Improved Multi-User Security Using the Squared-Ratio Method

Yu Long Chen[1], Wonseok Choi[2], and Changmin Lee[3]

[1] imec-COSIC, KU Leuven, Belgium
yulong.chen@kuleuven.be
[2] Purdue University, West Lafayette, IN, US
wonseok@purdue.edu
[3] KIAS, Seoul, Korea
changminlee@kias.re.kr

Abstract. Proving security bounds in contexts with a large number of users is one of the central problems in symmetric-key cryptography today. This paper introduces a new method for information-theoretic multi-user security proofs, called "the Squared-Ratio method". At its core, the method requires the expectation of the square of the ratio of observing the so-called good transcripts (from Patarin's H-coefficient technique) in the real and the ideal world. Central to the method is the observation that for information-theoretic adversaries, the KL-divergence for the multi-user security bound can be written as a summation of the KL-divergence of every single user.
We showcase the Squared-Ratio method on three examples: the Xor of two Permutations by Bellare et al. (EUROCRYPT '98) and Hall et al. (CRYPTO '98), the Encrypted Davies-Mayer by Cogliati and Seurin (CRYPTO '16), and the two permutation variant of the nEHtM MAC algorithm by Dutta et al. (EUROCRYPT '19). With this new tool, we provide improved bounds for the *multi-user* security of these constructions. Our approach is modular in the sense that the multi-user security can be obtained directly from single-user results.

Keywords: symmetric-key cryptography, provable security, multi-user security, pseudorandom function

1 Introduction

Commonly used cryptographic constructions in practice are usually deployed in contexts with a large number of users. An obvious question is to what extent the number of users will affect the security bound of these cryptographic constructions, this question leads to consider adversaries that may try to analyze the mode of operation with multiple independent keys at the same time. This setting is known as multi-user security and has been attracting more and more attention from researchers in recent years.

From a cryptographic perspective, a potential weakness of the multi-user security can be interpreted as the following. Let $\mathbf{Adv}(\mathcal{A})$ and $\mathbf{Adv}^u(\mathcal{A})$ be an advantage of single-user security and u-user security with an adversary $\mathcal{A}$, respectively. Under an assumption that each user exploits independent keys, it gives an obvious relation $\mathbf{Adv}^u(\mathcal{A}) \leq u \cdot \mathbf{Adv}(\mathcal{A})$ by the hybrid argument (for short, the factor u is called security loss). If the worst-case bound holds, the multi-user settings would not be as secure as the cryptographic scheme requires for a sufficiently large security loss, even if the single-user security is provably guaranteed. On the one hand, this worst-case loss is unfortunately unavoidable in the case of key-recovery attacks against block ciphers [9]. On the other hand, in some cases, it is shown that the gap between single-user and u-user security is relatively small [8, 14]. These results indicate that there is no general relationship between currently known single-user security and multi-user security. It simultaneously gives a natural question of how known single-user security results can be rearranged into multi-user security.

Multi-User Security. The multi-user security was first considered in the provable security setting by Mouha and Luykx [34], by proving the multi-user security of the Even-Mansour cipher. Since then, various constructions have been analyzed in the multi-user setting [10, 25, 26, 39, 38]. These works show that evaluating how security degrades as the number of users grows is a challenging technical problem. Firstly, a dedicated proof is required for each construction that we want to consider, even when the security is known in the single-user setting. Secondly, the security analysis of all the aforementioned work is performed in the ideal cipher model. Assuming that a construction is based on perfectly random primitives can be too strong, which can lead to an overly optimistic security bound that does not cover practical attacks. Recently at ASIACRYPT 2022, Chen [12] proposed a modular approach to proving the multi-user security of permutation-based constructions that satisfy certain properties. Unfortunately, as the author himself mentioned in the paper, his technique is not extendable to the block cipher-based setting. This is because his technique is based on the mirror theory in the ideal permutation model and therefore cannot be easily extended to the ideal cipher model.

A different avenue. We revisit the multi-user provable security suggested by Bhattacharya and Nandi [8]. To be precise, they have shown that a mu-prf advantage of multi-user security for bitwise-xor of three n-bit pseudorandom permutations (for short, XORP[3]) is bounded by $< \sqrt{u \cdot q_{max}}/2^n$, where u is the number of users and q_{max} is the allowed number of queries the adversary can make to each user. It implies that XORP[3] for $O(2^n)$ users with $O(2^n)$ queries to each user still guarantees the mu-prf security. For this purpose, the authors leverage the chi-squared method described by Dai et al. [21].

Subsequently, Choi et al. [14] have proposed two variants of truncated xor of two n-bit pseudorandom permutations, named SaT1 and SaT2 respectively. Here SaT1 uses a single n-bit pseudorandom permutation with domain separation, while SaT2 employs two independent permutations. At the same time, the

authors state that both SaT constructions also satisfy a multi-user security with the advanced techniques.

While this proof regime has the advantage that it proves a tighter security bound rather than the naive one for the multi-user security, it seems that this proof technique is not easily extendable to the other constructions. This obstacle arises from the characteristic that for the chi-square method, it is not easy to compute an expectation of chi-square divergence when responses adaptively depend on the adversary's queries.

Our contribution. This paper aims at investigating generic techniques that are applicable to more constructions in the case of *multi-user* security.

Technically, we describe two novel inequalities to achieve the goal. We assume that adversary $\mathcal{A}$ can access to one of two systems S_0 or S_1, where S_0 is an "ideal" system and S_1 is a real one. A common way to see if two systems are indistinguishable is to bound the statistical distance of $\|\mathsf{p}_{\mathcal{S}_1}(\cdot) - \mathsf{p}_{\mathcal{S}_0}(\cdot)\|$, where $\mathsf{p}_{\mathcal{S}_i}(\cdot)$ is the probability distributions of the responses of the q queries when $\mathcal{A}$ interacts with system $\mathcal{S}_i$. In the prior work by Dai et al. [21], the authors suggested using well-known relations to bound the statistical distance:

$$\begin{aligned}
\|\mathsf{p}_{\mathcal{S}_1}(\cdot) - \mathsf{p}_{\mathcal{S}_0}(\cdot)\| &\leq \left(\frac{1}{2}\Delta_{KL}\left(\mathsf{p}_{\mathcal{S}_1}(\cdot), \mathsf{p}_{\mathcal{S}_0}(\cdot)\right)\right)^{\frac{1}{2}} \\
\Delta_{KL}\left(\mathsf{p}_{\mathcal{S}_1}(\cdot), \mathsf{p}_{\mathcal{S}_0}(\cdot)\right) &\stackrel{\text{def}}{=} \sum_{z\in\Omega} \mathsf{p}_{\mathcal{S}_1}(z) \ln\left(\frac{\mathsf{p}_{\mathcal{S}_1}(z)}{\mathsf{p}_{\mathcal{S}_0}(z)}\right), \\
\Delta_{KL}\left(\mathsf{p}_{\mathcal{S}_1}(\cdot), \mathsf{p}_{\mathcal{S}_0}(\cdot)\right) &\leq \sum_{z\in\Omega} \frac{\left(\mathsf{p}_{\mathcal{S}_1}(z) - \mathsf{p}_{\mathcal{S}_0}(z)\right)^2}{\mathsf{p}_{\mathcal{S}_0}(z)}.
\end{aligned}$$

where Ω is the support of $\mathsf{p}_{\mathcal{S}_0}(\cdot)$.

In this work, we follow similar inequalities as above. Because we consider the multi-user security, we have the u-system $(\mathcal{S}_{i,1}, \ldots, \mathcal{S}_{i,u})$ for $i \in \{0,1\}$. For simplicity, we let $\mathcal{S}_i$ denote the u-system and $\mathbf{z}$ be a set of u-strings $\{z_1, \ldots, z_u\}$. We assume that the adversary gets u responses simultaneously from each query. Let $\mathsf{p}_{\mathcal{S}_i}(\mathbf{z})$ (resp. $\mathsf{p}_{\mathcal{S}_{i,j}}(z_j)$) be a probability that the j-th system answers z_j for all $1 \leq j \leq u$ (resp. for index j). Following the footsteps of [8, 14], we assume that in the standard model, an information-theoretic adversary $\mathcal{D}$ makes distinct queries to individual user interfaces. Since those interfaces have identical distribution (for the same transcript), previous interactions with other interfaces do not impact subsequent user interactions,, which means the systems are mutually independent. It gives one more relation:

$$\mathsf{p}_{\mathcal{S}_i}(\mathbf{z}) = \prod_{j=1}^{u} \mathsf{p}_{\mathcal{S}_{i,j}}(z_j).$$

Combining it together, this auxiliary relation enables to hold that

$$\begin{aligned}
&\Delta_{KL}\left(\mathsf{p}_{\mathcal{S}_1}(\cdot), \mathsf{p}_{\mathcal{S}_0}(\cdot)\right) = \sum_{z\in\Omega} \mathsf{p}_{\mathcal{S}_1}(z) \ln\left(\frac{\mathsf{p}_{\mathcal{S}_1(z)}}{\mathsf{p}_{\mathcal{S}_0(z)}}\right) \\
&= \sum_{z\in\Omega}\sum_{j=1}^{u} \mathsf{p}_{\mathcal{S}_1(z)} \ln\left(\frac{\mathsf{p}_{\mathcal{S}_{1,j}(z_j)}}{\mathsf{p}_{\mathcal{S}_{0,j}(z_j)}}\right) = \sum_{j=1}^{u}\sum_{z\in\Omega} \mathsf{p}_{\mathcal{S}_1(z)} \ln\left(\frac{\mathsf{p}_{\mathcal{S}_{1,j}(z_j)}}{\mathsf{p}_{\mathcal{S}_{0,j}(z_j)}}\right) \\
&= \sum_{j=1}^{u}\sum_{z_j\in\Omega_j} \mathsf{p}_{\mathcal{S}_{1,j}(z_j)} \ln\left(\frac{\mathsf{p}_{\mathcal{S}_{1,j}(z_j)}}{\mathsf{p}_{\mathcal{S}_{0,j}(z_j)}}\right) = u \cdot \Delta_{KL}\left(\mathsf{p}_{\mathcal{S}_{1,j}}(\cdot), \mathsf{p}_{\mathcal{S}_{0,j}}(\cdot)\right),
\end{aligned}$$

where the first equality comes from the properties of logarithm and the other equalities are trivially derived.

It can be interpreted as for information-theoretic adversaries, the KL-divergence for the multi-user security bound can be written as a summation of each security bound. It means that to guarantee the multi-user security it is sufficient to bound the KL-divergence for a single user. For this purpose, we mimic a standard proof based on Patarin's H-coefficient technique [36]. Patarin's H-coefficient shows that

$$\frac{P_{S_1,1}(z)}{P_{S_0,1}(z)} \geq 1-\epsilon. \tag{1}$$

In addition to this, we aim at proving that

$$\frac{P_{S_1,1}(z)}{P_{S_0,1}(z)} \leq 1+\epsilon,$$

except for bad cases. Combining it together, it holds that

$$\left|\frac{P_{S_1,1}(z)}{P_{S_0,1}(z)} - 1\right| \leq \epsilon. \tag{2}$$

It allows bounding the KL-divergence in a function of ϵ, which eventually gives a bound for the statistical distance between two systems.

Our approach, called the Squared-Ratio method, combines the chi-squared method with the H-coefficient technique. Here, we employed the notion of transcripts and good/bad partitioning. For $u = 1$, it appears more similar to the expectation-method [25, 26]. The requirement of our method is the same to that of expectation-method, but an upper bound of good ratio instead of a lower bound. This allows our method to be applicable to most constructions. Note that we utilize "each user's transcript" rather than "each query (chi-squared method)" or "entire transcript (H-coefficient technique)". We refer to Section 3 for more details.

From the explanation above, we see that the Squared-Ratio method allows us to get the multi-user security directly from the single-user bound, where Patarin's Mirror theory [37] is used for the counting arguments in the single-user case. Mirror theory allows one to sharply lower bound the number of solutions to

a certain type of system of equations and non-equations. In our security proof, we will consider the following system of equations; for two sets of unknowns $\mathcal{V}_P = \{P_1, \ldots, P_{q_P}\}$ and $\mathcal{V}_Q = \{Q_1, \ldots, Q_{q_Q}\}$, and for constants λ_i, $i = 1, \ldots, q$,

$$\Gamma : \begin{cases} P_{I_1} \oplus Q_{I_1} = \lambda_1, \\ P_{I_2} \oplus Q_{I_2} = \lambda_2, \\ \qquad \vdots \\ P_{I_q} \oplus Q_{I_q} = \lambda_q. \end{cases}$$

This system of equations can be represented by a simple graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \mathcal{V}_P \sqcup \mathcal{V}_Q$. The unknowns P_{I_i} and Q_{I_i} are connected by a λ_i-weighted edge for $i = 1, \ldots, q$ and are mapped to $\mathcal{V}_P$ and $\mathcal{V}_Q$ using two surjective index mappings. This graph consists of q edges, and the size of the largest component in this graph is denoted by $\xi_{\max}$. This system of equations has been studied in [37], and later revisited with more complete and detailed arguments [19, 22].

To apply our Squared-Ratio method here, we want an upper bound on the ratio of observing the good transcripts in the form as given in equation (2), instead of a lower bound in the form of $1 - \epsilon$ (as in (1)) given in the traditional mirror theory. We prove the result both when there are large components ($q_c > 0$) and when there are only isolated edges ($q_c = 0$), where q_c refers to the number of edges in the large components. We refer to Section 4 for more details.

We then illustrate the Squared-Ratio method by applying it to prove the *multi-user* prf security of Xor of Permutation (XoP), Encrypted Davies-Mayer (EDM), and nonce-based Enhance Hash-then-Mask (nEHtM). These three constructions have been chosen because of their practical relevance and a large amount of attention they have received in recent years. In the rest of this paper, we will use $q_{\max}$ to indicate the maximum number of queries the adversary can make against each of its u users in the *multi-user* setting, while q indicates the *total number of queries* that the adversary can execute in the *single-user* setting. Depending on the context, we have $q_{\max} \leq q \leq uq_{\max}$.

Applications: Xor of Permutations. Block ciphers are usually considered to be pseudorandom permutations (PRPs) under a uniform random key. That means someone cannot distinguish a secure block cipher from a random permutation before performing a specific number of encryption and decryption queries in a black-box manner. On the other hand, various cryptographic constructions such as encryption modes [2], MAC algorithms [3, 7] and authenticated encryption schemes [15] need pseudorandom functions (PRFs) to achieve beyond-birthday-bound security. When such PRFs are replaced with block ciphers, it may degrade security up to the birthday bound [4, 6, 11, 24, 27]. To solve the problem of security degradation, Bellare et al. [5] and Hall et al. [24] initiated the study of constructing a good PRF from block ciphers with security beyond the birthday-bound barrier, i.e., above $2^{n/2}$. Given two n-bit (keyed) PRPs P and Q, their sum, denoted as the Xor of Permutations (XoP), maps $x \in \{0,1\}^n$ to

$$\mathsf{XoP}[\mathsf{P}, \mathsf{Q}](x) \stackrel{\text{def}}{=} \mathsf{P}(x) \oplus \mathsf{Q}(x).$$

Subsequently, after the introduction of this XoP construction, a series of works improved this seminal result [1, 18, 31, 35], culminating with the proof by Dai et al. [21] and Dutta et al. [22] that the sum of two n-bit random permutations is (fully) secure up to $O(2^n)$ queries, using the chi-squared method and a verifiable version of the mirror theory respectively. Recently, Choi et al. [14] showed for the first time that the XoP construction achieves a multi-user security of $O(\sqrt{u}{q_{\max}}^{1.5}/2^{1.5n})$. As the first application of our Squared-Ratio method, we give a fairly simple proof giving us a multi-user security bound of $O(\sqrt{u}{q_{\max}}^{2}/2^{2n})$. One can argue that the improvement is small. However, we believe the analysis of the XoP construction is fundamental, and a tight security bound has been sought for nearly two decades. On the other hand, the result of Choi et al. requires a dedicated proof, while our approach is modular in that we can obtain the multi-user bound directly from the single-user result using our Squared-Ratio method. We refer to Section 5 for more details.

Application: The EDM Construction. As another application of the Squared-Ratio method, we consider the Encrypted Davis-Meyer (EDM) construction, proposed by Cogliati and Seurin [20], defined as

$$\mathsf{EDM}[\mathsf{P},\mathsf{Q}](x) \stackrel{\text{def}}{=} \mathsf{Q}(\mathsf{P}(x) \oplus x).$$

They proved PRF-security of EDM up to $O(2^{\frac{2n}{3}})$ queries. The best known multi-user security bound for EDM is $O\left(uq^2/2^{1.5n}\right)$, obtained from the combination of hybrid argument with the result of Dai et al. via the Chi-squared method [21]. Using our Squared-Ratio method, we show a significant improvement that achieves a multi-user security of $O\left(n\sqrt{u}{q_{\max}}^4/2^{3n}\right)$. We refer to Section 6 for more details. We note that in the work of Mennink and Neves [32], they proved that EDM achieves a single-user security of $O(q/2^n)$ for $q \leq 2^n/\xi_{\max}$. However, their result uses an unverified version of Patarin's mirror theory, while we aim for a simpler-to-use framework for multi-user security with verifiable proofs. Whether the multi-user security of EDM can be improved by improving the mirror theory result for the single-user security is an interesting future research direction.

Application: The nEHtM MAC Algorithm. As our final application, we consider the two-permutation variant of the nonce-based Enhanced Hash-then-Mask (nEHtM) construction, proposed by Dutta et al. [23], defined as

$$\mathsf{nEHtM}[\mathsf{P},\mathsf{Q}](x) \stackrel{\text{def}}{=} P(N) \oplus Q(H_{K_h}(M) \oplus N).$$

Note that nEHtM is structurally similar to the Enhanced Hash-then-Mask (EHtM) construction first proposed by Minematsu [33], except that the random salt is used instead of a nonce and a PRF instead of a block cipher. We also note this two permutation variant was the $F_{B_2}^{\mathsf{SoP}}$ construction considered in the work of Chen et al. [13]. For the original single permutation variant, Dutta et al. [23] proved that the single-user security of nEHtM is up to $2^{2n/3}$ MAC queries and 2^n verification queries in a nonce-respecting setting. Later, Choi et al. [16] improved this result, and showed that nEHtM is secure up to $2^{3n/4}$ MAC queries and 2^n verification queries. Chen et al. [13] considered the single-user PRF security of this two-permutation variant and showed that it is secure up to $O(2^{3n/4})$ queries.

Indeed the original construction was defined as the form:

$$\mathsf{nEHtM}[\mathsf{P}](x) \stackrel{\text{def}}{=} P(0 \,\|\, N) \oplus P(1 \,\|\, H_{K_h}(M) \oplus N).$$

It is obvious that this construction cannot yield a n-bit zero value. That is why this construction has a naive and tight advantage bound $uq/2^n$ for the mu-prf security. On the other hand, we show $\mathsf{nEHtM}[\mathsf{P}, \mathsf{Q}]$ can achieve better security than $\mathsf{nEHtM}[\mathsf{P}]$ in the nonce-respecting setting. Our application serves the evidence that there is a security gap between them in the case of multi-user security. As a result of our new Squared-Ratio method, we end up with a multi-user security bound that improves significantly over the previously best-known result when the number of users is large. When the number of users is $O(2^{n/2})$, previous results [16, 13] on nEHtM are totally insecure for the case $q = uq_{\max}$, and only reached $O(2^{n/2})$ birthday bound security for the case $q = q_{\max}$. While our new result shows that nEHtM achieves beyond birthday bound security for $u = O(2^{n/2})$, and is still birthday bound secure even when the number of users is close to $O(2^n)$. We refer to Section 7 and Figure 1 for more details.

We believe that a similar approach also works on the nonce-misuse setting, however, the combinatorics will be very complex. We emphasize that our contribution is providing a new hybrid method to prove better mu-security which can be applied to most constructions including hash-based ones. To the best of our knowledge, there is no proof via the chi-squared-method for MAC or AEAD security (hash-based). The chi-squared method is limited for some simple structures and often results in non-tight bounds.

Note that the expectation of chi-squared divergence should be taken over the real world. We can handle hash-based constructions like nEHtM thanks to expectation over ideal world. In this regard, our method is more versatile and can be applied to all constructions if they can be proven via the coefficient-H-technique/expectation-method. As a result, one can obtain a $\sqrt{u}\epsilon$ security where ϵ can be possibly better than that of chi-squared-method.

2 Preliminaries

NOTATION. Throughout this paper, we fix positive integers n and u to denote the block size and the number of users, respectively. For a non-empty finite set $\mathcal{X}$, we let $\mathcal{X}^{*\ell}$ denote a set $\{(x_1, \ldots, x_\ell) \in \mathcal{X}^\ell \mid x_i \neq x_j \text{ for } i \neq j\}$. For an integer A and b, we denote $(A)_b = A(A-1)\ldots(A-b+1)$. A notation $x \leftarrow_\$ \mathcal{X}$ means that x is chosen uniformly at random from $\mathcal{X}$. $|\mathcal{X}|$ means the number of elements in $\mathcal{X}$. The set of all permutations of $\{0,1\}^n$ is simply denoted $\mathsf{Perm}(n)$. The set of all functions with domain $\{0,1\}^n$ and codomain $\{0,1\}^m$ is simply denoted by $\mathsf{Func}(n,m)$. For a keyed function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ with key space $\mathcal{K}$ and non-empty sets $\mathcal{X}$ and $\mathcal{Y}$, we will denote $F(K, \cdot)$ by $F_K(\cdot)$ for $K \in \mathcal{K}$. When two sets $\mathcal{X}$ and $\mathcal{Y}$ are disjoint, their (disjoint) union is denoted $\mathcal{X} \sqcup \mathcal{Y}$. We write T_{re} and T_{id} as random variables following the distribution of the transcripts in the real world and the ideal world, respectively. For any positive integer i, and $a_1, \ldots, a_i, b \in \{0,1\}^n$, We denote $\{a_1, \ldots, a_i\} \oplus b \stackrel{\text{def}}{=} \{a_1 \oplus b, \ldots, a_i \oplus b\}$.

2.1 Security Notions

Pseudorandom Permutations. Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a keyed permutation with key space $\mathcal{K}$, where $E(K,\cdot)$ is a permutation for each $K \in \mathcal{K}$. We will denote $E_K(X)$ for $E(K,X)$. A (q,t)-distinguisher against E is an algorithm $\mathcal{D}$ with oracle access to an n-bit permutation and its inverse, making at most q oracle queries, running in time at most t, and outputting a single bit. The advantage of $\mathcal{D}$ in breaking the PRP-security of E, i.e., in distinguishing E from a uniform random permutation $\pi \leftarrow_{\$} \mathsf{Perm}(n)$, is defined as

$$\mathsf{Adv}^{\mathsf{prp}}_{E}(\mathcal{D}) = \left|\Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{D}^{E_K, E_K^{-1}} = 1\right] - \Pr\left[\pi \leftarrow_{\$} \mathsf{Perm}(n) : \mathcal{D}^{\pi,\pi^{-1}} = 1\right]\right|.$$

We define $\mathsf{Adv}^{\mathsf{prp}}_{E}(q,t)$ as the maximum of $\mathsf{Adv}^{\mathsf{prp}}_{E}(\mathcal{D})$ over all (q,t)-distinguishers against E. When we consider information-theoretic security, we will drop the parameter t. In the following analyses, we will consider PRP-based constructions, such as XoP, EDM, or nEHtM. Those constructions can be built upon a block cipher, and in this case, one can obtain a security bound by simply adding PRP-security of the given block cipher.

Multi-User Pseudorandom Function. Let $\mathsf{C} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$ be a keyed function with key space $\mathcal{K}$. We will consider an information-theoretic distinguisher $\mathcal{A}$ that makes oracle queries to C and returns a single bit. The advantage of $\mathcal{A}$ in breaking the mu-prf security of C, i.e., in distinguishing $\mathsf{C}(K_1,\cdot),\ldots,\mathsf{C}(K_u,\cdot)$ where $K_1,\ldots,K_u \leftarrow_{\$} \mathcal{K}$ from uniformly chosen functions $\mathsf{F}_1,\ldots,\mathsf{F}_u \leftarrow_{\$} \mathsf{Func}(n,m)$, is defined as

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{C}}(\mathcal{A}) = \Big|&\Pr\left[K_1,\ldots,K_u \leftarrow_{\$} \mathcal{K} : \mathcal{A}^{\mathsf{C}_{K_1}(\cdot),\ldots,\mathsf{C}_{K_u}(\cdot)} = 1\right] \\ &- \Pr\left[\mathsf{F}_1,\ldots,\mathsf{F}_u \leftarrow_{\$} \mathsf{Func}(n,m) : \mathcal{A}^{\mathsf{F}_1(\cdot),\ldots,\mathsf{F}_u(\cdot)} = 1\right]\Big|.\end{aligned}$$

We define $\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{C}}(u, q_{\max}, t)$ as the maximum of $\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{C}}(\mathcal{A})$ over all the distinguishers against C for u users making at most $q_{\max}$ queries to each user and running in time at most t. When we consider information-theoretic security, we will drop the parameter t.

Almost XOR Universal Hash Functions. Let $\delta > 0$, and let $H : \mathcal{K}_h \times \mathcal{M} \to \mathcal{X}$ be a keyed function for three non-empty sets $\mathcal{K}_h$, $\mathcal{M}$, and $\mathcal{X}$. H is said to be *δ-XOR almost universal* (δ-XAU) if for any distinct $M, M' \in \mathcal{M}$ and $X \in \mathcal{X}$,

$$\Pr\left[K_h \leftarrow_{\$} \mathcal{K}_h : H_{K_h}(M) \oplus H_{K_h}(M') = X\right] \le \delta.$$

2.2 Total Variation Distance, KL Divergence and Chi-Squared Divergence In a Subspace

Let P and Q be two probability distributions over discrete set Γ. The *total variation distance* of P and Q is denoted by

$$\|P(x) - Q(x)\| \stackrel{\text{def}}{=} \sum_{x \in \Gamma} \max\{P(x) - Q(x), 0\} = \frac{1}{2} \sum_{x \in \Gamma} |P(x) - Q(x)|.$$

This total variation distance is related to the Kullback–Leibler (KL) divergence by Pinsker's inequality, where the KL divergence is

$$\Delta_{KL}(P,Q) \stackrel{\text{def}}{=} \sum_{x\in\Gamma} P(x)\ln\left(\frac{P(x)}{Q(x)}\right)$$

and Pinsker's inequality says that

$$\|P-Q\| \le \left(\frac{1}{2}\Delta_{KL}(P,Q)\right)^{\frac{1}{2}}.$$

Note that Q should have full support to define KL-divergence well. On the other hand, there is well-known inequality between KL divergence and χ^2 divergence.

$$\Delta_{KL}(P,Q) \le \chi^2(P,Q) \stackrel{\text{def}}{=} \sum_{x\in\Gamma}\frac{(P(x)-Q(x))^2}{Q(x)}.$$

We modify these inequalities over a subset $\Gamma' \subset \Gamma$. In other words, we define the quantity

$$\Delta_{KL,\Gamma'}(P,Q) \stackrel{\text{def}}{=} \sum_{x\in\Gamma'} P(x)\ln\left(\frac{P(x)}{Q(x)}\right)$$

and prove the following lemmas:

Lemma 1. *For any subset $\Gamma' \subset \Gamma$, one has*

$$\sum_{x\in\Gamma'}|P(x)-Q(x)| \le \left(2\Delta_{KL,\Gamma'}(P,Q) + 2\sum_{x\in\Gamma\setminus\Gamma'} P(x)-Q(x)\right)^{\frac{1}{2}}.$$

The proof of this Lemma is given in Supplementary Material A.

Lemma 2. *For any subset $\Gamma' \subset \Gamma$, one has*

$$\Delta_{KL,\Gamma'}(P,Q) \le \sum_{x\in\Gamma'}\frac{(P(x)-Q(x))^2}{Q(x)} - \sum_{x\in\Gamma\setminus\Gamma'} P(x)-Q(x).$$

The proof of this Lemma is given in Supplementary Material B.

2.3 Useful Lemma

Lemma 3. *If $(\lambda_1,\dots,\lambda_q) \in (\{0,1\}^n)^q$ are uniformly randomly distributed and $\mathsf{C} = \left|\{(i,j)\in[q]^{*2} \mid (i<j)\wedge(\lambda_i=\lambda_j)\}\right|$, for any $A>0$, one has*

$$\mathbf{Ex}[\mathsf{C}] \le \frac{q^2}{2^{n+1}},$$

$$\mathbf{Ex}\left[\mathsf{C}^2\right] \le \frac{q^2}{2^{n+1}} + \frac{q^4}{2^{2n+2}},$$

$$\Pr\left[\mathsf{C} \ge \frac{q^2}{2^{n+1}} + A\right] \le \frac{q^2}{2^{n+1}A^2} + \frac{q^4}{2^{2n+2}A^2}.$$

The proof of this Lemma is given in Supplementary Material C.

This lemma will be used for the computation of $\mathbf{Ex}\left[\epsilon_1(z)^2\right]$ and ϵ_2 in Theorem 1. The expectation can be identified to an expectation taken over the distribution of all transcripts in the ideal world (and so, regardless of what is a real construction).

3 The Squared-Ratio Method

We fix a set of random systems and a deterministic distinguisher $\mathcal{A}$ that makes exactly $q(= uq_{\max})$ oracle queries to one of the random systems. Each random system has u interfaces with independent random but identical distribution, and $\mathcal{A}$ makes $q_{\max}$ queries to each interface in order. We also fix a set Ω that contains all possible transcripts for oracle queries to an interface of random systems. For a random system $\mathcal{S} = (\mathcal{S}^1, \ldots, \mathcal{S}^u)$ and $i \in \{1, \ldots, u\}$, let $Z_{\mathcal{S}^i}$ be the random variable over Ω that follows the distribution of the transcripts obtained by $\mathcal{A}$ interacting with $\mathcal{S}^i$. Let

$$\mathbf{Z}_{\mathcal{S}} \stackrel{\text{def}}{=} (Z_{\mathcal{S}^1}, \ldots, Z_{\mathcal{S}^u}),$$

$$\mathsf{p}_{\mathcal{S}^i}(z) \stackrel{\text{def}}{=} \Pr\left[Z_{\mathcal{S}^i} = z\right]$$

and

$$\mathsf{p}_{\mathcal{S}}(\mathbf{z}) \stackrel{\text{def}}{=} \Pr\left[\mathbf{Z}_{\mathcal{S}} = \mathbf{z}\right]$$

for $z \in \Omega$ and $\mathbf{z} \in \Omega^u$. $\mathcal{A}$'s distinguishing advantage is upper bounded by the total variation distance of $\mathsf{p}_{\mathcal{S}_0}(\cdot)$ and $\mathsf{p}_{\mathcal{S}_1}(\cdot)$. In the following, we aim to show that

$$\|\mathsf{p}_{\mathcal{S}_1}(\cdot) - \mathsf{p}_{\mathcal{S}_0}(\cdot)\| \leq O\left(\sqrt{u \cdot \mathbf{Ex}\left[\epsilon(z)^2\right]}\right),$$

where $\epsilon(z)$ is a function such that $\left|\frac{\mathsf{p}_{\mathcal{S}_1^1}(z)}{\mathsf{p}_{\mathcal{S}_0^1}(z)} - 1\right| \leq \epsilon(z)$. However, such a function $\epsilon(z)$ may not exist over Ω. Therefore, we try to show a similar upper bound under some constraints. To do this, we split the set Ω into two distinct sets $\Gamma_{\mathsf{good}} \sqcup \Gamma_{\mathsf{bad}} = \Omega$ in a way inspired by Patarin's H-Coefficient technique [36]. The sets satisfy following conditions:

1. For all $z \in \Gamma_{\mathsf{good}}$, there exists a function $\epsilon_1(z)$ such that

$$\left|\frac{\mathsf{p}_{\mathcal{S}_1^1}(z)}{\mathsf{p}_{\mathcal{S}_0^1}(z)} - 1\right| \leq \epsilon_1(z)$$

2. and there exists a constant ϵ_2 such that

$$\Pr\left[Z_{\mathcal{S}_0^1} \in \Gamma_{\mathsf{bad}}\right] \leq \epsilon_2.$$

Since we consider a multi-user case, the target set is multi-set Ω^u, not Ω. Whereas $\Omega \setminus \Gamma_{\mathsf{good}} = \Gamma_{\mathsf{bad}}$ by the definition, $\Omega^u \setminus \Gamma^u_{\mathsf{good}} \neq \Gamma^u_{\mathsf{bad}}$ for any $u \geq 2$. We thus rearrange the set $\Omega^u \setminus \Gamma^u_{\mathsf{good}}$. Let $\Gamma_{\mathsf{bad}\,i}$ denote an event $\{z_i \in \Gamma_{\mathsf{bad}}\}$. On the one hand, the event $\{\mathbf{z} \in \Omega^u \setminus \Gamma^u_{\mathsf{good}}\}$ can be interpreted as $\cup^u_{i=1}\Gamma_{\mathsf{bad}\,i}$. On the other hand, thanks to the inclusion-exclusion principle, the set includes a set $\Omega' \stackrel{def}{=} \cup^u_{i=1}\Gamma_{\mathsf{bad}\,i} \setminus \cup_{(i,j)} \left(\Gamma_{\mathsf{bad}\,i} \cap \Gamma_{\mathsf{bad}\,j}\right)$.

An adversary can adaptively choose queries on $\mathcal{S}^i$ after the end of the interaction with $\mathcal{S}^j$ for $i > j$; however, we assume that an information-theoretic adversary $\mathcal{D}$ makes distinct queries to individual user interfaces, and previous interactions with other interfaces do not impact interactions with next users. We are allowed to make this assumption since our work focuses on standard model proofs for information-theoretic adversaries. In the standard model, we assume an independent random distribution for each user (but the opponent already knows what the distribution is). In the information-theory setting, block-ciphers based on independent uniform keys will be replaced by independent random permutations. Each user in our construction uses independent keys based on random primitives, hence the other users' queries cannot increase the power of the adversary. This implies that the query-response pairs of one user cannot affect the selection of queries for other users. Therefore, querying all users simultaneously is equivalent to querying each user separately without loss of generality. The same assumption was previously used in [8, 14].

Since $Z_{\mathcal{S}^i}$ are mutually independent, for $\mathbf{z} = (z_1, \ldots, z_u)$, it holds that

$$\mathsf{p}_{\mathcal{S}}(\mathbf{z}) = \prod_{i=u}^{n} \mathsf{p}_{\mathcal{S}^i}(z_i).$$

Combining this equality and the set identity, it holds that

$$\sum_{i=1}^{u} \sum_{z_i \in \Gamma_{\mathsf{bad}}} \mathsf{p}_{\mathcal{S}^i_1}(z_i) - \sum_{i,j=1}^{u} \sum_{z_i, z_j \in \Gamma_{\mathsf{bad}}} \mathsf{p}_{\mathcal{S}^i_1}(z_i) \cdot \mathsf{p}_{\mathcal{S}^j}(z_j)$$
$$\leq \sum_{\mathbf{z} \in \Omega^u \setminus \Gamma^u_{\mathsf{good}}} \mathsf{p}_{\mathcal{S}_1}(\mathbf{z}) \leq \sum_{i=1}^{u} \sum_{z_i \in \Gamma_{\mathsf{bad}}} \mathsf{p}_{\mathcal{S}^i_1}(z_i)$$

Putting it together, we are now ready to bound the total variation of $\mathsf{p}_{\mathcal{S}_0}(\cdot)$ and $\mathsf{p}_{\mathcal{S}_1}(\cdot)$ using Lemma 1:

$$
\begin{aligned}
\|\mathsf{p}_{\mathcal{S}_1}(\cdot) - \mathsf{p}_{\mathcal{S}_0}(\cdot)\| &= \sum_{\mathbf{z}\in\Omega^u} \max\{\mathsf{p}_{\mathcal{S}_0}(\mathbf{z}) - \mathsf{p}_{\mathcal{S}_1}(\mathbf{z}), 0\} \\
&= \sum_{\mathbf{z}\in\Gamma^u_{\mathsf{good}}} \max\{\mathsf{p}_{\mathcal{S}_0}(\mathbf{z}) - \mathsf{p}_{\mathcal{S}_1}(\mathbf{z}), 0\} + \sum_{\mathbf{z}\in\Omega^u\setminus\Gamma^u_{\mathsf{good}}} \max\{\mathsf{p}_{\mathcal{S}_0}(\mathbf{z}) - \mathsf{p}_{\mathcal{S}_1}(\mathbf{z}), 0\} \\
&\leq \sum_{\mathbf{z}\in\Gamma^u_{\mathsf{good}}} |\mathsf{p}_{\mathcal{S}_1}(\mathbf{z}) - \mathsf{p}_{\mathcal{S}_0}(\mathbf{z})| + u\epsilon_2 \\
&\leq \sqrt{2\Delta_{KL,\Gamma^u_{\mathsf{good}}}(\mathsf{p}_{\mathcal{S}_1}(\cdot), \mathsf{p}_{\mathcal{S}_0}(\cdot)) + 2\sum_{\mathbf{z}\in\Omega^u\setminus\Gamma^u_{\mathsf{good}}} \mathsf{p}_{\mathcal{S}_1}(\mathbf{z}) - \mathsf{p}_{\mathcal{S}_0}(\mathbf{z})} + u\epsilon_2 \\
&\leq \sqrt{2\Delta_{KL,\Gamma^u_{\mathsf{good}}}(\mathsf{p}_{\mathcal{S}_1}(\cdot), \mathsf{p}_{\mathcal{S}_0}(\cdot)) + 2u\left(\sum_{z\in\Gamma_{\mathsf{bad}}} \mathsf{p}_{\mathcal{S}_1^1}(z) - \mathsf{p}_{\mathcal{S}_0^1}(z)\right) + 2\binom{u}{2}\sum_{z\in\Gamma_{\mathsf{bad}}} \mathsf{p}_{\mathcal{S}_0^1}(z)^2} + u\epsilon_2 \\
&\leq \sqrt{2\Delta_{KL,\Gamma^u_{\mathsf{good}}}(\mathsf{p}_{\mathcal{S}_1}(\cdot), \mathsf{p}_{\mathcal{S}_0}(\cdot)) + 2u\left(\sum_{z\in\Gamma_{\mathsf{bad}}} \mathsf{p}_{\mathcal{S}_1^1}(z) - \mathsf{p}_{\mathcal{S}_0^1}(z)\right) + u^2\epsilon_2^2} + u\epsilon_2 \\
&\leq \sqrt{2\Delta_{KL,\Gamma^u_{\mathsf{good}}}(\mathsf{p}_{\mathcal{S}_1}(\cdot), \mathsf{p}_{\mathcal{S}_0}(\cdot)) + 2u\left(\sum_{z\in\Gamma_{\mathsf{bad}}} \mathsf{p}_{\mathcal{S}_1^1}(z) - \mathsf{p}_{\mathcal{S}_0^1}(z)\right)} + 2u\epsilon_2
\end{aligned}
$$

We next rearrange the (partial) KL-divergence term with respect to one random system $\mathcal{S}^1$. It follows that

$$
\begin{aligned}
\Delta_{KL,\Gamma^u_{\mathsf{good}}}(\mathsf{p}_{\mathcal{S}_1}(\cdot), \mathsf{p}_{\mathcal{S}_0}(\cdot)) &= \sum_{\mathbf{z}\in\Gamma^u_{\mathsf{good}}} \mathsf{p}_{\mathcal{S}_1}(\mathbf{z}) \ln\left(\frac{\mathsf{p}_{\mathcal{S}_1}(\mathbf{z})}{\mathsf{p}_{\mathcal{S}_0}(\mathbf{z})}\right) \\
&= \sum_{\mathbf{z}=(z_1,\ldots,z_u)\in\Gamma^u_{\mathsf{good}}} \mathsf{p}_{\mathcal{S}_1}(\mathbf{z}) \ln\left(\prod_{i=1}^{u} \frac{\mathsf{p}_{\mathcal{S}_1^i}(z_i)}{\mathsf{p}_{\mathcal{S}_0^i}(z_i)}\right) \\
&= \sum_{\mathbf{z}=(z_1,\ldots,z_u)\in\Gamma^u_{\mathsf{good}}} \sum_{i=1}^{u} \mathsf{p}_{\mathcal{S}_1}(\mathbf{z}) \ln\left(\frac{\mathsf{p}_{\mathcal{S}_1^i}(z_i)}{\mathsf{p}_{\mathcal{S}_0^i}(z_i)}\right) \\
&\leq \sum_{i=1}^{u} \sum_{\mathbf{z}=(z_1,\ldots,z_u)\in\Gamma^u_{\mathsf{good}}} \mathsf{p}_{\mathcal{S}_1}(\mathbf{z}) \ln\left(\frac{\mathsf{p}_{\mathcal{S}_1^i}(z_i)}{\mathsf{p}_{\mathcal{S}_0^i}(z_i)}\right) \\
&= \sum_{i=1}^{u} \sum_{z_i\in\Gamma_{\mathsf{good}}} \mathsf{p}_{\mathcal{S}_1^i}(z_i) \ln\left(\frac{\mathsf{p}_{\mathcal{S}_1^i}(z_i)}{\mathsf{p}_{\mathcal{S}_0^i}(z_i)}\right) \\
&= \sum_{i=1}^{u} \Delta_{KL,\Gamma_{\mathsf{good}}}\left(\mathsf{p}_{\mathcal{S}_1^i}(\cdot), \mathsf{p}_{\mathcal{S}_0^i}(\cdot)\right) \\
&= u \cdot \Delta_{KL,\Gamma_{\mathsf{good}}}\left(\mathsf{p}_{\mathcal{S}_1^1}(\cdot), \mathsf{p}_{\mathcal{S}_0^1}(\cdot)\right).
\end{aligned}
$$

where the last equality comes from the fact that the distributions of $\mathcal{S}^i$ are the same. A remarkable property is that this conversion replaces the u-product term with the u-summation term. This rearrangement is quite helpful in understanding the security of multiple systems. From Lemma 2, we have

$$\begin{aligned}\Delta_{KL,\Gamma_{\mathsf{good}}}\left(\mathsf{p}_{\mathcal{S}_1^1}(\cdot),\mathsf{p}_{\mathcal{S}_0^1}(\cdot)\right) &\leq \sum_{z\in\Gamma_{\mathsf{good}}}\frac{\left(\mathsf{p}_{\mathcal{S}_1^1}(z)-\mathsf{p}_{\mathcal{S}_0^1}(z)\right)^2}{\mathsf{p}_{\mathcal{S}_0^1}(z)}-\sum_{z\in\Gamma_{\mathsf{bad}}}\left(\mathsf{p}_{\mathcal{S}_1^1}(z)-\mathsf{p}_{\mathcal{S}_0^1}(z)\right)\\ &\leq \sum_{z\in\Gamma_{\mathsf{good}}}\mathsf{p}_{\mathcal{S}_0^1}(z)\epsilon_1(z)^2-\sum_{z\in\Gamma_{\mathsf{bad}}}\left(\mathsf{p}_{\mathcal{S}_1^1}(z)-\mathsf{p}_{\mathcal{S}_0^1}(z)\right)\\ &\leq \mathbf{Ex}\left[\epsilon_1(z)^2\right]-\sum_{z\in\Gamma_{\mathsf{bad}}}\left(\mathsf{p}_{\mathcal{S}_1^1}(z)-\mathsf{p}_{\mathcal{S}_0^1}(z)\right).\end{aligned}$$

Putting it together, we have

$$\|\mathsf{p}_{\mathcal{S}_1}(\cdot)-\mathsf{p}_{\mathcal{S}_0}(\cdot)\|\leq\sqrt{2u\mathbf{Ex}\left[\epsilon_1(z)^2\right]}+2u\epsilon_2\,.$$

where the expectation is taken over the distribution of $Z_{\mathcal{S}_0^1}$. In summary, we can prove the following theorem.

Theorem 1. *Suppose whenever* $\mathsf{p}_{\mathcal{S}_1^1}(\cdot)>0$ *then* $\mathsf{p}_{\mathcal{S}_0^1}(\cdot)>0$. *Let* $\Omega=\Gamma_{\mathsf{good}}\sqcup\Gamma_{\mathsf{bad}}$. *If a function* $\epsilon_1(z)$ *and a constant* ϵ_2 *holds the following constraints*

$$\left|\frac{\mathsf{p}_{\mathcal{S}_1^1}(z)}{\mathsf{p}_{\mathcal{S}_0^1}(z)}-1\right|\leq\epsilon_1(z)$$

for all attainable $z\in\Gamma_{\mathsf{good}}$ *and*

$$\Pr\left[Z_{\mathcal{S}_0^1}\in\Gamma_{\mathsf{bad}}\right]\leq\epsilon_2,$$

one has

$$\|\mathsf{p}_{\mathcal{S}_1}(\cdot)-\mathsf{p}_{\mathcal{S}_0}(\cdot)\|\leq\sqrt{2u\mathbf{Ex}\left[\epsilon_1(z)^2\right]}+2u\epsilon_2$$

where the expectation is taken over the distribution of $Z_{\mathcal{S}_0^1}$.

Remark. Many typical proofs based on Patarin's H-Coefficient technique shows

$$\frac{\mathsf{p}_{\mathcal{S}_1^1}(z)}{\mathsf{p}_{\mathcal{S}_0^1}(z)}\geq 1-\epsilon(z)$$

for almost all z as good transcripts. Compared to the prior one, we need one step more to apply our method:

$$\frac{\mathsf{p}_{\mathcal{S}_1^1}(z)}{\mathsf{p}_{\mathcal{S}_0^1}(z)}\leq 1+\epsilon(z).$$

Indeed, there is a lack of such analysis due to no requirement for the previous proofs. In the following section, we show that the $\epsilon(z)$ is well bounded for highly secure constructions.

4 Upper Bounds from Mirror Theory

For any two systems $\mathcal{S}_0$ and $\mathcal{S}_1$ except for $\mathsf{p}_{\mathcal{S}_0^1}(z) = 0$, it is obvious that there exists $\epsilon(z)$ such that

$$\left| \frac{\mathsf{p}_{\mathcal{S}_1^1}(z)}{\mathsf{p}_{\mathcal{S}_0^1}(z)} - 1 \right| \leq \epsilon(z).$$

From the result of the Section 3, it is desirable to show that the $\epsilon(z)$ function is as small as possible so that the two systems are indistinguishable. In this section, we aim to serve a useful theorem to sharply bound the ratio of the probabilities when $\mathcal{S}_0$ is an ideal world and $\mathcal{S}_1$ is a real world via revisiting the Mirror theory.

Definitions and Notations. For fixed positive integers q, q_P, q_Q, let $\mathcal{P} = \{P_1, \ldots, P_{q_P}\}$ and $\mathcal{Q} = \{Q_1, \ldots, Q_{q_Q}\}$ be sets of *unknowns* such that $P_i, Q_j \in \{0,1\}^n$ for $i \in [q_P]$ and $j \in [q_Q]$. For a sequence of constants $(\lambda_1, \ldots, \lambda_q) \in (\{0,1\}^n)^q$, consider a system of equations

$$\Gamma : \begin{cases} P_{\varphi_P(1)} \oplus Q_{\varphi_Q(1)} = \lambda_1, \\ P_{\varphi_P(2)} \oplus Q_{\varphi_Q(2)} = \lambda_2, \\ \qquad \vdots \\ P_{\varphi_P(q)} \oplus Q_{\varphi_Q(q)} = \lambda_q, \end{cases}$$

where φ_P and φ_Q are two surjective index mappings such that

$$\varphi_P \colon \{1, \ldots, q\} \to \{1, \ldots, q_P\},$$
$$\varphi_Q \colon \{1, \ldots, q\} \to \{1, \ldots, q_Q\},$$

for $q_P, q_Q \leq q$. This equation system Γ is then uniquely determined by $(\varphi_P, \varphi_Q, (\lambda_1, \ldots, \lambda_q))$.

We will represent this system of equations Γ by a simple graph containing no loops or multiple edges. Let $\mathcal{G}(\Gamma) = (\mathcal{V}, \mathcal{E})$ be a graph where $\mathcal{V} = \mathcal{P} \sqcup \mathcal{Q}$, and let $\overline{PQ} \in \mathcal{E}$ be an edge for P, $Q \in \mathcal{V}$. If this edge is labeled with λ_i for $i = 1, \ldots, q$, then it represents the equation $P \oplus Q = \lambda_i$. We will sometimes write $P \overset{\star}{-} Q$ when an edge $\overline{PQ}$ is labeled with $\star \in \{\lambda_1, \ldots, \lambda_q\}$. Here, $\mathcal{G}(\Gamma)$ contains no isolated vertex; every vertex is incident with at least one edge.

As a natural extension of the label over an edge, we consider a trail of ℓ-length

$$\mathcal{L} : V_0 \overset{\lambda_1}{-} V_1 \overset{\lambda_2}{-} \cdots \overset{\lambda_\ell}{-} V_\ell$$

in $\mathcal{G}(\Gamma)$, its label is defined as

$$\lambda(\mathcal{L}) \overset{\text{def}}{=} \lambda_1 \oplus \lambda_2 \oplus \cdots \oplus \lambda_\ell.$$

Since we only consider acyclic graphs, the label between two vertices is uniquely determined, and thus the following definition is well-defined: $\lambda(V_0, V_\ell) \overset{\text{def}}{=} \lambda(\mathcal{L})$.

When there is no trail between V and V', we denote $\lambda(V,V') \stackrel{\text{def}}{=} \perp$. Additionally, a connected path is called a component. For a component $\mathcal{C}$, we let $\xi(\mathcal{C})$ denote the number of vertices in $\mathcal{C}$. We then define the maximum component size $\xi_{\max} \stackrel{\text{def}}{=} \max\{\xi(\mathcal{C}) \mid \mathcal{C} \in \mathcal{G}(\Gamma)\}$. We also define two notions related to the graph:

Definition 1 (acyclic). *In case $\mathcal{G}$ contains no cycle, we call the graph acyclic.*

Definition 2 (non-degenerate). $\lambda(\mathcal{L}) \neq \mathbf{0}$ *for any trails $\mathcal{L}$ of even length in $\mathcal{G}$.*

Any graph $\mathcal{G}(\Gamma)$ which is acyclic and non-degenerate will be called a *nice* graph [30, 16]. For a nice graph $\mathcal{G}(\Gamma)$, $\mathcal{G}$ is a bipartite graph with no cycle, where every edge connects a vertex in $\mathcal{P}$ to one in $\mathcal{Q}$. So $\mathcal{G}$ is decomposed into its connected components, all of which are trees; let

$$\mathcal{G} = \mathcal{C}_1 \sqcup \mathcal{C}_2 \sqcup \cdots \sqcup \mathcal{C}_\alpha \sqcup \mathcal{C}_{\alpha+1} \sqcup \mathcal{C}_{\alpha+2} \sqcup \cdots \sqcup \mathcal{C}_{\alpha+\beta}$$

for some $\alpha, \beta \geq 0$, where $\mathcal{C}_1, \ldots, \mathcal{C}_\alpha$ denote the components of size greater than 2, and $\mathcal{C}_{\alpha+1}, \ldots, \mathcal{C}_{\alpha+\beta}$ denote the components of size 2. We also define the following sets for $i \in [\alpha+\beta]$ to state our theorem.

$$\mathcal{R}_i \stackrel{\text{def}}{=} \left\{ (\{V_1, V_1'\}, \{V_2, V_2'\}) \in {\mathcal{C}_i}^{*2} \times {\mathcal{C}_j}^{*2} \,\middle|\, j < i \text{ and } \lambda(V_1, V_1') = \lambda(V_2, V_2') \right\}.$$

Any solution to $\mathcal{G}(\Gamma)$ (identifying $\mathcal{G}(\Gamma)$ with its corresponding system of equations) should satisfy all the equations in Γ, while all the variables in $\mathcal{P}$ (resp. $\mathcal{Q}$) should take on different values. The number of solutions to $\mathcal{G}(\Gamma)$ will be denoted $h(\mathcal{G}(\Gamma))$. We remark that if we assign any value to a vertex P, then the labeled edges determine the values of all the other vertices in the component containing P, where the assignment is unique since $\mathcal{G}(\Gamma)$ contains no cycle. The values in the same part are all distinct since $\lambda(\mathcal{L}) \neq \mathbf{0}$ for any trail $\mathcal{L}$ of even length. For any nice graph, we can then bound the term $\frac{h(\mathcal{G})N^q}{(N)_{q_P}(N)_{q_Q}}$, which will be appeared in computing the ratio $\frac{\mathsf{p}_{\mathcal{S}_1^1}(z)}{\mathsf{p}_{\mathcal{S}_0^1}(z)}$. To be precise, we have the following:

Theorem 2. *Let $\mathcal{G}$ be a nice graph, let q denote the number of edges of $\mathcal{G}$, and let q_c denote the number of edges of $\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_\alpha$ of size > 2. We then have*

(a) When $q \leq \frac{2^n}{4\xi_{\max}}$ and $0 < q_c \leq q$, it holds that

$$\left| \frac{h(\mathcal{G})N^q}{(N)_{q_P}(N)_{q_Q}} - 1 \right| \leq \exp\left(\frac{2\sum_{i=1}^{\alpha+\beta} |\mathcal{R}_i| + 2\xi_{\max} q_c}{N} + \frac{4\xi_{\max} q_c q^2}{N^2} + \frac{20\xi_{\max} q^4}{N^3} \right) - 1,$$

(b) When $q \leq \frac{2^n}{13}$ and $q_c = 0$, it holds that

$$\left| \frac{h(\mathcal{G})N^q}{(N)_{q_P}(N)_{q_Q}} - 1 \right| \leq \exp\left(\frac{3\sum_{i=1}^{\alpha+\beta} |\mathcal{R}_i|}{N} + \frac{2q^2}{N^2} + \frac{6(n+1)^2}{N} \right) - 1.$$

The full proof is given in Supplementary Material D. From Theorem 2, the below corollary immediately follows from the fact $e^X - 1 \le 2X$ for $X \le 1$.

Corollary 1. *With the same notation of Theorem 2, we have*

(a) When $q \le \frac{2^n}{4\xi_{\max}}$, $0 < q_c \le q$, *and*

$$\frac{2\sum_{i=1}^{\alpha+\beta}|\mathcal{R}_i| + 2\xi_{\max}q_c}{N} + \frac{4\xi_{\max}q_cq^2}{N^2} + \frac{20\xi_{\max}q^4}{N^3} \le 1\,,$$

it holds that

$$\left|\frac{h(\mathcal{G})N^q}{(N)_{q_P}(N)_{q_Q}} - 1\right| \le \frac{4\sum_{i=1}^{\alpha+\beta}|\mathcal{R}_i| + 4\xi_{\max}q_c}{N} + \frac{8\xi_{\max}q_cq^2}{N^2} + \frac{40\xi_{\max}q^4}{N^3}\,;$$

(b) When $q \le \frac{2^n}{13}$, $q_c = 0$, *and*

$$\frac{3\sum_{i=1}^{\alpha+\beta}|\mathcal{R}_i|}{N} + \frac{2q^2}{N^2} + \frac{6(n+1)^2}{N} \le 1\,,$$

it holds that

$$\left|\frac{h(\mathcal{G})N^q}{(N)_{q_P}(N)_{q_Q}} - 1\right| \le \frac{6\sum_{i=1}^{\alpha+\beta}|\mathcal{R}_i|}{N} + \frac{4q^2}{N^2} + \frac{12(n+1)^2}{N}\,.$$

Proof Overview. We give here a brief overview of the proof. The proof is almost similar to that of the existing Mirror theory. To be precise, the former proof shows that $\frac{h(\mathcal{G})N^q}{(N)_{q_P}(N)_{q_Q}} - 1$ has a lower bound. We complete the proof by showing that $\frac{h(\mathcal{G})N^q}{(N)_{q_P}(N)_{q_Q}} - 1$ has an upper bound in the same vein. To prove it, we count the number of solutions in each component involved in $\mathcal{G} = \sqcup_{i=1}^{\alpha+\beta}\mathcal{C}_i$ as shown by the lower bound. We do that first for the part consisting of components of size greater than two and then for the part of components of size two. We abuse the aforementioned notation $h(\cdot)$ for ease of description. Let $h(i)$ be the number of solutions to $\sqcup_{j=1}^{i}\mathcal{C}_j$ and $h(0) = 1$. Under this notation, it holds that $h(\alpha+\beta) = h(\mathcal{G})$. The key strategy is to show that $h(i+1)$ is bounded by a function of $h(i)$. Then the term $h(\mathcal{G}) = h(\alpha+\beta)$ can be computed by the recursive relation between $h(i)$ and $h(i+1)$.

In order to perform a sharp estimation, we also need to bound a term, namely $h'(P,Q)$, that appeared in the recursive relation tightly. Depending on whether there are large components (whether $q_c > 0$), we can distinguish the analysis of $h'(P,Q)$ into two cases, namely for $q_c > 0$ and $q_c = 0$. For the case $q_c = 0$, we reuse some results of [17] to obtain optimal bound. □

5 Multi-User Security of XoP

In this section, we consider the XoP construction that was first proposed by Bellare et al. [5]. This construction is used to obtain a secure pseudorandom

function from a block cipher. Here, in particular, we consider a version that involves two independent permutations.

Let $n \in \mathbb{N}$ and $\mathsf{P}, \mathsf{Q} \leftarrow_{\$} \mathsf{Perm}(n)$. One can define $\mathsf{XoP} : \mathsf{Perm}(n) \times \mathsf{Perm}(n) \times \{0,1\}^n \to \{0,1\}^n$ as the generic construction that takes permutations $\mathsf{P}, \mathsf{Q} \in \mathsf{Perm}(n)$ as keys, and on input X it returns

$$\mathsf{XoP}(X) \stackrel{\text{def}}{=} \mathsf{P}(X) \oplus \mathsf{Q}(X)\,.$$

Theorem 3 below gives the new mu-prf security of XoP.

Theorem 3. *Let n, u and $q_{\max}$ be positive integers such that $n > 10$ and $q_{\max} \leq \frac{2^n}{4n}$. Then one has*

$$\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{XoP}}(u, q_{\max}) \leq \frac{10u^{\frac{1}{2}}{q_{\max}}^2}{2^{2n}} + \frac{17u^{\frac{1}{2}}(n+1)^2}{2^n}\,.$$

The upper bound of adversarial advantage to distinguish between (multi-user) XoP and the uniformly random function in terms of the threshold number of queries is given by $O\left(\sqrt{u}{q_{\max}}^2/2^{2n}\right)$. This is strictly better bound to compare with the previous result of Choi et al. [14] by setting $m = n$ for SaT2 at ASIACRYPT 2022, where the result is $O\left(\sqrt{u}{q_{\max}}^{1.5}/2^{1.5n}\right)$. The difference between the above bounds comes from the difference between single-user bounds obtained by the Mirror theory and the χ^2 method. This way, the Squared-Ratio method can prove multi-user security tighter than previous analyses.

Proof. Suppose that a distinguisher $\mathcal{D}$ makes $q_{\max}$ queries $X_i \in \{0,1\}^n$, obtaining the corresponding responses $Z_i \in \{0,1\}^n$ for $i = 1, \ldots, q_{\max}$. In this way, $\mathcal{D}$ obtains a transcript

$$\tau = ((X_1, Z_1), \ldots, (X_{q_{\max}}, Z_{q_{\max}})).$$

In the real world, $P_i \stackrel{\text{def}}{=} \mathsf{P}(X_i)$ and $Q_i \stackrel{\text{def}}{=} \mathsf{Q}(X_i)$ should be a solution to the following system of equations.

$$\begin{cases} P_1 \oplus Q_1 = Z_1, \\ P_2 \oplus Q_2 = Z_2, \\ \qquad\vdots \\ P_{q_{\max}} \oplus Q_{q_{\max}} = Z_{q_{\max}}. \end{cases}$$

"Bad" Transcript Analysis. To upper-bound $|\mathcal{R}_i|$ corresponding to this system of equations for any $i \in [q_{\max}]$, we define a bad event as follows:

– $\mathsf{bad} \Leftrightarrow \exists (i_1, i_2 \ldots, i_n) \in [q_{\max}]^{*n}$ such that $Z_{i_1} = Z_{i_2} = \cdots = Z_{i_n}$.

For this bad event, we have

$$\Pr[\mathsf{bad}] = \frac{\binom{q_{\max}}{n}}{2^{n(n-1)}} \leq \frac{{q_{\max}}^n}{2^{n^2}} = \left(\frac{q_{\max}}{2^n}\right)^n . \tag{3}$$

"Good" Transcript Analysis. Let T_{re} and T_{id} be random variables following the distribution of the transcripts in the real world and the ideal world, respectively. Then we have

$$\frac{\Pr[\mathsf{T}_{\mathrm{re}} = \tau]}{\Pr[\mathsf{T}_{\mathrm{id}} = \tau]} = \frac{h(\mathcal{G}(\tau))2^{nq_{\max}}}{(2^n)_{q_{\max}}(2^n)_{q_{\max}}}.$$

Furthermore, since we ignore the "Bad" transcript, it holds that $|\mathcal{R}_i| \leq n$ for all indices i. It then implies that

$$\frac{3\sum_{i=1}^{q_{\max}} |\mathcal{R}_i|}{2^n} + \frac{2{q_{\max}}^2}{2^{2n}} + \frac{6(n+1)^2}{2^n} \leq \frac{3nq_{\max}}{2^n} + \frac{2{q_{\max}}^2}{2^{2n}} + \frac{6(n+1)^2}{2^n} \leq 1$$

for $n > 10$ and $q_{\max} \leq \frac{2^n}{4n}$. Therefore, by Corollary 1,

$$\left| \frac{h(\mathcal{G})2^{nq_{\max}}}{(2^n)_{|\mathcal{P}|}(2^n)_{|\mathcal{Q}|}} - 1 \right| \leq \frac{6\sum_{i=1}^{q_{\max}} |\mathcal{R}_i|}{2^n} + \frac{4{q_{\max}}^2}{2^{2n}} + \frac{12(n+1)^2}{2^n} .$$

Concluding the proof. Therefore, we can define

$$\epsilon_1(\tau) = \frac{6\sum_{i=1}^{q_{\max}} |\mathcal{R}_i|}{2^n} + \frac{4{q_{\max}}^2}{2^{2n}} + \frac{12(n+1)^2}{2^n} ,$$

and $\epsilon_2 = \left(\frac{q_{\max}}{2^n}\right)^n$. To apply the Theorem 1, we need to bound the expectation of $\epsilon_1(\tau)^2$ where the expectation is taken over the distribution of the ideal world. To be precise, we have

$$\begin{aligned}\mathbf{Ex}\left[\epsilon_1(\tau)^2\right] = \frac{36}{2^{2n}}\mathbf{Ex}\left[\left(\sum_{i=1}^{q_{\max}} |\mathcal{R}_i|\right)^2\right] + \left(\frac{4{q_{\max}}^2}{2^{2n}} + \frac{12(n+1)^2}{2^n}\right)^2 \\ + \frac{12}{2^n} \cdot \left(\frac{4{q_{\max}}^2}{2^{2n}} + \frac{12(n+1)^2}{2^n}\right) \cdot \mathbf{Ex}\left[\sum_{i=1}^{q_{\max}} |\mathcal{R}_i|\right] .\end{aligned} \tag{4}$$

On the other hand, by Lemma 3, we have

$$\begin{aligned}\mathbf{Ex}\left[\sum_{i=1}^{q_{\max}} |\mathcal{R}_i|\right] &\leq \frac{{q_{\max}}^2}{2^{n+1}} , \\ \mathbf{Ex}\left[\left(\sum_{i=1}^{q_{\max}} |\mathcal{R}_i|\right)^2\right] &\leq \frac{{q_{\max}}^2}{2^{n+1}} + \frac{{q_{\max}}^4}{2^{2n+2}} .\end{aligned}$$

Using the derived bounds in (4), we obtain

$$\begin{aligned}\mathbf{Ex}\left[\epsilon_1(\tau)^2\right] &\le \frac{49{q_{\max}}^4}{2^{4n}} + \frac{18{q_{\max}}^2}{2^{3n}} + \frac{168{q_{\max}}^2(n+1)^2}{2^{3n}} + \frac{144(n+1)^4}{2^{2n}} \\ &\le \frac{49{q_{\max}}^4}{2^{4n}} + \frac{169{q_{\max}}^2(n+1)^2}{2^{3n}} + \frac{144(n+1)^4}{2^{2n}}\,. \end{aligned} \tag{5}$$

By utilizing (5) and (3) in the Theorem 1, we have

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{XoP}}(u, q_{\max}) &\le \sqrt{2u\mathbf{Ex}\left[\epsilon_1(\tau)^2\right]} + 2u\epsilon_2(\tau) \\ &\le \sqrt{2u\left(\frac{49{q_{\max}}^4}{2^{4n}} + \frac{169{q_{\max}}^2(n+1)^2}{2^{3n}} + \frac{144(n+1)^4}{2^{2n}}\right)} + 2u\left(\frac{q_{\max}}{2^n}\right)^n \\ &\le \sqrt{\frac{98u{q_{\max}}^4}{2^{4n}}} + \sqrt{\frac{288u(n+1)^4}{2^{2n}}} + 2u\left(\frac{q_{\max}}{2^n}\right)^n \\ &\le \frac{10u^{\frac{1}{2}}{q_{\max}}^2}{2^{2n}} + \frac{17u^{\frac{1}{2}}(n+1)^2}{2^n}\,. \end{aligned}$$

This completes the proof. □

6 Multi-User Security of EDM

In this section, we consider the EDM construction proposed by Cogliati and Seurin [20]. Let $n \in \mathbb{N}$ and $\mathsf{P}, \mathsf{Q} \leftarrow_{\$} \mathsf{Perm}(n)$. One can define $\mathsf{EDM} : \mathsf{Perm}(n) \times \mathsf{Perm}(n) \times \{0,1\}^n \to \{0,1\}^n$ as the generic construction that takes permutations $\mathsf{P}, \mathsf{Q} \in \mathsf{Perm}(n)$ as keys, and on input X it returns

$$\mathsf{EDM}(X) \stackrel{\text{def}}{=} \mathsf{Q}(\mathsf{P}(X) \oplus X)\,.$$

Theorem 4 below gives the new mu-prf security of EDM.

Theorem 4. *Let n, u and $q_{\max}$ be positive integers such that $n > 5$ and $q_{\max} \le \frac{2^{3n/4}}{4n}$. Then one has*

$$\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{EDM}}(u, q_{\max}) \le \frac{9u^{1/2}n{q_{\max}}^3}{2^{2.5n}} + \frac{122u^{1/2}n{q_{\max}}^4}{2^{3n}}\,.$$

Therefore, the upper bound of adversarial advantage to distinguish between (multi-user) EDM and the uniformly random function in terms of the threshold number of queries is given by $O\left(n\sqrt{u}{q_{\max}}^4/2^{3n}\right)$, significantly better than the result of Dai et al. [21] at CRYPTO 2017 with the hybrid argument: $O\left(uq^2/2^{1.5n}\right)$. Note that for the case where $q = uq_{\max}$, the result of Dai et al. only gives us $O\left(u^3{q_{\max}}^2/2^{1.5n}\right)$, which makes EDM insecure even for $q_{\max} = O(1)$ when the number of users is $u = O\left(2^{\frac{n}{2}}\right)$. On the other hand, our bound ensures that EDM is still beyond birthday-bound secure with the same u.

Proof. Suppose that a distinguisher $\mathcal{D}$ makes $q_{\max}$ queries $X_i \in \{0,1\}^n$, obtaining the corresponding responses $Z_i \in \{0,1\}^n$ for $i = 1, \ldots, q_{\max}$. In this way, $\mathcal{D}$ obtains a transcript

$$\tau = ((X_1, Z_1), \ldots, (X_{q_{\max}}, Z_{q_{\max}})).$$

In the real world, $P_i \stackrel{\text{def}}{=} \mathsf{P}(X_i)$ and $Q_i \stackrel{\text{def}}{=} \mathsf{Q}^{-1}(Z_i)$ should be a solution to the following system of equations while regarding Q^{-1} as a permutation.

$$\begin{cases} P_1 \oplus Q_1 = X_1, \\ P_2 \oplus Q_2 = X_2, \\ \qquad \vdots \\ P_{q_{\max}} \oplus Q_{q_{\max}} = X_{q_{\max}}. \end{cases}$$

"Bad" Transcript Analysis. To upper-bound $\xi_{\max}$ (bad_1), $\sum_{i=1}^{\alpha+\beta} |\mathcal{R}_i|$ (bad_2), and q_c (bad_3), for a fixed $A > 0$, we define bad events as follows:

- $\mathsf{bad}_1 \Leftrightarrow \exists (i_1, i_2 \ldots, i_n) \in [q_{\max}]^{*n}$ such that $Z_{i_1} = Z_{i_2} = \cdots = Z_{i_n}$,
- $\mathsf{bad}_2 \Leftrightarrow \exists (i_1, i'_1, i_2, i'_2 \ldots, i_{n-1}, i'_{n-1}) \in [q_{\max}]^{*(2n-2)}$ such that $X_{i_1} \oplus X_{i'_1} = X_{i_j} \oplus X_{i'_j}$ and $Z_{i_j} = Z_{i'_j}$ for all $j \in [n-1]$,
- $\mathsf{bad}_3 \Leftrightarrow q_c \geq \frac{{q_{\max}}^2}{2^{n+1}} + \frac{2^{2n}}{8n{q_{\max}}^2}$.

1. We have

$$\Pr[\mathsf{bad}_1] = \frac{\binom{q_{\max}}{n}}{2^{n(n-1)}} \leq \frac{{q_{\max}}^n}{2^{n^2}} = \left(\frac{q_{\max}}{2^n}\right)^n .$$

2. Let $\mathcal{B} = \{(i_1, i'_1, i_2, i'_2 \ldots, i_{n-1}, i'_{n-1}) \in [q_{\max}]^{*(2n-2)} \mid X_{i_1} \oplus X_{i'_1} = X_{i_j} \oplus X_{i'_j}$ for all $j \in [n-1]\}$, we have

$$\Pr[\mathsf{bad}_2] = \frac{|\mathcal{B}|}{2^{n(n-2)}} \leq \frac{2^n \binom{q_{\max}/2}{n-1}}{2^{n(n-2)}} \leq \left(\frac{q_{\max}}{2^n}\right)^{n-1} .$$

3. By Lemma 3 with $A = \frac{2^{2n}}{8n{q_{\max}}^2}$, we have

$$\Pr[\mathsf{bad}_3] \leq \frac{32n^2{q_{\max}}^6}{2^{5n}} + \frac{16n^2{q_{\max}}^8}{2^{6n}} .$$

In conclusion, we have

$$\Pr[\mathsf{bad}_1 \vee \mathsf{bad}_2 \vee \mathsf{bad}_3] \leq 2\left(\frac{q_{\max}}{2^n}\right)^{n-1} + \frac{32n^2{q_{\max}}^6}{2^{5n}} + \frac{16n^2{q_{\max}}^8}{2^{6n}} .$$

"Good" Transcript Analysis. Note that

$$\frac{\Pr[\mathsf{T}_{\text{re}} = \tau]}{\Pr[\mathsf{T}_{\text{id}} = \tau]} = \frac{h(\mathcal{G}(\tau))2^{nq_{\max}}}{(2^n)_{|\mathcal{P}|}(2^n)_{|\mathcal{Q}|}}$$

and $\sum_{i=1}^{\alpha}(\xi(\mathcal{C}_i)-1) = q_c$. In order to upper-bound $|\mathcal{R}_i|$, we distinguish into following two cases, namely when $i \in [\alpha]$ and $i \in [\alpha+1, \alpha+\beta]$. We first consider $i \in [\alpha]$, note that we have $\xi_{\max} \leq n$ by $\neg\mathsf{bad}_1$, hence there are at most

$$\binom{\xi(\mathcal{C}_i)+1}{2} \leq \frac{(n+1)\xi(\mathcal{C}_i)}{2}$$

ways to choose trails of i-th component. For each of those trails, there can be at most $n-1$ trails with the same label by $\neg\mathsf{bad}_2$. So we have

$$|\mathcal{R}_i| \leq \frac{(n+1)\xi(\mathcal{C}_i)}{2} \cdot (n-1) \leq \frac{n^2\xi(\mathcal{C}_i)}{2}\,.$$

Now we consider $i \in [\alpha+1, \alpha+\beta]$, note that since we are considering the nonce-respecting adversary, two nonces can never collide, therefore the label values of two single-edge trails cannot be the same. Hence there are at most

$$\sum_{k=1}^{\alpha}\binom{\xi(\mathcal{C}_k)}{2} \leq \frac{nq_c}{2}$$

trails of two joint edges (in the first α components) of which the label can be the same as the unique label of the i-th component (consists of one edge). Also, a label of any trail of two joint edges cannot simultaneously collide with the labels of two different components i and j, for any $j \neq i \in [\alpha+1, \alpha+\beta]$. Since that means the unique label values of components i and j are the same, which contradicts the nonce-respecting assumption. This observation makes us have

$$\sum_{i=\alpha+1}^{\alpha+\beta}|\mathcal{R}_i| \leq \frac{nq_c}{2}\,.$$

It follows that

$$\sum_{i=1}^{\alpha+\beta}|\mathcal{R}_i| \leq \left(\sum_{i=1}^{\alpha}\frac{n^2\xi(\mathcal{C}_i)}{2}\right) + \frac{nq_c}{2} \leq \frac{3n^2q_c}{4} + \frac{nq_c}{2}\,.$$

Furthermore, by $\neg\mathsf{bad}_3$ and $n > 5$, we also have

$$\begin{aligned}&\frac{2\sum_{i=1}^{\alpha+\beta}|\mathcal{R}_i| + 2nq_c}{2^n} + \frac{4nq_c{q_{\max}}^2}{2^{2n}} + \frac{20n{q_{\max}}^4}{2^{3n}}\\ &\quad\leq \frac{2n^2q_c}{2^n} + \frac{4nq_c{q_{\max}}^2}{2^{2n}} + \frac{20n{q_{\max}}^4}{2^{3n}} \leq 1\,.\end{aligned}$$

By Corollary 1 and the above, we have

$$\left|\frac{h(\mathcal{G})2^{nq}}{(2^n)_{|\mathcal{P}|}(2^n)_{|\mathcal{Q}|}} - 1\right| \leq \frac{4n^2q_c}{2^n} + \frac{8nq_c{q_{\max}}^2}{2^{2n}} + \frac{40n{q_{\max}}^4}{2^{3n}}\,.$$

Concluding the proof. Hence we can set

$$\epsilon_1(\tau) = \frac{4n^2 q_c}{2^n} + \frac{8nq_c {q_{\max}}^2}{2^{2n}} + \frac{40n{q_{\max}}^4}{2^{3n}},$$

and

$$\epsilon_2 = 2\left(\frac{q_{\max}}{2^n}\right)^{n-1} + \frac{32n^2{q_{\max}}^6}{2^{5n}} + \frac{16n^2{q_{\max}}^8}{2^{6n}}$$

for Theorem 1. We need to compute the expectation of $\epsilon_1(\tau)^2$ where the expectation is taken over the distribution of the ideal world. It gives an identity:

$$\begin{aligned}\mathbf{Ex}\left[\epsilon_1(\tau)^2\right] = &\left(\frac{4n^2}{2^n} + \frac{8n{q_{\max}}^2}{2^{2n}}\right)^2 \mathbf{Ex}\left[q_c^2\right] + \frac{1600n^2{q_{\max}}^8}{2^{6n}} \\ &+ 2\left(\frac{4n^2}{2^n} + \frac{8n{q_{\max}}^2}{2^{2n}}\right)\frac{40n{q_{\max}}^4}{2^{3n}}\mathbf{Ex}\left[q_c\right].\end{aligned}$$

By Lemma 3, we have

$$\begin{aligned}\mathbf{Ex}\left[q_c\right] &\le \frac{{q_{\max}}^2}{2^{n+1}}, \\ \mathbf{Ex}\left[q_c^2\right] &\le \frac{{q_{\max}}^2}{2^{n+1}} + \frac{{q_{\max}}^4}{2^{2n+2}}\end{aligned}$$

Combining it together, it implies that:

$$\begin{aligned}\mathbf{Ex}\left[\epsilon_1(\tau)^2\right] = &\left(\frac{{q_{\max}}^2}{2^{n+1}} + \frac{{q_{\max}}^4}{2^{2n+2}}\right)\left(\frac{4n^2}{2^n} + \frac{8n{q_{\max}}^2}{2^{2n}}\right)^2 + \frac{1600n^2{q_{\max}}^8}{2^{6n}} \\ &+ \frac{{q_{\max}}^2}{2^{n+1}}\left(\frac{4n^2}{2^n} + \frac{8n{q_{\max}}^2}{2^{2n}}\right)\frac{80n{q_{\max}}^4}{2^{3n}}. \qquad (6)\end{aligned}$$

Under the constraint $q_{\max} \le \frac{2^{3n/4}}{4n}$, it holds that $\frac{4n^2}{2^n} + \frac{8n{q_{\max}}^2}{2^{2n}} \le \frac{9n{q_{\max}}^2}{2^{2n}} \le 1$. Using the inequality, the equality (6) can be bounded by:

$$\mathbf{Ex}\left[\epsilon_1(\tau)^2\right] \le \left(\frac{{q_{\max}}^2}{2^{n+1}} + \frac{{q_{\max}}^4}{2^{2n+2}}\right)\frac{81n^2{q_{\max}}^4}{2^{4n}} + \frac{360n^2{q_{\max}}^8}{2^{6n}} + \frac{1600n^2{q_{\max}}^8}{2^{6n}}.$$

The Theorem 1 then gives

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{EDM}}(u, q_{\max}) \le &\left(\frac{q_{\max}}{2^{n/2}} + \frac{{q_{\max}}^2}{2^{n+1}}\right)\frac{9\sqrt{2u}n{q_{\max}}^2}{2^{2n}} + \frac{\sqrt{720u}n{q_{\max}}^4}{2^{3n}} \\ &+ \frac{\sqrt{3200u}n{q_{\max}}^4}{2^{3n}} + 4u\left(\frac{q_{\max}}{2^n}\right)^{n-1} + \frac{64un^2{q_{\max}}^6}{2^{5n}} + \frac{32un^2{q_{\max}}^8}{2^{6n}}.\end{aligned}$$

When $q_{\max} \le \frac{2^{3n/4}}{4n}$, it can be bounded by

$$\frac{9u^{1/2}n{q_{\max}}^3}{2^{2.5n}} + \frac{122u^{1/2}n{q_{\max}}^4}{2^{3n}}.$$

This completes the proof. □

7 Multi-User Security of a Variant of nEHtM in the Nonce-Respecting Setting

In this section, we consider mu-prf security of a variant of nEHtM proposed by Dutta et al. [23], based on an n-bit δ-AXU hash function H with a hash key K_h and two random permutations P and Q. A tag T is an output of nEHtM generated by a message M with an n-bit nonce N:

$$T = P(N) \oplus Q(H_{K_h}(M) \oplus N).$$

We will consider a nonce-respecting setting that assumes nonces never repeat. we have the following theorem.

Theorem 5. *Let $\delta > 0$, and let $H : \mathcal{K} \times \mathcal{M} \to \{0,1\}^n$ be a δ-almost AXU hash function. For positive integers u, $q_{\max}$, and L such that $4 \le n \le L \le \min\left\{\frac{2^n}{4q_{\max}}, \frac{2^{3n}}{20{q_{\max}}^4}\right\}$, we have*

$$\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{nEHtM}}(u, q_{\max}) \le \frac{4(2u)^{1/2}}{2^n}\left(\frac{q_{\max}}{2^{n/2}} + \frac{{q_{\max}}^2}{2^{n+1}}\right) + \frac{47u^{1/2}(n+1)L{q_{\max}}^2\delta}{2^n}$$
$$+ \frac{36u^{1/2}L{q_{\max}}^4\delta}{2^{2n}} + \frac{2u{q_{\max}}^2\delta}{2^n} + \frac{4uq_{\max}^2\delta}{L^2} + 2u\left(\frac{q_{\max}L}{2^n}\right)^{n-1} + \frac{65u^{1/2}L{q_{\max}}^4}{2^{3n}}.$$

Suppose that $\delta = O\left(\frac{\ell}{2^n}\right)$ for a constant ℓ. We can now optimize the advantage over L in the Theorem 5 via arithmetic-geometric mean inequality. In other words, we can set the L to $\left(\frac{2^n\sqrt{u}}{n}\right)^{1/3}$ and $\left(\frac{2^{2n}\sqrt{u}}{q_{\max}^2}\right)^{1/3}$ for sufficiently small u, respectively. We thus have the following corollary:

Corollary 2. *Assume $\delta = O\left(\frac{\ell}{2^n}\right)$ for a constant ℓ. Then one has*

$$\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{nEHtM}}(u, q_{\max}) \le \begin{cases} O\left(\frac{\ell u{q_{\max}}^2}{2^{2n}} + \frac{\ell(un)^{\frac{2}{3}}{q_{\max}}^2}{2^{\frac{5n}{3}}}\right) & \text{if } q_{\max} \le O(2^{\frac{n}{2}}) \\ O\left(\frac{\ell u{q_{\max}}^2}{2^{2n}} + \frac{\ell u^{\frac{2}{3}}{q_{\max}}^{\frac{10}{3}}}{2^{\frac{7n}{3}}}\right) & \text{if } q_{\max} \ge O(2^{\frac{n}{2}}) \end{cases}.$$

Since the previous bound of two permutations case [13] is slightly worst than that of a single permutation [16] in the multi-user setting, we will recall the result by Choi et al. [16] for comparison (by ignoring the nonce-misuse terms):

$$\frac{uq}{2^n} + \frac{u\ell^{\frac{1}{2}}q^2}{2^{\frac{3n}{2}}},$$

where $q_{\max} \le q \le u \cdot q_{\max}$ in our notation. Figure 1 shows the results of graphing our bounds and the previous bounds as functions of $\log_2(u)$: the level of security given by Choi et al. is in the shaded area of Figure 1 and depends on the value of q. For example, fixing $\log_2(u) = n/2$, the security bound of Choi et al. lies between $O(1)$ (for $q = u \cdot q_{\max}$) and $O(2^{\frac{n}{2}})$ (for $q = q_{\max}$). We see that our new bound improves over the result of Choi et al. [16] when the number of users becomes large, and is superior for $u \ge O\left(2^{\frac{n}{26}}\right)$ and $2^{\frac{n}{26}} \approx 30.3$ if $n = 128$ and $q = u \cdot q_{\max}$.

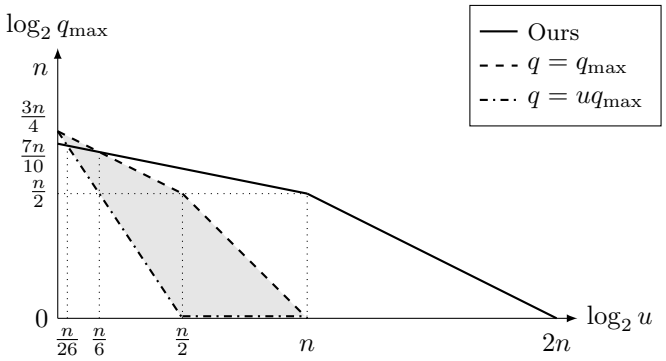

Fig. 1: Comparison of the security bounds (in terms of the threshold number of queries per user) as functions of $\log_2 u$. The solid line represents our bounds, and the dashed line (resp. the dash-dotted line) represents the previous bound by the hybrid argument where $q = q_{\max}$ (resp. $q = u \cdot q_{\max}$). We neglect the logarithmic term n.

Proof (of Theorem 5). Suppose that a distinguisher $\mathcal{D}$ makes $q_{\max}$ queries (N_i, M_i), obtaining the corresponding responses $T_i \in \{0,1\}^n$ for $i = 1, \ldots, q_{\max}$. Recall that $N_i \neq N_j$ if $i \neq j$ for all $i, j \in [q_{\max}]$ by the nonce-respecting assumption. $\mathcal{D}$ obtains a transcript

$$\tau = ((N_1, M_1, T_1), \ldots, (N_{q_{\max}}, M_{q_{\max}}, T_{q_{\max}}), K_h),$$

where K_h is given for free at the end of the attack. From τ, one can fix $X_i \stackrel{\text{def}}{=} H_{K_h}(M_i) \oplus N_i$ for $i = 1, \ldots, q_{\max}$. In the real world, $P_i \stackrel{\text{def}}{=} \mathsf{P}(N_i)$ and $Q_i \stackrel{\text{def}}{=} \mathsf{Q}(X_i)$ should be a solution to the following system of equations.

$$\begin{cases} P_1 \oplus Q_1 = T_1, \\ P_2 \oplus Q_2 = T_2, \\ \qquad \vdots \\ P_{q_{\max}} \oplus Q_{q_{\max}} = T_{q_{\max}}. \end{cases}$$

"Bad" Transcript Analysis. Let L be an arbitrary number such that $4 \leq n \leq L \leq \min\left\{\frac{2^n}{4q_{\max}}, \frac{2^{3n}}{20{q_{\max}}^4}\right\}$. To satisfy the non-degeneracy property (bad_1) and to upper-bound $\xi_{\max}$ (bad_2), $\sum_{i=1}^{\alpha+\beta} |\mathcal{R}_i|$ (bad_3 and bad_4) and q_c (bad_5), we define bad events as follows:

- $\mathsf{bad}_1 \Leftrightarrow$ there exists $(i, j) \in [q_{\max}]^{*2}$ such that $X_i = X_j$ and $T_i = T_j$;
- $\mathsf{bad}_2 \Leftrightarrow \exists (i_1, i_2 \ldots, i_L) \in [q_{\max}]^{*L}$ such that $X_{i_1} = X_{i_2} = \cdots = X_{i_L}$,
- $\mathsf{bad}_3 \Leftrightarrow \exists (i_1, i_2, \ldots, i_n) \in [q_{\max}]^{*n}$ such that $T_{i_1} = T_{i_2} = \cdots = T_{i_n}$,
- $\mathsf{bad}_4 \Leftrightarrow \exists (i_1, i'_1, i_2, i'_2 \ldots, i_{n-1}, i'_{n-1}) \in [q_{\max}]^{*2n-2}$ such that $T_{i_1} \oplus T_{i'_1} = T_{i_j} \oplus T_{i'_j}$ and $X_{i_j} = X_{i'_j}$ for all $j \in [n-1]$.

– $\mathsf{bad}_5 \Leftrightarrow q_c \geq \frac{{q_{\max}}^2}{2^{n+1}} + \frac{2^{2n}}{4L{q_{\max}}^2}$.

1. For $(i,j) \in [q_{\max}]^{*2}$ such that $X_i = X_j$, since $N_i \neq N_j$, $\Pr[T_i = T_j] = \frac{1}{2^n}$ in the ideal world. There are at most $q_{\max}^2\delta$ pairs (i,j), and thus
$$\Pr[\mathsf{bad}_1] \leq \frac{{q_{\max}}^2\delta}{2^n}.$$
2. Let Col be the number of pairs $(i,j) \in [q_{\max}]^{*2}$ such that $X_i = X_j$ and $i < j$. Since $\mathbf{Ex}[\mathsf{Col}] \leq \frac{q_{\max}^2\delta}{2}$ and $(N_i, M_i) \neq (N_j, M_j)$ for all $i \neq j$, we can bound the probability that bad_2 happens as
$$\begin{aligned}\Pr[\mathsf{bad}_2] &= \Pr[\xi_{\max} - 1 \geq L] = \Pr\left[(\xi_{\max}-1)^2 \geq L^2\right] \\ &\leq \Pr\left[\sum_{i=1}^{\alpha} (\xi(C_i)-1)^2 \geq L^2\right] \\ &\leq \Pr\left[2\mathsf{Col} + \sum_{i=1}^{\alpha} (\xi(C_i)-1) \geq L^2\right] \\ &\leq \Pr\left[4\mathsf{Col} \geq L^2\right] \leq \frac{2q_{\max}^2\delta}{L^2}.\end{aligned}$$
Note that this is the same technique as Corollary 4.1. in Jha and Nandi [28], where our result relies on the δ-AXU property instead of the almost universal property.
3. We have
$$\Pr[\mathsf{bad}_3] = \frac{\binom{q_{\max}}{n}}{2^{n(n-1)}} \leq \frac{{q_{\max}}^n}{2^{n^2}} = \left(\frac{q_{\max}}{2^n}\right)^n.$$
4. We will bound the probability of bad_4 under the condition of $\neg\mathsf{bad}_2$. Let $\mathcal{B} = \{(i_1, i'_1, i_2, i'_2 \ldots, i_{n-1}, i'_{n-1}) \in [q_{\max}]^{*(2n-2)} \mid X_{i_j} = X_{i'_j} \text{ for all } j \in [n-1]\}$. By $\neg\mathsf{bad}_2$, we have
$$|\mathcal{B}| \leq \binom{q_{\max}}{n-1}(L-1)^{n-1} \leq \frac{(q_{\max}(L-1))^{n-1}}{2^n}.$$
Thus we have
$$\Pr\left[T_{i_1} \oplus T_{i'_1} = T_{i_j} \oplus T_{i'_j}\right] = \frac{1}{2^n}$$
and
$$\Pr[\mathsf{bad}_4 \mid \neg\mathsf{bad}_2] = \frac{|\mathcal{B}|}{2^{n(n-2)}} \leq \left(\frac{q_{\max}(L-1)}{2^n}\right)^{n-1}.$$
5. By Lemma 3 with $A = \frac{2^{2n}}{4L{q_{\max}}^2}$, we have
$$\Pr[\mathsf{bad}_5] \leq \frac{2L^2{q_{\max}}^6}{2^{5n}} + \frac{64L^2{q_{\max}}^8}{2^{6n}}.$$

In conclusion, we have

$$\begin{aligned}
&\Pr[\mathsf{bad}_1 \vee \mathsf{bad}_2 \vee \mathsf{bad}_3 \vee \mathsf{bad}_4 \vee \mathsf{bad}_5] \\
&\quad \leq \Pr[\mathsf{bad}_1] + \Pr[\mathsf{bad}_2] + \Pr[\mathsf{bad}_3] + \Pr[\mathsf{bad}_4 \mid \neg\mathsf{bad}_2] + \Pr[\mathsf{bad}_5] \\
&\quad \leq \frac{{q_{\max}}^2\delta}{2^n} + \frac{2q_{\max}^2\delta}{L^2} + \left(\frac{q_{\max}}{2^n}\right)^n + \left(\frac{q_{\max}(L-1)}{2^n}\right)^{n-1} + \frac{2L{q_{\max}}^6}{2^{5n}} + \frac{4L^2{q_{\max}}^8}{2^{6n}} \\
&\quad \leq \frac{{q_{\max}}^2\delta}{2^n} + \frac{2q_{\max}^2\delta}{L^2} + \left(\frac{q_{\max}L}{2^n}\right)^{n-1} + \frac{2L^2{q_{\max}}^6}{2^{5n}} + \frac{4L^2{q_{\max}}^8}{2^{6n}} .
\end{aligned}$$

"Good" Transcript Analysis. Note that

$$\frac{\Pr\left[\mathsf{T}_{\mathrm{re}} = \tau\right]}{\Pr\left[\mathsf{T}_{\mathrm{id}} = \tau\right]} = \frac{h(\mathcal{G}(\tau))N^{q_{\max}}}{(N)_{|\mathcal{P}|}(N)_{|\mathcal{Q}|}}$$

and we denote the transcript graph $\mathcal{G}(\tau) = (\mathcal{V}, \mathcal{E})$. We define the following sets

$$\begin{aligned}
\mathcal{S}_i &= \left\{ (\{V_1, V_1'\}, \{V_2, V_2'\}) \in \mathcal{R}_i \,\middle|\, \overline{V_1V_1'}, \overline{V_2V_2'} \in \mathcal{E} \right\} , \\
\mathcal{D}_i &= \mathcal{R}_i \setminus \mathcal{S}_i .
\end{aligned}$$

Since $|\mathcal{R}_i| = |\mathcal{S}_i| + |\mathcal{D}_i|$, we will first focus on upper-bounding $|\mathcal{D}_i|$. Recall that $\sum_{i=1}^{\alpha} (\xi(\mathcal{C}_i) - 1) = q_c$. In order to upper-bound $|\mathcal{D}_i|$, we distinguish into following two cases, namely when $i \in [\alpha]$ and $i \in [\alpha+1, \alpha+\beta]$. We first consider $i \in [\alpha]$, note that we have $\xi_{\max} \leq L$ by $\neg\mathsf{bad}_2$, hence there are at most

$$\binom{\xi(\mathcal{C}_i)+1}{2} \leq \frac{(L+1)\xi(\mathcal{C}_i)}{2}$$

ways to choose trails of i-th component. By $\neg\mathsf{bad}_3$ and $\neg\mathsf{bad}_4$, if the chosen trail consists of two edges, there are at most n trails of a single edge and $(n-2)$ trails of two joint edges with the same label to the chosen trail. Similarly, if the chosen trail consists of a single edge, there are at most $(n-1)$ trails of two joint edges. For each case, there can be at most $(2n-2)$ trails with the same label. So we have

$$|\mathcal{D}_i| \leq \frac{(L+1)\xi(\mathcal{C}_i)}{2} \cdot (2n-2) \leq nL\xi(\mathcal{C}_i)$$

since $L \geq n$. Now we consider $i \in [\alpha+1, \alpha+\beta]$, note that there are at most

$$\sum_{k=1}^{\alpha} \binom{\xi(\mathcal{C}_k)}{2} \leq \frac{Lq_c}{2}$$

trails of two joint edges (in the first α components) of which the label can be the same as the unique label of the i-th component (consists of one edge). Also, by $\neg\mathsf{bad}_3$, there are at most n different components in $[\alpha+1, \alpha+\beta]$ that share the same label value (single edge components) with the label of i-th component. This observation makes us have

$$\sum_{i=\alpha+1}^{\alpha+\beta} |\mathcal{D}_i| \leq \frac{nLq_c}{2} .$$

It follows that

$$\sum_{i=1}^{\alpha+\beta} |\mathcal{D}_i| \le \left(\sum_{i=1}^{\alpha} nL\xi(\mathcal{C}_i) \right) + \frac{nLq_c}{2} \le \frac{3nLq_c}{2} + \frac{nLq_c}{2} \le 2nLq_c \,.$$

Furthermore, by $\neg\mathsf{bad}_3$ and $\neg\mathsf{bad}_5$, we also have $4 \le n \le L \le \min\left\{ \frac{2^n}{4q_{\max}}, \frac{2^{3n}}{20{q_{\max}}^4} \right\}$

$$\begin{aligned} &\frac{2\sum_{i=1}^{\alpha+\beta} |\mathcal{S}_i|}{2^n} + \frac{2(n+1)Lq_c}{2^n} + \frac{4Lq_c{q_{\max}}^2}{2^{2n}} + \frac{20L{q_{\max}}^4}{2^{3n}} \\ &\quad \le \frac{2nq_{\max}}{2^n} + \frac{2(n+1)Lq_c}{2^n} + \frac{4Lq_c{q_{\max}}^2}{2^{2n}} + \frac{20L{q_{\max}}^4}{2^{3n}} \le 1 \,. \end{aligned}$$

By Corollary 1 and the above, we have

$$\left| \frac{h(\mathcal{G})2^{nq_{\max}}}{(2^n)_{|\mathcal{P}|}(2^n)_{|\mathcal{Q}|}} - 1 \right| \le \frac{4\sum_{i=1}^{\alpha+\beta} |\mathcal{S}_i|}{2^n} + \frac{4(n+1)Lq_c}{2^n} + \frac{8Lq_c{q_{\max}}^2}{2^{2n}} + \frac{40L{q_{\max}}^4}{2^{3n}} \,.$$

Concluding the proof. Now we can set

$$\epsilon_1(\tau) = \frac{4\sum_{i=1}^{\alpha+\beta} |\mathcal{S}_i|}{2^n} + \frac{4(n+1)Lq_c}{2^n} + \frac{8Lq_c{q_{\max}}^2}{2^{2n}} + \frac{40L{q_{\max}}^4}{2^{3n}} \,,$$

and

$$\epsilon_2 = \frac{{q_{\max}}^2\delta}{2^n} + \frac{2q^2\delta}{L^2} + \left(\frac{q_{\max}L}{2^n} \right)^{n-1} + \frac{2L^2{q_{\max}}^6}{2^{5n}} + \frac{4L^2{q_{\max}}^8}{2^{6n}}$$

for Theorem 1. We need to compute the expectation of $\epsilon_1(\tau)^2$ where the expectation is taken over the distribution of the ideal world. To be precise, we have

$$\begin{aligned} \mathbf{Ex}\left[\epsilon_1(\tau)^2\right] &= \frac{16}{2^{2n}}\mathbf{Ex}\left[\left(\sum_{i=1}^{\alpha+\beta} |\mathcal{S}_i| \right)^2 \right] + \left(\frac{4(n+1)L}{2^n} + \frac{8L{q_{\max}}^2}{2^{2n}} \right)^2 \mathbf{Ex}\left[q_c^2\right] \\ &\quad + \frac{8}{2^n}\left(\frac{4(n+1)L}{2^n} + \frac{8L{q_{\max}}^2}{2^{2n}} \right) \mathbf{Ex}\left[q_c \sum_{i=1}^{\alpha+\beta} |\mathcal{S}_i| \right] + \frac{1600L^2{q_{\max}}^8}{2^{6n}} \\ &\quad + \frac{8}{2^n} \cdot \frac{40L{q_{\max}}^4}{2^{3n}}\mathbf{Ex}\left[\sum_{i=1}^{\alpha+\beta} |\mathcal{S}_i| \right] + \left(\frac{4(n+1)L}{2^n} + \frac{8L{q_{\max}}^2}{2^{2n}} \right) \frac{80L{q_{\max}}^4}{2^{3n}}\mathbf{Ex}\left[q_c\right] \,, \end{aligned}$$

By Lemma 3, we have

$$\mathbf{Ex}\left[\sum_{i=1}^{\alpha+\beta}|\mathcal{S}_i|\right] \le \frac{{q_{\max}}^2}{2^{n+1}}\,,$$
$$\mathbf{Ex}\left[\left(\sum_{i=1}^{\alpha+\beta}|\mathcal{S}_i|\right)^2\right] \le \frac{{q_{\max}}^2}{2^{n+1}} + \frac{{q_{\max}}^4}{2^{2n+2}}\,,$$
$$\mathbf{Ex}\left[q_c\right] \le \frac{{q_{\max}}^2\delta}{2}\,,$$
$$\mathbf{Ex}\left[q_c^2\right] \le \frac{{q_{\max}}^2\delta}{2} + \frac{{q_{\max}}^4\delta^2}{4}\,.$$

Note that

$$\mathbf{Ex}\left[q_c\sum_{i=1}^{\alpha+\beta}|\mathcal{S}_i|\right] = \mathbf{Ex}\left[q_c\right]\mathbf{Ex}\left[\sum_{i=1}^{\alpha+\beta}|\mathcal{S}_i|\right] \le \frac{{q_{\max}}^4\delta}{2^{n+2}}\,,$$

since q_c and $\mathcal{S}_i$ are independent in the ideal world. Combining it together, it implies that:

$$\begin{aligned}\mathbf{Ex}\left[\epsilon_1(\tau)^2\right] \le{}& \frac{16}{2^{2n}}\left(\frac{{q_{\max}}^2}{2^{n+1}} + \frac{{q_{\max}}^4}{2^{2n+2}}\right) + \left(\frac{4(n+1)L}{2^n} + \frac{8L{q_{\max}}^2}{2^{2n}}\right)\frac{2{q_{\max}}^4\delta}{2^{2n}}\\ &+ \left(\frac{4(n+1)L}{2^n} + \frac{8L{q_{\max}}^2}{2^{2n}}\right)^2\left(\frac{{q_{\max}}^2\delta}{2} + \frac{{q_{\max}}^4\delta^2}{4}\right) + \frac{160L{q_{\max}}^6}{2^{5n}}\\ &+ \left(\frac{4(n+1)L}{2^n} + \frac{8L{q_{\max}}^2}{2^{2n}}\right)\frac{40L{q_{\max}}^6\delta}{2^{3n}} + \frac{1600L^2{q_{\max}}^8}{2^{6n}}\,,\end{aligned}$$

and Theorem 1 then gives

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{nEHtM}}(u, q_{\max}) \le{}& \frac{4\sqrt{2u}}{2^n}\left(\frac{q_{\max}}{2^{n/2}} + \frac{{q_{\max}}^2}{2^{n+1}}\right) + \frac{4\sqrt{u(n+1)L\delta}{q_{\max}}^2}{2^{1.5n}} + \frac{\sqrt{32uL\delta}{q_{\max}}^3}{2^{2n}}\\ &+ \left(\frac{4\sqrt{2u}(n+1)L}{2^n} + \frac{8\sqrt{2u}L{q_{\max}}^2}{2^{2n}}\right)\left(q_{\max}\delta^{1/2} + \frac{{q_{\max}}^2\delta}{2}\right)\\ &+ \frac{\sqrt{320uL}{q_{\max}}^3}{2^{2.5n}} + \frac{\sqrt{320u(n+1)\delta L}{q_{\max}}^3}{2^{2n}} + \frac{\sqrt{640u\delta}L{q_{\max}}^4}{2^{2.5n}} + \frac{\sqrt{3200u}L{q_{\max}}^4}{2^{3n}}\\ &+ \frac{2u{q_{\max}}^2\delta}{2^n} + \frac{4uq_{\max}^2\delta}{L^2} + 2u\left(\frac{q_{\max}L}{2^n}\right)^{n-1} + \frac{4uL^2{q_{\max}}^6}{2^{5n}} + \frac{8uL^2{q_{\max}}^8}{2^{6n}}\,.\end{aligned}$$

When $L \le \min\left\{\frac{2^n}{4q_{\max}}, \frac{2^{3n}}{20{q_{\max}}^4}\right\}$, it can be bounded by

$$\begin{aligned}&\frac{4(2u)^{1/2}}{2^n}\left(\frac{q_{\max}}{2^{n/2}} + \frac{{q_{\max}}^2}{2^{n+1}}\right) + \frac{3u^{1/2}(n+1)L{q_{\max}}^2\delta}{2^n} + \frac{6u^{1/2}L{q_{\max}}^4\delta}{2^{2n}}\\ &\quad+ \frac{2u{q_{\max}}^2\delta}{2^n} + \frac{4uq_{\max}^2\delta}{L^2} + 2u\left(\frac{q_{\max}L}{2^n}\right)^{n-1} + \frac{65u^{1/2}L{q_{\max}}^4}{2^{3n}}\,.\end{aligned}$$

This completes the proof. □

Acknowledgement. Yu Long Chen was supported by in part by the Research Council KU Leuven: GOA TENSE (C16/15/058). Wonseok Choi was Supported in part by the Sunday Group and the Algorand Centres of Excellence program managed by the Algorand Foundation. Changmin Lee was supported by a KIAS Individual Grant CG080601 at the Korea Institute for Advanced Study. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Algorand Foundation. We would like to express our appreciation to the anonymous reviewers of CRYPTO 2023 for their valuable feedback and insightful suggestions. Special thanks are extended to Jooyoung Lee, Byeonghak Lee, and Minki Hhan for their assistance and fruitful discussions, which greatly contributed to the development of this research paper.

References

[1] Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. Cryptology ePrint Archive, Report 1999/024 (1999), `https://eprint.iacr.org/1999/024`

[2] Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption. In: 38th FOCS. pp. 394–403

[3] Bellare, M., Guérin, R., Rogaway, P.: XOR MACs: New methods for message authentication using finite pseudorandom functions. In: CRYPTO'95. LNCS, vol. 963, pp. 15–28

[4] Bellare, M., Kilian, J., Rogaway, P.: The security of cipher block chaining. In: CRYPTO'94. LNCS, vol. 839, pp. 341–358

[5] Bellare, M., Krovetz, T., Rogaway, P.: Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible. In: EUROCRYPT'98. LNCS, vol. 1403, pp. 266–280

[6] Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426

[7] Bernstein, D.J.: How to stretch random functions: The security of protected counter sums. Journal of Cryptology **12**(3), 185–192

[8] Bhattacharya, S., Nandi, M.: Luby-rackoff backwards with more users and more security. In: ASIACRYPT 2021, Part III. LNCS, vol. 13092, pp. 345–375

[9] Biham, E.: How to decrypt or even substitute des-encrypted messages in 2^{28} steps. Inf. Process. Lett. **84**(3), 117–124

[10] Bose, P., Hoang, V.T., Tessaro, S.: Revisiting AES-GCM-SIV: Multi-user security, faster key derivation, and better bounds. In: EUROCRYPT 2018, Part I. LNCS, vol. 10820, pp. 468–499

[11] Chang, D., Nandi, M.: A short proof of the PRP/PRF switching lemma. Cryptology ePrint Archive, Report 2008/078 (2008), `https://eprint.iacr.org/2008/078`

[12] Chen, Y.L.: A modular approach to the security analysis of two-permutation constructions. In: ASIACRYPT 2022, Part I. LNCS, vol. 13791, pp. 379–409

[13] Chen, Y.L., Mennink, B., Preneel, B.: Categorization of faulty nonce misuse resistant message authentication. In: ASIACRYPT 2021, Part III. LNCS, vol. 13092, pp. 520–550

[14] Choi, W., Kim, H., Lee, J., Lee, Y.: Multi-user security of the sum of truncated random permutations. In: ASIACRYPT 2022, Part II. LNCS, vol. 13792, pp. 682–710
[15] Choi, W., Lee, B., Lee, J., Lee, Y.: Toward a fully secure authenticated encryption scheme from a pseudorandom permutation. In: ASIACRYPT 2021, Part III. LNCS, vol. 13092, pp. 407–434
[16] Choi, W., Lee, B., Lee, Y., Lee, J.: Improved security analysis for nonce-based enhanced hash-then-mask MACs. In: ASIACRYPT 2020, Part I. LNCS, vol. 12491, pp. 697–723
[17] Choi, W., Lee, J., Lee, Y.: Building PRFs from TPRPs: Beyond the Block and the Tweak Length Bounds. Cryptology ePrint Archive, Paper 2022/918 (2022), https://eprint.iacr.org/2022/918, https://eprint.iacr.org/2022/918
[18] Cogliati, B., Lampe, R., Patarin, J.: The indistinguishability of the XOR of k permutations. In: FSE 2014. LNCS, vol. 8540, pp. 285–302
[19] Cogliati, B., Patarin, J.: Mirror theory: A simple proof of the pi+pj theorem with $\xi_{\max} = 2$. Cryptology ePrint Archive, Report 2020/734 (2020), https://eprint.iacr.org/2020/734
[20] Cogliati, B., Seurin, Y.: EWCDM: An efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 121–149
[21] Dai, W., Hoang, V.T., Tessaro, S.: Information-theoretic indistinguishability via the chi-squared method. In: CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 497–523
[22] Dutta, A., Nandi, M., Saha, A.: Proof of mirror theory for $\xi_{\max} = 2$. IEEE Trans. Inf. Theory **68**(9), 6218–6232
[23] Dutta, A., Nandi, M., Talnikar, S.: Beyond birthday bound secure MAC in faulty nonce model. In: EUROCRYPT 2019, Part I. LNCS, vol. 11476, pp. 437–466
[24] Hall, C., Wagner, D., Kelsey, J., Schneier, B.: Building PRFs from PRPs. In: CRYPTO'98. LNCS, vol. 1462, pp. 370–389
[25] Hoang, V.T., Tessaro, S.: Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In: CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 3–32
[26] Hoang, V.T., Tessaro, S.: The multi-user security of double encryption. In: EUROCRYPT 2017, Part II. LNCS, vol. 10211, pp. 381–411
[27] Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: CRYPTO'88. LNCS, vol. 403, pp. 8–26
[28] Jha, A., Nandi, M.: Tight security of cascaded LRW2. Journal of Cryptology **33**(3), 1272–1317
[29] Jha, A., Nandi, M.: Tight Security of Cascaded LRW2. Journal of Cryptology **33**(3), 1272–1317
[30] Kim, S., Lee, B., Lee, J.: Tight security bounds for double-block hash-then-sum MACs. In: EUROCRYPT 2020, Part I. LNCS, vol. 12105, pp. 435–465
[31] Lucks, S.: The sum of PRPs is a secure PRF. In: EUROCRYPT 2000. LNCS, vol. 1807, pp. 470–484
[32] Mennink, B., Neves, S.: Encrypted Davies-Meyer and its dual: Towards optimal security using mirror theory. In: CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 556–583
[33] Minematsu, K.: How to thwart birthday attacks against MACs via small randomness. In: FSE 2010. LNCS, vol. 6147, pp. 230–249
[34] Mouha, N., Luykx, A.: Multi-key security: The Even-Mansour construction revisited. In: CRYPTO 2015, Part I. LNCS, vol. 9215, pp. 209–223

[35] Patarin, J.: A proof of security in o(2n) for the xor of two random permutations. In: ICITS 2008. LNCS, vol. 5155, pp. 232–248
[36] Patarin, J.: The "coefficients H" technique (invited talk). In: SAC 2008. LNCS, vol. 5381, pp. 328–345
[37] Patarin, J.: Mirror theory and cryptography. Appl. Algebra Eng. Commun. Comput. **28**(4), 321–338
[38] Shen, Y., Wang, L., Gu, D., Weng, J.: Revisiting the security of DbHtS MACs: Beyond-birthday-bound in the multi-user setting. In: CRYPTO 2021, Part III. LNCS, vol. 12827, pp. 309–336
[39] Tessaro, S.: Optimally secure block ciphers from ideal primitives. In: ASIACRYPT 2015, Part II. LNCS, vol. 9453, pp. 437–462

Supplementary Material

A Proof of Lemma 1

We will need the following relationship in our proofs. Since $\sum_{x\in\Gamma} P(x) = \sum_{x\in\Gamma} Q(x) = 1$, we have

$$\sum_{x\in\Gamma}(P(x)-Q(x)) = 0 \Leftrightarrow \sum_{x\in\Gamma'}(P(x)-Q(x)) + \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x)) = 0 \quad (7)$$

Showing Lemma 1 is equivalent to showing that

$$\Delta_{KL,\Gamma'}(P,Q) \geq \frac{1}{2}\left(\sum_{x\in\Gamma'}|P(x)-Q(x)|\right)^2 - \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x)).$$

Remark that $\Delta_{KL,\Gamma'}(P,Q)$ is defined as

$$\Delta_{KL,\Gamma'}(P,Q) = \sum_{x\in\Gamma'} P(x)\ln\left(\frac{P(x)}{Q(x)}\right)$$

Plugging $r(x) = \frac{P(x)}{Q(x)} - 1 \geq -1$ into this equation, we have

$$\begin{aligned}\Delta_{KL,\Gamma'}(P,Q) &= \sum_{x\in\Gamma'} Q(x)\cdot(1+r(x))\cdot\ln(1+r(x)) \\ &= \sum_{x\in\Gamma'} Q(x)\cdot(1+r(x))\cdot\ln(1+r(x)) - \sum_{x\in\Gamma}(P(x)-Q(x)) \\ &= \sum_{x\in\Gamma'} Q(x)\cdot((1+r(x))\cdot\ln(1+r(x)) - r(x)) - \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x)) \quad (8)\end{aligned}$$

using the relationship defined in (7) (since the extra term added is equal to 0). Furthermore, we can prove the following claim

Claim.

$$F(r) \stackrel{\text{def}}{=} (1+r)\cdot\ln(1+r) - r - \frac{r^2}{2(1+r/3)} \geq 0$$

for all $r \geq -1$[4].

The proof of the claim is deferred to the end of the proof.

[4] We will define $F(-1) \stackrel{\text{def}}{=} \lim_{r\to-1^+} F(r) = \frac{1}{4}$ since $\lim_{t\to0^+} t\ln t = 0$. This slight abuse of notation is also used for the definition of KL-divergence.

Using the above claim, we derive the following lower bound for (8)

$$\begin{aligned}(8) &\geq \sum_{x\in\Gamma'} Q(x)\cdot\left(\frac{r(x)^2}{2\,(1+r(x)/3)}\right) - \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x))\\ &= \sum_{x\in\Gamma'} Q(x)\cdot\left(\frac{1}{2}\frac{Q(x)\cdot|r(x)|^2}{(Q(x)\cdot(1+r(x)/3))}\right) - \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x))\\ &\geq \frac{1}{2}\frac{\left(\sum_{x\in\Gamma'} Q(x)\cdot|r(x)|\right)^2}{\sum_{x\in\Gamma'} Q(x)\cdot(1+r(x)/3)} - \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x)). \qquad (9)\end{aligned}$$

where the last inequality is obtained by applying Sedrakyan's inequality.

On the other hand, from the definition, we have $Q(x)\cdot(1+r(x)/3) = \frac{2}{3}Q(x)+\frac{1}{3}P(x)$. It directly implies that $\sum_{x\in\Gamma'} Q(x)\cdot(1+r(x)/3) = \sum_{x\in\Gamma'}\frac{2}{3}Q(x)+\frac{1}{3}P(x)\leq 1$. Hence (9) can be lower bounded by

$$\begin{aligned}(9) &\geq \frac{1}{2}\left(\sum_{x\in\Gamma'} Q(x)\cdot|r(x)|\right)^2 - \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x))\\ &= \frac{1}{2}\left(\sum_{x\in\Gamma'}|P(x)-Q(x)|\right)^2 - \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x))\,.\end{aligned}$$

where the last equality is obtained by substituting $r(x)=\frac{P(x)}{Q(x)}-1$ into (9). This completes the proof of Lemma 1.

Proof (of the claim). Remark that

$$F(r) = (1+r)\cdot\ln(1+r) - r - \frac{r^2}{2(1+r/3)}\,.$$

We have the following first and second derivatives:

$$F'(r) = \ln(1+r) - \frac{3r(6+r)}{2(3+r)^2}$$

and

$$F''(r) = \frac{1}{1+r} - \frac{27}{(3+r)^3}\,.$$

Note that $F'(0)=F''(0)=0$.

Assume that $r>0$. One can see that $F''(r)>0$. By Mean Value Theorem, there exist $r_1,r_2\in(0,r)$ such that $F(r)=F'(r_1)r$ and $F'(r_1)=F''(r_2)r_1$. It follows that $F(r)=F''(r_2)r_1r$. Since $F''(r_2)$, r_1, and r are all positive, $F(r)$ is positive.

Now assume that $-1\leq r<0$. One can see that $F''(r)>0$. By Mean Value Theorem, there exist $r_1,r_2\in(r,0)$ such that $F(r)=F'(r_1)r$ and $F'(r_1)=F''(r_2)r_1$. It follows that $F(r)=F''(r_2)r_1r$. Since $F''(r_2)$ is positive and r_1 and r are negative, $F(r)$ is positive. □

B Proof of Lemma 2

Since $\ln t \leq t-1$ for all $t>0$, by replacing t with $\frac{P(x)}{Q(x)}$, we see that

$$\ln\left(\frac{P(x)}{Q(x)}\right) \leq \frac{P(x)}{Q(x)} - 1$$

for all $x \in \Gamma$. We then have

$$\Delta_{KL,\Gamma'}(P,Q) = \sum_{x\in\Gamma'} P(x)\ln\left(\frac{P(x)}{Q(x)}\right) \leq \sum_{x\in\Gamma'}\left(\frac{P(x)^2}{Q(x)} - P(x)\right).$$

Note that this property also holds when $P(x)=0 \Leftrightarrow t=0$ with a slight abuse of notation in KL-divergence, i.e., $P(x)\ln\left(\frac{P(x)}{Q(x)}\right)=0$. On the other hand, by subtracting the identity $\sum_{x\in\Gamma}(P(x)-Q(x))=0$ defined in (7), we also have

$$\begin{aligned}\Delta_{KL,\Gamma'}(P,Q) &\leq \sum_{x\in\Gamma'}\left(\frac{P(x)^2}{Q(x)} - P(x)\right) - \sum_{x\in\Gamma}(P(x)-Q(x)) \\ &= \sum_{x\in\Gamma'}\left(\frac{P(x)^2}{Q(x)} - 2P(x) + Q(x)\right) - \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x)).\end{aligned}$$

It is obvious that the last term equals to $\sum_{x\in\Gamma'}\frac{(P(x)-Q(x))^2}{Q(x)} - \sum_{x\in\Gamma\setminus\Gamma'}(P(x)-Q(x))$. This concludes the proof.

C Proof of Lemma 3.

For $u<v\in[q]$, let $I_{u,v}$ be an indicator variable such that

$$I_{u,v}=1 \Leftrightarrow \lambda_u=\lambda_v.$$

Observe that

$$\mathsf{C} = \sum_{u<v\in[q]} I_{u,v}$$

and, for $u<v\in[q]$,

$$\mathbf{Ex}[I_{u,v}] = \frac{1}{2^n}.$$

Therefore we have

$$\mathbf{Ex}[\mathsf{C}] = \mathbf{Ex}\left[\sum_{u<v\in[q]} I_{u,v}\right] = \frac{q(q-1)}{2^{n+1}} \leq \frac{q^2}{2^{n+1}}. \tag{10}$$

On the other hand,

$$\mathsf{C}^2 = \left(\sum_{u<v\in[q]} I_{u,v}\right)^2 = \sum_{u<v\in[q]} I_{u,v} + \sum_{u<v\in[q]} \sum_{\substack{u'<v'\in[q]\\(u',v')\neq(u,v)}} I_{u,v}I_{u',v'}.$$

Note that, unless $(u,v) = (u',v')$, $I_{u,v}$ and $I_{u',v'}$ are independent since at least three of $\{\lambda_u, \lambda_v, \lambda_{u'}, \lambda_{v'}\}$ are mutually independent. Hence the following computation holds:

$$\begin{aligned}
\mathbf{Ex}\left[\mathsf{C}^2\right] &= \mathbf{Ex}\left[\sum_{u<v\in[q]} I_{u,v} + \sum_{u<v\in[q]} \sum_{\substack{u'<v'\in[q]\\(u',v')\neq(u,v)}} I_{u,v}I_{u',v'}\right] \\
&= \mathbf{Ex}\left[\sum_{u<v\in[q]} I_{u,v}\right] + \mathbf{Ex}\left[\sum_{u<v\in[q]} I_{u,v} \sum_{\substack{u'<v'\in[q]\\(u',v')\neq(u,v)}} I_{u',v'}\right] \\
&= \frac{q(q-1)}{2^{n+1}} + \frac{q(q-1)}{2^{n+1}} \cdot \frac{q(q-1)-2}{2^{n+1}} \\
&\leq \frac{q^2}{2^{n+1}} + \frac{q^4}{2^{2n+2}}. \qquad (11)
\end{aligned}$$

By (10), (11) and Chebyshev's inequality, the proof is complete.

D Proof of Theorem 2

For readability, we use $N = 2^n$ and $\mathcal{G}$ instead of $\mathcal{G}(\Gamma)$. For $i = 1, \ldots, \alpha+\beta$, $\mathcal{C}_i$ is a bipartite graph, where one part consists of the vertices in $\mathcal{V}_P$ and the other vertices in $\mathcal{V}_Q$; the two parts are denoted $\mathcal{P}_i$ and $\mathcal{Q}_i$, respectively. For $i \in [\alpha+\beta]$, we will also write $\mathcal{X}_i = \mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_i$, and $\mathcal{Y}_i = \mathcal{Q}_1 \sqcup \cdots \sqcup \mathcal{Q}_i$. Let $h_c(i)$ be the number of solutions to $\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i$ and $h_c(0) = 1$. In order to find a relation between $h_c(i)$ and $h_c(i+1)$, we fix a solution to $\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i$.

Fix a vertex $V^* \in \mathcal{C}_{i+1}$. If we assign any value to V^*, the other unknowns are uniquely determined since there is a unique trail from V^* to any other vertex in $\mathcal{C}_{i+1}$. We can choose the solution to V^* from

$$\{0,1\}^n \setminus \bigcup_{V\in\mathcal{C}_{i+1}} \mathcal{W}_V \oplus \lambda_V,$$

where

$$\mathcal{W}_V \stackrel{\text{def}}{=} \bigsqcup_{1\leq j\leq i} \mathcal{P}_j \text{ if } V \in \mathcal{P}_{i+1},$$

$$\mathcal{W}_V \stackrel{\text{def}}{=} \bigsqcup_{1\leq j\leq i} \mathcal{Q}_j \text{ if } V \in \mathcal{Q}_{i+1},$$

and $\lambda_V \stackrel{\text{def}}{=} \lambda(V, V^*)$ (if $V = V^*$, then $\lambda_V = 0$). Let $u_i = |\mathcal{P}_i|$, $v_i = |\mathcal{Q}_i|$, $U_i = \sum_{j=1}^{i} u_j$, $V_i = \sum_{j=1}^{i} v_j$, and $\Lambda_V = \mathcal{W}_V \oplus \lambda_V$. For $i = 0, \ldots, \alpha - 1$, we have

$$\begin{aligned} h_c(i+1) &= \sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i}} \left(N - \bigcup_{V \in \mathcal{C}_{i+1}} \Lambda_V \right) \\ &\leq \sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i}} \left(N - u_{i+1} U_i - v_{i+1} V_i + \sum_{V \neq V' \in \mathcal{C}_{i+1}} |\Lambda_V \cap \Lambda_{V'}| \right) \\ &= (N - u_{i+1} U_i - v_{i+1} V_i) h_c(i) + \sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i}} \sum_{V \neq V' \in \mathcal{C}_{i+1}} |\Lambda_V \cap \Lambda_{V'}| \,. \end{aligned}$$

For $V_1, V_1' \in \mathcal{C}_{i+1}$, $V_2 \in \mathcal{W}_{V_1}$ and $V_2' \in \mathcal{W}_{V_1'}$, let $h'(V_1, V_1', V_2, V_2')$ denote the number of solutions to $\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i$ such that $V_2 \oplus V_2' = \lambda_{V_1} \oplus \lambda_{V_1'}$. Let

$$\mathbb{L}_{i+1} \stackrel{\text{def}}{=} \left\{ (\{V_1, V_1'\}, \{V_2, V_2'\}) \,\middle|\, V_1 \neq V_1' \in \mathcal{C}_{i+1}, V_2 \in \mathcal{W}_{V_1}, V_2' \in \mathcal{W}_{V_1'}, \text{ and } \lambda(V_2, V_2') = \perp \right\}.$$

Then we have

$$\sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i}} \sum_{V \neq V' \in \mathcal{C}_{i+1}} |\Lambda_V \cap \Lambda_{V'}| = |\mathcal{R}_{i+1}| \, h_c(i) + \sum_{(\{V_1, V_1'\}, \{V_2, V_2'\}) \in \mathbb{L}_{i+1}} h'(V_1, V_1', V_2, V_2') \,. \tag{12}$$

Let $h''(V, V')$ denote the number of solutions to $(\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i) \setminus (\mathcal{C}_V \sqcup \mathcal{C}_{V'})$ where $V \in \mathcal{C}_V$ and $V' \in \mathcal{C}_{V'}$. For $(\{V_1, V_1'\}, \{V_2, V_2'\}) \in \mathbb{L}_{i+1}$, we have

$$\begin{aligned} h'(V_1, V_1', V_2, V_2') &\leq N \cdot h''(V_2, V_2') \\ &\leq \frac{N \cdot h_c(i)}{(N - \xi_{\max}(U_i + V_i))^2} \\ &\leq \frac{h_c(i)}{N} \left(1 + \frac{2\xi_{\max}(U_i + V_i)N - \xi_{\max}^2 (U_i + V_i)^2}{(N - \xi_{\max}(U_i + V_i))^2} \right) \\ &\leq \frac{h_c(i)}{N} \left(1 + \frac{2\xi_{\max}(U_i + V_i)N}{(N - \xi_{\max}(U_i + V_i))^2} \right) \\ &\leq \frac{h_c(i)}{N} \left(1 + \frac{192\xi_{\max} q_c}{25N} \right) \\ &\leq \frac{73 h_c(i)}{25N} \end{aligned} \tag{13}$$

since $U_i + V_i \leq \frac{3q_c}{2}$ and $q_c \leq q \leq N/4\xi_{\max}$. By (12) and (13), and since

$$|\mathbb{L}_{i+1}| \leq \binom{u_{i+1} + v_{i+1}}{2} \binom{U_i + V_i}{2} \leq \frac{(\xi(\mathcal{C}_{i+1}))_2 \, (U_i + V_i)^2}{4} \leq \frac{9 \, (\xi(\mathcal{C}_{i+1}))_2 \, q_c^2}{16},$$

we have

$$h_c(i+1) \leq \left(N - u_{i+1}U_i - v_{i+1}V_i + |\mathcal{R}_{i+1}| + \frac{2\left(\xi(\mathcal{C}_{i+1})\right)_2 q_c^2}{N} \right) h_c(i),$$

and,

$$\begin{aligned}
\frac{h_c(i+1)N^{\xi(\mathcal{C}_{i+1})-1}}{h_c(i)(N-U_i)_{u_{i+1}}(N-V_i)_{v_{i+1}}} \leq & \frac{N^{\xi(\mathcal{C}_{i+1})} - (u_{i+1}U_i + v_{i+1}V_i - |\mathcal{R}_{i+1}|)N^{\xi(\mathcal{C}_{i+1})-1}}{N^{\xi(\mathcal{C}_{i+1})} - (u_{i+1}U_{i+1} - v_{i+1}V_{i+1})N^{\xi(\mathcal{C}_{i+1})-1}} \\
& + \frac{2\left(\xi(\mathcal{C}_{i+1})\right)_2 q_c^2 N^{\xi(\mathcal{C}_{i+1})-2}}{N^{\xi(\mathcal{C}_{i+1})} - (u_{i+1}U_{i+1} - v_{i+1}V_{i+1})N^{\xi(\mathcal{C}_{i+1})-1}} \\
\leq & 1 + \frac{(u_{i+1}^2 + s_{i+1}^2 + |\mathcal{R}_{i+1}|)N^{\xi(\mathcal{C}_{i+1})-1}}{N^{\xi(\mathcal{C}_{i+1})} - (u_{i+1}U_{i+1} - v_{i+1}V_{i+1})N^{\xi(\mathcal{C}_{i+1})-1}} \\
& + \frac{2\left(\xi(\mathcal{C}_{i+1})\right)_2 q_c^2 N^{\xi(\mathcal{C}_{i+1})-2}}{N^{\xi(\mathcal{C}_{i+1})} - (u_{i+1}U_{i+1} - v_{i+1}V_{i+1})N^{\xi(\mathcal{C}_{i+1})-1}} \\
\leq & 1 + \frac{2\left(\xi(\mathcal{C}_{i+1})\right)_2 + 2|\mathcal{R}_{i+1}|}{N} + \frac{4\left(\xi(\mathcal{C}_{i+1})\right)_2 q_c^2}{N^2} \\
\leq & 1 + \frac{2|\mathcal{R}_{i+1}|}{N} + \left(\xi(\mathcal{C}_{i+1})\right)_2 \left(\frac{2}{N} + \frac{4q_c^2}{N^2} \right). \quad (14)
\end{aligned}$$

By denoting

$$C = \frac{\xi_{\max}}{N} \left(2 + \frac{4q_c^2}{N} \right)$$

and using the relation

$$\sum_{i=1}^{\alpha} \left(\xi(\mathcal{C}_i) - 1 \right) = q_c,$$

it follows that

$$\begin{aligned}
\frac{h_c(\alpha)N^{q_c}}{(N)_{R_0}(N)_{S_0}} \leq & \prod_{i=0}^{\alpha-1} \left(\frac{h_c(i+1)N^{\xi(\mathcal{C}_{i+1})-1}}{h_c(i)(N-U_i)_{u_{i+1}}(N-V_i)_{v_{i+1}}} \right) \\
\leq & \prod_{i=0}^{\alpha-1} \left(1 + \frac{2|\mathcal{R}_{i+1}|}{N} + C\left(\xi(\mathcal{C}_{i+1}) - 1\right) \right) \\
\leq & \prod_{i=0}^{\alpha-1} \left(1 + \frac{2|\mathcal{R}_{i+1}|}{N} \right) \times \prod_{i=0}^{\alpha-1} \left(1 + C\left(\xi(\mathcal{C}_{i+1}) - 1\right) \right) \\
\leq & \left(1 + \frac{2\sum_{i=1}^{\alpha} |\mathcal{R}_i|}{N\alpha} \right)^{\alpha} \times \left(1 + \frac{Cq_c}{\alpha} \right)^{\alpha} \\
\leq & e^{\delta_1} \quad (15)
\end{aligned}$$

where

$$\delta_1 = \frac{2\sum_{i=1}^{\alpha} |\mathcal{R}_i|}{N} + Cq_c = \frac{2\sum_{i=1}^{\alpha} |\mathcal{R}_i| + 2\xi_{\max}q_c}{N} + \frac{4\xi_{\max}q_c^3}{N^2}.$$

For $i = 1, \ldots, \beta$, we will write

$$\mathcal{C}_{\alpha+i} : P'_i \overset{\lambda'_i}{-} Q'_i.$$

Let $h_d(i)$ be the number of solutions to $\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{\alpha+i}$ for $i = 1, \ldots, \beta$. Note that $h_d(0) = h_c(\alpha)$ and $h_d(\beta) = h(\mathcal{G})$. In order to find a relation between $h_d(i)$ and $h_d(i+1)$, we fix a solution to $\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{\alpha+i}$. Then we can choose P'_{i+1} from $\{0,1\}^n \setminus \left(\mathcal{X}'_i \cup (\mathcal{Y}'_i \oplus \lambda'_{i+1})\right)$, where

$$\mathcal{X}'_i \overset{\text{def}}{=} \bigsqcup_{1 \le j \le \alpha} \mathcal{P}_j \sqcup \{P'_1, \ldots, P'_i\} (= \mathcal{X}_{\alpha+i}),$$
$$\mathcal{Y}'_i \overset{\text{def}}{=} \bigsqcup_{1 \le j \le \alpha} \mathcal{Q}_j \sqcup \{Q'_1, \ldots, Q'_i\} (= \mathcal{Y}_{\alpha+i}).$$

For $i = 0, \ldots, \beta - 1$, since

$$|\mathcal{X}'_i| = u_1 + \cdots + u_\alpha + i,$$
$$|\mathcal{Y}'_i| = v_1 + \cdots + v_\alpha + i,$$

we have

$$\begin{aligned} h_d(i+1) &= \sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{\alpha+i}}} \left(N - |\mathcal{X}'_i \cup (\mathcal{Y}'_i \oplus \lambda'_{i+1})|\right) \\ &= \sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{\alpha+i}}} \left(N - |\mathcal{X}'_i| - |\mathcal{Y}'_i| + |\mathcal{X}'_i \cap (\mathcal{Y}'_i \oplus \lambda'_{i+1})|\right) \\ &= (N - |\mathcal{X}'_i| - |\mathcal{Y}'_i|) h_d(i) + \sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{\alpha+i}}} |\mathcal{X}'_i \cap (\mathcal{Y}'_i \oplus \lambda'_{i+1})|. \end{aligned} \tag{16}$$

For $P \in \mathcal{X}'_i$ and $Q \in \mathcal{Y}'_i$, let $h'(P,Q)$ denote the number of solutions to $\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{\alpha+i}$ such that $P \oplus Q = \lambda'_{i+1}$. Let

$$\mathcal{A}_i \overset{\text{def}}{=} \{(P,Q) \in \mathcal{X}'_i \times \mathcal{Y}'_i \mid \lambda(P,Q) \neq \perp\},$$
$$\mathcal{B}_i \overset{\text{def}}{=} (\mathcal{X}'_i \times \mathcal{Y}'_i) \setminus \mathcal{A}_i,$$

Then we have

$$\begin{aligned} \sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{\alpha+i}}} |\mathcal{X}'_i \cap (\mathcal{Y}'_i \oplus \lambda_{i+1})| &= \sum_{P \in \mathcal{X}'_i, Q \in \mathcal{Y}'_i} h'(P,Q) \\ &= \sum_{(P,Q) \in \mathcal{A}_i} h'(P,Q) + \sum_{(P,Q) \in \mathcal{B}_i} h'(P,Q) \\ &= |\mathcal{R}_{\alpha+i+1}|\, h_d(i) + \sum_{(P,Q) \in \mathcal{B}_i} h'(P,Q), \end{aligned} \tag{17}$$

Depending on whether there are large components (whether $q_c > 0$), we can distinguish the analysis of $\sum_{(P,Q) \in \mathcal{B}_i} h'(P,Q)$ into the following two cases.

Case 1 ($q_c > 0$). Let $h''(P,Q)$ denote the number of solutions to $(\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{\alpha+i}) \setminus (\mathcal{C}_P \sqcup \mathcal{C}_Q)$ where $P \in \mathcal{C}_P$, $Q \in \mathcal{C}_Q$ and $\mathcal{C} \neq \mathcal{Q} \in \{\mathcal{C}_1, \ldots, \mathcal{C}_{\alpha+i}\}$. We have

$$\begin{aligned} h'(P,Q) &\leq N \cdot h''(P,Q) \\ &\leq \frac{N \cdot h_d(i)}{(N - \xi_{\max}(|\mathcal{X}_i'| + |\mathcal{Y}_i'|))^2} \\ &\leq \frac{h_d(i)}{N}\left(1 + \frac{2\xi_{\max}(|\mathcal{X}_i'| + |\mathcal{Y}_i'|)N - \xi_{\max}^2(|\mathcal{X}_i'| + |\mathcal{Y}_i'|)^2}{(N - \xi_{\max}(|\mathcal{X}_i'| + |\mathcal{Y}_i'|))^2}\right) \\ &\leq \frac{h_d(i)}{N}\left(1 + \frac{2\xi_{\max}(|\mathcal{X}_i'| + |\mathcal{Y}_i'|)N}{(N - \xi_{\max}(|\mathcal{X}_i'| + |\mathcal{Y}_i'|))^2}\right) \\ &\leq \frac{h_d(i)}{N}\left(1 + \frac{16\xi_{\max} q}{N}\right) \end{aligned} \tag{18}$$

since $|\mathcal{X}_i'| + |\mathcal{Y}_i'| \leq 2q \leq \frac{N}{2\xi_{\max}}$. By (17), (18), and since $|\mathcal{B}_i| \leq |\mathcal{X}_i'||\mathcal{Y}_i'|$, we have

$$\sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_{\alpha+i}}} |\mathcal{X}_i' \cap (\mathcal{Y}_i' \oplus \lambda_{i+1})| \leq \left(|\mathcal{R}_{\alpha+i+1}| + \frac{|\mathcal{X}_i'||\mathcal{Y}_i'|}{N}\left(1 + \frac{16\xi_{\max} q}{N}\right)\right) h_d(i)$$

and by (16),

$$h_d(i+1) \leq \left(N - |\mathcal{X}_i'| - |\mathcal{Y}_i'| + |\mathcal{R}_{\alpha+i+1}| + \frac{|\mathcal{X}_i'||\mathcal{Y}_i'|}{N} + \frac{16\xi_{\max} q^3}{N^2}\right) h_d(i).$$

Since $|\mathcal{X}_i'| + |\mathcal{Y}_i'| \leq 2q \leq \frac{N}{6}$, we have

$$\begin{aligned} \frac{h_d(i+1)N}{h_d(i)(N - |\mathcal{X}_i'|)(N - |\mathcal{Y}_i'|)} &\leq \frac{N^2 - (|\mathcal{X}_i'| + |\mathcal{Y}_i'| - |\mathcal{R}_{\alpha+i+1}|)N + |\mathcal{X}_i'||\mathcal{Y}_i'| + \frac{16\xi_{\max} q^3}{N}}{N^2 - (|\mathcal{X}_i'| + |\mathcal{Y}_i'|)N + |\mathcal{X}_i'||\mathcal{Y}_i'|} \\ &\leq 1 + \frac{|\mathcal{R}_{\alpha+i+1}|\, N + \frac{16\xi_{\max} q^3}{N}}{N^2 - (|\mathcal{X}_i'| + |\mathcal{Y}_i'|)N + |\mathcal{X}_i'||\mathcal{Y}_i'|} \\ &\leq 1 + \frac{6\,|\mathcal{R}_{\alpha+i+1}|}{5N} + \frac{96\xi_{\max} q^3}{5N^3}\,. \end{aligned} \tag{19}$$

Since $q = q_c + \beta$, $|\mathcal{P}| = |\mathcal{X}_0'| + \beta$, $|\mathcal{Q}| = |\mathcal{Y}_0'| + \beta$ and $\alpha + q_c = |\mathcal{X}_0'| + |\mathcal{Y}_0'|$, and by (15) and (19), we have

$$\begin{aligned}
\frac{h(\mathcal{G})N^q}{(N)_{|\mathcal{P}|}(N)_{|\mathcal{Q}|}} &= \frac{h(\mathcal{G})N^{q_c+\beta}}{(N)_{|\mathcal{X}_0|}(N-|\mathcal{X}_0|)_\beta (N)_{|\mathcal{Y}_0|}(N-|\mathcal{Y}_0|)_\beta} \\
&= \frac{h_c(\alpha)N^{q_c}}{(N)_{|\mathcal{X}_0|}(N)_{|\mathcal{Y}_0|}} \prod_{i=0}^{\beta-1} \left(\frac{h_d(i+1)N}{h_d(i)(N-|\mathcal{X}_i|)(N-|\mathcal{Y}_i|)} \right) \\
&\leq e^{\delta_1} \prod_{i=0}^{\beta-1} \left(1 + \frac{6\,|\mathcal{R}_{\alpha+i+1}|}{5N} + \frac{96\xi_{\max}q^3}{5N^3} \right) \\
&\leq e^{\delta_1} \left(1 + \frac{2\sum_{i=1}^{\beta} |\mathcal{R}_{\alpha+i}|}{N\beta} + \frac{20\xi_{\max}q^3}{N^3} \right)^\beta \\
&\leq e^{\delta_1+\delta_2}
\end{aligned}$$

where

$$\delta_2 = \frac{2\sum_{i=1}^{\beta} |\mathcal{R}_{\alpha+i}|}{N} + \frac{20\xi_{\max}q^4}{N^3},$$

and therefore

$$\delta_1 + \delta_2 = \frac{2\sum_{i=1}^{\alpha+\beta} |\mathcal{R}_i| + 2\xi_{\max}q_c}{N} + \frac{4\xi_{\max}q_c^3}{N^2} + \frac{20\xi_{\max}q^4}{N^3},$$

On the other hand, from the Mirror theory of Jha and Nandi [29], we have

$$\begin{aligned}
\frac{h(\mathcal{G})N^q}{(N)_{|\mathcal{P}|}(N)_{|\mathcal{Q}|}} &\geq 1 - \frac{4q^2}{N^2} \sum_{i=1}^{\alpha} \left(\xi(\mathcal{C}_i) - 1\right)^2 - \frac{2q^2}{N^2} - \frac{13q^4}{N^3} \\
&\geq 1 - \frac{4(\xi_{\max}-1)q_c q^2}{N^2} - \frac{2q^2}{N^2} - \frac{13q^4}{N^3} \\
&\geq 1 - \frac{4\xi_{\max}q_c q^2}{N^2} - \frac{13q^4}{N^3}\,.
\end{aligned}$$

In other words,

$$1 - \frac{h(\mathcal{G})N^q}{(N)_{|\mathcal{P}|}(N)_{|\mathcal{Q}|}} \leq \frac{4\xi_{\max}q_c q^2}{N^2} + \frac{13q^4}{N^3} \leq e^{\delta_3} - 1$$

where

$$\delta_3 = \frac{4\xi_{\max}q_c q^2}{N^2} + \frac{13q^4}{N^3}\,.$$

To sum up, since $\frac{4\xi_{\max}q_c^3}{N^2} \leq \frac{4\xi_{\max}q_c q^2}{N^2}$ and $\frac{13q^4}{N^3} \leq \frac{20\xi_{\max}q^4}{N^3}$, we have

$$\left| \frac{h(\mathcal{G})N^q}{(N)_{|\mathcal{P}|}(N)_{|\mathcal{Q}|}} - 1 \right| \leq e^{\epsilon} - 1$$

where

$$\epsilon = \frac{2\sum_{i=1}^{\alpha+\beta} |\mathcal{R}_i| + 2\xi_{\max} q_c}{N} + \frac{4\xi_{\max} q_c q^2}{N^2} + \frac{20\xi_{\max} q^4}{N^3}$$

which completes the proof for the case of $q_c > 0$.

Case 2 ($q_c = 0$). Since there are no large components in this case ($\alpha = 0$), we have $h_d(0) = 1$. Recall that $h'(P,Q)$ denote the number of solutions to $\mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i$ such that $P \oplus Q = \lambda'_{i+1}$ and here we consider the case $(P,Q) \in \mathcal{B}_i$. If $i \geq 2n+2$, then we have

$$\left| \frac{h_d(i)}{N} - h'(P,Q) \right| \leq \frac{(15\,|\mathcal{R}_{i+1}| + 17) h_d(i)}{N^2}$$

by Lemma 8 of [17]. So we have

$$h'(P,Q) \leq \frac{h_d(i)}{N} \left(1 + \frac{15\,|\mathcal{R}_{i+1}| + 17}{N} \right). \tag{20}$$

By (17), (20), and since $|\mathcal{B}_i| \leq |\mathcal{X}_i||\mathcal{Y}_i|$, we have

$$\sum_{\substack{\text{solutions to} \\ \mathcal{C}_1 \sqcup \cdots \sqcup \mathcal{C}_i}} |\mathcal{X}_i \cap (\mathcal{Y}_i \oplus \lambda_{i+1})| \leq \left(|\mathcal{R}_{i+1}| + \frac{|\mathcal{X}_i||\mathcal{Y}_i|}{N} \left(1 + \frac{15\,|\mathcal{R}_{i+1}| + 17}{N} \right) \right) h_d(i)$$

and by (16),

$$h_d(i+1) \leq \left(N - |\mathcal{X}_i| - |\mathcal{Y}_i| + |\mathcal{R}_{i+1}| \left(1 + \frac{15q^2}{N^2} \right) + \frac{|\mathcal{X}_i||\mathcal{Y}_i|}{N} + \frac{17q^2}{N^2} \right) h_d(i).$$

Since $|\mathcal{X}_i|, |\mathcal{Y}_i| \leq N/13$, we have

$$\begin{aligned}
\frac{h_d(i+1)N}{h_d(i)(N - |\mathcal{X}_i|)(N - |\mathcal{Y}_i|)} &\leq \frac{N^2 - (|\mathcal{X}_i| + |\mathcal{Y}_i|)N + |\mathcal{R}_{i+1}| \left(N + \frac{15q^2}{N} \right) + |\mathcal{X}_i||\mathcal{Y}_i| + \frac{17q^2}{N}}{N^2 - (|\mathcal{X}_i| + |\mathcal{Y}_i|)N + |\mathcal{X}_i||\mathcal{Y}_i|} \\
&\leq 1 + \frac{|\mathcal{R}_{i+1}| \left(N + \frac{15q^2}{N} \right) + \frac{17q^2}{N}}{N^2 - (|\mathcal{X}_i| + |\mathcal{Y}_i|)N + |\mathcal{X}_i||\mathcal{Y}_i|} \\
&\leq 1 + \frac{2\,|\mathcal{R}_{i+1}|}{N} + \frac{18\,|\mathcal{R}_{i+1}|\,q^2}{N^3} + \frac{20q^2}{N^3} \\
&\leq 1 + \frac{3\,|\mathcal{R}_{i+1}|}{N} + \frac{20q^2}{N^3}\,.
\end{aligned}$$

Let $m = 2n + 2$. Then we have

$$\begin{aligned}
\frac{h(\mathcal{G}) N^{q-m}}{h_d(m)(N - |\mathcal{X}_m|)_{q-m}(N - |\mathcal{Y}_m|)_{q-m}} &\leq \prod_{i=m}^{q-1} \left(1 + \frac{3\,|\mathcal{R}_{i+1}|}{N} + \frac{20q^2}{N^3} \right) \\
&\leq \left(1 + \frac{3\sum_{i=1}^{q} |\mathcal{R}_i|}{Nq} + \frac{20q^2}{N^3} \right)^q \\
&\leq e^{\delta_1}\,,
\end{aligned} \tag{21}$$

where

$$\delta_1 = \frac{3\sum_{i=1}^{q}|\mathcal{R}_i|}{N} + \frac{20q^3}{N^3}\,.$$

If $i \le 2n+1$, then we have

$$h_d(i+1) \le N \cdot h_d(i).$$

Then it follows that

$$\begin{aligned}\frac{h_d(i+1)N}{h_d(i)(N-|\mathcal{X}_i|)(N-|\mathcal{Y}_i|)} &\le \frac{N\cdot N}{(N-|\mathcal{X}_i|)(N-|\mathcal{Y}_i|)}\\ &\le 1 + \frac{N\left(|\mathcal{X}_i|+|\mathcal{Y}_i|\right)}{(N-|\mathcal{X}_i|)(N-|\mathcal{Y}_i|)}\,.\end{aligned}$$

Since $|\mathcal{X}_i|, |\mathcal{Y}_i| \le \min\{i, N/13\}$, we have

$$\begin{aligned}\frac{h_d(2n+2)N^{2n+2}}{h_d(1)(N)_{2n+2}(N)_{2n+2}} &\le \left(1 + \sum_{i=1}^{2n+1}\frac{3i}{N}\right)\\ &\le 1 + \frac{3(2n+1)(n+1)}{N} \le 1 + \frac{6(n+1)^2}{N}\,. \qquad (22)\end{aligned}$$

By combining (21) and (22), we have

$$\frac{h(\mathcal{G})N^q}{(N)_{|\mathcal{P}|}(N)_{|\mathcal{Q}|}} \le e^{\delta_1}\left(1 + \frac{6(n+1)^2}{N}\right) \le e^{\delta_1+\delta_2}\,.$$

where

$$\delta_2 = \frac{6(n+1)^2}{N}\,,$$

and therefore

$$\delta_1 + \delta_2 = \frac{3\sum_{i=1}^{\alpha+\beta}|\mathcal{R}_i|}{N} + \frac{20q^3}{N^3} + \frac{6(n+1)^2}{N}\,.$$

On the other hand, from the Mirror theory of Choi et al. [17], we have

$$\begin{aligned}\frac{h(\mathcal{G})N^q}{(N)_{|\mathcal{P}|}(N)_{|\mathcal{Q}|}} &\ge 1 - \frac{6(n+1)^3}{N^2} - \sum_{i=0}^{q-1}\left(\frac{2i}{N^2} + \frac{20i^2}{N^3}\right)\\ &\ge 1 - \frac{6(n+1)^3}{N^2} - \frac{q^2}{N^2} - \frac{7q^3}{N^3}\\ &\ge 1 - \frac{6(n+1)^3}{N^2} - \frac{2q^2}{N^2}\,.\end{aligned}$$

In other words,

$$1 - \frac{h(\mathcal{G})N^q}{(N)_{|\mathcal{P}|}(N)_{|\mathcal{Q}|}} \le \frac{6(n+1)^3}{N^2} + \frac{2q^2}{N^2} \le e^{\delta_3} - 1\,,$$

where

$$\delta_3 = \frac{6(n+1)^3}{N^2} + \frac{2q^2}{N^2}\,.$$

To sum up, since $\frac{6(n+1)^3}{N^2} \leq \frac{6(n+1)^2}{N}$ and $\frac{20q^3}{N^3} \leq \frac{2q^2}{N^2}$, we have

$$\left| \frac{h(\mathcal{G})N^q}{(N)_{|\mathcal{P}|}(N)_{|\mathcal{Q}|}} - 1 \right| \leq e^{\epsilon} - 1$$

where

$$\epsilon = \frac{3\sum_{i=1}^{\alpha+\beta} |\mathcal{R}_i|}{N} + \frac{2q^2}{N^2} + \frac{6(n+1)^2}{N}\,,$$

which completes the proof for the case of $q_c = 0$.