eqn. (12). Since $(\gamma^{q-d}, x \oplus y) \subseteq \lambda^q$ is a 1-linked label, of size $(q-d+1)$, the second part now follows from the first part of the lemma.

<u>Link-Deletion Operation.</u> Let $\tau = (\gamma^q, \mathcal{S})$ be an ℓ-linked label with $\ell \geq 1$. For every $x \in \mathcal{S}$, we define the following set:

$$I_{x,\tau} := \{i \in (q] : \gamma_i \oplus x \notin \mathcal{S} \cup 0^n\}.$$ [3]

Now, for every $x \in \mathcal{S}$ and for every $i \in I_{x,\tau}$, we define the following set:

$$\mathcal{S}_{x,i} := \mathcal{S} \cup \{x \oplus \gamma_i\}.$$

For a given ℓ-linked label $\tau = (\gamma^q, \mathcal{S})$ and for $i \in I_{x,\tau}$, we define $(\ell+1)$-linked label $\tau_{i \to x} := (\gamma^q_{-i}, \mathcal{S}_{x,i})$, which signifies the deletion of the i-th base element and xor it with the link element x and finally included the result in $\mathcal{S}$. Similarly, for $x \in \mathcal{S}$, we define the label τ_{-x} to denote the pair $(\gamma^q, \mathcal{S} \setminus \{x\})$, which signifies the deletion of a link element from $\mathcal{S}$. A graphical representation of both of these notions are depicted in Fig. 4.1.

Lemma 5 (Link-Deletion Lemma). *Let τ be an ℓ-linked label. Then, for all $x \in \mathcal{S}$ and following the above notations, we have*

$$\mathsf{P}(\tau) = \mathsf{P}(\tau_{-x}) - \frac{1}{2^{n-1}} \sum_{i \in I_x} \mathsf{P}(\tau_{i \to x})$$

[3] We often write the set as I_x, omitting the label τ, whenever it is clear from the context.

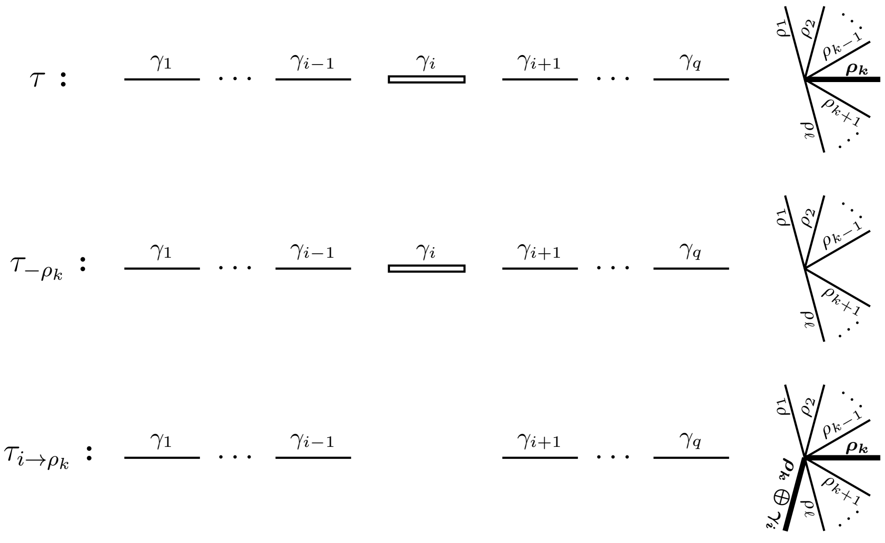

Fig. 4.1: Upper part of the figure depicts the graphical view of a linked label, which is made up of a finite collection of disjoint edges, called the *base edges* and a star component, whose edges are called the *linked edges*. Middle part of the figure depicts the graphical view when the bold link edge of the star component with label ρ_k, is removed. The lower part of the figure depicts the graph when the hollow base edge with label γ_i is deleted and a bold link edge with label $\gamma_i \oplus \rho_k$ is added to the star component.

Proof. From the definition, it is obvious that $\mathsf{dist}(\tau_{-x})$ is true whenever $\mathsf{dist}(\tau)$ is true. So $\mathsf{dist}(\tau_{-x}) \setminus \mathsf{dist}(\tau)$ [4] holds if and only if $\mathsf{dist}(\tau_{-x})$ holds and for some $i \in I_x$, $\mathsf{R}_0 \oplus x \in \{\mathsf{R}_i, \mathsf{R}'_i\}$. Clearly, these cannot happen simultaneously for more than one i and so we can write

$$
\begin{aligned}
&\Pr\left(\mathsf{dist}(\tau_{-x}) \setminus \mathsf{dist}(\tau)\right) = \mathsf{P}(\tau_{-x}) - \mathsf{P}(\tau) \\
&= \sum_{i \in I_x} \mathsf{Pr}(\underbrace{\mathsf{dist}(\tau_{-x}) \wedge \mathsf{R}_i \oplus \mathsf{R}_0 = x}_{\mathsf{E}_i}) \\
&+\mathsf{Pr}(\underbrace{\mathsf{dist}(\tau_{-x}) \wedge \mathsf{R}'_i \oplus \mathsf{R}_0 = x}_{\mathsf{E}'_i}). \qquad (13)
\end{aligned}
$$

Note that the event E_i implies that the elements of $\mathsf{R}_0 \oplus (\mathcal{S} \setminus x)$ and the elements $\mathsf{R}_0 \oplus x, \mathsf{R}_0 \oplus x \oplus \gamma_i$, $\mathsf{R}_j, \mathsf{R}'_j$ for $j \in \{1, 2, \ldots, q\} \setminus i$ are distinct. In other words, E_i is equivalent to the event that (1) $\mathsf{dist}(\gamma^q_{-i}, \mathcal{S}_{x,i})$ holds for the random source $\mathsf{R}_0, \mathsf{R}_1, \ldots, \mathsf{R}_{i-1}, \mathsf{R}_{i+1}, \ldots, \mathsf{R}_q$ and (2) $\mathsf{R}_i = \mathsf{R}_0 \oplus x$. Since these two events are independent we have $\mathsf{Pr}(\mathsf{E}_i) = \mathsf{Pr}(\mathsf{dist}(\tau_{i \to x})) \times 2^{-n}$. Similarly, we have the probability for the event E'_i and this proves the lemma.

[4] This notation denotes the set difference of two events $\mathsf{dist}(\tau_{-x})$ and $\mathsf{dist}(\tau)$.

By applying Lemma 5 to a 1-linked label $\tau = (\gamma^q, \{\gamma_0\})$ (equivalently $\tau = (\gamma_0, \gamma^q)$), we have

$$\mathsf{P}((\gamma_0, \gamma^q)) = \mathsf{P}(\gamma^q, \varnothing) - \frac{1}{2^{n-1}} \sum_{i \in I_{\gamma_0}} \mathsf{P}((\gamma_0, \gamma^q)_{i \to \gamma_0}). \tag{14}$$

<u>Multiplicity.</u> Given $x \in \{0,1\}^n$ and a tuple γ of n-bit strings, we define the following two quantities:

$$(a)\ \delta_\gamma(x) = \#\{i \in (|\gamma|] \mid \gamma_i = x\}, \quad (b)\ \Delta_\gamma := \max_{x \in \{0,1\}^n} \delta_\gamma(x).$$

In words, (a) refers to the multiplicity of the element x in the tuple γ and (b) refers to the maximum multiplicity of the tuple γ, where the maximum is taken over all the n-bit strings. We now state the "*Core Lemma*", which is used to prove our main theorem. We defer its proof in Sect. 5.

Lemma 6 (Core Lemma). *Let* (γ_0, γ^q) *with* $q \geq 2n$ *be any* 1*-linked label. Then, following the notations above, we have*

$$\mathsf{P}((\gamma_0, \gamma^q)_{i \to \gamma_0}) \leq \mathsf{P}(\gamma^q, \varnothing) \left(1 + \frac{29\Delta_{(\gamma_0, \gamma^q)}}{2^n}\right). \tag{15}$$

4.2 Resuming the Proof of Lemma 2

Having stated the Core Lemma and the Link-Deletion Lemma, our stage is now set for proving Lemma 2. Note that for any non-zero n-bit binary string γ_1, the 1-linked label γ^1 is viewed as having zero base element and one link element γ_1. Therefore, $\mathsf{P}(\gamma^1)$ implies the probability that the random variables R_0 and $\mathsf{R}'_0 \overset{\text{def}}{=} \mathsf{R}_0 \oplus \gamma_1$ are distinct, which occurs with probability 1 and hence $\mathsf{P}(\gamma^1) = 1$ and so the statement is true for $q = 1$, which proves the base case of the induction. We now show that for each q such that $1 \leq q \leq 2^n/58$, the following inequality holds:

$$\begin{aligned} \frac{\mathsf{P}(\gamma^{q+1})}{\mathsf{P}(\gamma^q)} &\geq \left(1 - \frac{2q}{2^n}\right)\left(1 - \frac{2q+1}{2^n}\right) \\ &= \frac{(2^n - 2q)(2^n - 2q - 1)}{2^{2n}}. \end{aligned}$$

For the notational purpose, we prove the following inequality as we know that the probability of distinctness for 1-linked label does not depend on the order of the tuple.

$$\frac{\mathsf{P}((\gamma_0, \gamma^q))}{\mathsf{P}(\gamma^q)} \geq \left(1 - \frac{2q}{2^n}\right)\left(1 - \frac{2q+1}{2^n}\right).$$

We prove the inequality in two steps. In the first step, we prove it for all $q \leq 2n$ and in the second step we prove for all q such that $2n \leq q \leq 2^n/58$ holds.

First Step: By setting $d = 0$ in Eqn. (11), we have

$$\frac{\mathsf{P}((\gamma_0, \gamma^q))}{\mathsf{P}(\gamma^q)} \geq \left(1 - \frac{4q}{2^n}\right) \geq \left(1 - \frac{2q}{2^n}\right)\left(1 - \frac{2q+1}{2^n}\right),$$

where the last inequality follows from the condition $q \leq 2^{\frac{n}{2}-1} - 1$. Note that $n \geq 12$ implies $2n < 2^{n/2-1}$ and so our claim is true for all $q \leq 2n$.

Second Step: Let (γ_0, γ^q) be a 1-linked label with q base elements such that $q \geq 2n$. Recall that, I_{γ_0} is the set of all $i \in (q]$ such that $\gamma_i \neq \gamma_0$. As the probability of distinctness does not depend on the order of the elements of the label, we rearrange the elements in the label in such a way so that $\Delta := \Delta_{(\gamma_0,\gamma^q)} = \delta + 1$ is achieved. Let $|I_{\gamma_0}| = q - \Delta + 1$, where $\delta := \delta_{\gamma^q}(\gamma_0)$. By applying Eqn. (14) and Lemma 6, we can bound $\mathsf{P}((\gamma_0, \gamma^q))$ from below as follows:

$$\begin{aligned}
\mathsf{P}((\gamma_0, \gamma^q)) &\overset{(a)}{=} \mathsf{P}(\gamma^q, \varnothing) - \frac{1}{2^{n-1}} \sum_{i \in I_{\gamma_0}} \mathsf{P}((\gamma_0, \gamma^q)_{i \to \gamma_0}) \\
&\overset{(a)}{\geq} \mathsf{P}(\gamma^q, \varnothing) - \frac{1}{2^{n-1}} \sum_{i \in I_{\gamma_0}} \mathsf{P}(\gamma^q, \varnothing)(1 + 29\Delta/2^n) \\
&= \mathsf{P}(\gamma^q, \varnothing)\left(1 - \frac{q - \Delta + 1}{2^{n-1}}\left(1 + \frac{29\Delta}{2^n}\right)\right) \\
&\overset{(b)}{\geq} \mathsf{P}(\gamma^q)\left(1 - \frac{2q}{2^n}\right)\left(1 - \frac{q - \Delta + 1}{2^{n-1}}\left(1 + \frac{29\Delta}{2^n}\right)\right) \\
&\geq \mathsf{P}(\gamma^q)\left(1 - \frac{2q}{2^n}\right)\left(1 - \frac{2q+1}{2^n}\right),
\end{aligned}$$

where (a) follows from Eqn. 14, (b) follows from Lemma 6 and (c) follows from Lemma 3. Moreover, the last inequality follows as $q \leq \frac{2^n}{58}$, $\Delta \geq 1$ and the simplification as given below

$$\frac{q - \Delta + 1}{2^{n-1}}\left(1 + \frac{29\Delta}{2^n}\right) \leq \frac{2q+1}{2^n}.$$

5 Proof of Core Lemma (Lemma 6)

To prove the Core Lemma, it is sufficient to prove the following upper bound

$$|\mathsf{P}((\gamma_0, \gamma^q)_{i \to \gamma_0}) - \mathsf{P}(\gamma^q, \varnothing)| \leq \frac{29\Delta_{(\gamma_0,\gamma^q)} \cdot \mathsf{P}(\gamma^q, \varnothing)}{2^n}, \qquad (16)$$

where (γ_0, γ^q) is a 1-linked label. Before we prove Eqn. (16), we first identify the relationship between $(\gamma_0, \gamma^q)_{i \to \gamma_0} = (\gamma^q_{-i}, \{\gamma_0, \gamma_0 \oplus \gamma_i\})$ and $(\gamma^q, \varnothing)$. The label $(\gamma_0, \gamma^q)_{i \to \gamma_0}$ contains two linked elements γ_0 and $\gamma_0 \oplus \gamma_i$ whose sum is γ_i. Now, if we remove these two linked elements and include their xor to the tuple of the base elements, we obtain $(\gamma^q, \varnothing)$. We generalize the above notion for any ℓ-linked label $\tau = (\lambda^\alpha, \mathcal{S})$. In order to do this, we introduce the notion of *double-link separation* as follows:

Double Link Separation Operation. For a given ℓ-linked label $\tau = (\lambda^\alpha, \mathcal{S})$ such that $x, y \in \mathcal{S}$, we define the double-link separation operation (see Fig. 5.1) as

$$\tau_{-(x,y)} := ((\lambda_1, \ldots, \lambda_\alpha, \lambda_{\alpha+1} := x \oplus y), \mathcal{S} \setminus \{x, y\}).$$

The notion of double-link separation operation leads us to define the *"differential term"* as follows:

Definition 1 (Differential Term). *For a positive integer q, for all $\ell \geq 0$ and $1 \leq \alpha \leq q$, we define*

$$D(\alpha, \ell) = \max_{\tau,x,y} \left|\mathsf{P}(\tau) - \mathsf{P}(\tau_{-(x,y)})\right|, \tag{17}$$

where the maximum is taken over all $\tau := (\lambda^{\alpha-1}, \mathcal{S})$ and $x, y \in \mathcal{S}$ such that $|\mathcal{S}| = \ell + 2$ and $(\lambda_1, \ldots, \lambda_{\alpha-1}, x \oplus y) \subseteq \gamma^q$. For all $\ell < 0$, we define $D(\alpha, \ell) = 0$.

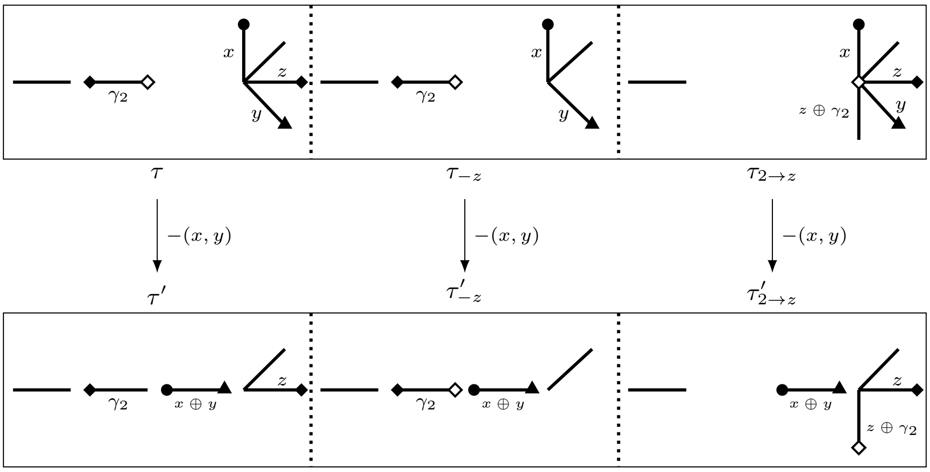

Fig. 5.1: Graphical view of the double-link separation. The extreme left figure depicts the separation of double-links (x, y) results to a graph with a star component having no link-edges with label x and y and include their xor (i.e., $x \oplus y$) as the label of a base edge. A similar view is depicted for the middle and the extreme right figures.

We recall that for a fixed integer $q \geq 2n$, (γ_0, γ^q) is a 1-linked label. Let $\beta := 2q/2^n$, and for all $0 \leq d \leq q$, and $\ell \leq 2d - 1$, we write $\alpha = q - d$. Finally, we define a double sequence $a_{d,\ell}$ as follows:

$$a_{d,\ell} := \frac{\beta^d}{2\mathsf{P}(\gamma^q)} \times D(\alpha, \ell).$$

Now we state the following claim which establishes the following upper bound on $a_{0,0}$ as follows:

Claim.

$$a_{0,0} \leq \frac{14\mathit{\Delta}_{(\gamma_0,\gamma^q)}}{2^n}. \tag{18}$$

Proof of Eqn. (16). We complete the proof of Eqn. (16) using the above claim as follows:

$$\begin{aligned} |\mathsf{P}((\gamma_0,\gamma^q)_{i\to\gamma_0}) - \mathsf{P}(\gamma^q,\varnothing)| &\leq D(q,0) \\ &\leq \frac{28\mathit{\Delta}_{(\gamma_0,\gamma^q)}\cdot\mathsf{P}(\gamma^q)}{2^n} \\ &\leq \frac{29\mathit{\Delta}_{(\gamma_0,\gamma^q)}\cdot\mathsf{P}(\gamma^q,\varnothing)}{2^n}, \end{aligned}$$

where the second inequality follows since $D(q,0) = a_{0,0} \times 2\mathsf{P}(\gamma^q)$ and the last inequality follows since $\mathsf{P}(\gamma^q) = \mathsf{P}(\gamma^q,\varnothing)/(1-2q/2^n) \leq \frac{29}{28}\cdot\mathsf{P}(\gamma^q,\varnothing)$ and $q/2^n \leq 1/58$.

5.1 Proof of the Claim (Equation (18))

We prove the claim using recursive inequality lemma. Let $\tau = (\lambda^{\alpha-1}, \mathcal{S})$ be any label, where $x,y \in \mathcal{S}$ such that $|\mathcal{S}| = \ell+2$ and $\lambda^\alpha \overset{\text{def}}{=} (\lambda_1,\ldots,\lambda_{\alpha-1}, x\oplus y) \subseteq \gamma^q$ be a 1-linked label. By using the second part of Lemma 4 on label τ, we have

$$\mathsf{P}(\tau) \leq \mathsf{P}(\gamma^q)/(1-4q/2^n)^{q-\alpha}, \tag{19}$$

and by using the first part of Lemma 4 on label τ, we have

$$\mathsf{P}(\tau_{-(x,y)}) \leq \mathsf{P}(\lambda^\alpha) \leq \mathsf{P}(\gamma^q)/(1-4q/2^n)^{q-\alpha}. \tag{20}$$

Using Eqn. (19), Eqn. (20), and Defn. 1, we have

$$D(\alpha,\ell) \leq 2\mathsf{P}(\gamma^q)/(1-4q/2^n)^{q-\alpha}, \tag{21}$$

where the above inequality holds due to the fact that for two positive integers a and b, one has $|a-b| \leq |a+b|$. Using the definition of $a_{d,\ell}$ and from Eqn. (21), the double sequence $\langle a_{d,\ell}\rangle$ satisfies

$$a_{d,\ell} \leq \left(\frac{\beta}{1-2\beta}\right)^d \leq \left(\frac{1}{4e}\right)^d, \tag{22}$$

where the last inequality follows from the assumption that $q \leq 2^n/59$. Note that, the above bound (i.e., Eqn. (22)) is same as the initial bound of our Recursive Inequality Lemma (i.e., Lemma 1). Now, it only remains to establish the recursive inequality of the double sequence $\langle a_{d,\ell}\rangle$. To establish the recursive inequality, we need to establish a recursive inequality on D-terms.

Lemma 7 (Recursive Inequality of D-Term). *For any $\alpha \leq q$, $\ell \geq 0$,*

$$D(\alpha, \ell) \leq D(\alpha, \ell - 1) + \frac{2q}{2^n} D(\alpha - 1, \ell + 1) + \Theta,$$

where $\Theta \overset{\mathrm{def}}{=} \frac{6\Delta_{(\gamma_0, \gamma^q)} \mathsf{P}(\gamma^q)}{2^n (1 - 4q/2^n)^{q-\alpha}}$.

Proof. Let $\tau = (\gamma^{\alpha-1}, \mathcal{S})$ be any label such that $\gamma^{\alpha-1} \subseteq \lambda^q$ and $|\mathcal{S}| = \ell + 2$. For such a given $\tau = (\gamma^{\alpha-1}, \mathcal{S})$, let $x, y \in \mathcal{S}$ such that $\tau' := \tau_{-(x,y)} = (\gamma^{\alpha}, \mathcal{S}' := \mathcal{S} \setminus \{x, y\})$ be a ℓ-linked label which is double-link separated from τ. Now, we consider the label $\tau = (\lambda^{\alpha-1}, \mathcal{S})$ and $x, y \in \mathcal{S}$ with $|\mathcal{S}| = \ell + 2$ and $(\lambda_1, \ldots, \lambda_{\alpha-1}, x \oplus y) \subseteq \gamma^q$, such that $|\mathsf{P}(\tau) - \mathsf{P}(\tau')|$ is maximum. Hence, for such a label τ, we prove the result in two cases: (a) when $\ell = 0$ and (b) $\ell > 0$ as follows:

Case-I: $\ell = 0$: In this case, we consider the label $\tau = (\lambda^{\alpha-1}, \{x, y\})$, where $(\lambda_1, \ldots, \lambda_{\alpha-1}, x \oplus y) \subseteq \gamma^q$, such that $|\mathsf{P}(\tau) - \mathsf{P}(\tau')|$ is maximum, where recall that $\tau' = \tau_{-(x,y)} = ((\lambda^{\alpha-1}, x \oplus y), \varnothing)$. From the label τ, we define another label $\tau^* = (\lambda^{\alpha-1}, \{x, x \oplus y\})$ from τ. It is easy to see that $\mathsf{P}(\tau) = \mathsf{P}(\tau^*)$. By applying Lemma 5 on the label τ^*, we have

$$\mathsf{P}(\tau^*) = \mathsf{P}(\tau^*_{-x}) - \frac{1}{2^{n-1}} \sum_{i \in I_x} \mathsf{P}(\tau^*_{i \to x}), \tag{23}$$

where $\tau^*_{-x} = (\lambda^{\alpha-1}, \{x \oplus y\})$ and $\tau^*_{i \to x} = (\lambda^{\alpha-2}, \{x, x \oplus y, x \oplus \lambda_i\})$. Similarly, by applying Lemma 3 on the label τ', we have

$$\mathsf{P}(\tau') = \left(1 - \frac{2\alpha}{2^n}\right) \mathsf{P}(\lambda^{\alpha-1}, \{x \oplus y\}). \tag{24}$$

It is to be noted here that the label $(\tau^*_{i \to x})_{-(x, x \oplus \lambda_i)} = (\lambda^{\alpha-1}, \{x \oplus y\})$. Therefore, by substracting Eqn. (23) from Eqn. (24) and by having $|I_x| \geq (\alpha - 3\Delta_{(\gamma_0, \gamma^q)})$, we have

$$\begin{aligned} D(\alpha, \ell) = |\mathsf{P}(\tau) - \mathsf{P}(\tau')| &= |\frac{2\alpha}{2^n} \mathsf{P}(\gamma^{\alpha-1}, \{x \oplus y\}) \\ &\quad - \frac{2}{2^n} \sum_{i \in I_x} \mathsf{P}(\gamma^{\alpha-2}, \{x, x \oplus y, x \oplus \lambda_i\})| \\ &\leq \frac{2\alpha}{2^n} D(\alpha - 1, \ell + 1) + \frac{6\Delta_{(\gamma_0, \gamma^q)} \mathsf{P}(\gamma^q)}{2^n (1 - 2\beta)^{q-\alpha}}, \end{aligned} \tag{25}$$

which completes the proof for the first case.

Case-II: $\ell > 0$: To prove the second case, i.e., $\ell > 0$, we consider the label $\tau = (\lambda^{\alpha-1}, \mathcal{S})$ and $x, y \in \mathcal{S}$ with $|\mathcal{S}| = \ell + 2$ and $(\lambda_1, \ldots, \lambda_{\alpha-1}, x \oplus y) \subseteq \gamma^q$, such that $|\mathsf{P}(\tau) - \mathsf{P}(\tau')|$ is maximum. Fix any $z \in \mathcal{S}'$ and apply the Link-Deletion

Lemma (i.e., Lemma 5) for τ and τ' by removing z from them. In particular, we have

$$(a)\ \mathsf{P}(\tau) = \mathsf{P}(\tau_{-z}) - \sum_{i \in I_z} \frac{\mathsf{P}(\tau_{i \to z})}{2^{n-1}},$$
$$(b)\ \mathsf{P}(\tau') = \mathsf{P}(\tau'_{-z}) - \sum_{i \in I'_z} \frac{\mathsf{P}(\tau'_{i \to z})}{2^{n-1}},,$$

where $I_z = \{i \in (\alpha - 1] \mid \gamma_i \oplus z \notin \mathcal{S} \cup \{0^n\}\}$ and $I'_z = \{i \in (\alpha] \mid \gamma_i \oplus z \notin \mathcal{S} \cup \{0^n\} \setminus \{x, y\}\}$. Thus, $I_z \subseteq I'_z$. Moreover, $i \in I'_z \setminus I_z$, implies that either $i = \alpha$ or $\gamma_i \oplus z \in \{x, y\}$. The number of i's such that $\gamma_i = z \oplus x$ (similarly for $z \oplus y$) is at most $\Delta_{\gamma^\alpha} \leq \Delta_{(\gamma_0,\gamma^q)}$. So, $|I'_z \setminus I_z| \leq 2\Delta_{(\gamma_0,\gamma^q)} + 1 \leq 3\Delta_{(\gamma_0,\gamma^q)}$. Clearly, (1) $(\tau_{-z})_{-(x,y)} = \tau'_{-z}$ and (2) for every $i \in I_z$, $(\tau_{i \to z})_{-(x,y)} = \tau'_{i \to z} = (\gamma^{\alpha-1}, \mathcal{S})$ with $|\mathcal{S}| = \ell + 2$. Hence, for such a label τ, we have the following:

$$\begin{aligned}
D(\alpha, \ell) &= |\mathsf{P}(\tau) - \mathsf{P}(\tau')| \\
&\leq \left|\mathsf{P}(\tau_{-z}) - \mathsf{P}(\tau'_{-z})\right| + 2^{-n+1} \sum_{i \in I'_z \setminus I_z} \mathsf{P}(\tau'_{i \to z}) \\
&+ 2^{-n+1} \sum_{i \in I_z} \left|\mathsf{P}(\tau_{i \to z}) - \mathsf{P}(\tau'_{i \to z})\right| \\
&\leq D(\alpha, \ell - 1) + \frac{2\alpha}{2^n} D(\alpha - 1, \ell + 1) \\
&+ 2^{-n+1} \sum_{i \in I'_z \setminus I_z} \mathsf{P}(\tau'_{i \to z}) \\
&\leq D(\alpha, \ell - 1) + \beta D(\alpha - 1, \ell + 1) \\
&+ \sum_{i \in I'_z \setminus I_z} \frac{\mathsf{P}(\gamma^q)}{2^{n-1}(1 - 4q/2^n)^{q-\alpha}} \\
&\leq D(\alpha, \ell - 1) + \beta D(\alpha - 1, \ell + 1) \\
&+ \frac{6\Delta_{(\gamma_0,\gamma^q)} \mathsf{P}(\gamma^q)}{2^n(1 - 2\beta)^{q-\alpha}}.
\end{aligned}$$

This completes the proof of the lemma.

Following the definition of $a_{d,\ell}$ and $\beta/(1 - 2\beta) \leq 1/4e$, we have the recursive inequality

$$a_{d,\ell} \leq a_{d,\ell-1} + a_{d+1,\ell+1} + \frac{3\Delta_{(\gamma_0,\gamma^q)}}{2^n} \cdot \left(\frac{1}{4e}\right)^d. \tag{26}$$

Therefore, applying the recursive inequality lemma, i.e., Lemma 1 on Eqn. (22) and Eqn. (26) with $C = 3\Delta_{(\gamma_0,\gamma^q)}$, we have

$$a_{0,0} \leq \frac{12\Delta_{(\gamma_0,\gamma^q)} + 2}{2^n} \leq \frac{14\Delta_{(\gamma_0,\gamma^q)}}{2^n}.$$

6 Mirror theory for Independent Permutations

Let $\mathcal{S} := \{\rho_1, \ldots, \rho_\ell\}$ and $\mathcal{S}' := \{\rho'_1, \ldots, \rho'_{\ell'}\}$ be two sets of (possibly empty, i.e. $\ell = 0, \ell' = 0$) n-bit strings satisfying $0 \leq |\mathcal{S}'| - |\mathcal{S}| \leq 1$. Let $\gamma^q = (\gamma_1, \ldots, \gamma_q)$ be an ordered tuple of n-bit strings. We call the pair $\tau = (\gamma^q, \mathcal{S}, \mathcal{S}')$ *an L-linked label* (where $L = |\mathcal{S}| + |\mathcal{S}'| = \ell + \ell'$) or simply *label*. The elements of γ^q will be called the *base elements* and those of $\mathcal{S}$ and $\mathcal{S}'$ the *linked elements*. Let $\mathsf{R}_0, \mathsf{R}_1, \ldots, \mathsf{R}_q \leftarrow\!\!\$ \{0,1\}^n$ and $\mathsf{R}'_i = \mathsf{R}_i \oplus \gamma_i$ for all $i \in (q]$. We now define the distinctness event $\mathsf{dist}(\tau)$ corresponding to the label τ as follows:

1. **Case $\mathcal{S}, \mathcal{S}' \neq \varnothing$:** $\mathsf{dist}(\tau)$ is true `if` $\mathsf{R}_0, \ldots, \mathsf{R}_q, \mathsf{R}_0 \oplus \rho_1, \ldots, \mathsf{R}_0 \oplus \rho_\ell$ are all distinct and $\mathsf{R}'_1, \ldots, \mathsf{R}'_q, \mathsf{R}_0 \oplus \rho'_1, \ldots, \mathsf{R}_0 \oplus \rho'_{\ell'}$ are all distinct.
2. **Case $\mathcal{S} = \varnothing, \mathcal{S}' = \{\rho'_1\}$:** $\mathsf{dist}(\tau)$ is true `if` $\mathsf{R}_0, \ldots, \mathsf{R}_q$ are all distinct and $\mathsf{R}'_1, \ldots, \mathsf{R}'_q, \mathsf{R}_0 \oplus \rho'_1$ are all distinct. In this case we call τ a 1-*linked label.*
3. **Case $\mathcal{S} = \mathcal{S}' = \varnothing$:** $\mathsf{dist}(\tau)$ is true `if` $\mathsf{R}_0, \ldots, \mathsf{R}_q$ are all distinct and $\mathsf{R}'_1, \ldots, \mathsf{R}'_q$ are all distinct. In this case, we call τ a 0-*linked label.*

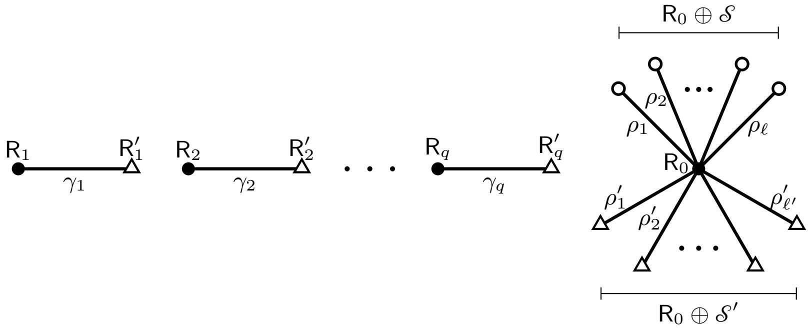

Fig. 6.1: Graphical representation of the distinctness event for an $(\ell + \ell')$-linked label $\tau = (\gamma^q, \mathcal{S}, \mathcal{S}')$, where $\mathcal{S} = \{\rho_1, \cdots, \rho_\ell\}$ and $\mathcal{S}' = \{\rho'_1, \cdots, \rho'_{\ell'}\}$. The vertices are the random variables and the label of edges are the base elements and link elements. The solid vertices denote the n-bit numbers sampled independently and uniformly at random and the hollow vertices are the derived random variables. When $\mathsf{dist}(\tau)$ holds, all the circular vertices are distinct and all the triangular vertices are distinct.

1-LINKED LABEL. A 1-linked label $\tau = (\gamma^q, \mathcal{S} = \varnothing, \mathcal{S}' = \{\rho\})$ with q many base elements is equivalently represented by $(\gamma_0, \gamma^q) := (\gamma_0, \gamma_1, \ldots, \gamma_q)$, where $\gamma_0 = \rho$. Similarly, a tuple γ^q can be equivalently viewed as a 1-linked label $\tau = (\gamma^q_{-1}, \varnothing, \{\gamma_1\})$. As before, the distinctness event for a zero-linked label $(\gamma^q, \varnothing, \varnothing)$ and a 1-linked label γ^q are not same. We write the distinctness event as $\mathsf{dist}(\tau \mid (\mathsf{R}_0, \mathsf{R}^q))$ to explicitly denote the random sources involved in the event. We denote the probability

$$\mathsf{P}(\tau) := \Pr(\mathsf{dist}(\tau \mid (\mathsf{R}_0, \mathsf{R}^q))).$$

It is easy to observe that the probability $\mathsf{P}(\gamma, \mathscr{S}, \mathscr{S}')$ does not depend on the order of the tuple γ. In other words, if γ' is a permutation of the tuple γ then $\mathsf{P}(\gamma, \mathscr{S}, \mathscr{S}') = \mathsf{P}(\gamma', \mathscr{S}, \mathscr{S}')$. Having defined the notion of probability of distinctness and 1-linked label, we are now ready to state the main theorem of mirror theory for the independent permutations case.

Lemma 8 (Main Result for Independent Permutations). *For $n \geq 7$ and any 1-linked label γ^q with $1 \leq q \leq 2^n/17$, we have*

$$\mathsf{P}(\gamma^q) \geq \frac{((2^n)^{\underline{q}})^2}{(2^n)^{2q}} \left(1 - \frac{8n^3}{2^{2n}} - \frac{19q^2}{2^{2n}}\right). \tag{27}$$

6.1 Proof of Theorem 3

Using Lemma 8, we can now prove Theorem 3, which is stated as follows: let $\gamma_1, \ldots, \gamma_q$ be any n-bit strings and $x_1, x_2, \ldots, x_q$ be distinct n-bit strings where $q \leq 2^n/17$. Then,

$$\mathsf{I} := \mathsf{Pr}(\boldsymbol{\pi}_1(x_1) \oplus \boldsymbol{\pi}_2(x_1) = \gamma_1, \ldots, \boldsymbol{\pi}_1(x_q) \oplus \boldsymbol{\pi}_2(x_q) = \gamma_q),$$

where $\boldsymbol{\pi}_1$ and $\boldsymbol{\pi}_2$ are two independent n-bit random permutations. Let A be the set of all $\mathsf{z} := (z_1, \cdots, z_q) \in (\{0,1\}^n)^q$ such that $z_1, z_2, \ldots, z_q$ are all distinct and $z_1 \oplus \gamma_1, z_2 \oplus \gamma_2, \ldots, z_q \oplus \gamma_q$ are all distinct. Then, we have $\mathsf{I} = \frac{|A|}{(2^n)^{\underline{q}}(2^n)^{\underline{q}}}$ and $\mathsf{P}(\gamma^\alpha) = \frac{|A|}{2^{nq}}$. Therefore, Theorem 3 immediately follows from Lemma 8.

6.2 Proof of Corollary 2

In this proof, there is no bad transcript. Therefore, for any transcript τ, probability of realizing it in the real world is equivalent to count the number of distinct solutions to the following system of equations: $\mathscr{E} = \{\boldsymbol{\pi}_1(x_1) \oplus \boldsymbol{\pi}_2(x_1) = y_1, \boldsymbol{\pi}_1(x_2) \oplus \boldsymbol{\pi}_2(x_2) = y_2, \ldots, \boldsymbol{\pi}_1(x_q) \oplus \boldsymbol{\pi}_2(x_q) = y_q\}$, which is $(2^n)_q \cdot (2^n)_q / 2^{nq} \cdot (1 - \epsilon)$, where $\epsilon = 19q^2/2^{2n} + 8n^3/2^{2n}$ that follows from our main theorem of the paper as we are dealing with $\xi_{\max} = 2$. Therefore,

$$\Pr[\mathsf{X}_{\text{re}} = \tau] \geq \frac{1}{2^{nq}} \cdot \left(1 - \frac{19q^2}{2^{2n}} - \frac{8n^3}{2^{2n}}\right).$$

Hence, by the result of H-Coefficient technique, our result follows.

7 Proof of Lemma 8

To complete the proof of the Mirror theory for the independent permutations case, it now only remains to prove Lemma 8. Similar to the proof of Lemma 2, we first exploit the properties of the probabilities of the distinctness event between related labels for independent permutations case through Lemma 9 and Lemma 10. Similar to the single permutation case, we introduce the notion of the link-deletion operation and the Link-Deletion Lemma (i.e., Lemma 11). These results together will allows us to state the Core-Lemma (i.e., Lemma 12), which allows us to prove Lemma 8.

7.1 Properties of Probability of Distinctness for Pairwise Independent Permutation

Similar to Lemma 3, we establish the relationship between probabilities of distinctness for a 0-linked label $(\gamma^q, \varnothing, \varnothing)$ and for a 1-linked label γ^q in Lemma 9. In Lemma 10, we establish the relationship between probabilities of distinctness for two 1-linked labels such that one is a sub-tuple of the other.

Lemma 9 (1-link-0-link). $\mathsf{P}(\gamma^q, \varnothing, \varnothing) = \mathsf{P}(\gamma^q)(1 - \frac{q}{2^n})$.

Proof. The event $\mathsf{dist}(\gamma^q, \varnothing, \varnothing \mid (\mathsf{R}_0, \mathsf{R}^q))$ holds if and only if $\mathsf{dist}(\gamma^q \mid (\mathsf{R}_0, \mathsf{R}^q))$ and $\mathsf{R}_0 \notin \{\mathsf{R}_1, \ldots, \mathsf{R}_q\}$. By using the independence of R_0, the result follows.

Lemma 10 (1-link-1-link). *Let γ^{q-d} be a 1-linked label such that $\gamma^{q-d} \subseteq \lambda^q$. Then,*

$$\mathsf{P}(\gamma^{q-d}) \leq \mathsf{P}(\lambda^q) / \left(1 - \frac{2q}{2^n}\right)^d. \tag{28}$$

Let $\tau = (\gamma^{q-d}, \mathcal{S}, \mathcal{S}')$ be a label such that there exists $x \in \mathcal{S}$ and $y \in \mathcal{S}'$ with $(\gamma_0, \gamma^{q-d}) \subseteq \lambda^q$ where $\gamma_0 = x \oplus y$. Then,

$$\mathsf{P}(\tau) \leq \mathsf{P}(\lambda^q) / \left(1 - \frac{2q}{2^n}\right)^{d-1}. \tag{29}$$

The proof of this lemma is similar to that of Lemma 4 and hence we omit its proof.

<u>Link-Deletion Operation.</u> Let $\tau = (\gamma^q, \mathcal{S}, \mathcal{S}')$ be an ℓ-linked label with $\ell \geq 1$. Unlike single permutation case, we remove the links alternately from $\mathcal{S}$ and $\mathcal{S}'$ in the following manner: If $\ell \equiv 0 \pmod 2$, then we remove a link element $x \in \mathcal{S}$, otherwise, we remove a link element $x \in \mathcal{S}'$. Thus, for every $x \in \mathcal{S}$, we define the following set:

$$I'_x = \{i \in (q] : \gamma_i \oplus x \notin \mathcal{S}'\},$$

and for every $x \in \mathcal{S}'$, we define the following set:

$$I_x = \{i \in (q] : \gamma_i \oplus x \notin \mathcal{S}\}.$$

Now, for every $x \in \mathcal{S}$ and for every $i \in I'_x$, we define the set:

$$\mathcal{S}'_{x,i} = \mathcal{S}' \cup \{x \oplus \gamma_i\},$$

and for every $x \in \mathcal{S}'$ and for every $i \in I_x$, we define the set

$$\mathcal{S}_{x,i} = \mathcal{S} \cup \{x \oplus \gamma_i\}.$$

For a given ℓ-linked label $\tau = (\gamma^q, \mathcal{S}, \mathcal{S}')$, for $x \in \mathcal{S}$ and for $i \in I_x$, we define $(\ell + 1)$-linked label $\tau'_{i \to x} := (\gamma^q_{-i}, \mathcal{S}, \mathcal{S}'_{x,i})$. Similarly, for $x \in \mathcal{S}'$ and for $i \in I_x$, we define $(\ell + 1)$-linked label $\tau_{i \to x} := (\gamma^q_{-i}, \mathcal{S}_{x,i}, \mathcal{S}')$. Similarly, for $x \in \mathcal{S}$, we define the label τ_{-x} to denote $(\gamma^q, \mathcal{S} \setminus x, \mathcal{S}')$ and τ_{-x} to denote $(\gamma^q, \mathcal{S}, \mathcal{S}' \setminus x)$ for $x \in \mathcal{S}'$.

Lemma 11 (Link-Deletion Lemma). *Let $\tau = (\gamma^q, \mathcal{S}, \mathcal{S}')$ be a ℓ-linked label with $\ell \geq 1$. Then, using the above notations, we have the followings:*

$$\mathsf{P}(\tau) = \mathsf{P}(\tau_{-x}) - \sum_{i \in I'_x} \frac{\mathsf{P}(\tau'_{i \to x})}{2^n} \ (\textit{ for } \ell \equiv 0 \pmod 2).$$

$$\mathsf{P}(\tau) = \mathsf{P}(\tau_{-x}) - \sum_{i \in I_x} \frac{\mathsf{P}(\tau_{i \to x})}{2^n} \ (\textit{ for } \ell \equiv 1 \pmod 2).$$

The proof of this lemma is similar to that of Lemma 5 and hence we omit it. We would just want to point out, that the reason of two different cases here stems from the requirement that $0 \leq |\mathcal{S}'| - |\mathcal{S}| \leq 1$. If $\ell \equiv 0 \pmod 2$, then $|\mathcal{S}| = |\mathcal{S}'|$, and then the link is removed from $\mathcal{S}$, otherwise, if $\ell \equiv 1 \pmod 2$, then $|\mathcal{S}'| = |\mathcal{S}| + 1$, and then the link is removed from $\mathcal{S}'$.

By applying Lemma 11 to a 1-linked label $\tau = (\gamma^q, \varnothing, \{\gamma_0\})$ (equivalently $\tau = (\gamma_0, \gamma^q)$), we have

$$\mathsf{P}((\gamma_0, \gamma^q)) = \mathsf{P}(\gamma^q, \varnothing, \varnothing) - \frac{1}{2^n} \sum_{i \in I_{\gamma_0}} \mathsf{P}(\gamma^q_{i \to \gamma_0}). \tag{30}$$

We now state the "*Core Lemma for the pairwise independent permutations*", which is used to prove our main theorem. We defer its proof in Subsect. 7.3.

Lemma 12 (Core Lemma). *Let $(\gamma_0, \gamma^q) = (\gamma_0, \gamma_1, \ldots, \gamma_q)$ with $q \geq 2n$ be any 1-linked label. Then, we have*

$$\mathsf{P}((\gamma_0, \gamma^q)_{i \to \gamma_0}) \leq \mathsf{P}(\gamma^q, \varnothing, \varnothing) \left(1 + \frac{17\varDelta_{(\gamma_0, \gamma^q)}}{2^n}\right).$$

7.2 Resuming the Proof of Lemma 8

We prove the result in two steps. In the first step, we prove that

$$\mathsf{P}(\gamma^{2n}) \geq \frac{((2^n)_{\underline{2n}})^2}{(2^n)^{4n}} \left(1 - \frac{8n^3}{2^{2n}}\right), \tag{31}$$

and in the second step we prove that

$$\mathsf{P}(\gamma^q) \geq \mathsf{P}(\gamma^{2n}) \times \frac{((2^n - 2n)_{\underline{q-2n}})^2}{(2^{2n})^{q-2n}} \left(1 - \frac{19q^2}{2^{2n}}\right) \tag{32}$$

holds. Combining Eqn. (31) and Eqn. (32), we have our result,

$$\begin{aligned} \mathsf{P}(\gamma^q) &\geq \frac{((2^n)_{\underline{q}})^2}{(2^n)^{2q}} \times \left(1 - \frac{19q^2}{2^{2n}}\right)\left(1 - \frac{8n^3}{2^{2n}}\right) \\ &\geq \frac{((2^n)_{\underline{q}})^2}{(2^n)^{2q}} \times \left(1 - \frac{19q^2}{2^{2n}} - \frac{8n^3}{2^{2n}}\right). \end{aligned}$$

FIRST STEP: For any $q \leq 2^{n-1}$, we take an arbitrary 1-linked label $\tau = (\gamma_0, \gamma^q)$ with q base elements. So

$$\begin{aligned} \mathsf{P}((\gamma_0, \gamma^q)) &\geq \mathsf{P}(\gamma^q) \times \left(1 - \frac{2q}{2^n}\right) \\ &= \mathsf{P}(\boldsymbol{\gamma}^q) \times \left(1 - \frac{q}{2^n}\right)^2 \left(1 - \frac{q^2/2^{2n}}{(1-q/2^n)^2}\right). \end{aligned}$$

Since ordering of elements does not affect the probability of distinctness, we have

$$\frac{\mathsf{P}(\gamma^{q+1})}{\mathsf{P}(\gamma^q)} \geq \left(1 - \frac{q}{2^n}\right)^2 \left(1 - \frac{q^2/2^{2n}}{(1-q/2^n)^2}\right). \tag{33}$$

Let us denote $\zeta(q) = \frac{q^2/2^{2n}}{(1-q/2^n)^2}$. Note that, $\zeta(q)$ is an increasing function and $(1-\zeta(q))^q \geq 1 - q \cdot \zeta(q)$. Therefore, by multiplying Eqn. (33) for $1 \leq q \leq 2n-1$, we get

$$\begin{aligned} \mathsf{P}(\gamma^{2n}) &\geq \frac{((2^n)^{\underline{2n}})^2}{(2^n)^{4n}} \left(1 - \frac{(2n-1)^3/2^{2n}}{(1-(2n-1)/2^n)^2}\right) \\ &\geq \frac{((2^n)^{\underline{2n}})^2}{(2^n)^{4n}} \left(1 - \frac{8n^3}{2^{2n}}\right), \end{aligned}$$

where the last inequality holds because $1 - \frac{(2n-1)^3/2^{2n}}{(1-(2n-1)/2^n)^2} \geq 1 - 8n^3/2^{2n}$ for $n \geq 7$.

SECOND STEP. In the second step, we prove that for all α with $2n \leq \alpha \leq 2^n/17$, the following

$$\frac{\mathsf{P}(\gamma^{\alpha+1})}{\mathsf{P}(\gamma^\alpha)} \geq \frac{(2^n-\alpha)^2}{2^{2n}}(1-\eta(\alpha)) \tag{34}$$

holds, where $\eta(\alpha) := \frac{17\alpha/2^{2n}}{1-\alpha/2^n}$. Note that, $\eta(\alpha)$ is a non-decreasing function, and $(1-\eta(q-1))^q \geq 1-(q-1)\eta(q-1) \geq 1 - q \cdot \eta(q)$. Moreover, for all $q \leq 2^n/17$, we have $17/(1-q/2^n) \leq 19$. Therefore, by multiplying Eqn. (34) for all $2n \leq \alpha \leq q-1$, we have Eqn. (32).

Since the ordering of the elements does not matter, for notational simplicity, we prove the following statement, which is equivalent to Eqn. (34):

$$\frac{\mathsf{P}((\gamma_0, \gamma^\alpha))}{\mathsf{P}(\gamma^\alpha)} \geq \frac{(2^n-\alpha)^2}{2^{2n}}(1-\eta(\alpha)).$$

Let $(\gamma_0, \gamma^\alpha)$ be a 1-linked label with α base elements. As the probability of distinctness does not depend on the order of the elements of the label, we rearrange the elements in the label in such a way so that $\varDelta := \varDelta_{(\gamma_0,\gamma^\alpha)} = \delta + 1$, where $\delta := \delta_{\gamma^\alpha}(\gamma_0)$, is achieved. Let $I_{\gamma_0} := \{i \in (\alpha] \mid \gamma_i \neq \gamma_0\}$ be the set of all indices i

for which γ_i does not collide with γ_0. It is easy to see that $|I_{\gamma_0}| = \alpha - \Delta + 1$. By applying Eqn. 30 and Lemma 12, we can bound $\mathsf{P}(\gamma^{[\alpha]})$ from below as follows:

$$\begin{aligned}
\mathsf{P}((\gamma_0, \gamma^\alpha)) &= \mathsf{P}(\gamma^\alpha, \varnothing, \varnothing) - \frac{1}{2^n} \sum_{i \in I_{\gamma_0}} \mathsf{P}(\gamma^\alpha_{i \to \gamma_0}) \\
&\geq \mathsf{P}(\gamma^\alpha, \varnothing, \varnothing) - \frac{1}{2^n} \sum_{i \in I_{\gamma_0}} \mathsf{P}(\gamma^\alpha, \varnothing, \varnothing) \left(1 + 17 \frac{\Delta}{2^n}\right) \\
&\geq \mathsf{P}(\gamma^\alpha, \varnothing, \varnothing) \left(1 - \frac{\alpha - \delta}{2^n} \left(1 + \frac{17(\delta + 1)}{2^n}\right)\right) \\
&\overset{[1]}{\geq} \mathsf{P}(\gamma^\alpha, \varnothing, \varnothing) \left(1 - \frac{\alpha}{2^n} - \frac{17\alpha}{2^{2n}}\right) \\
&\overset{[2]}{\geq} \mathsf{P}(\gamma^\alpha) \times \frac{(2^n - \alpha)^2}{2^{2n}} (1 - \eta(\alpha))
\end{aligned}$$

where [1] follows from the calculation

$$\begin{aligned}
\frac{\alpha - \delta}{2^n} \left(1 + \frac{17(\delta + 1)}{2^n}\right) &\leq \frac{\alpha}{2^n} + \frac{17\alpha}{2^{2n}} - \frac{\delta}{2^n} \left(1 - \frac{17\alpha}{2^n}\right) \\
&\leq \frac{\alpha}{2^n} + \frac{17\alpha}{2^{2n}},
\end{aligned}$$

and [2] follows from Lemma 9.

7.3 Proof of Core Lemma (Lemma 12)

To prove the Core Lemma, it is sufficient to prove the following upper bound

$$|\mathsf{P}((\gamma_0, \gamma^q)_{i \to \gamma_0}) - \mathsf{P}(\gamma^q, \varnothing, \varnothing)| \leq \frac{17\Delta_{(\gamma_0, \gamma^q)} \cdot \mathsf{P}(\gamma^q, \varnothing, \varnothing)}{2^n}. \tag{35}$$

As before, we first identify the relationship between $(\gamma_0, \gamma^q)_{i \to \gamma_0} = (\gamma^q_{-i}, \{\gamma_i \oplus \gamma_0\}, \{\gamma_0\})$ and $(\gamma^q, \varnothing, \varnothing)$. The label $(\gamma_0, \gamma^q)_{i \to \gamma_0}$ contains one linked element $\gamma_0 \oplus \gamma_i$ in $\mathcal{S}$ and the linked element γ_0 in $\mathcal{S}'$ whose sum is γ_i. Now, if we remove these linked element from $\mathcal{S}$ and $\mathcal{S}'$ and include their xor to the tuple of the base elements, we obtain $(\gamma^q, \varnothing, \varnothing)$. We generalize this notion for any ℓ-linked label $\tau = (\lambda^\alpha, \mathcal{S}, \mathcal{S}')$ and call it the *double-link separation.*

DOUBLE LINK SEPARATION OPERATION. Let $\tau = (\lambda^\alpha, \mathcal{S}, \mathcal{S}')$ and $x \in \mathcal{S}, y \in \mathcal{S}'$. We define

$$\tau_{-(x,y)} := ((\lambda_1, \cdots, \lambda_\alpha, \lambda_{\alpha+1} := x \oplus y), \mathcal{S} \setminus \{x\}, \mathcal{S}' \setminus \{y\}),$$

When we write $\tau_{-(x,y)}$, it is implicitly assumed that $x \in \mathcal{S}$ and $y \in \mathcal{S}'$ are linked elements of τ.

The notion of double-link separation operation leads us to define the "differential term" as follows:

Definition 2 (Differential Term). *For a positive integer q, for all $\ell \geq 0$ and $1 \leq \alpha \leq q$, we define*

$$D(\alpha, \ell) = \max_{\tau,x,y} \left| \mathsf{P}(\tau) - \mathsf{P}(\tau_{-(x,y)}) \right|, \tag{36}$$

where the maximum is over all $\tau := (\lambda^{\alpha-1}, \mathcal{S}, \mathcal{S}')$ and $x \in \mathcal{S}, y \in \mathcal{S}'$ such that $|\mathcal{S}| + |\mathcal{S}'| = \ell + 2$ and $(\lambda_1, \dots, \lambda_{\alpha-1}, x \oplus y) \subseteq \gamma^q$. For all $\ell < 0$, we define $D(\alpha, \ell) = 0$.

Recall that for $q \geq 2n$, $(\gamma_0, \gamma^q) = (\gamma_0, \gamma_1, \dots, \gamma_q)$ is an 1-linked label. Let $\beta := q/2^n$ [5]. For all $0 \leq d \leq q$, and $\ell \leq 2d - 1$, we write $\alpha = q - d$ and define

$$a_{d,\ell} := \frac{\beta^d D(\alpha, \ell)}{2\mathsf{P}(\gamma^q)}.$$

Now we state the following claim which establishes the following upper bound on $a_{0,0}$ as follows:

Claim.

$$a_{0,0} \leq \frac{8\Delta_{(\gamma_0,\gamma^q)}}{2^n}. \tag{37}$$

PROOF OF EQN. (35). We complete the proof of the Core Lemma, using the above claim.

$$\begin{aligned} |\mathsf{P}((\gamma_0, \gamma^q)_{i \to \gamma_0}) - \mathsf{P}(\gamma^q, \varnothing, \varnothing)| &\leq \frac{16\Delta_{(\gamma_0,\gamma^q)} \cdot \mathsf{P}(\gamma^q)}{2^n} \\ &\leq \frac{17\Delta_{(\gamma_0,\gamma^q)}}{2^n} \cdot \mathsf{P}(\gamma^q, \varnothing, \varnothing), \end{aligned}$$

where the second inequality follows since $D(q, 0) = a_{0,0} \times 2\mathsf{P}(\gamma^q)$ and the last inequality follows since $\mathsf{P}(\gamma^q) = \mathsf{P}(\gamma^q, \varnothing, \varnothing)/(1 - q/2^n) \leq \frac{17}{16} \cdot \mathsf{P}(\gamma^q, \varnothing, \varnothing)$ and $q/2^n \leq 1/17$.

7.3.1 Proof of the Claim (Equation (37))

Let $\tau = (\gamma^{\alpha-1}, \mathcal{S}, \mathcal{S}')$ be any label, where $x \in \mathcal{S}$ and $y \in \mathcal{S}'$ such that $|\mathcal{S}| + |\mathcal{S}'| = \ell + 2$ and $(\gamma_1, \dots, \gamma_{\alpha-1}, x \oplus y) \subseteq \gamma^q$. Then using Lemma 10 and Defn. 2, we have

$$D(\alpha, \ell) \leq \frac{2\mathsf{P}(\gamma^q)}{(1 - 2q/2^n)^{q-\alpha}}. \tag{38}$$

Using the definition of $a_{d,\ell}$ and from Eqn. (38), the double sequence $\langle a_{d,\ell} \rangle$ satisfies

$$a_{d,\ell} \leq \left(\frac{\beta}{1 - 2\beta} \right)^d \leq \left(\frac{1}{4e} \right)^d, \tag{39}$$

where the last inequality follows from the assumption that $q \leq 2^n/17$. Note that, the above bound (i.e., Eqn. (39)) is same as the initial bound of our Recursive Inequality Lemma (i.e., Lemma 1). Now, it only remains to establish the recursive inequality of the double sequence $\langle a_{d,\ell} \rangle$.

[5] For the single permutation case, we defined β to be $2q/2^n$

Lemma 13 (Recursive Inequality of D-Term). *For any $\alpha \leq q$ and $\ell \geq 0$,*

$$D(\alpha, \ell) \leq D(\alpha, \ell - 1) + \frac{q}{2^n} \cdot D(\alpha - 1, \ell + 1)$$
$$+ \frac{3\varDelta_{(\gamma_0, \gamma^q)}}{2^n} \times \frac{\mathsf{P}(\gamma^q)}{(1 - 2q/2^n)^{q-\alpha}}.$$

Proof. We prove the lemma for the case when $\ell \equiv 1 \pmod 2$. Other case can be proved in exactly the same way. Let $\tau = (\gamma^{\alpha-1}, \mathcal{S}, \mathcal{S}')$ be any label such that $\gamma^{\alpha-1} \subseteq \lambda^q$ and $|\mathcal{S}| + |\mathcal{S}'| = \ell + 2$. For such a given $\tau = (\gamma^{\alpha-1}, \mathcal{S}, \mathcal{S}')$, let $x \in \mathcal{S}$ and $y \in \mathcal{S}'$ such that $\tau' := \tau_{-(x,y)} = (\gamma^{\alpha}, \mathcal{S} \setminus \{x\}, \mathcal{S}' \setminus \{y\})$ be a ℓ-linked label which is double-link separated from τ. Now, we fix any $z \in \mathcal{S}'$ and apply the link deletion lemma (Lemma 5) for τ and $\tau^\star = \tau_{-(x,y)}$ by removing z from them. In particular, we have

$$(a)\ \mathsf{P}(\tau) = \mathsf{P}(\tau_{-z}) - \sum_{i \in I_z} \frac{\mathsf{P}(\tau_{i \to z})}{2^n},$$
$$(b)\ \mathsf{P}(\tau^\star) = \mathsf{P}(\tau^\star_{-z}) - \sum_{i \in I^\star_z} \frac{\mathsf{P}(\tau^\star_{i \to z})}{2^n}, \tag{40}$$

where $I_z = \{i \in (\alpha] \mid \gamma_i \oplus z \notin \mathcal{S} \cup \{0^n\}\}$, $I^\star_z = \{i \in (\alpha + 1] \mid \gamma^\star_i \oplus z \notin \mathcal{S}^\star \cup \{0^n\}\}$. Thus, $I_z \subseteq I^\star_z$. Also counting in precisely the same way as we did in the proof of Lemma 7, we have $|I^\star_z \setminus I_z| \leq 2\varDelta_{(\gamma_0, \gamma^q)} + 1 \leq 3\varDelta_{\gamma^q}$. Hence, by subtracting the above two link deletion relations and doing the similar calculations as we did in the proof of Lemma 7, we obtain the result.

Following the definition of $a_{d,\ell}$ and $\beta/(1 - 2\beta) \leq 1/4e$, we have the recursive inequality

$$a_{d,\ell} \leq a_{d,\ell-1} + a_{d+1,\ell+1} + \frac{1.5\varDelta_{(\gamma_0,\gamma^q)}}{2^n} \cdot \left(\frac{1}{4e}\right)^d. \tag{41}$$

Therefore, applying the recursive inequality lemma on Eqn. (39) and Eqn. (41) with $C = 1.5\varDelta_{(\gamma_0,\gamma^q)}$, we have the result.

8 Conclusion and Future Work

In this paper, we provide a complete and verifiable proof of Mirror theory for the single permutation case and pair of independent permutations case. Our result on Mirror theory for the single permutation case directly gives an optimal and tight PRF security on the XOR_1 construction, whereas our result on Mirror theory for a pair of independent permutations gives a security bound of $O(q^2/2^{2n})$ for the XOR_2 construction. However, our bound for XOR_2 is not known to be tight and hence it leaves room for the bound to be improved. Also, our result is applicable only for $\xi_{\max} = 2$, whereas Patarin[Theorem 6, [34]] claimed that the same result holds for a general $\xi_{\max} > 2$ with $\theta = 134$, and $\alpha \leq \frac{2^n}{(\xi_{\max}-1)\cdot\theta}$. Unfortunately, there is no proof available in support of this claim (only a very high-level sketchy proof can be found in [34]). One can inevitably notice from our proof that the analysis of the same for general $\xi_{\max}$ is a lot more complicated. Nevertheless, this is an interesting problem to address. In fact, coming up with a concrete security proof for general $\xi_{\max}$ result would eventually help to correctly establish the improved security bounds of many cryptographic constructions.

References

1. Mihir Bellare and Russell Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. *IACR Cryptology ePrint Archive*, 1999:24, 1999.
2. Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *J. Comput. Syst. Sci.*, 61(3):362–399, 2000.
3. Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding*, pages 266–280, 1998.
4. Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 409–426, 2006.
5. Arghya Bhattacharjee, Avijit Dutta, Eik List, and Mridul Nandi. Cencpp* - beyond-birthday-secure encryption from public permutations. Cryptology ePrint Archive, Report 2020/602, 2020. `https://eprint.iacr.org/2020/602`.
6. John Black and Phillip Rogaway. A block-cipher mode of operation for parallelizable message authentication. In *EUROCRYPT 2002*, pages 384–397, 2002.
7. Donghoon Chang and Mridul Nandi. A short proof of the PRP/PRF switching lemma. *IACR Cryptology ePrint Archive*, 2008:78, 2008.
8. 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*, pages 285–302, 2014.
9. Benoît Cogliati and Jacques Patarin. Mirror theory: A simple proof of the pi+pj theorem with xi_max=2. *IACR Cryptol. ePrint Arch.*, 2020:734, 2020.
10. Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*, pages 497–523, 2017.
11. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Goutam Paul. Double-block hash-then-sum: A paradigm for constructing bbb secure prf. *IACR Trans. Symmetric Cryptol.*, 2018(3):36–92, 2018.
12. Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul, and Liting Zhang. Single key variant of pmac_plus. *IACR Trans. Symmetric Cryptol.*, 2017(4):268–305, 2017.
13. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or decrypt? to make a single-key beyond birthday secure nonce-based MAC. In *Advances in Cryptology - CRYPTO 2018. Proceedings, Part I*, pages 631–661, 2018.

14. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. sfdwcdm+: A BBB secure nonce based MAC. *Adv. in Math. of Comm.*, 13(4):705–732, 2019.
15. Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond birthday bound secure MAC in faulty nonce model. In *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*, pages 437–466, 2019.
16. Tetsu Iwata. New blockcipher modes of operation with beyond the birthday bound security. In *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, pages 310–327, 2006.
17. Tetsu Iwata, Bart Mennink, and Damian Vizár. CENC is optimally secure. *IACR Cryptology ePrint Archive*, 2016:1087, 2016.
18. Tetsu Iwata and Kazuhiko Minematsu. Stronger security variants of GCM-SIV. *IACR Trans. Symmetric Cryptol.*, 2016(1):134–157, 2016.
19. Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A fast tweakable block cipher mode for highly secure message authentication. In *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*, pages 34–65, 2017.
20. Eik List and Mridul Nandi. Revisiting full-prf-secure PMAC and using it for beyond-birthday authenticated encryption. In *Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings*, pages 258–274, 2017.
21. Eik List and Mridul Nandi. ZMAC+ - an efficient variable-output-length variant of ZMAC. *IACR Trans. Symmetric Cryptol.*, 2017(4):306–325, 2017.
22. Stefan Lucks. The sum of prps is a secure PRF. In *EUROCRYPT 2000*, pages 470–484, 2000.
23. David A. McGrew and John Viega. The security and performance of the galois/counter mode (GCM) of operation. In *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, pages 343–355, 2004.
24. Bart Mennink and Samuel Neves. Encrypted davies-meyer and its dual: Towards optimal security using mirror theory. In *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*, pages 556–583, 2017.
25. Alexander Moch and Eik List. Parallelizable macs based on the sum of prps with security beyond the birthday bound. In *Applied Cryptography and Network Security - 17th International Conference, ACNS 2019, Bogota, Colombia, June 5-7, 2019, Proceedings*, pages 131–151, 2019.
26. Valérie Nachef, Jacques Patarin, and Emmanuel Volte. *Feistel Ciphers - Security Proofs and Cryptanalysis.* Springer, 2017.
27. Yusuke Naito. Full prf-secure message authentication code based on tweakable block cipher. In *Provable Security - 9th International Conference, ProvSec 2015, Kanazawa, Japan, November 24-26, 2015, Proceedings*, pages 167–182, 2015.
28. Yusuke Naito. Blockcipher-based macs: Beyond the birthday bound without message length. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part III*, pages 446–470, 2017.
29. Jacques Patarin. Luby-rackoff: 7 rounds are enough for $2^{\mathrm{n(1\text{-}epsilon)}}$security. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 513–529, 2003.

30. Jacques Patarin. On linear systems of equations with distinct variables and small block size. In *Information Security and Cryptology - ICISC 2005, 8th International Conference, Seoul, Korea, December 1-2, 2005, Revised Selected Papers*, pages 299–321, 2005.
31. Jacques Patarin. The "coefficients H“ technique. In *Selected Areas in Cryptography - SAC 2008. Revised Selected Papers*, pages 328–345, 2008.
32. Jacques Patarin. The "coefficients h" technique. In *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, pages 328–345, 2008.
33. Jacques Patarin. A proof of security in o(2n) for the xor of two random permutations. In *Information Theoretic Security, Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings*, pages 232–248, 2008.
34. 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.
35. Jacques Patarin. Security in o(2^{n}) for the xor of two random permutations \\ - proof with the standard H technique -. *IACR Cryptology ePrint Archive*, 2013:368, 2013.
36. Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 373–390, 2006.
37. Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptology ePrint Archive*, 2004:332, 2004.
38. Kan Yasuda. The sum of CBC macs is a secure PRF. In *CT-RSA 2010*, pages 366–381, 2010.
39. Kan Yasuda. A new variant of PMAC: beyond the birthday bound. In *Advances in Cryptology - CRYPTO 2011. Proceedings*, pages 596–609, 2011.
40. Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. 3kf9: Enhancing 3gpp-mac beyond the birthday bound. In *ASIACRYPT 2012*, pages 296–312, 2012.
41. Ping Zhang, Honggang Hu, and Qian Yuan. Close to optimally secure variants of GCM. *Security and Communication Networks*, 2018:9715947:1–9715947:12, 2018.