

Quantum Security of XOR of Permutations via Fourier Analysis

Wonseok Choi¹ Minki Hhan² Junyoung Jang²

¹DGIST, Daegu, Korea
wonseok@dgist.ac.kr

²KAIST, Daejeon, Korea
minkihhan@kaist.ac.kr, junsarang74@kaist.ac.kr

Abstract

The XOR of two or more independent random permutations (XoP) is the prototypical pseudorandom function built from permutations achieving the security beyond the birthday bound. The security of the XoP construction is now well established against classical adversaries, however, its security against quantum adversaries that query the construction in superposition has remained widely open.

We prove that the XOR of $r \geq 2$ independent random permutations over $\{0, 1\}^n$ is indistinguishable from a random function by any q -query quantum algorithm with advantage

$$O\left(\min\left\{\frac{q^3}{2^{rn}}, \frac{q^{1.5}}{2^{(r-0.5)n}}, \frac{1}{2^{(r-1.5)n}}\right\}\right)$$

for all $q \leq 2^n/57774$, where the hidden factors depend only on r . In particular, the XoP construction remains secure throughout the entire query range, far beyond the $2^{n/3}$ quantum birthday bound due to the quantum collision finding attack. To our knowledge, this is the first construction from permutations that achieves the quantum version of the beyond birthday bound security.

We present several heuristic attacks suggesting the tightness of our bounds. For $q \lesssim 2^{n/2}$, the quantum collision finding-based attacks heuristically give the advantage $\Omega(q^3/2^{rn})$ and $\Omega(q^{1.5}/2^{(r-0.5)n})$, and for $q \approx 2^n$, the heuristic collision counting-based attack appears to have the advantage about $2^{-(r-1.5)n}$.

We use a Fourier-analytic variant of the polynomial method on the space of functions: the distinguishing advantage of any q -query quantum algorithm is controlled by the Fourier components of degree at most $2q$, which is controlled by $2q$ input-output data of the construction. Most components are bounded as a ℓ_2 norm of the Fourier weights of the XOR of permutations, which gives the bound $2^{-(r-3/2)n}$.

For the bound $q^3/2^{rn}$, few low-degree components are too large. We reinterpret these low-degree components as (sums of) distinguishing advantages of the other problems. For example, the degree-2 and degree-4 terms are interpreted as the advantages against random functions with and without *planted collisions*, which in turn are bounded using Zhandry's small-range distributions.

Finally, the $q^{1.5}/2^{(r-0.5)n}$ bound can be proven using another bound for the planted collisions. This new bound is proven using the compressed oracle by interpreting the advantage as the other bound about random functions. It also gives a new bound for the small-range indistinguishability for (ironically) large ranges, which is of independent interest.

AI use disclosure. The Fourier-analytic approach to the quantum security of XoP was formulated by the authors, with assistance from ChatGPT 5.4 and 5.5 Pro in formalizing many technical details. From the authors' perspective, the first nontrivial mathematical contribution from AI was a proof of the $O(q^3/N^r)$ bound of the degree-2 components (Lemma 6.7), obtained through a series of conversation with ChatGPT 5.5 Pro. Initial proofs of several other lemmas were also generated by ChatGPT 5.5, 5.6 Pro and Astra (in the Ultra mode), as well as Fable 5.0 and 5.1. The authors subsequently simplified these proofs and, in many cases, developed substantially different proofs that they considered more natural and accessible. The current paper is mostly written by human authors from scratch, while AI assisted in writing some paragraphs.

Contents

1	Introduction	3
1.1	Our results	3
1.2	Technical overview	4
1.3	Heuristic Attacks	8
1.4	Related Works	8
2	Preliminaries	9
3	Fourier Analysis of Functionals	9
3.1	Fourier analysis of the functionals	10
3.2	Quantum oracle algorithms as functional	12
4	Quantum Security of XoP	14
5	XoP Security for Many Quantum Queries	15
5.1	Proofs for low degrees	15
5.2	Proofs for high degrees	20
5.3	Maximal Magnitude and Weight of the components of $\mu_{\mathbf{P}}$	22
6	Few Quantum Query Security via Planted Collisions	25
6.1	Preparation: Distributions with planted constraints	26
6.2	Degree-2 component as planted collision	27
6.3	Degree-3 component as planted-three-collision	28
6.4	Degree-4 component as planted two collisions plus small terms	29
6.5	Degree-6 component as planted three collisions plus small terms	31
7	Middle Quantum Query Security via Improved Small-range Indistinguishability	33
7.1	Planted collisions in the compressed oracle	35
7.2	The number of collisions in the database	36
7.3	Proof of the planted-collision bound	37
A	Collision Bias and Heuristic Attacks	42
B	Reductions between Planted Distributions	44
B.1	Several planted collisions	44
B.2	A planted triple from a planted pair	45
B.3	Planted 4-XOR by splitting outputs	46
C	Missing Proofs for the Compressed Oracles	47

1 Introduction

Random permutations are arguably the most important idealized object in cryptography. Even in symmetric-key cryptography, *the standard model* assumes a keyed block cipher to be a private (pseudo)random permutation due to the wide adoption of the standardized block ciphers such as DES and AES [27, 1]. In this regard, earlier practical symmetric-key schemes are instantiated with block ciphers (i.e., random permutations) while the schemes could enjoy better security if instantiated with random functions [6, 38]. The representative examples are Wegman-Carter(-Shoup) MACs and counter mode [55, 53, 8].

The subsequent research on symmetric-key construction designs has sought to achieve better security, especially the security beyond the birthday bound—namely the *beyond-birthday-bound* security. In its heart, the Luby-Rackoff backward problem [6] asks how to construct (pseudo)random functions (PRFs) using random permutations. It has become a prominent cryptographic field intersecting theory and practice [6, 38, 41, 47, 43, 25, 36, 9, 18, 20, 37, 10, 19, 28, 29]. See the related works for a more detailed discussion.

This paper studies the PRF constructions based on random permutations in the quantum setting, where the question becomes substantially more difficult. A quantum PRF (QPRF) [58] is a function that is indistinguishable from random functions even allowing coherent access to the function. The coherent queries prevent the classical security proofs as it potentially *sees* all data of the constructions. Worse, unlike the random functions, these coherent queries potentially reveal the *correlation* between the input-output pairs of the permutations, which hinders or complicates the beautiful compressed oracle method [57] for permutations; the known results are very lossy or restrictive [16, 39, 50, 2, 35, 24]. This difficulty appears in the current disappointing state-of-the-art, establishing tight quantum security of permutation-based cryptography remains very challenging. In particular, no permutation-based QPRFs is known to be secure beyond $q = 2^{n/3}$ queries for n -bit permutations, which is already (and optimally) achieved by the plain random permutations [56, 15].

This leads to a practical concern for the future quantum cryptographic primitives. We are currently uncertain about the quantum security of any PRFs from permutations and applications [11, 12, 54, 3]. Importantly, any instantiation of these applications using block ciphers such as AES256 is only known to be secure up to $2^{128/3} \approx 2^{43}$ quantum queries, which is unsatisfactory to cryptographers. Resolving this question would give more efficient schemes for cryptography with quantum states and unitaries [40, 4, 45, 42] as well.

1.1 Our results

This paper shows that the exclusive-or of two or more permutations, i.e., the XoP constructions, also have a strong security in the quantum setting. This construction processes the input x by

$$\text{XoP}[r](x) := P_1(x) + \cdots + P_r(x),$$

which we simply refer to as the XoP[r] construction, where $+$ denotes bitwise XOR and $P_1, \dots, P_r$ are independent random permutations over n -bit strings.

In the classical setting, the tight security of the XoP construction for $r = 2$ was $O\left(\min\left(\frac{q^2}{2^{2n}}, \frac{q}{2^{1.5n}}\right)\right)$. The first bound dominates for $q \lesssim 2^{0.5n}$ and is proven in [30, 17]. The second bound dominates for $q \gtrsim 2^{0.5n}$ and recently proven in [28, 31] using Fourier analysis. The latter bound can be generalized to $q/2^{r-0.5}$ for $r \geq 2$. These bounds are tight, matching the known attack by Patarin [47].

Our main theorem proves the quantum security of the XoP construction.

Theorem 1.1 (Informal). *Fix a constant $r \geq 2$. For every $0 \leq q \ll 2^n$, any quantum distinguisher making q quantum queries to either the XoP[r] construction or the random functions has advantage at most*

$$O\left(\min\left(\frac{q^3}{2^{rn}}, \frac{q^{1.5}}{2^{(r-0.5)n}}, \frac{1}{2^{(r-1.5)n}}\right)\right).$$

In particular, the XoP[r] construction for $r \geq 2$ is secure up to $q \approx 2^n$ queries.

The above theorem concerns an ideal setting where the adversary does not have access to the primitive queries to $P_1, \dots, P_r$. In practice, the XoP constructions can be instantiated using block ciphers with independent random keys in the quantum ideal cipher model. When the underlying block cipher has a sufficiently long key, say κ -bit keys, the corresponding keyed permutations can be viewed as private random permutations in the quantum ideal cipher model, with the distinguishing advantage loss $rq^2/2^\kappa$ by applying the quantum search bound r times [7, 13] (assuming there is no collisions in the r keys). Therefore, our result can be lifted to the quantum ideal cipher model with such a key length; for example, AES256 provides a heuristic instantiation with $\kappa = 256$.

To our knowledge, this gives the first QPRF constructions in the quantum ideal cipher model whose security goes beyond the $2^{n/3}$ quantum queries. In fact, our theorem shows that the XoP construction is still indistinguishable from random functions near 2^n queries; we are not even aware of any construction secure against $2^{n/2}$ queries.

1.2 Technical overview

We focus on the XOR of two permutations in this overview. Our proof can be viewed as a quantum analogue of the Fourier analytic security proofs developed in a recent line of works [31, 32, 28, 29], which have established tight classical security bounds for the XoP constructions. The main object in these analyses is the classical response transcript. More precisely, after fixing the q distinct query points, the corresponding response vector lies in $(\{0, 1\}^n)^q$. For the XoP construction, this vector is distributed as the sum of two vectors sampled without replacement, while this vector is uniform random for the truly random functions. The Fourier analysis compares these two distributions of vectors in the Fourier domain.

Polynomial method. In our quantum setting, however, there is no proper notion of the transcript because of the coherent quantum queries. We instead employ a Fourier-analytic variant of the polynomial method [5]. Our starting point is the following well-known observation. Let $|\hat{a}\rangle := \frac{1}{\sqrt{2^n}} \sum_{z \in \{0, 1\}^n} \chi_a(z) |z\rangle = H^{\otimes n} |a\rangle$ be a Fourier basis state where $\chi_a(z) = (-1)^{\langle a, z \rangle}$. For an oracle O_f that evaluates a function f , i.e., that maps $|x, y\rangle \mapsto |x, y + f(x)\rangle$ coherently, we have

$$O_f |x, \hat{a}\rangle = (-1)^{\langle a, f(x) \rangle} |x, \hat{a}\rangle = \chi_a(f(x)) |x, \hat{a}\rangle.$$

Motivated by this, we consider a vector $\gamma = (\gamma_x)_{x \in \{0, 1\}^n} \in (\{0, 1\}^n)^{2^n}$ and define its Fourier degree by $|\gamma| := |\{x \in \{0, 1\}^n : \gamma(x) \neq 0^n\}|$. Each vector gives its Fourier character defined by

$$\chi_\gamma(f) := (-1)^{\sum_{x \in \{0, 1\}^n} \langle \gamma(x), f(x) \rangle}, \quad \chi_{\gamma+\eta}(f) = \chi_\gamma(f) \cdot \chi_\eta(f).$$

The above observation shows that the amplitudes of each basis vector can be written as a linear sum of the Fourier characters, and each query increases the degree of amplitudes by at most 1.

The acceptance probability $\Pr[A^{O_f} = 1]$ therefore must be represented by a low-degree polynomial of the Fourier characters. By regarding it as a function from f to the real number in $[0, 1]$,¹ the Fourier expansion gives

$$P_A(f) := \Pr[A^{O_f} = 1] = \sum_{|\gamma| \leq 2q} \hat{P}_A(\gamma) \cdot \chi_\gamma(f), \quad \hat{P}_A(\gamma) = \mathbb{E}_{g \leftarrow \mathbf{F}} \left[\overline{\chi_\gamma(g)} P_A(g) \right].$$

Here, $g \leftarrow \mathbf{F}$ denotes a sample from the uniformly random functions. The degree bound $\leq 2q$ is because the amplitudes of the final state of a q -query algorithm are Fourier polynomials of degree at most q . This observation, or closely related variants in representation-theoretic language, has been used in many analyses of quantum algorithms [58, 51, 57, 50, 2]. It allows us to bound the probability of the oracle algorithm through their bounded-degree Fourier statistics.

¹That is, this is a *functional* that maps a function to a scalar. In the main body, we refer this Fourier analysis as the Fourier analysis of functionals to distinguish the different use of the term function.

Distinguishing advantage as an inner product. We introduce some definitions to proceed the overview. Let $N := 2^n$, and let $\mathbf{F} = \{f : \{0, 1\}^n \rightarrow \{0, 1\}^n\}$ be the space of functions. We write

$$\langle g, h \rangle := \mathbb{E}_{f \leftarrow \mathbf{F}}[\overline{g(f)}h(f)] \quad \text{and} \quad \|g\|_2^2 := \langle g, g \rangle.$$

With this notation, we can write

$$\Pr_{f \leftarrow \mathbf{F}}[\mathcal{A}^{O_f} = 1] = \sum_{f \in \mathbf{F}} \frac{P_{\mathcal{A}}(f)}{|\mathbf{F}|} = \mathbb{E}_{f \leftarrow \mathbf{F}}[\mathbf{1}(f)P_{\mathcal{A}}(f)] = \langle \mathbf{1}, P_{\mathcal{A}} \rangle$$

where $\mathbf{1}$ is a constant function with output 1. Similarly, define the density of the XoP distribution relative to this uniform measure by

$$\mu_{\text{XoP}}(f) := \frac{\Pr_{P, Q \leftarrow \mathbf{P}}[P + Q = f]}{\Pr_{P \leftarrow \mathbf{P}}[P = f]} = N^N \Pr_{P, Q \leftarrow \mathbf{P}}[P + Q = f].$$

An analogous calculation gives

$$\Pr_{P, Q \leftarrow \mathbf{P}}[\mathcal{A}^{O_{P+Q}} = 1] = \langle \mu_{\text{XoP}}, P_{\mathcal{A}} \rangle$$

and the distinguishing advantage can be written as

$$\Pr_{P, Q \leftarrow \mathbf{P}}[\mathcal{A}^{O_{P+Q}} = 1] - \Pr_{f \leftarrow \mathbf{F}}[\mathcal{A}^{O_f} = 1] = \langle P_{\mathcal{A}}, \mu_{\text{XoP}} - \mathbf{1} \rangle.$$

The above discussion about the Fourier analysis applies on these probabilities, showing that $P_{\mathcal{A}}$ has Fourier degree at most $2q$ and $\|P_{\mathcal{A}}\|_2 \leq 1$.

Decomposition by Fourier degree. We consider the following two terms:

1. $(\cdot)^{=d}$ that denotes the sum of all Fourier components of degree exactly d ;
2. $(\cdot)^{\leq d}$ that denotes the sum of all Fourier components of degree $\leq d$, i.e., the sum of all $(\cdot)^{=k}$ for $k \leq d$.

The orthogonality of the Fourier components, following the so-called Efron–Stein orthogonal decomposition [46, Chapter 8], gives the advantage bound by

$$|\langle P_{\mathcal{A}}, \mu_{\text{XoP}} - \mathbf{1} \rangle| = |\langle P_{\mathcal{A}}, (\mu_{\text{XoP}} - \mathbf{1})^{\leq 2q} \rangle| = \left| \sum_{k=1}^{2q} \langle P_{\mathcal{A}}, \mu_{\text{XoP}}^{\overline{k}} \rangle \right| \leq \sum_{k=1}^{2q} |\langle P_{\mathcal{A}}, \mu_{\text{XoP}}^{\overline{k}} \rangle|$$

where we use the fact that $P_{\mathcal{A}}$ is of degree at most $2q$ in the first equality, and use $(\mu_{\text{XoP}} - \mathbf{1})^{=0} = 0$ and $(\mathbf{1})^{=k} = 0$ for all $k \geq 1$. The Cauchy–Schwarz inequality gives the first way to bound this:

$$\leq \sum_{k=1}^{2q} \|P_{\mathcal{A}}\|_2 \|\mu_{\text{XoP}}^{\overline{k}}\|_2 \leq \sum_{k=1}^{2q} \|\mu_{\text{XoP}}^{\overline{k}}\|_2$$

where we use $\|P_{\mathcal{A}}\|_2 \leq 1$. For most degrees, we obtain the required bound directly by estimating $\|\mu_{\text{XoP}}^{\overline{k}}\|_2$ through a delicate combinatorial argument. In particular, the second advantage bound $2^{-0.5n}$ is obtained by this strategy alone.

Turning Fourier term into planted collision distinguisher. To prove the security $q^3/2^{2n}$ for the XoP construction, the above strategy turns out to be insufficient. In particular, the degree-2,3,4,6 components have too large ℓ_2 -norm. We use a different proof strategy; namely, we turn the Fourier-analytic components $\langle P_{\mathcal{A}}, \mu_{\text{XoP}}^{\overline{k}} \rangle$ to the distinguishing advantage to *some other problems*.

We focus on the degree-2 component, or more precisely $\langle P_{\mathcal{A}}, \mu_{\text{XoP}}^{\overline{2}} \rangle$, in this overview. The degree-2 term exhibits the statistics of two outputs of the functions, such as collisions. This component turns out to be the dominant term in the bound, which was the dominant term in the classical security as well [48, 28].

This intuition holds in the quantum setting as well. Write $\llbracket X \rrbracket$ to denote the truth value of the statement X . We will establish the following identity at the end of the overview:

$$\mu_{\text{XoP}}^{\bar{2}}(f) = \left(\frac{1}{N-1} \right)^2 \sum_{x < x'} (N \llbracket f(x) = f(x') \rrbracket - 1), \quad (1)$$

which means that the degree-two component can be understood as a collision statistic up to a multiplicative factor; the truth value $\llbracket f(x) = f(x') \rrbracket$ is 1 if and only if f collides at $x \neq x'$.

Fix $x \neq x'$ and fix a function f . Observe that

- $\frac{1}{N^N}$ is the probability that f is sampled from $\mathbf{F}$;
- $\frac{1}{N^N} \cdot N \llbracket f(x) = f(x') \rrbracket$ is the probability that f is sampled from $\mathbf{F}$ conditioned on $f(x) = f(x')$.

From this observation, we can interpret $\mu_{\text{XoP}}^{\bar{2}}(f)$ as, up to a constant factor, the difference between the density functions of 1) the distribution of the true random function $\mathbf{F}$ and 2) the distribution of random functions conditioned on a *planted collision* $f(x) = f(x')$ for random $x \neq x'$. That is, we can reinterpret the inner product

$$|\langle P_{\mathcal{A}}, \mu_{\text{XoP}}^{\bar{2}} \rangle| = O \left(\left| \Pr_{f \leftarrow \mathcal{D}_{\text{PC}}} [A^{O_f} = 1] - \Pr_{f \leftarrow \mathbf{F}} [A^{O_f} = 1] \right| \right)$$

as a distinguishing advantage of *another problem*: 1) a random function with a planted collision and 2) an unconditional random function. Here, $\mathcal{D}_{\text{PC}}$ denote the planted collision distribution described above.

Planted collisions vs. random functions. We directly prove the distinguishing advantage $O(q^3/N^2)$ of this problem using Zhandry’s small range distribution indistinguishability [58], which shows that the distinguishing advantage of the following two distributions is bounded above by $O(q^3/R)$: The first one is the uniformly random functions from $\{0, 1\}^n$ to $\{0, 1\}^n$, and the second one is the distribution D_R of random “small-range” functions, which are obtained by composing two independent random functions $g \circ h$ where $h : \{0, 1\}^n \rightarrow [R]$ and $g : \text{Im}(h) \rightarrow \{0, 1\}^n$.

Ironically, we use the *large range* function with $R \gtrsim N^2$. In this case, h has a unique collision with a constant probability, in which case $g \circ h$ is distributed according to the planted collision distribution. Therefore, the distinguishing D_R and $\mathbf{F}$ is closely related to the above problem. It turns out that any $R \gtrsim N^2$ exhibits such a relation; when there is no collision in h , the distribution of $g \circ h$ becomes the uniformly random function so that the related terms are canceled out, and $R \rightarrow \infty$ makes the unique collision dominate among the other terms, deriving the upper bound $O(q^3/N^2)$.

The other degrees are more involved, but similar strategies show the desired bounds. Very roughly, we connect the degree-3,4,6 terms with the other problems using similarly to Eq. (1); for example, the degree-3 term is related to the distinguishing advantage between the random functions and the random planted-3-collision functions with a constraint $f(x_1) = f(x_2) = f(x_3)$. The degree-4 term is related to the random functions with two planted collisions together with the random functions with the planted 4-XOR $f(x_1) + f(x_2) + f(x_3) + f(x_4) = 0^n$. We reduce the hardness of these problems to the planted collision advantage similarly to the above (yet in a slightly more involved way). The bound for the degree-2 is tight in the relevant parameter range, as suggested by the corresponding quantum collision-statistics attack below.

Another bound for the planted collisions. To derive the $O(q^{1.5}/N^{1.5})$ security bound, we observe that the term in Eq. (1) can be interpreted some collision-related term in the language of the compressed oracle [57, 22]. By writing the overall final state $|\Psi\rangle$ of the algorithm and (purified) database by $\frac{1}{\sqrt{N^N}} \sum_g |\psi^g\rangle |g\rangle$,

the advantage can be expressed by

$$\begin{aligned}
\langle \mu_{\text{PC}} - \mathbf{1}, P_{\mathcal{A}} \rangle &= \frac{2}{N-1} \mathbb{E}_{f \leftarrow \mathbf{F}} \left[P_{\mathcal{A}}(f) \sum_{x < y} \left(\mathbb{I}[f(x) = f(y)] - \frac{1}{N} \right) \right] \\
&= \frac{2}{N^N(N-1)} \sum_{f, g \in \mathbf{F}} \langle \psi_q^g | \Pi | \psi_q^f \rangle \langle g | \left(\sum_{x < y} \left(\text{Col}_{xy} - \frac{1}{N} I \right) \right) | f \rangle \\
&= \frac{2}{N-1} \langle \Psi | \Pi \left(\sum_{x < y} \left(\text{Col}_{xy} - \frac{1}{N} I \right) \right) | \Psi \rangle
\end{aligned}$$

where Π is the projection to the acceptance space of the algorithm, and Col_{xy} is the indicator function for the database on inputs x, y . This expression can be bounded by $O(q^{1.5}/N^{1.5})$ using the compressed oracle machinery alone, proving the desired result. Intriguingly, the above-discussed small-range to planted collision can be reversed, and $q^{1.5}/N^{1.5}$ gives an alternative bound for the small-range distribution indistinguishability for large range. See [Corollary 7.3](#).

Proof of Eq. (1). We now discuss how to prove [Eq. \(1\)](#). Let $\mathbf{P}$ be the distribution of uniformly random permutations, and let $\mu_{\mathbf{P}}(f) = N^N \Pr_{p \leftarrow \mathbf{P}}[p = f]$ be the density function of $\mathbf{P}$. The degree-2 term expands, together with the convolution formula,

$$\mu_{\text{XoP}}^2(f) = \sum_{|\gamma|=2} \hat{\mu}_{\text{XoP}}^2(\gamma) \chi_{\gamma}(f) = \sum_{|\gamma|=2} \hat{\mu}_{\mathbf{P}}^2(\gamma) \chi_{\gamma}(f). \quad (2)$$

We extensively use the following basic observation $\sum_{x \in \{0,1\}^n} (-1)^{\langle a, x \rangle} = N \mathbb{I}[a = 0^n]$ and its variations. For example, for $y, y' \neq 0^n$, we have

$$\sum_{u \neq v} (-1)^{\langle u, y \rangle + \langle v, y' \rangle} = \sum_{u, v} (-1)^{\langle u, y \rangle + \langle v, y' \rangle} - \sum_u (-1)^{\langle u, y+y' \rangle} = -N \mathbb{I}[y = y']$$

where all $u, v \in \{0,1\}^n$. In the second equality, the first term vanishes because of $\mathbb{I}[y = 0^n] = 0$, and the last term is simplified using $\mathbb{I}[y + y' = 0^n] = \mathbb{I}[y = y']$.

Let $\gamma = (\gamma_x)_{x \in \{0,1\}^n} \in (\{0,1\}^n)^{2^n}$ be such that $|\gamma| = |\text{supp}(\gamma)| = 2$ where $\text{supp}(\gamma) = \{x \in \{0,1\}^n : \gamma(x) \neq 0^n\}$. Let x, x' be the elements of $\text{supp}(\gamma)$. Observe that for a uniform random permutation $p \leftarrow \mathbf{P}$, $(p(x), p(x'))$ is uniform over ordered distinct pairs, hence

$$\mathbb{E}_{p \leftarrow \mathbf{P}}[\chi_{\gamma}(p)] = \frac{1}{N(N-1)} \sum_{p(x) \neq p(x')} (-1)^{p(x) \cdot \gamma(x) + p(x') \cdot \gamma(x')} = -\frac{\mathbb{I}[\gamma(x) = \gamma(x')]}{N-1}.$$

It is not hard to see that the above term coincides with $\hat{\mu}_{\mathbf{P}}(\gamma)$ using the definition of the Fourier coefficient and the fact that χ_{γ} is real-valued. We omit this proof in this overview.

Now we go back to [Eq. \(2\)](#). Plugging the above identity gives

$$\sum_{|\gamma|=2} \hat{\mu}_{\mathbf{P}}^2(\gamma) \chi_{\gamma}(f) = \sum_{\text{supp}(\gamma) = \{x < x'\}} \frac{\mathbb{I}[\gamma(x) = \gamma(x')]^2 \chi_{\gamma}(f)}{(N-1)^2}$$

where we use the lexicographic order in $x < x'$. Writing $\gamma(x) = \gamma(x') = y \neq 0^n$ and using $\chi_{\gamma}(f) = (-1)^{\langle y, f(x)+f(x') \rangle}$, we can write this as

$$\begin{aligned}
\sum_{x < x', y \neq 0^n} \frac{(-1)^{\langle y, f(x)+f(x') \rangle}}{(N-1)^2} &= \sum_{x < x', y} \frac{(-1)^{\langle y, f(x)+f(x') \rangle}}{(N-1)^2} - \sum_{x < x'} \frac{1}{(N-1)^2} \\
&= \sum_{x < x'} \frac{N \mathbb{I}[f(x) = f(x')] - 1}{(N-1)^2}.
\end{aligned}$$

This proves [Eq. \(1\)](#). Similar calculations derive analogous algorithmic interpretations of different degrees.

1.3 Heuristic Attacks

We briefly discuss the (potential) distinguishing attack for the XoP constructions in [Appendix A](#). The description focuses on the high-level ideas of the attack, with some statistical evidence or heuristic reasoning of their advantages. Formalizing them needs further analysis. Most attacks for $q \ll N$ are related to the pairwise statistics, i.e., collisions of the construction. On the other hand, the attack for $q \geq N/2$ uses the quantum parity algorithm [34], achieving the advantage $1/2$.

[Table 1](#) summarizes the different attacks and security bounds on XoP[r]. Our lower bounds match to the heuristic attacks for $q \lesssim N^{1/2}$ and $q \approx N$. It is unclear which is tight for the range $N^{1/2} \lesssim q < N/2$.

Range	Classical	Q. attack	Our bound	Q. attack type
$q \lesssim N^{1/3}$	$\Theta\left(\frac{q^2}{N^r}\right) \star$	$\frac{q^3}{N^r} ?$	$O\left(\frac{q^3}{N^r}\right)$	Collision finding
$N^{1/3} \lesssim q \lesssim N^{1/2}$	$\Theta\left(\frac{q^2}{N^r}\right)$	$\frac{q^{3/2}}{N^{r-1/2}} ?$	$O\left(\frac{q^{3/2}}{N^{r-1/2}}\right)$	Collision counting
$N^{1/2} \lesssim q < N/2$	$\Theta\left(\frac{q}{N^{r-1/2}}\right)$	$\frac{\sqrt{q}}{N^{r-1}} ?$	$O\left(N^{3/2-r}\right)$	Collision counting
$q \geq N/2$	-	$\Theta(1)$	-	Parity

Table 1: The classical results, quantum attacks and our bounds. $\star$ denotes that the security bound is only known for $r = 2$. The question mark (?) denotes that the attack analysis is heuristic.

Collision probability. All attacks above except for the parity attack exploit the collision statistics as follows from [48]. For two distinct inputs x, x' , it holds that

$$\Pr[\text{XoP}[r](x) = \text{XoP}[r](x')] = \frac{1}{N} + \frac{(-1)^r}{N(N-1)^{r-1}}.$$

On the other hand, the collision probability of random functions is $1/N$, having the bias $\delta_r = \frac{(-1)^r}{N(N-1)^{r-1}} \approx (-1)^r N^{-r}$ in the collision probability in two cases. This bias allows the collision-based distinguishing attack. For example, running the quantum collision finding algorithm [15] and outputs 1 when a collision is found has the advantage q^3/N^r for $q \lesssim N^{1/3}$. The details of the attacks are described in [Appendix A](#).

1.4 Related Works

Classical analyses of XoP and variants. Most of the security analysis of XoP is focused on the $r = 2$ case. Various proof techniques have been developed, and the XoP construction has been a testbed of the techniques. Lucks [41] first gave an early asymptotic analysis. Patarin [47] claimed to prove the bound $O(q^2/N^2)$, but the proof was incomplete. Dai, Hoang, and Tessaro [25] proved the bound $O(q^{1.5}/N^{1.5})$. Dutta, Nandi, and Saha [30] resurrect the bound of Patarin [47]. The multi-user security was tightened by Chen, Choi, and Lee [17].

Independently, the tight bound $O(q/N^{1.5})$ was proven using the Fourier analysis by Eberhard [31] but had been unknown to the symmetric-key cryptography community. Dinur extended this to XoP[r] with $r > 2$ even in the multi-user setting [28], improving the previous analysis for $r > 2$ [23, 19].

There are XoP-like constructions based on other building blocks rather than block ciphers. For example, the sum of the Even-Mansour encryption [18] and the XOR of the tweakable permutation [21] have been studied in the literature.

Quantum analyses of XoP and variants. As far as we are aware of, the only quantum result of the XoP construction is [44]. They study the XoP in the Q1 model, where the underlying block cipher can be quantumly accessible but the XoP is only available through classical queries. They proved the security

about $rq^2/2^\kappa + q/2^n$ in the Q1 model.² Our result gives the Q2 model security bound about $rq^2/2^\kappa + \min(q^3/2^{rn}, 1/2^{(r-1.5)n})$, which is even better than their Q1 bound for $r \geq 2$.

The variants have been studied in the quantum setting as well. The keyed sum of permutations and other variants are proven secure up to $2^{n/3}$ queries in the Q1 model [26]. For the sum of Even-Mansour, a polynomial time quantum attack is known in the Q2 model [52].

2 Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field of two elements 0 and 1. For $x = (x_i)_{i \in [n]}, y = (y_i)_{i \in [n]} \in \{0, 1\}^n$, we define their exclusive OR (XOR) by $x + y := (x_i \oplus y_i)_{i \in [n]}$ and inner product by $\langle x, y \rangle := \sum_{i=1}^n x_i \cdot y_i \bmod 2$. For a finite set S , we write $s \leftarrow S$ to denote that s is sampled uniformly at random from S . We also write $(s_1, \dots, s_t) \leftarrow S^{(*t)}$ to denote that the elements of $\{s_i\}_{i \in [1..t]}$ are sampled uniformly at random from S *without replacement*, i.e., $\{s_i\}_{i \in [1..t]}$ is pairwise distinct. For an event X , we write $\llbracket X \rrbracket$ for its indicator, i.e., $\llbracket X \rrbracket = 1$ if X occurs and $\llbracket X \rrbracket = 0$ otherwise. Throughout this paper, n denotes a fixed positive integer, and we write $N := 2^n$. For integers $a \geq b \geq 0$, we write

$$(a)_b := a(a-1) \cdots (a-b+1).$$

Probability distributions. For a probabilistic distribution $\mathcal{D}_D$ over a finite set X , we write $\mu_D(x) = |X| \cdot \Pr_{y \leftarrow \mathcal{D}_D}[x = y] = |X| \cdot \Pr[x \leftarrow \mathcal{D}_D]$. Observe that $\mathbb{E}_{x \leftarrow X}[\mu_D(x)] = 1$ and the following identity

$$\mathbb{E}_{x \leftarrow X}[\mu_D(x) h(x)] = \sum_{x \in X} \frac{1}{|X|} \cdot \frac{\Pr[x \leftarrow \mathcal{D}_D]}{1/|X|} \cdot h(x) = \mathbb{E}_{x \leftarrow \mathcal{D}_D}[h(x)] \quad (3)$$

which shows that the multiplicative factor μ_D converts the expectation with respect to the uniform distribution on X into the expectation with respect to our interested distribution $\mathcal{D}_D$.

Let $\mathbf{F}$ be a finite function space, and let $\mathcal{D}_D$ and $\mathcal{D}_E$ be two probability distributions over $\mathbf{F}$. For $f \in \mathbf{F}$, write O_f for the quantum oracle associated with f . Namely, O_f maps $|x, y\rangle$ to $|x, y + f(x)\rangle$ coherently.

For a quantum oracle algorithm $\mathcal{A}$, we define its distinguishing advantage between two distributions $\mathcal{D}_D$ and $\mathcal{D}_E$ by

$$\text{Adv}^{\text{dist}}(\mathcal{D}_D, \mathcal{D}_E; \mathcal{A}) := \left| \Pr_{f \leftarrow \mathcal{D}_D}[\mathcal{A}^{O_f} \rightarrow 1] - \Pr_{f \leftarrow \mathcal{D}_E}[\mathcal{A}^{O_f} \rightarrow 1] \right|.$$

For $q \geq 0$, we define the advantage over all q -query algorithms

$$\text{Adv}_q^{\text{dist}}(\mathcal{D}_D, \mathcal{D}_E) := \max_{q\text{-query } \mathcal{A}} \text{Adv}^{\text{dist}}(\mathcal{D}_D, \mathcal{D}_E; \mathcal{A})$$

where the maximum is over all quantum oracle algorithms making at most q quantum queries to the oracle.

3 Fourier Analysis of Functionals

We denote the set of all functions from n -bit inputs to n -bit outputs by

$$\mathbf{F}_n = \{f : \{0, 1\}^n \rightarrow \{0, 1\}^n\}.$$

When the bit-length is clear from the context, we omit the subscript and just denote them by $\mathbf{F}$. The set $\mathbf{F}$ has a natural group structure by extending the XOR operation by $(f + g)(x) = f(x) + g(x)$ for $f, g \in \mathbf{F}$ and $x \in \{0, 1\}^n$. We sometimes use the notation $\widehat{\mathbf{F}}$ with the elements denoted by Greek characters, e.g., γ or η , to denote the identical group $(\mathbf{F}, +)$ to distinguish their use.³ Looking ahead, we will use $\widehat{\mathbf{F}}$ to denote the set of Fourier basis only.

²To be precise, they assumed that the Grover algorithm is optimal in this attack for the concrete block cipher. This can be proven in the ideal cipher model using [7] as discussed above.

³ $\widehat{\mathbf{F}}$ denotes the (Pontryagin) dual group, which is isomorphic to $\mathbf{F}$ since it is finite.

Functionals. We use the Fourier analysis on the set of *functions of functions*:

$$\mathcal{H} = \{H : \mathbf{F} \rightarrow \mathbb{C}\}.$$

To clarify the difference, we use the term functionals to denote the elements in $\mathcal{H}$ with the upper case letters. By identifying $\mathbf{F}$ as $(\{0, 1\}^n)^{2^n}$, the Fourier analysis of the functionals is essentially equivalent to one of the Boolean functions with an exponentially long input.

The set of functionals $\mathcal{H}$ is equipped with the inner product for $H, G \in \mathcal{H}$

$$\langle H, G \rangle = \mathbb{E}_{f \leftarrow \mathbf{F}} \left[\overline{H(f)} G(f) \right] = \sum_{f \in \mathbf{F}} \frac{\overline{H(f)} G(f)}{|\mathbf{F}|}.$$

The corresponding norm is defined by $\|H\|_2 = |\langle H, H \rangle|^{1/2}$. The Cauchy–Schwarz inequality implies that

$$\langle H, G \rangle \leq \|H\|_2 \cdot \|G\|_2.$$

3.1 Fourier analysis of the functionals

Characters. For $a \in \{0, 1\}^n$, let $\chi_a : \{0, 1\}^n \rightarrow \{-1, 1\}$, $\chi_a(x) := (-1)^{\langle a, x \rangle}$. These satisfy, for all $a, b, x \in \{0, 1\}^n$,

$$\chi_a(x) \chi_b(x) = \chi_{a+b}(x) \quad \text{and} \quad \mathbb{E}_{x \leftarrow \{0, 1\}^n} \left[\overline{\chi_a(x)} \chi_b(x) \right] = \mathbb{I}[a = b]. \quad (4)$$

For $\gamma \in \widehat{\mathbf{F}}$, the character $\chi_\gamma \in \mathcal{H}$ is

$$\chi_\gamma(f) := \prod_{x \in \{0, 1\}^n} \chi_{\gamma(x)}(f(x)) = (-1)^{\sum_{x \in \{0, 1\}^n} \langle \gamma(x), f(x) \rangle}. \quad (5)$$

The support and the degree of $\gamma \in \widehat{\mathbf{F}}$ are

$$\text{supp}(\gamma) := \{x \in \{0, 1\}^n : \gamma(x) \neq 0^n\} \quad \text{and} \quad |\gamma| := |\text{supp}(\gamma)|,$$

so $|\gamma|$ is the number of nontrivial factors in Eq. (5). Clearly $|\gamma + \eta| \leq |\gamma| + |\eta|$. By Eq. (4), characters are multiplicative and orthonormal: for $\gamma, \eta \in \widehat{\mathbf{F}}$,

$$\begin{aligned} \langle \chi_\gamma, \chi_\eta \rangle &= \mathbb{E}_{f \leftarrow \mathbf{F}} \left[\overline{\chi_\gamma(f)} \chi_\eta(f) \right] = \mathbb{I}[\gamma = \eta], \\ \chi_\gamma \chi_\eta &= \chi_{\gamma + \eta}, \quad \chi_\gamma(f + g) = \chi_\gamma(f) \chi_\gamma(g). \end{aligned} \quad (6)$$

Since $|\widehat{\mathbf{F}}| = |\mathbf{F}| = \dim \mathcal{H}$, the characters form an orthonormal basis of $\mathcal{H}$.

Fourier expansions. The orthonormal basis of characters gives the Fourier expansion of $H : \mathbf{F} \rightarrow \mathbb{C}$ (i.e., $H \in \mathcal{H}$) as follows.

Theorem 3.1 (Fourier expansion of functionals). *A functional $H : \mathbf{F} \rightarrow \mathbb{C}$ can be decomposed by*

$$H(f) = \sum_{\gamma \in \widehat{\mathbf{F}}} \widehat{H}(\gamma) \chi_\gamma(f), \quad \text{such that} \quad \widehat{H}(\gamma) = \langle \chi_\gamma, H \rangle = \mathbb{E}_{f \leftarrow \mathbf{F}} \left[\overline{\chi_\gamma(f)} H(f) \right],$$

where $\widehat{H}(\gamma)$ is called the Fourier coefficient of H at γ .

Proof. Since $\{\chi_\gamma\}_{\gamma \in \widehat{\mathbf{F}}}$ forms an orthonormal basis of $\mathcal{H}$, every $H \in \mathcal{H}$ admits a unique expansion of the form

$$H = \sum_{\gamma \in \widehat{\mathbf{F}}} c_\gamma \chi_\gamma$$

for some coefficients $c_\gamma \in \mathbb{C}$.

Taking the inner product with χ_η and using orthonormality, we obtain

$$\langle \chi_\eta, H \rangle = \langle \chi_\eta, \sum_{\gamma \in \widehat{\mathbf{F}}} c_\gamma \chi_\gamma \rangle = \sum_{\gamma \in \widehat{\mathbf{F}}} c_\gamma \langle \chi_\eta, \chi_\gamma \rangle = c_\eta.$$

Therefore,

$$c_\eta = \langle \chi_\eta, H \rangle = \mathbb{E}_{f \leftarrow \mathbf{F}} \left[\overline{\chi_\eta(f)} H(f) \right].$$

Since this holds for every $\eta \in \widehat{\mathbf{F}}$, we have

$$H(f) = \sum_{\gamma \in \widehat{\mathbf{F}}} \widehat{H}(\gamma) \chi_\gamma(f), \quad \widehat{H}(\gamma) = \langle \chi_\gamma, H \rangle.$$

This proves the theorem. □

The Fourier spectrum of H is the collection of all Fourier coefficients

$$\left(\widehat{H}(\gamma) \right)_{\gamma \in \widehat{\mathbf{F}}}.$$

The Fourier support of H is the set of γ such that $\widehat{H}(\gamma)$ is nonzero.

The orthogonality of the characters show that for $H, G \in \mathcal{H}$,

$$\langle H, G \rangle = \sum_{\gamma \in \widehat{\mathbf{F}}} \overline{\widehat{H}(\gamma)} \widehat{G}(\gamma). \quad (7)$$

For a nonnegative integer d , the degree- d component of H , denoted by $H^{=d}$, and the low-degree components of H up to degree d , denoted by $H^{\leq d}$, are defined as follows:

$$H^{=d} := \sum_{|\gamma|=d} \widehat{H}(\gamma) \chi_\gamma, \quad \text{and} \quad H^{\leq d} := \sum_{i \leq d} H^{=i}.$$

It is worth noting that $H^{=0} = \mathbb{E}_{f \leftarrow \mathbf{F}}[H(f)] \cdot \mathbf{1}$. We refer to the degree- d weight⁴ and the degree- d maximal magnitude of H as

$$\|H^{=d}\|_2^2 = \sum_{|\gamma|=d} \left| \widehat{H}(\gamma) \right|^2, \quad M^{=d}[H] := \max_{|\gamma|=d} \left\{ \left| \widehat{H}(\gamma) \right| \right\} \quad (8)$$

where the equality holds due to the orthogonality of the characters.

For a functional $H \in \mathcal{H}$, we say the Fourier degree of H , denoted by $\deg(H)$, by the minimum nonnegative integer d such that $H = H^{\leq d}$ holds, which means that H is the sum of Fourier characters of degree $\leq d$. Constant functionals have Fourier degree 0. Taking conjugate does not change the degree. For $H, G \in \mathcal{H}$, we have

$$\deg(H + G) \leq \max(\deg(H), \deg(G)), \quad \deg(HG) \leq \deg(H) + \deg(G). \quad (9)$$

⁴Dinur [28] uses $W^{=d}[H]$ instead of $\|H^{=d}\|_2^2$ to refer to the degree- d weight of H .

Convolution. The *convolution* of $G, H \in \mathcal{H}$ is $(G * H)(f) := \mathbb{E}_{g \leftarrow \mathbf{F}}[G(f + g)H(g)]$.

Lemma 3.2. $\widehat{H * G}(\gamma) = \widehat{H}(\gamma)\widehat{G}(\gamma)$.

Proof. In [46, Theorem 1.27], the same statement for real-valued boolean functions is proven. It can be extended to our case as follows.

$$\begin{aligned}\widehat{H * G}(\gamma) &= \mathbb{E}_{f \leftarrow \mathbf{F}} \left[\overline{\chi_\gamma(f)} H * G(f) \right] \\ &= \mathbb{E}_{f \leftarrow \mathbf{F}} \left[\overline{\chi_\gamma(f)} \mathbb{E}_{g \leftarrow \mathbf{F}} [H(f + g)G(g)] \right] \\ &= \mathbb{E}_{g, h \leftarrow \mathbf{F}} \left[\overline{\chi_\gamma(g + h)} H(h)G(g) \right] \\ &= \mathbb{E}_{g, h \leftarrow \mathbf{F}} \left[\overline{\chi_\gamma(h)} H(h) \overline{\chi_\gamma(g)} G(g) \right] \\ &= \widehat{H}(\gamma)\widehat{G}(\gamma)\end{aligned}$$

since $\overline{\chi_\gamma} = \chi_\gamma$ and by Eq. (6). $\square$

Distributions of XOR of functions. One main target of the functional Fourier analysis is the probabilistic density functions over $\mathbf{F}$. Let $\mathcal{D}_D, \mathcal{D}_E$ be distributions over $\mathbf{F}$ and write μ_D, μ_E to denote their density functions, i.e., $\mu_D(f) = \frac{\Pr[f \leftarrow \mathcal{D}_D]}{1/|\mathbf{F}|}$.

Lemma 3.3. $\mu_D * \mu_E$ is the density of the distribution of $h = f + g$ where $f \leftarrow \mathcal{D}$ and $g \leftarrow \mathcal{E}$ are independent.

Proof. Using $\mu_D(f) = |\mathbf{F}| \Pr_D[f]$,

$$\begin{aligned}(\mu_D * \mu_E)(h) &= \sum_{g \in \mathbf{F}} \frac{\mu_D(h + g)\mu_E(g)}{|\mathbf{F}|} = |\mathbf{F}| \sum_{g \in \mathbf{F}} \Pr_{f \leftarrow \mathcal{D}}[f = h + g] \Pr_{g' \leftarrow \mathcal{E}}[g' = g] \\ &= |\mathbf{F}| \Pr_{f \leftarrow \mathcal{D}, g \leftarrow \mathcal{E}}[f + g = h].\end{aligned}\quad \square$$

3.2 Quantum oracle algorithms as functional

Recall the quantum oracle O_f for f computes $O_f : |x, y\rangle \rightarrow |x, y + f(x)\rangle$ coherently. For $a \in \{0, 1\}^n$, we define the state $|\hat{a}\rangle$ by

$$|\hat{a}\rangle := \frac{1}{\sqrt{2^n}} \sum_{z \in \{0, 1\}^n} \chi_a(z) |z\rangle = H^{\otimes n} |a\rangle, \quad (10)$$

then, it is immediate that

$$O_f |x, \hat{a}\rangle = (-1)^{\langle a, f(x) \rangle} |x, \hat{a}\rangle = \chi_a(f(x)) |x, \hat{a}\rangle \quad (11)$$

where χ_a is a character. This means that a single query increases the degree of the amplitudes by 1. The following theorem shows that this gives a polynomial-like representation of the success probability of the algorithm.

Theorem 3.4. Let f be a function from $\{0, 1\}^n$ to $\{0, 1\}^n$. Let $\mathcal{A}$ be a quantum oracle algorithm having access to O_f and outputting a bit $b \in \{0, 1\}$. Then, there exists a functional $P_{\mathcal{A}}$ (which may depend on the input of $\mathcal{A}$, if any) of Fourier degree $\leq 2q$ such that the probability that $\mathcal{A}$ outputs 1 equals to $P_{\mathcal{A}}(f)$. In other words, the functional $P_{\mathcal{A}}(f) := \Pr[\mathcal{A}^{O_f} \rightarrow 1]$ has the Fourier degree $\leq 2q$ and can be decomposed by

$$\Pr[\mathcal{A}^{O_f} \rightarrow 1] = P_{\mathcal{A}}(f) = \sum_{|\gamma| \leq 2q} \widehat{P}_{\mathcal{A}}(\gamma) \chi_\gamma(f).$$

In particular, $\|P_{\mathcal{A}}\|_2 \leq 1$.

We call the functional $P_{\mathcal{A}}$ above the *representing polynomial* of $\mathcal{A}$. The proof of this theorem is essentially the same as the proof used in the lower bounds by polynomials [5]. We defer the proof of this theorem to the end of this section.

We extensively use the following theorem derived from the above theorem.

Theorem 3.5. *Let $\mathcal{D}_D$ be a distribution of the functions in $\mathbf{F} = \{\{0,1\}^n \rightarrow \{0,1\}^n\}$. Let $\mathcal{A}$ be a binary output quantum algorithm making at most q quantum queries to the oracle. Let $P_{\mathcal{A}} = \Pr[\mathcal{A}^{O_f} \rightarrow 1]$ be the functional from Theorem 3.4. Then, it holds that*

$$\Pr_{f \leftarrow \mathcal{D}_D}[\mathcal{A}^{O_f} \rightarrow 1] - \Pr_{f \leftarrow \mathbf{F}}[\mathcal{A}^{O_f} \rightarrow 1] = \langle \mu_D - 1, P_{\mathcal{A}} \rangle = \langle (\mu_D - 1)^{\leq 2q}, P_{\mathcal{A}} \rangle$$

where $f \leftarrow \mathbf{F}$ denotes the uniform random sampling and $\mu_D(f)$ denotes the density function $\Pr[f \leftarrow \mathcal{D}_D]/(1/|\mathbf{F}|)$ of $\mathcal{D}_D$.

Proof. For the random function f sampled from $\mathcal{D}_D$, the averaged probability that $\mathcal{A}$ outputs 1 is

$$\begin{aligned} \Pr_{f \leftarrow \mathcal{D}_D}[\mathcal{A}^{O_f} \rightarrow 1] &= \sum_{f \in \mathbf{F}} \Pr[f \leftarrow \mathcal{D}_D] \Pr[\mathcal{A}^{O_f} \rightarrow 1] \\ &= \sum_{f \in \mathbf{F}} \frac{1}{|\mathbf{F}|} \frac{\Pr[f \leftarrow \mathcal{D}_D]}{1/|\mathbf{F}|} P_{\mathcal{A}}(f) = \mathbb{E}_{f \leftarrow \mathbf{F}}[\mu_D(f) P_{\mathcal{A}}(f)] = \langle \mu_D, P_{\mathcal{A}} \rangle \end{aligned}$$

where in the last equality we use the fact that μ_D is real-valued so $\mu_D = \overline{\mu_D}$. Noting that the density function of the uniform distribution is the constant function $\mathbf{1}$, we have

$$\Pr_{f \leftarrow \mathcal{D}_D}[\mathcal{A}^{O_f} \rightarrow 1] - \Pr_{f \leftarrow \mathbf{F}}[\mathcal{A}^{O_f} \rightarrow 1] = \langle \mu_D, P_{\mathcal{A}} \rangle - \langle \mathbf{1}, P_{\mathcal{A}} \rangle = \langle \mu_D - \mathbf{1}, P_{\mathcal{A}} \rangle.$$

The final equality holds because $P_{\mathcal{A}}$ is of Fourier degree $\leq 2q$ and Eq. (7). $\square$

The theorem immediately yields the following advantage bound.

Theorem 3.6. *Let $\mathcal{D}_{\mathbf{F}}$ be the uniform distribution over $\mathbf{F}$ and $\mathcal{D}_D$ be an arbitrary distribution over $\mathbf{F}$. For any q -query quantum algorithm $\mathcal{A}$, one has*

$$\text{Adv}^{\text{dist}}(\mathcal{D}_D, \mathcal{D}_{\mathbf{F}}; \mathcal{A}) = |\langle (\mu_D - 1)^{\leq 2q}, P_{\mathcal{A}} \rangle|.$$

By decomposing $\mu_D - \mathbf{1}$ into the degree- d components for $d \leq 2q$, we have

$$\langle (\mu_D - \mathbf{1})^{\leq 2q}, P_{\mathcal{A}} \rangle = \sum_{d=0}^{2q} \langle (\mu_D - \mathbf{1})^{\leq d}, P_{\mathcal{A}} \rangle = \sum_{d=1}^{2q} \langle \mu_D^{\leq d}, P_{\mathcal{A}} \rangle \quad (12)$$

because the constant function $\mathbf{1}$ has degree 0 and $\mu_D^{\leq 0} = \mathbb{E}_{f \leftarrow \mathbf{F}}[\mu_D(f)] \mathbf{1} = \mathbf{1}$. Therefore, this theorem reduces the PRF advantage for $f \leftarrow \mathcal{D}_D$ to analyze the low-degree components of μ_D .

We now prove Theorem 3.4.

Proof. We first show the following claim.

Claim 3.7. The final state of a q -query algorithm (with the deferred measurement) can be written by

$$\sum_z p_z^{(q)}(f) |z\rangle$$

where $p_z^{(q)}$ is a functional of degree $\leq q$.

Proof of Claim. Note that a q -query algorithm is represented by an alternating sequence of oracle query O_f and an oracle-independent unitary U . Applying unitary U , as a linear map, does not increase the Fourier degree. We only focus on the oracle queries.

Before proceeding, observe that for each query for the Fourier basis (Eq. (10)) it holds that

$$O_f(\chi_\gamma(f) |x, \hat{a}\rangle) = \chi_\gamma(f) \cdot \chi_a(f(x)) |x, \hat{a}\rangle = \chi_{\gamma+a\delta_x}(f) |x, \hat{a}\rangle$$

where $a\delta_x \in \hat{\mathbf{F}}$ is such that $a\delta_x(x) = a$ and $a\delta_x(y) = 0^n$ for $y \neq x$. We use Eq. (11) and Eq. (6) in the first and second equality. It holds that

$$|\gamma + a\delta_x| \leq |\gamma| + |a\delta_x| \leq |\gamma| + 1.$$

We use the mathematical induction to prove the claim. For the state before any query, $p_z^{(0)}$ is independent of f , thus the base step holds.

Next, consider the state before applying the k -th query $\sum_z p_z^{(k-1)}(f) |z\rangle$ for $k \leq q$. The Fourier degree of $p_z^{(k-1)}$ is bounded above by $k-1$ by the inductive hypothesis. Then, a single query increases the Fourier degree of each term in $p_z^{(k-1)}$ by at most 1, so that the degree after the query is bounded above by $(k-1) + 1 = k$. This proves the claim. $\square$

Write $|\phi_q\rangle = \sum_z p_z(f) |z\rangle$ to denote the final state of the algorithm where p_z is a functional of Fourier degree $\leq q$. Let $(\Pi_0, \Pi_1 = I - \Pi_0)$ be the final binary measurement of the algorithm. Then, the probability that $\mathcal{A}$ outputs 1 is

$$\begin{aligned} \Pr[\mathcal{A}^{O_f} \rightarrow 1] &= \langle \phi_q | \Pi_1 | \phi_q \rangle \\ &= \sum_{z,w} \langle z | \overline{p_z(f)} \Pi_1 p_w(f) | w \rangle \\ &= \sum_{z,w} \langle z | \Pi_1 | w \rangle \cdot \overline{p_z(f)} p_w(f) \end{aligned}$$

where $\deg(\overline{p_z} p_w) \leq \deg(\overline{p_z}) + \deg(p_w) \leq 2q$ because of Eq. (9). Since the summation does not increase the Fourier degree, $P_{\mathcal{A}}(f) = \Pr[\mathcal{A}^{O_f} \rightarrow 1]$ is a functional of Fourier degree $\leq 2q$.

The final “in particular” part is obvious because $|P_{\mathcal{A}}(f)| \leq 1$ for all f . $\square$

4 Quantum Security of XoP

This section introduces notation and states our main security theorem for XoP constructions. We first define the set of all permutations on n -bit strings by

$$\mathbf{P}_n = \{p \in \mathbf{F}_n : p \text{ is injective}\}.$$

In the following, we fix n , omit the subscript, and just denote $\mathbf{P}_n$ by $\mathbf{P}$. Recall that we defined the XOR of permutations

$$\text{XoP}[r] := P_1 + \dots + P_r$$

where $P_1, \dots, P_r \leftarrow \mathbf{P}$. We denote the distribution of $\text{XoP}[r]$ as $\mathcal{D}_{\text{XoP}[r]}$. In particular, $\mathcal{D}_{\text{XoP}} = \mathcal{D}_{\text{XoP}[2]}$.

We consider quantum-accessible $\text{XoP}[r]$ constructions in which a quantum adversary can make at most q quantum queries to a given $\text{XoP}[r]$ but has no access to the inner primitives P_r . We note that the asymptotic formula hides multiplicative factors depending on r , as r is typically chosen as a constant.

In this setting, the quantum security of XoP can be stated as follows:

Theorem 4.1 (Quantum security of XoP). *Let n, r, q be integers such that $n \geq 5$, $2 \leq r \leq 2^n/16$ and $0 \leq q \leq 2^n/57774$. Let $N = 2^n$. It holds that*

$$\text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{XoP}[r]}, \mathcal{D}_{\mathbf{F}}) = O\left(\min\left\{\frac{q^3}{N^r}, \frac{q^{3/2}}{N^{r-1/2}}, \frac{1}{N^{r-3/2}}\right\}\right).$$

We prove the last bound in Section 5, the first bound in Section 6, and the second bound in Section 7.

5 XoP Security for Many Quantum Queries

The goal of this section is to prove the following lemma. We assume that $n \geq 5, 2 \leq r \leq N/16$, and $q \leq N/57774$ hold in this section.

Lemma 5.1. *If $n \geq 5, r \leq \frac{N}{16}$, and $q \leq \frac{N}{57774}$, then*

$$\text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{XoP}[r]}, \mathcal{D}_{\mathbf{F}}) = O\left(\frac{1}{N^{r-1.5}}\right).$$

To prove the above lemma, we will use Fourier analysis explained in [Section 3](#). We denote the density function of $\text{XoP}[r]$ as $\mu_{\text{XoP}[r]}$. Then we can express the advantage of q -query quantum algorithm $\mathcal{A}$ attacking $\text{XoP}[r]$ by [Theorem 3.6](#) and [Equation \(12\)](#) as follows:

$$\text{Adv}^{\text{dist}}(\mathcal{D}_{\text{XoP}[r]}, \mathcal{D}_{\mathbf{F}}; \mathcal{A}) = |\langle (\mu_{\text{XoP}[r]} - 1)^{\leq 2q}, P_{\mathcal{A}} \rangle| \leq \sum_{d=1}^{2q} \left| \langle \mu_{\text{XoP}[r]}^{\overline{d}}, P_{\mathcal{A}}^{\overline{d}} \rangle \right|. \quad (13)$$

We bound the advantage using the Cauchy–Schwarz inequality as follows

$$\leq \sum_{d=1}^{2q} \|\mu_{\text{XoP}[r]}^{\overline{d}}\|_2 \cdot \|P_{\mathcal{A}}^{\overline{d}}\|_2 \leq \left(\sum_{d=1}^{2q} \|\mu_{\text{XoP}[r]}^{\overline{d}}\|_2^2 \right)^{\frac{1}{2}} \quad (14)$$

where we use $\sum_d \|P_{\mathcal{A}}^{\overline{d}}\|_2^2 \leq \|P_{\mathcal{A}}\|_2^2 \leq 1$ as shown in [Theorem 3.4](#).

The only remaining task is bounding the sum of $\mu_{\text{XoP}[r]}^{\overline{d}}$. The following lemma shows such upper bounds. We separately deal with $d \in \{1, 2, 3, 4, 6\}$, which will be used in the later section. The remainder of this section will be dedicated to prove this lemma.

Lemma 5.2. *For $r \geq 2$ and $N = 2^n \geq \max\{16r, 96\}$ and $5 \leq d_{\max} \leq N/28887$,*

- $\mu_{\text{XoP}[r]}^{\overline{1}} = \mathbf{0}$,
- $\|\mu_{\text{XoP}[r]}^{\overline{2}}\|_2^2 \leq 1/N^{2r-3}$,
- $\|\mu_{\text{XoP}[r]}^{\overline{3}}\|_2^2 \leq O(1/N^{4r-5})$,
- $\|\mu_{\text{XoP}[r]}^{\overline{4}}\|_2^2 \leq O(1/N^{4r-6})$,
- $\|\mu_{\text{XoP}[r]}^{\overline{6}}\|_2^2 \leq O(1/N^{6r-9})$, and
- $\|\mu_{\text{XoP}[r]}^{\overline{5}}\|_2^2 + \sum_{d=7}^{d_{\max}} \|\mu_{\text{XoP}[r]}^{\overline{d}}\|_2^2 \leq O(1/N^{6r-8})$.

In particular, all of the above terms are bounded above by $O(1/N^{2r-3})$.

Now we can give an upper bound of [Equation \(14\)](#) by plugging the last part of [Lemma 5.2](#) by decomposing the summand accordingly.

$$\left(\sum_{d=1}^{2q} \|\mu_{\text{XoP}[r]}^{\overline{d}}\|_2^2 \right)^{\frac{1}{2}} \leq \left(O\left(\frac{1}{N^{2r-3}}\right) \right)^{\frac{1}{2}} = O\left(\frac{1}{N^{r-1.5}}\right).$$

which directly proves [Lemma 5.1](#) as it is an upper bound of $\text{Adv}^{\text{dist}}(\mathcal{D}_{\text{XoP}[r]}, \mathcal{D}_{\mathbf{F}}; \mathcal{A})$.

5.1 Proofs for low degrees

We first observe that the density function of the distribution of $\text{XoP}[r]$ follows the convolution $\mu_{\mathbf{P}} * \dots * \mu_{\mathbf{P}}$ of r $\mu_{\mathbf{P}}$'s because of [Lemma 3.3](#). Then, by [Lemma 3.2](#), we have

$$\widehat{\mu}_{\text{XoP}[r]}(\gamma) = \widehat{\mu}_{\mathbf{P}}(\gamma)^r. \quad (15)$$

Therefore, our analysis boils down to analyze the Fourier coefficient $\widehat{\mu}_{\mathbf{P}}(\gamma)$ of uniformly random permutations. We will use the following formula. Here, recall $z_1, \dots, z_d \leftarrow (\{0, 1\}^n)^{(*d)}$ denotes the sampling without replacement, i.e., $z_i \neq z_j$ for $1 \leq i < j \leq d$.

Lemma 5.3. Suppose $|\gamma| = d$ with $\text{supp}(\gamma) = \{x_1, \dots, x_d\}$. Then

$$\widehat{\mu}_{\mathbf{P}}(\gamma) = \mathbb{E}_{z_1, \dots, z_d \leftarrow ((\{0,1\}^n)^{(*d)})} \left[\prod_{i=1}^d \chi_{\gamma(x_i)}(z_i) \right].$$

Proof. We expand $\widehat{\mu}_{\mathbf{P}}(\gamma)$ using the Fourier expansion formula in [Theorem 3.1](#) by

$$\widehat{\mu}_{\mathbf{P}}(\gamma) = \langle \chi_{\gamma}, \mu_{\mathbf{P}} \rangle = \mathbb{E}_{f \leftarrow \mathbf{F}} [\chi_{\gamma}(f) \mu_{\mathbf{P}}(f)] = \mathbb{E}_{p \leftarrow \mathbf{P}} [\chi_{\gamma}(p)]$$

where we use the property of density from [Eq. \(3\)](#) in the last equality. Using [Eq. \(5\)](#) and $\text{supp}(\gamma) = \{x_1, \dots, x_d\}$, we can compute this as follows

$$\mathbb{E}_{p \leftarrow \mathbf{P}} \left[\prod_{i=1}^d \chi_{\gamma(x_i)}(p(x_i)) \right] = \mathbb{E}_{z_1, \dots, z_d \leftarrow ((\{0,1\}^n)^{(*d)})} \left[\prod_{i=1}^d \chi_{\gamma(x_i)}(z_i) \right]$$

which completes the proof. $\square$

We also use the following identity occasionally, which can be easily seen by writing $\chi_y(z) = (-1)^{\langle y, z \rangle}$:

$$\sum_{z \in \{0,1\}^n} \chi_y(z) = N \llbracket y = 0^n \rrbracket, \quad \text{and} \quad \sum_{y \in \{0,1\}^n} \chi_y(z) = N \llbracket z = 0^n \rrbracket. \quad (16)$$

5.1.1 Degree-1 Component Vanishes

We first show that the degree-1 component becomes $\mathbf{0}$. Fix $\gamma \in \widehat{\mathbf{F}}$ with $|\gamma| = 1$, then there exists a unique x_1 such that $\gamma(x_1) = y_1 \neq 0^n$. Using [Lemma 5.3](#) and [Eq. \(16\)](#), we have

$$\widehat{\mu}_{\mathbf{P}}(\gamma) = \mathbb{E}_{z \leftarrow \{0,1\}^n} [\chi_{y_1}(z)] = 0.$$

This shows the degree-1 Fourier coefficient of $\widehat{\mu}_{\text{XoP}[r]}(\gamma) = \widehat{\mu}_{\mathbf{P}}(\gamma)^r$ is all zero, proving the first item of [Lemma 5.2](#).

5.1.2 Degree-2 Component

For $d = 2$, fix $\gamma \in \widehat{\mathbf{F}}$ with $\text{supp}(\gamma) = \{x_1, x_2\}$. Write $\gamma(x_1) = y_1 \neq 0^n, \gamma(x_2) = y_2 \neq 0^n$. [Lemma 5.3](#) gives

$$\begin{aligned} \widehat{\mu}_{\mathbf{P}}(\gamma) &= \mathbb{E}_{z_1, z_2 \leftarrow ((\{0,1\}^n)^{(*2)})} [\chi_{y_1}(z_1) \chi_{y_2}(z_2)] = \sum_{z_1 \neq z_2} \frac{\chi_{y_1}(z_1) \chi_{y_2}(z_2)}{N(N-1)} \\ &= \frac{\sum_{z_1, z_1} \chi_{y_1}(z_1) \chi_{y_2}(z_2)}{N(N-1)} - \frac{\sum_z \chi_{y_1}(z) \chi_{y_2}(z)}{N(N-1)} \end{aligned}$$

where we omit $z_1, z_2, z \in \{0,1\}^n$ in the last terms. By [Eq. \(16\)](#), the first term vanishes because $y_1, y_2 \neq 0^n$, and the second term is computed by

$$- \sum_{z \in \{0,1\}^n} \frac{\chi_{y_1}(z) \chi_{y_2}(z)}{N(N-1)} = - \sum_{z \in \{0,1\}^n} \frac{\chi_{y_1+y_2}(z)}{N(N-1)} = - \frac{\llbracket y_1 + y_2 = 0^n \rrbracket}{N-1} = - \frac{\llbracket y_1 = y_2 \rrbracket}{N-1}$$

where we use the bilinearity ([Eq. \(4\)](#)) and [Eq. \(16\)](#).

Consequently, the degree-2 component becomes

$$\mu_{\text{XoP}[r]}^{=2} = \sum_{|\gamma|=2} \widehat{\mu}_{\mathbf{P}}(\gamma)^r \chi_{\gamma} = \sum_{\text{supp}(\gamma)=\{x_1 < x_2\}} \frac{(-1)^r \llbracket y_1 = y_2 \rrbracket \chi_{\gamma}}{(N-1)^r} \quad (17)$$

where we use $\llbracket y_1 = y_2 \rrbracket^r = \llbracket y_1 = y_2 \rrbracket$. Consequently, the degree-2 weight is, by letting $y = y_1 (= \gamma(x_1)) = y_2 (= \gamma(x_2))$, computed as in [Eq. \(8\)](#) by

$$\begin{aligned} \|\mu_{\mathbf{XoP}[r]}^{\equiv 2}\|_2^2 &= \sum_{|\gamma|=2} |\hat{\mu}_{\mathbf{P}}(\gamma)|^{2r} = \sum_{x_1 < x_2} \sum_{y \neq 0^n} \frac{1}{(N-1)^{2r}} = \binom{N}{2} (N-1) \frac{1}{(N-1)^{2r}} \\ &= \frac{N}{2(N-1)^{2r-2}} \leq \frac{1}{2N^{2r-4}(N-2r+2)} \leq \frac{1}{N^{2r-3}} \end{aligned}$$

where the last inequalities use $N/2 \geq 2r-2$. This proves the second item of [Lemma 5.2](#).

5.1.3 Degree-3 Component

Fix $\gamma \in \hat{\mathbf{F}}$ with $\text{supp}(\gamma) = \{x_1, x_2, x_3\}$. Write $\gamma(x_i) = y_i \neq 0^n$ for $i = 1, 2, 3$. We first prove that

$$\hat{\mu}_{\mathbf{P}}(\gamma) = \frac{\llbracket y_1 + y_2 + y_3 = 0^n \rrbracket}{\binom{N-1}{2}}. \quad (18)$$

The proof of this equation uses some combinatorial argument using the inclusion-exclusion principle. The reader may skip the proof of this equation.

Proof of [Eq. \(18\)](#). By [Lemma 5.3](#), this can be written as

$$\begin{aligned} \hat{\mu}_{\mathbf{P}}(\gamma) &= \sum_{z_1, z_2, z_3 \text{ distinct}} \frac{\chi_{y_1}(z_1) \chi_{y_2}(z_2) \chi_{y_3}(z_3)}{(N)_3} \\ &= \sum_{z_1, z_2, z_3 \in \{0,1\}^n} \frac{\llbracket z_1, z_2, z_3 \text{ distinct} \rrbracket \chi_{y_1}(z_1) \chi_{y_2}(z_2) \chi_{y_3}(z_3)}{(N)_3}. \end{aligned}$$

For three variables z_1, z_2, z_3 , applying the inclusion-exclusion principle to the three events $E_{ij} = [z_i = z_j]$ gives

$$\llbracket z_1, z_2, z_3 \text{ distinct} \rrbracket = 1 - \sum_{i < j} \llbracket z_i = z_j \rrbracket + 2 \llbracket z_1 = z_2 = z_3 \rrbracket.$$

where the last term comes from

$$\llbracket E_{12} \cap E_{13} \rrbracket + \llbracket E_{12} \cap E_{23} \rrbracket + \llbracket E_{13} \cap E_{23} \rrbracket - \llbracket E_{12} \cap E_{13} \cap E_{23} \rrbracket,$$

all of which are the same event $[z_1 = z_2 = z_3]$.

Applying this identity to the summation over all z_1, z_2, z_3 , we have

$$\begin{aligned} \hat{\mu}_{\mathbf{P}}(\gamma) &= \sum_{z_1, z_2, z_3 \in \{0,1\}^n} \frac{\chi_{y_1}(z_1) \chi_{y_2}(z_2) \chi_{y_3}(z_3)}{(N)_3} \\ &\quad - \sum_{i < j} \sum_{z_1, z_2, z_3 \in \{0,1\}^n : z_i = z_j} \frac{\chi_{y_1}(z_1) \chi_{y_2}(z_2) \chi_{y_3}(z_3)}{(N)_3} \\ &\quad + 2 \sum_{z \in \{0,1\}^n} \frac{\chi_{y_1}(z) \chi_{y_2}(z) \chi_{y_3}(z)}{(N)_3}. \end{aligned}$$

This can be factored into

$$\begin{aligned}
&= \frac{(\sum_{z_1 \in \{0,1\}^n} \chi_{y_1}(z_1))(\sum_{z_2 \in \{0,1\}^n} \chi_{y_2}(z_2))(\sum_{z_3 \in \{0,1\}^n} \chi_{y_3}(z_3))}{(N)_3} \\
&- \sum_{1 \leq i < j \leq 3; k=6-i-j} \frac{(\sum_{z \in \{0,1\}^n} \chi_{y_i}(z) \chi_{y_j}(z))(\sum_{z_k \in \{0,1\}^n} \chi_{y_k}(z_k))}{(N)_3} \\
&+ 2 \sum_{z \in \{0,1\}^n} \frac{\chi_{y_1}(z) \chi_{y_2}(z) \chi_{y_3}(z)}{(N)_3}
\end{aligned}$$

where k is chosen so that $\{i, j, k\} = \{1, 2, 3\}$. The first and second terms become 0 by [Eq. \(16\)](#), because they have a factor $\sum_{z_w \in \{0,1\}^n} \chi_{y_w}(z_w) = 0$ for some w . Thus only the last term remains, proving

$$\begin{aligned}
\hat{\mu}_{\mathbf{P}}(\gamma) &= \sum_{z \in \{0,1\}^n} \frac{2\chi_{y_1}(z) \chi_{y_2}(z) \chi_{y_3}(z)}{(N)_3} = \sum_{z \in \{0,1\}^n} \frac{2\chi_{y_1+y_2+y_3}(z)}{(N)_3} \\
&= \frac{2N}{(N)_3} \llbracket y_1 + y_2 + y_3 = 0^n \rrbracket = \frac{\llbracket y_1 + y_2 + y_3 = 0^n \rrbracket}{\binom{N-1}{2}},
\end{aligned}$$

where we use [Eq. \(16\)](#) in the third equality.

Bounding the degree-3 component. Recall $\hat{\mu}_{\text{XoP}[r]}(\gamma) = \hat{\mu}_{\mathbf{P}}(\gamma)^r$ from [Eq. \(15\)](#). Therefore, the degree-3 weight is

$$\|\mu_{\text{XoP}[r]}^{\equiv 3}\|_2^2 = \sum_{|\gamma|=3} |\hat{\mu}_{\mathbf{P}}(\gamma)|^{2r} = \sum_{\substack{\text{supp}(\gamma) = \{x_1 < x_2 < x_3\} \\ \gamma(x_i) = y_i \neq 0^n}} \frac{\llbracket y_1 + y_2 + y_3 = 0^n \rrbracket}{\binom{N-1}{2}^{2r}}.$$

The last term is straightforward to calculate. The number of possible support is $\binom{N}{3}$, and the number of nonzero triples (y_1, y_2, y_3) such that $y_1 + y_2 + y_3 = 0^n$ is $(N-1)(N-2)$.⁵ Therefore,

$$\begin{aligned}
\|\mu_{\text{XoP}[r]}^{\equiv 3}\|_2^2 &= \binom{N}{3} (N-1)(N-2) \frac{1}{\binom{N-1}{2}^{2r}} = \frac{2^{2r-1}}{3N^{4r-5} (1 - \frac{1}{N})^{2r-2} (1 - \frac{2}{N})^{2r-2}} \\
&\leq \frac{2^{2r-1}}{3N^{4r-5} (1 - \frac{6r-6}{N})} \leq \frac{2^{2r}}{3N^{4r-5}} < \frac{2^{2r-1}}{N^{4r-5}}.
\end{aligned}$$

where we use $(1 - \frac{1}{N})^{2r-2} (1 - \frac{2}{N})^{2r-2} \geq 1 - \frac{6r-6}{N}$ in the first inequality. The last two inequalities follow from $N/2 \geq 6r-6$ and $3 > 2$. This concludes the proof of the third item of [Lemma 5.2](#).

5.1.4 Degree-4 Component

Fix $\gamma \in \hat{\mathbf{F}}$ with $\text{supp}(\gamma) = \{x_1, x_2, x_3, x_4\}$. Write $\gamma(x_i) = y_i \neq 0^n$ for $i = 1, 2, 3, 4$. We prove the following identity at the end of this section.

$$\hat{\mu}_{\mathbf{P}}(\gamma) = \frac{N C_{2,2}(\gamma) - 6 C_4(\gamma)}{(N-1)_3} \tag{19}$$

using the inclusion-exclusion principle similar to the proof of [Eq. \(18\)](#), where

$$\begin{aligned}
C_{2,2}(\gamma) &:= \llbracket y_1 = y_2 \rrbracket \llbracket y_3 = y_4 \rrbracket + \llbracket y_1 = y_3 \rrbracket \llbracket y_2 = y_4 \rrbracket + \llbracket y_1 = y_4 \rrbracket \llbracket y_2 = y_3 \rrbracket, \\
C_4(\gamma) &:= \llbracket y_1 + y_2 + y_3 + y_4 = 0^n \rrbracket.
\end{aligned}$$

⁵Choose $y_1 \neq 0^n$ and $y_2 \neq 0^n$, y_1, y_2 are nonzero, then y_3 is determined and nonzero.

In the main body, we derive the upper bound of the degree-4 component of the $\text{XoP}[r]$ using this formula. Observe that $0 \leq C_{2,2}(\gamma) \leq 3$ and $0 \leq C_4(\gamma) \leq 1$. This gives the upper bound of the maximal magnitude

$$M^{=4}[\mu_{\mathbf{P}}] = \max_{|\gamma|=4} |\hat{\mu}_{\mathbf{P}}(\gamma)| \leq \frac{3N}{(N-1)_3}.$$

Using $(a-b)^2 \leq a^2 + b^2$ for $a, b \geq 0$, we have

$$\begin{aligned} |\hat{\mu}_{\mathbf{P}}(\gamma)|^{2r} &\leq (M^{=4}[\mu_{\mathbf{P}}])^{2r-2} |\hat{\mu}_{\mathbf{P}}(\gamma)|^2 \\ &\leq \left(\frac{3N}{(N-1)_3} \right)^{2r-2} \frac{N^2 C_{2,2}(\gamma)^2 + 36 C_4(\gamma)}{((N-1)_3)^2}. \end{aligned} \quad (20)$$

Again, using $0 \leq C_{2,2}(\gamma) \leq 3$ and $0 \leq C_4(\gamma) \leq 1$, we can give upper bounds

$$\sum_{|\gamma|=4} C_{2,2}(\gamma)^2 \leq 3 \sum_{|\gamma|=4} C_{2,2}(\gamma) = 9 \binom{N}{4} (N-1)^2, \quad \sum_{|\gamma|=4} C_4(\gamma) \leq \binom{N}{4} (N-1)^3$$

where $\binom{N}{4}$ denotes the number of the support of γ , and $(N-1)^2$ and $(N-1)^3$ is the number of $y_1, y_2, y_3, y_4 \neq 0^n$ satisfying the constraints from $C_{2,2}(\gamma)$ and $C_4(\gamma)$, e.g., $\llbracket y_1 = y_2 \rrbracket \llbracket y_3 = y_4 \rrbracket$. Therefore, [Eq. \(20\)](#) is bounded above by

$$\left(\frac{3N}{(N-1)_3} \right)^{2r-2} \frac{\binom{N}{4} (9N^2(N-1)^2 + 36(N-1)^3)}{((N-1)_3)^2} \leq \frac{3^{2r-1}}{N^{4r-6}} \quad (21)$$

The detailed calculation is as follows:

$$\begin{aligned} &\left(\frac{3N}{(N-1)_3} \right)^{2r-2} \frac{\binom{N}{4} (9N^2(N-1)^2 + 36(N-1)^3)}{((N-1)_3)^2} \\ &= \frac{3^{2r}}{N^{4r-6}} \frac{\frac{1}{24} + \frac{N-1}{6N^2}}{\left(1 - \frac{1}{N}\right)^{2r-3} \left(1 - \frac{2}{N}\right)^{2r-1} \left(1 - \frac{3}{N}\right)^{2r-1}}. \end{aligned}$$

Observe that $\frac{1}{24} + \frac{N-1}{6N^2} \leq \frac{1}{12}$ for $N \geq 4$ and

$$\left(1 - \frac{1}{N}\right)^{2r-3} \left(1 - \frac{2}{N}\right)^{2r-1} \left(1 - \frac{3}{N}\right)^{2r-1} \geq 1 - \frac{12r-8}{N} \geq \frac{1}{4}$$

for $N \geq 16r$. This bounds the above term by

$$\leq \frac{3^{2r}}{N^{4r-6}} \cdot \frac{1/12}{1/4} = \frac{3^{2r-1}}{N^{4r-6}}$$

as desired. Hence

$$\|\mu_{\text{XoP}[r]}^{=4}\|_2^2 \leq \frac{3^{2r-1}}{N^{4r-6}}.$$

This concludes the proof of the fourth item of [Lemma 5.2](#).

Proof of [Eq. \(19\)](#). Fix $\gamma \in \hat{\mathbf{F}}$ with $\text{supp}(\gamma) = \{x_1, x_2, x_3, x_4\}$. Write $\gamma(x_i) = y_i \neq 0^n$ for $i \in [4]$. For convenience, we recall [Eq. \(19\)](#):

$$\hat{\mu}_{\mathbf{P}}(\gamma) = \frac{N C_{2,2}(\gamma) - 6 C_4(\gamma)}{(N-1)_3}.$$

By Lemma 5.3,

$$\widehat{\mu}_{\mathbf{P}}(\gamma) = \sum_{z_1, z_2, z_3, z_4 \text{ distinct}} \frac{\chi_{y_1}(z_1)\chi_{y_2}(z_2)\chi_{y_3}(z_3)\chi_{y_4}(z_4)}{(N)_4}. \quad (22)$$

For four variables z_1, z_2, z_3, z_4 , the inclusion-exclusion principle for the six events $E_{ij} = [z_i = z_j]$ gives, after simplification,

$$\begin{aligned} \llbracket z_1, z_2, z_3, z_4 \text{ distinct} \rrbracket &= 1 - \sum_{i < j} \llbracket z_i = z_j \rrbracket + 2 \sum_{i < j < k} \llbracket z_i = z_j = z_k \rrbracket \\ &+ \sum_{i < j, k < \ell, \{i, j, k, \ell\} = \{1, 2, 3, 4\}} \llbracket z_i = z_j \wedge z_k = z_\ell \rrbracket - 6 \llbracket z_1 = z_2 = z_3 = z_4 \rrbracket. \end{aligned}$$

Applying this to Eq. (22) over all z_1, z_2, z_3, z_4 , every term with a separated single vertex vanishes by Eq. (16). Hence only the last two terms remain:

$$\begin{aligned} \widehat{\mu}_{\mathbf{P}}(\gamma) &= \sum_{\substack{i < j, k < \ell \\ \{i, j, k, \ell\} = \{1, 2, 3, 4\}}} \sum_{z, w \in \{0, 1\}^n} \frac{\chi_{y_i + y_j}(z)\chi_{y_k + y_\ell}(w)}{(N)_4} - \sum_{z \in \{0, 1\}^n} \frac{6\chi_{y_1 + y_2 + y_3 + y_4}(z)}{(N)_4} \\ &= \sum_{\substack{i < j, k < \ell \\ \{i, j, k, \ell\} = \{1, 2, 3, 4\}}} \frac{N \llbracket y_i = y_j \rrbracket \llbracket y_k = y_\ell \rrbracket}{(N-1)_3} - \frac{6 \llbracket y_1 + y_2 + y_3 + y_4 = 0^n \rrbracket}{(N-1)_3} \\ &= \frac{NC_{2,2}(\gamma) - 6C_4(\gamma)}{(N-1)_3}, \end{aligned}$$

where we use Eq. (16) in the second equality. This proves Eq. (19).

5.2 Proofs for high degrees

We prove the high-degree upper bounds. The proof of the following two lemmas can be found in the next subsection.

Lemma 5.4. *For $1 \leq d \leq N$, it holds that $M^{=d}[\mu_{\mathbf{P}}] \leq (2d/N)^{\lceil d/2 \rceil}$.*

Lemma 5.5. *For $5 \leq d \leq N/16$, it holds that $\sum_{|\gamma|=d} |\widehat{\mu}_{\mathbf{P}}(\gamma)|^2 \leq 3^{3d} (N/d)^{\lfloor d/2 \rfloor}$.*

Now we extend the low-degree calculations to the higher-degree terms. We prove the following lemma.

Lemma 5.6. *For $r \geq 2$ and $5 \leq d_{\max} \leq N/28887$, it holds that $\|\mu_{\text{XoP}[r]}^{=6}\|_2^2 \leq 3^{18} 2^3 \left(\frac{12}{N}\right)^{6r-9}$ and*

$$\|\mu_{\text{XoP}[r]}^{=5}\|_2^2 + \sum_{d=7}^{d_{\max}} \|\mu_{\text{XoP}[r]}^{=d}\|_2^2 \leq 3^{22} 2^{11} \left(\frac{10}{N}\right)^{6r-8}, \quad \|\mu_{\text{XoP}[r]}^{=6}\|_2^2 = O\left(\frac{1}{N^{6r-9}}\right)$$

Proof. Lemmas 5.4 and 5.5 give, for every $5 \leq d \leq d_{\max}$,

$$\begin{aligned} \|\mu_{\text{XoP}[r]}^{=d}\|_2^2 &= \sum_{|\gamma|=d} |\widehat{\mu}_{\mathbf{P}}(\gamma)|^{2r} \\ &\leq (M^{=d}[\mu_{\mathbf{P}}])^{2r-2} \sum_{|\gamma|=d} |\widehat{\mu}_{\mathbf{P}}(\gamma)|^2 \\ &\leq \left(\frac{2d}{N}\right)^{(2r-2)\lceil d/2 \rceil} 3^{3d} \left(\frac{N}{d}\right)^{\lfloor d/2 \rfloor} \\ &= 3^{3d} 2^{(2r-2)\lceil d/2 \rceil} \left(\frac{d}{N}\right)^{(2r-1)\lceil d/2 \rceil - d} =: W_d, \end{aligned}$$

where we use the following in the last line

$$\left\lfloor \frac{d}{2} \right\rfloor + \left\lceil \frac{d}{2} \right\rceil = d.$$

Degree-6 is immediate by W_6 , in particular $N \geq 96$. We will prove

$$\frac{W_{d+2}}{W_d} \leq \frac{1}{2}$$

for every $5 \leq d \leq d_{\max} - 2$. Since $\lceil \frac{d+2}{2} \rceil = \lceil \frac{d}{2} \rceil + 1$, we have

$$\frac{W_{d+2}}{W_d} = 3^6 2^{2r-2} \left(1 + \frac{2}{d}\right)^{(2r-1)\lceil d/2 \rceil - d} \left(\frac{d+2}{N}\right)^{2r-3}.$$

For $d \geq 5$,

$$\left\lceil \frac{d}{2} \right\rceil \leq \frac{3d}{5},$$

and hence

$$(2r-1) \left\lceil \frac{d}{2} \right\rceil - d \leq \frac{6r-8}{5}d.$$

Using $1+x \leq e^x$, we obtain

$$\left(1 + \frac{2}{d}\right)^{(2r-1)\lceil d/2 \rceil - d} \leq \exp\left(\frac{2}{d} \left((2r-1) \left\lceil \frac{d}{2} \right\rceil - d\right)\right) \leq e^{(12r-16)/5}.$$

In addition, we observe that, for all $r \geq 2$,

$$3^6 2^{2r-2} e^{(12r-16)/5} < \frac{1}{2} \cdot 28887^{2r-3}.$$

Using the above,

$$\frac{W_{d+2}}{W_d} \leq 3^6 2^{2r-2} e^{(12r-16)/5} \left(\frac{d+2}{N}\right)^{2r-3} \leq \frac{1}{2} (28887)^{2r-3} \left(\frac{d_{\max}}{N}\right)^{2r-3} \leq \frac{1}{2}$$

Summing the odd and even degrees separately gives

$$\begin{aligned} \|\mu_{\text{XoP}[r]}^{\bar{5}}\|_2^2 + \sum_{d=7}^{d_{\max}} \|\mu_{\text{XoP}[r]}^{\bar{d}}\|_2^2 &\leq W_5 + \sum_{d=7}^{d_{\max}} W_d \\ &\leq \left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) (W_5 + W_8) = 2(W_5 + W_8). \end{aligned}$$

Moreover,

$$\frac{W_5}{W_8} = \frac{5^{6r-8}}{3^9 \cdot 2^{26r-38}} N^{2r-4} = \frac{5^4}{3^9 \cdot 2^{14}} \left(\frac{125N}{8192}\right)^{2r-4} \geq \frac{5^4}{3^9 \cdot 2^{14}}.$$

Consequently,

$$\begin{aligned} \|\mu_{\text{XoP}[r]}^{\bar{5}}\|_2^2 + \sum_{d=7}^{d_{\max}} \|\mu_{\text{XoP}[r]}^{\bar{d}}\|_2^2 &\leq 2 \cdot \left(1 + \frac{3^9 \cdot 2^{14}}{5^4}\right) W_5 \\ &\leq 2 \cdot \frac{3^9 \cdot 2^{14}}{3^2 \cdot 2^6} \cdot 3^{15} \cdot 2^{6r-6} \left(\frac{5}{N}\right)^{6r-8} = 3^{22} 2^{11} \left(\frac{10}{N}\right)^{6r-8}. \end{aligned}$$

□

5.3 Maximal Magnitude and Weight of the components of $\mu_{\mathbf{P}}$

5.3.1 Maximal magnitude of components

The goal of this section is to prove [Lemma 5.4](#), or more precisely

$$M^{=d}[\mu_{\mathbf{P}}] \leq \left(\frac{2d}{N}\right)^{\lceil d/2 \rceil}.$$

Let $\gamma \in \widehat{\mathbf{F}}$ be a character with $|\gamma| = d$ such that $\text{supp}(\gamma) = \{x_1 < \dots < x_d\}$. Write $\gamma(x_i) = y_i$ for $i \in [d]$. As shown in [Lemma 5.3](#), we can write

$$\widehat{\mu}_{\mathbf{P}}(\gamma) = \mathbb{E}_{(z_1, \dots, z_d) \leftarrow (\{0,1\}^n)^{(*d)}} \left[\prod_{i=1}^d \chi_{y_i}(z_i) \right].$$

We observe the following fact: The conditional distribution of z_d given the other elements $(z_1, \dots, z_{d-1})$ is uniform over the set $\{0,1\}^n \setminus \{z_1, \dots, z_{d-1}\}$, which has size $N - d + 1$. From this, we have

$$\begin{aligned} & \mathbb{E}_{z_d \leftarrow \{0,1\}^n \setminus \{z_1, \dots, z_{d-1}\}} [\chi_{y_d}(z_d)] \\ &= \frac{1}{N - d + 1} \sum_{z \notin \{z_1, \dots, z_{d-1}\}} \chi_{y_d}(z) \\ &= \frac{1}{N - d + 1} \left(\sum_{z \in \{0,1\}^n} \chi_{y_d}(z) - \sum_{i=1}^{d-1} \chi_{y_d}(z_i) \right) \\ &= -\frac{1}{N - d + 1} \sum_{i=1}^{d-1} \chi_{y_d}(z_i), \end{aligned}$$

where the last equality follows from $\sum_{z \in \{0,1\}^n} \chi_{y_d}(z) = 0$ because $y_d \neq 0^n$.

Using this equation, we have

$$\begin{aligned} \widehat{\mu}_{\mathbf{P}}(\gamma) &= \mathbb{E}_{(z_1, \dots, z_d) \leftarrow (\{0,1\}^n)^{(*d)}} \left[\chi_{y_d}(z_d) \prod_{j=1}^{d-1} \chi_{y_j}(z_j) \right] \\ &= \mathbb{E}_{(z_1, \dots, z_{d-1}) \leftarrow (\{0,1\}^n)^{*(d-1)}} \left[\mathbb{E}_{z_d \leftarrow \{0,1\}^n \setminus \{z_1, \dots, z_{d-1}\}} [\chi_{y_d}(z_d)] \prod_{j=1}^{d-1} \chi_{y_j}(z_j) \right] \\ &= -\frac{1}{N - d + 1} \sum_{i=1}^{d-1} \mathbb{E}_{(z_1, \dots, z_{d-1}) \leftarrow (\{0,1\}^n)^{*(d-1)}} \left[\chi_{y_d}(z_i) \prod_{j=1}^{d-1} \chi_{y_j}(z_j) \right] \\ &= -\frac{1}{N - d + 1} \sum_{i=1}^{d-1} \mathbb{E}_{(z_1, \dots, z_{d-1}) \leftarrow (\{0,1\}^n)^{*(d-1)}} \left[\chi_{y_i + y_d}(z_i) \prod_{\substack{j=1 \\ j \neq i}}^{d-1} \chi_{y_j}(z_j) \right]. \end{aligned}$$

To simplify the above expression, define $\gamma^{(i \leftarrow d)} \in \widehat{\mathbf{F}}$ by

$$\gamma^{(i \leftarrow d)}(x) := \begin{cases} y_i + y_d, & x = x_i, \\ y_j, & x = x_j \text{ for some } j \in [d-1] \setminus \{i\}, \\ 0^n, & \text{otherwise.} \end{cases}$$

If $y_i + y_d = 0^n$, then $\gamma^{(i \leftarrow d)}(x_i) = 0$ and therefore $\gamma^{(i \leftarrow d)}$ has degree $d - 2$. In other cases, $\gamma^{(i \leftarrow d)}$ has degree $d - 1$. This gives the following recursion.

Lemma 5.7. *Let $2 \leq d \leq N$, and let $\gamma \in \widehat{\mathbf{F}}$ satisfy $|\gamma| = d$. Then*

$$\widehat{\mu}_{\mathbf{P}}(\gamma) = -\frac{1}{N-d+1} \sum_{i=1}^{d-1} \widehat{\mu}_{\mathbf{P}}(\gamma^{(i \leftarrow d)}).$$

We are now ready to prove Lemma 5.4.

Proof of Lemma 5.4. It is immediate that $M^{=0}[\mu_{\mathbf{P}}] = 1$ and $M^{=1}[\mu_{\mathbf{P}}] = 0$. Now fix $2 \leq d \leq N$, and let $\gamma \in \widehat{\mathbf{F}}$ satisfy $|\gamma| = d$. By Lemma 5.7,

$$\widehat{\mu}_{\mathbf{P}}(\gamma) = -\frac{1}{N-d+1} \sum_{i=1}^{d-1} \widehat{\mu}_{\mathbf{P}}(\gamma^{(i \leftarrow d)}).$$

For each $i \in [d-1]$, the character $\gamma^{(i \leftarrow d)}$ has support size either $d-1$ or $d-2$. Therefore,

$$\left| \widehat{\mu}_{\mathbf{P}}(\gamma^{(i \leftarrow d)}) \right| \leq \max \left\{ M^{=(d-1)}[\mu_{\mathbf{P}}], M^{=(d-2)}[\mu_{\mathbf{P}}] \right\}.$$

Since the recursion holds for every degree- d character, taking absolute values gives

$$M^{=d}[\mu_{\mathbf{P}}] \leq \frac{d-1}{N-d+1} \max \left\{ M^{=(d-1)}[\mu_{\mathbf{P}}], M^{=(d-2)}[\mu_{\mathbf{P}}] \right\}. \quad (23)$$

We now prove the claimed bound by induction on $d \geq 2$. If $d > N/2$, the bound is immediate as $M^{=d}[\mu_{\mathbf{P}}] \leq 1 \leq (2d/N)^{\lceil d/2 \rceil}$. So let $2 \leq d \leq N/2$ and assume the claim for all smaller degrees. Since $2d/N \leq 1$ and $\lceil (d-1)/2 \rceil \geq \lceil (d-2)/2 \rceil$, the induction hypothesis gives

$$\begin{aligned} & \max \left\{ M^{=(d-1)}[\mu_{\mathbf{P}}], M^{=(d-2)}[\mu_{\mathbf{P}}] \right\} \\ & \leq \max \left\{ \left(\frac{2(d-1)}{N} \right)^{\lceil (d-1)/2 \rceil}, \left(\frac{2(d-2)}{N} \right)^{\lceil (d-2)/2 \rceil} \right\} \leq \left(\frac{2d}{N} \right)^{\lceil (d-2)/2 \rceil}. \end{aligned}$$

Moreover, $\frac{d-1}{N-d+1} \leq \frac{2d}{N}$ for $d \leq N/2$. Plugging both bounds into (23),

$$M^{=d}[\mu_{\mathbf{P}}] \leq \frac{2d}{N} \left(\frac{2d}{N} \right)^{\lceil (d-2)/2 \rceil} = \left(\frac{2d}{N} \right)^{\lceil d/2 \rceil},$$

this completes the induction and proves the lemma. $\square$

5.3.2 Weight of components

We prove that, for $5 \leq d \leq N/16$, it holds that

$$\sum_{|\gamma|=d} |\widehat{\mu}_{\mathbf{P}}(\gamma)|^2 \leq 3^{3d} \left(\frac{N}{d} \right)^{\lfloor d/2 \rfloor}.$$

Proof of Lemma 5.5. By Lemma 5.3, $\widehat{\mu}_{\mathbf{P}}(\gamma)$ depends only on the labels of γ , so for a support S of size d the quantity

$$B_d := \sum_{\text{supp}(\gamma)=S} |\widehat{\mu}_{\mathbf{P}}(\gamma)|^2$$

does not depend on S , and $\sum_{|\gamma|=d} |\widehat{\mu}_{\mathbf{P}}(\gamma)|^2 = \binom{N}{d} B_d$. We will show that

$$B_d = \sum_{j=0}^d (-1)^{d-j} \binom{d}{j} \frac{N^j}{(N)_j} \quad (24)$$

and

$$B_d \leq 2^{d+1} \left(\frac{8d}{N} \right)^{\lceil d/2 \rceil} \quad \text{for } 5 \leq d \leq N/16. \quad (25)$$

Given (25), the lemma follows from $\binom{N}{d} \leq (eN/d)^d$ and $d - \lceil d/2 \rceil = \lfloor d/2 \rfloor$:

$$\begin{aligned} \sum_{|\gamma|=d} |\widehat{\mu}_{\mathbf{P}}(\gamma)|^2 &= \binom{N}{d} B_d \leq 2^{d+1} \left(\frac{eN}{d} \right)^d \left(\frac{8d}{N} \right)^{\lceil d/2 \rceil} \\ &= 2^{d+1} 8^{\lceil d/2 \rceil} e^d \left(\frac{N}{d} \right)^{\lfloor d/2 \rfloor} \leq 3^{3d} \left(\frac{N}{d} \right)^{\lfloor d/2 \rfloor}, \end{aligned}$$

where the last inequality uses $2^{d+1} 8^{\lceil d/2 \rceil} \leq 8^d$ for $d \geq 5$ (equivalently, $d+1 \leq 3\lfloor d/2 \rfloor$) and $8e < 27$.

The identity Eq. (24). Fix $S = \{x_1, \dots, x_d\}$ and, for $y = (y_1, \dots, y_d) \in (\{0, 1\}^n)^d$, let $\gamma_y \in \widehat{\mathbf{F}}$ be the index with $\gamma_y(x_i) = y_i$ and $\gamma_y(x) = 0^n$ for $x \notin S$; thus $\text{supp}(\gamma_y) = \{x_i : y_i \neq 0^n\}$. Let ν be the uniform distribution on $(\{0, 1\}^n)^{*(d)}$, viewed as a probability mass function on $(\{0, 1\}^n)^d$. By (5.3) (which does not require the y_i to be nonzero),

$$\widehat{\mu}_{\mathbf{P}}(\gamma_y) = \sum_{z \in (\{0, 1\}^n)^d} \nu(z) \prod_{i=1}^d \chi_{y_i}(z_i) \quad \text{for all } y \in (\{0, 1\}^n)^d,$$

i.e., $(\widehat{\mu}_{\mathbf{P}}(\gamma_y))_y$ is N^d times the Fourier transform of ν on the group $(\{0, 1\}^n)^d$. Parseval's identity on $(\{0, 1\}^n)^d$ therefore gives

$$\sum_{y \in (\{0, 1\}^n)^d} |\widehat{\mu}_{\mathbf{P}}(\gamma_y)|^2 = N^{2d} \cdot \frac{1}{N^d} \sum_{z \in (\{0, 1\}^n)^d} \nu(z)^2 = N^d \cdot \frac{(N)_d}{(N)_d^2} = \frac{N^d}{(N)_d}.$$

On the other hand, if exactly the coordinates in $J \subseteq [d]$ of y are nonzero, then $\widehat{\mu}_{\mathbf{P}}(\gamma_y)$ is the Fourier coefficient of a degree- $|J|$ index, so grouping the y according to J yields $\sum_{y \in (\{0, 1\}^n)^d} |\widehat{\mu}_{\mathbf{P}}(\gamma_y)|^2 = \sum_{J \subseteq [d]} B_{|J|} = \sum_{j=0}^d \binom{d}{j} B_j$, with $B_0 := 1$. Hence $N^d/(N)_d = \sum_{j=0}^d \binom{d}{j} B_j$ for every $d \geq 0$, and binomial inversion gives Eq. (24).

The bound Eq. (25). The right-hand side of Eq. (24) resembles the binomial expansion of $(1-1)^d = 0$, and we exploit the resulting cancellations. Recall the elementary fact that

$$\sum_{j=0}^d (-1)^{d-j} \binom{d}{j} p(j) = 0 \quad \text{for every polynomial } p \text{ with } \deg(p) < d. \quad (26)$$

Write

$$\frac{N^j}{(N)_j} = \prod_{\ell=0}^{j-1} \frac{1}{1 - \ell/N} = u_j(1/N), \quad u_j(t) := \prod_{\ell=0}^{j-1} \frac{1}{1 - \ell t} = \sum_{k \geq 0} p_k(j) t^k,$$

where the last expression is the Taylor expansion of u_j at $t = 0$, which converges absolutely for $|t| < 1/(j-1)$, and in particular at $t = 1/N$ for all $j \leq d \leq N/16$. Comparing the coefficients of t^k in $u_{j+1}(t) = u_j(t)/(1 - jt) = u_j(t) \sum_{\ell \geq 0} j^\ell t^\ell$ gives

$$p_k(j+1) = \sum_{\ell=0}^k j^\ell p_{k-\ell}(j), \quad \text{i.e.,} \quad p_k(j+1) - p_k(j) = \sum_{\ell=1}^k j^\ell p_{k-\ell}(j),$$

with $p_0(j) = 1$ and $p_k(0) = 0$ for $k \geq 1$ (since $u_0 = 1$).

We claim that $j \mapsto p_k(j)$ is a polynomial of degree at most $2k$. This is clear for $k = 0$. If it holds for all $k' < k$, then each summand $j^\ell p_{k-\ell}(j)$ on the right-hand side above has degree at most $\ell + 2(k - \ell) \leq 2k - 1$, so the forward difference $p_k(j+1) - p_k(j)$ is a polynomial of degree at most $2k - 1$; since $p_k(j) = \sum_{i < j} (p_k(i+1) - p_k(i))$ and partial sums of a polynomial of degree at most $2k - 1$ form a polynomial of degree at most $2k$, the claim follows. Consequently, by [Eq. \(24\)](#) and [Eq. \(26\)](#), all terms with $2k < d$, i.e., with $k < \lceil d/2 \rceil$, cancel:

$$\begin{aligned} B_d &= \sum_{j=0}^d (-1)^{d-j} \binom{d}{j} \sum_{k \geq 0} p_k(j) N^{-k} \\ &= \sum_{k \geq 0} N^{-k} \sum_{j=0}^d (-1)^{d-j} \binom{d}{j} p_k(j) \\ &= \sum_{k \geq \lceil d/2 \rceil} N^{-k} \sum_{j=0}^d (-1)^{d-j} \binom{d}{j} p_k(j). \end{aligned}$$

It remains to bound $|p_k(j)|$ for $j \leq d$ and $k \geq \lceil d/2 \rceil$. For $j \geq 2$, expanding each factor of $u_j(t) = \prod_{\ell=1}^{j-1} (1 - \ell t)^{-1}$ as a geometric series shows that

$$p_k(j) = \sum_{\substack{s_1, \dots, s_{j-1} \geq 0 \\ s_1 + \dots + s_{j-1} = k}} \prod_{\ell=1}^{j-1} \ell^{s_\ell}$$

is a sum of $\binom{j+k-2}{k} \leq 2^{j+k-1}$ nonnegative terms, each at most j^k ; hence $0 \leq p_k(j) \leq j^k 2^{j+k-1}$, and this also holds for $j \in \{0, 1\}$ since $p_k(0) = p_k(1) = 0$ for $k \geq 1$. For $j \leq d \leq 2k$ we get

$$|p_k(j)| \leq d^k 2^{j+k-1} \leq d^k 2^{3k} = (8d)^k.$$

Therefore, using $\sum_j \binom{d}{j} = 2^d$ and $8d/N \leq 1/2$,

$$B_d \leq \sum_{k \geq \lceil d/2 \rceil} N^{-k} \sum_{j=0}^d \binom{d}{j} |p_k(j)| \leq 2^d \sum_{k \geq \lceil d/2 \rceil} \left(\frac{8d}{N} \right)^k \leq 2^{d+1} \left(\frac{8d}{N} \right)^{\lceil d/2 \rceil},$$

which is [Eq. \(25\)](#). □

6 Few Quantum Query Security via Planted Collisions

This section proves the following lemma.

Lemma 6.1. *If $n \geq 5$, $2 \leq r \leq \frac{N}{16}$, and $q \leq \frac{N}{57774}$, then*

$$\text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{XoP}[r]}, \mathcal{D}_{\mathbf{F}}) = O\left(\frac{q^3}{N^r}\right).$$

Recall that the query-independent ℓ_2 -norm bounds in [Lemma 5.2](#): For $d = 5$ and $7 \leq d \leq N/28887$, that lemma give $O(N^{-3r+4}) = O(N^{-r})$ upper bounds. We give the following alternative query-dependent bounds for $d = 2, 3, 4, 6$ in the subsections.

Lemma 6.2. *If $n \geq 5$, $2 \leq r \leq \frac{N}{16}$, and $q \leq \frac{N}{57774}$, then*

$$|\langle \mu_{\text{XoP}[r]}^{\overline{d}}, P_A \rangle| = O\left(\frac{q^3}{N^r}\right)$$

for $d = 2, 3, 4, 6$.

Proof of Lemma 6.1. Let $\mathcal{A}$ be a q -query algorithm. As shown in Eq. (13), Theorem 3.6 and Eq. (12) gives

$$\text{Adv}^{\text{dist}}(\mathcal{D}_{\text{XoP}[r]}, \mathcal{D}_{\mathbf{F}}; \mathcal{A}) \leq \sum_{d=1}^{2q} \langle \mu_{\text{XoP}[r]}^{\bar{d}}, P_{\mathcal{A}}^{\bar{d}} \rangle.$$

By decomposing the above term for $d = 2, 3, 4, 6$ and the others, we have the following upper bound

$$\left(\sum_{d=2,3,4,6} \langle \mu_{\text{XoP}[r]}^{\bar{d}}, P_{\mathcal{A}}^{\bar{d}} \rangle \right) + \sum_{d=5,7 \leq d \leq 2q} \|\mu_{\text{XoP}[r]}^{\bar{d}}\|_2 \|P_{\mathcal{A}}^{\bar{d}}\|_2$$

where the second term is bounded above by the Cauchy-Schwarz as in Eq. (14)

$$\left(\sum_{d=5,7 \leq d \leq 2q} \|\mu_{\text{XoP}[r]}^{\bar{d}}\|_2^2 \right)^{\frac{1}{2}} = O\left(\frac{1}{N^{3r-4}}\right) = O\left(\frac{1}{N^r}\right)$$

where we use the last inequality of Lemma 5.2 and $r \geq 2$. The remainder terms are bounded by $O(q^3/N^r)$ Lemma 6.2 for $d = 2, 3, 4, 6$, we have the overall upper bound $O(q^3/N^r)$. $\square$

6.1 Preparation: Distributions with planted constraints

We will use the indistinguishability of the small-range distributions [58].

Definition 6.3 (Small-range distributions). *For an integer $R \geq 1$, the distribution $\mathcal{S}_R$ over $\mathbf{F} = \mathbf{F}_n$ is sampled as follows:*

1. *sample a uniformly random function $f : \{0, 1\}^n \rightarrow [R]$ and let I be its image;*
2. *sample a uniformly random function $g : I \rightarrow \{0, 1\}^n$;*
3. *output $h := g \circ f$.*

Note that $\mathcal{S}_{\infty}$ is identical to the distributions of random functions. The following result is proven in [58].

Theorem 6.4. $\text{Adv}_q^{\text{dist}}(\mathcal{S}_R, \mathcal{S}_{\infty}) \leq \frac{27q^3}{R}$.

We use the several distributions of functions with some specific constraints. First one is the distribution $\mathcal{D}_{\text{PC}}$ of random functions with a planted collision, which is defined as follows:

$\mathcal{D}_{\text{PC}}$: Sample $x_1 \neq x_2$ from $\{0, 1\}^n$. Then, sample a uniform random $f \leftarrow \mathbf{F}$ such that $f(x_1) = f(x_2)$.

It is not hard to see that its density function is computed by

$$\mu_{\text{PC}}(f) = \binom{N}{2}^{-1} \sum_{\{x_1, x_2\}} N \mathbb{I}[f(x_1) = f(x_2)]. \quad (27)$$

We use the following observation.

Lemma 6.5. *Let $N \geq 4$ and $R \geq N^2$. For $h \leftarrow \mathcal{S}_R$ which is defined by $h = g \circ f$, let $C_f := |\{\{x, x'\} : x \neq x', f(x) = f(x')\}|$. Then*

$$\Pr[C_f = 1] \geq \frac{N^2}{8R}, \quad \Pr[C_f \geq 2] \leq \frac{N^4}{8R^2}.$$

Moreover, conditioned on $C_f = 0$, the distribution of h is identical to the uniform distribution $\mathcal{D}_{\mathbf{F}}$. Conditioned on $C_f = 1$, the distribution of h is $\mathcal{D}_{\text{PC}}$.

Proof. Observe that $\Pr[f(x) = f(x')] = 1/R$ for any $x \neq x'$, and any two distinct pairs (x, x') and (z, z') collide simultaneously with probability $1/R^2$, even when they share an input. Thus

$$\mathbb{E}[C_f] = \frac{\binom{N}{2}}{R}, \quad \mathbb{E}\left[\binom{C_f}{2}\right] = \frac{\binom{\binom{N}{2}}{2}}{R^2} \leq \frac{N^4}{8R^2}.$$

Using $\llbracket C \geq 2 \rrbracket \leq \binom{C}{2}$ and $\llbracket C = 1 \rrbracket \geq C - 2\binom{C}{2}$ for nonnegative integers C , we obtain

$$\Pr[C_f \geq 2] \leq \frac{N^4}{8R^2}, \quad \Pr[C_f = 1] \geq \frac{N(N-1)}{2R} - \frac{N^4}{4R^2} \geq \frac{N^2}{8R}.$$

where the last inequality uses $N \geq 4$ and $R \geq N^2$.

If $C_f = 0$, the values of h are independent and uniform because of g . If $C_f = 1$, the colliding pair of f is uniform by symmetry, thus the conditional distribution is exactly $\mathcal{D}_{\text{PC}}$. $\square$

Lemma 6.6. $\text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\mathbf{F}}) = O(q^3/N^2)$.

Proof. Fix a q -query algorithm $\mathcal{A}$. Recall $\langle \mu_{\mathcal{D}}, P_{\mathcal{A}} \rangle = \Pr_{h \leftarrow \mathcal{D}}[\mathcal{A}^h = 1]$ for any oracle distribution $\mathcal{D}$.

Let $r \geq N^2$ and choose $h \leftarrow \mathcal{S}_R$. Let p_0, p_1, p_2 be the probabilities of $C_f = 0$, $C_f = 1$, and $C_f \geq 2$, respectively, as defined in Lemma 6.5. By the same lemma, there exists a distribution $\mathcal{R}_R$ such that, writing μ_R and ρ_R for the densities of $\mathcal{S}_R$ and $\mathcal{R}_R$, respectively,

$$\mu_R = p_0 \cdot \mathbf{1} + p_1 \cdot \mu_{\text{PC}} + p_2 \cdot \rho_R, \quad p_1 \geq \frac{N^2}{8R}, \quad p_2 \leq \frac{N^4}{8R^2} \quad (28)$$

where $\mathbf{1}$ denotes the density function of $\mathcal{D}_{\mathbf{F}}$. Since $p_0 + p_1 + p_2 = 1$, we have

$$\mu_R - \mathbf{1} = p_1(\mu_{\text{PC}} - \mathbf{1}) + p_2(\rho_R - \mathbf{1}).$$

Taking inner products with $P_{\mathcal{A}}$ and applying the triangle inequality gives

$$p_1 |\langle \mu_{\text{PC}} - \mathbf{1}, P_{\mathcal{A}} \rangle| \leq |\langle \mu_R - \mathbf{1}, P_{\mathcal{A}} \rangle| + p_2 |\langle \rho_R - \mathbf{1}, P_{\mathcal{A}} \rangle| \leq \frac{27q^3}{R} + p_2$$

where we use Theorem 6.4 for the first term and $|\langle \rho_R - \mathbf{1}, P_{\mathcal{A}} \rangle| \leq 1$ for the second term. This proves

$$|\langle \mu_{\text{PC}} - \mathbf{1}, P_{\mathcal{A}} \rangle| \leq \frac{8R}{N^2} \left(\frac{27q^3}{R} + \frac{N^4}{8R^2} \right) = \frac{216q^3}{N^2} + \frac{N^2}{R}.$$

Taking R sufficiently large, we have the same bound $O(q^3/N^2)$ for all q -query algorithms $\mathcal{A}$. This completes the proof. $\square$

6.2 Degree-2 component as planted collision

We first prove Lemma 6.2 for $d = 2$.

Lemma 6.7. $|\langle \mu_{\text{XoP}[r]}^{-2}, P_{\mathcal{A}} \rangle| = O\left(\frac{q^3}{N^r}\right)$.

Proof. We start from the degree-2 component represented in Eq. (17). The equation shows that it suffices to consider the degree-2 $\gamma \in \widehat{\mathbf{F}}$ with the support $\{x_1 < x_2\}$ satisfying $\gamma(x_1) = \gamma(x_2)$. Letting $\gamma(x_1) = \gamma(x_2) = y$ and plugging f ,

$$\begin{aligned} \mu_{\text{XoP}[r]}^{-2}(f) &= \sum_{\text{supp}(\gamma) = \{x_1 < x_2\}} \frac{(-1)^r \llbracket \gamma(x_1) = \gamma(x_2) \rrbracket \chi_{\gamma}(f)}{(N-1)^r} \\ &= \sum_{x_1 < x_2; y \neq 0^n} \frac{(-1)^r}{(N-1)^r} \chi_y(f(x_1) + f(x_2)) \\ &= \sum_{x_1 < x_2} \frac{(-1)^r}{(N-1)^r} (N \cdot \llbracket f(x_1) = f(x_2) \rrbracket - \mathbf{1}) = \frac{(-1)^r \cdot N}{2(N-1)^{r-1}} (\mu_{\text{PC}}(f) - \mathbf{1}) \end{aligned}$$

where we use [Eq. \(16\)](#) in the third equality, and use [Eq. \(27\)](#) in the last equality. Therefore,

$$|\langle \mu_{\text{XoP}[r]}^2, P_A \rangle| = \frac{N}{2(N-1)^{r-1}} |\langle \mu_{\text{PC}}, P_A \rangle - \langle \mathbf{1}, P_A \rangle|.$$

The right hand side is the distinguishing advantage between the planted collision function and random functions up to the multiplicative factor $\frac{N}{2(N-1)^{r-1}}$. Plugging [Lemma 6.6](#) here gives the desired upper bound. $\square$

6.3 Degree-3 component as planted-three-collision

To bound the degree-3 component, we need to define $\mathcal{D}_{3\text{PC}}$ of random functions with a planted 3-collision, which is defined as follows:

$\mathcal{D}_{3\text{PC}}$: Sample three distinct x_1, x_2, x_3 from $\{0, 1\}^n$. Then, sample a uniform random $f \leftarrow \mathbf{F}$ such that $f(x_1) = f(x_2) = f(x_3)$.

Its density function is

$$\mu_{3\text{PC}}(f) = \frac{1}{(N)_3} \sum_{(x_1, x_2, x_3) \in (\{0, 1\}^n)^{*3}} N^2 \mathbb{I}[f(x_1) = f(x_2) = f(x_3)].$$

We prove the following lemma in [Appendix B](#).

Lemma 6.8. $\text{Adv}_q^{\text{dist}}(\mathcal{D}_{3\text{PC}}, \mathcal{D}_{\mathbf{F}}) = O(q^2/N)$.

We actually prove the following stronger bound than $O(q^3/N^r)$.

Lemma 6.9. $|\langle \mu_{\text{XoP}[r]}^3, P_A \rangle| = O\left(\frac{q^2}{N^r}\right)$.

Proof. For $\text{supp}(\gamma) = \{x_1 < x_2 < x_3\}$, write $y_i = \gamma(x_i)$. Recall

$$\mu_{\text{XoP}[r]}(\gamma) = \hat{\mu}_{\mathbf{P}}(\gamma)^r = \frac{\mathbb{I}[y_1 + y_2 + y_3 = 0^n]}{\binom{N-1}{2}^r}.$$

Expanding the degree-3 component with plugging f becomes

$$\begin{aligned} \binom{N-1}{2}^r \mu_{\text{XoP}[r]}^3(f) &= \sum_{\text{supp}(\gamma) = \{x_1 < x_2 < x_3\}} \mathbb{I}[y_1 + y_2 + y_3 = 0^n] \chi_{\gamma}(f) \\ &= \sum_{\substack{x_1 < x_2 < x_3 \\ y_1 \neq 0^n, y_2 \neq 0^n, y_1 \neq y_2}} \chi_{y_1}(f(x_1)) \chi_{y_2}(f(x_2)) \chi_{y_1+y_2}(f(x_3)) \\ &= \sum_{\substack{x_1 < x_2 < x_3 \\ y_1 \neq 0^n, y_2 \neq 0^n, y_1 \neq y_2}} \chi_{y_1}(f(x_1) + f(x_3)) \chi_{y_2}(f(x_2) + f(x_3)). \end{aligned}$$

For each x_1, x_2, x_3 , observe that

$$\begin{aligned} &\sum_{y_1 \neq 0^n, y_2 \neq 0^n, y_1 \neq y_2} \chi_{y_1}(f(x_1) + f(x_3)) \chi_{y_2}(f(x_2) + f(x_3)) \\ &= \sum_{y_1 \neq 0^n, y_2 \neq 0^n} \chi_{y_1}(f(x_1) + f(x_3)) \chi_{y_2}(f(x_2) + f(x_3)) - \sum_{y \neq 0} \chi_y(f(x_1) + f(x_2)) \\ &= (N \mathbb{I}[f(x_1) = f(x_3)] - \mathbf{1})(N \mathbb{I}[f(x_2) = f(x_3)] - \mathbf{1}) - (N \mathbb{I}[f(x_1) = f(x_2)] - \mathbf{1}) \end{aligned}$$

where we use [Eq. \(16\)](#) in the last equality. Noting that $\llbracket f(x_1) = f(x_3) \rrbracket \llbracket f(x_2) = f(x_3) \rrbracket = \llbracket f(x_1) = f(x_2) = f(x_3) \rrbracket$, the overall sum becomes

$$\begin{aligned} & \sum_{x_1 < x_2 < x_3} \left(N^2 \llbracket f(x_1) = f(x_2) = f(x_3) \rrbracket \right. \\ & \quad \left. - N \llbracket f(x_1) = f(x_2) \rrbracket - N \llbracket f(x_1) = f(x_3) \rrbracket - N \llbracket f(x_2) = f(x_3) \rrbracket + 2 \cdot \mathbf{1} \right) \\ & = \binom{N}{3} ((\mu_{3\text{PC}}(f) - \mathbf{1}) - 3(\mu_{\text{PC}}(f) - \mathbf{1})). \end{aligned}$$

Hence, $|\langle \mu_{\text{XoP}[r]}^{\equiv 3}, P_{\mathcal{A}} \rangle|$ can be decomposed into a linear sum of the distinguishing advantage of the planted 3-collision and the planted collision functions from random functions up to the multiplicative factor $\binom{N}{3} / \binom{N-1}{2}^r$. This gives

$$|\langle \mu_{\text{XoP}[r]}^{\equiv 3}, P_{\mathcal{A}} \rangle| \leq O\left(\frac{2^r}{N^{2r-3}}\right) \cdot \left(O\left(\frac{q^2}{N}\right) + O\left(\frac{q^3}{N^2}\right)\right) = O\left(\frac{q^2}{N^r}\right)$$

where we omit the factor regarding r and use $q \leq N$ and [Lemmas 6.6](#) and [6.8](#). $\square$

6.4 Degree-4 component as planted two collisions plus small terms

We define the distributions of random functions with multiple planted collisions to bound the degree-4 component. For $k \in \mathbb{N}$, they are defined as follows.

$\mathcal{D}_{\text{PC},k}$: Sample a tuple $(x_1, \dots, x_{2k}) \leftarrow (\{0,1\}^n)^{*(2k)}$ of distinct inputs. Then sample a uniform random $f \leftarrow \mathbf{F}$ such that $f(x_{2j-1}) = f(x_{2j})$ for all $j \in [k]$.

$\mathcal{D}_{4\text{X}}$: Sample four distinct $x_1, \dots, x_4$ from $\{0,1\}^n$. Then, sample a uniform random $f \leftarrow \mathbf{F}$ such that $f(x_1) + f(x_2) + f(x_3) + f(x_4) = 0^n$.

The density functions of these distributions can be computed as follows

$$\begin{aligned} \mu_{\text{PC},k}(f) &= \frac{1}{(N)_{2k}} \sum_{(x_1, \dots, x_{2k}) \in (\{0,1\}^n)^{*(2k)}} N^k \prod_{j=1}^k \llbracket f(x_{2j-1}) = f(x_{2j}) \rrbracket, \\ \mu_{4\text{X}}(f) &= \frac{1}{(N)_4} \sum_{(x_1, \dots, x_4) \in (\{0,1\}^n)^{*4}} N \llbracket f(x_1) + f(x_2) + f(x_3) + f(x_4) = 0^n \rrbracket. \end{aligned}$$

Note that $\mathcal{D}_{\text{PC}} = \mathcal{D}_{\text{PC},1}$ and $\mathcal{D}_{\text{PC},0} = \mathcal{D}_{\mathbf{F}}$. Similarly to the previous distributions, we prove the following two lemmas in [Appendix B](#).

Lemma 6.10. $\text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{PC},k}, \mathcal{D}_{\mathbf{F}}) = O(q^3/N^2)$ for $k = 2, 3$.

Lemma 6.11. $\text{Adv}_q^{\text{dist}}(\mathcal{D}_{4\text{X}}, \mathcal{D}_{\mathbf{F}}) = O(q^3/N^2)$.

We prove the following lemma in this subsection using the above lemmas.

Lemma 6.12. $|\langle \mu_{\text{XoP}[r]}^{\equiv 4}, P_{\mathcal{A}} \rangle| = O\left(\frac{q^3}{N^r}\right)$.

Proof. Let γ be such that $|\gamma| = 4$. For $\text{supp}(\gamma) = \{x_1 < x_2 < x_3 < x_4\}$, write $y_i = \gamma(x_i)$. We begin with the degree-4 Fourier component from [Eq. \(19\)](#)

$$\hat{\mu}_{\mathbf{P}}(\gamma) = \frac{NC_{2,2}(\gamma) - 6C_4(\gamma)}{(N-1)_3}$$

where we recall the following for convenience.

$$\begin{aligned} C_{2,2}(\gamma) &= \llbracket y_1 = y_2 \rrbracket \llbracket y_3 = y_4 \rrbracket + \llbracket y_1 = y_3 \rrbracket \llbracket y_2 = y_4 \rrbracket + \llbracket y_1 = y_4 \rrbracket \llbracket y_2 = y_3 \rrbracket, \\ C_4(\gamma) &= \llbracket y_1 + y_2 + y_3 + y_4 = 0^n \rrbracket. \end{aligned}$$

We write X, Y, Z to denote $\llbracket y_1 = y_2 \rrbracket \llbracket y_3 = y_4 \rrbracket$, $\llbracket y_1 = y_3 \rrbracket \llbracket y_2 = y_4 \rrbracket$, and $\llbracket y_1 = y_4 \rrbracket \llbracket y_2 = y_3 \rrbracket$, respectively, so that $C_{2,2}(\gamma) = X + Y + Z$. Observe the following.

1. $X^2 = X, Y^2 = Y, Z^2 = Z$ and $C_4^2 = C_4$ as they are in $\{0, 1\}$,
2. $XY = YZ = ZX = \llbracket y_1 = y_2 = y_3 = y_4 \rrbracket =: E(\gamma)$,
3. $C_{2,2}(\gamma) \geq 1$ implies $C_4(\gamma) = 1$, thus $C_{2,2}(\gamma)C_4(\gamma) = C_{2,2}(\gamma)$,
4. similarly $C_{2,2}E = 3E$ and $C_4E = E$.

From this, we have $C_{2,2}^k = C_{2,2} + (3^k - 3)E$ inductively for $k \in \mathbb{N}$. Further calculation based on the above gives the following identity

$$\hat{\mu}_{\mathbf{P}}(\gamma)^r = \left(\frac{NC_{2,2}(\gamma) - 6C_4(\gamma)}{(N-1)_3} \right)^r = \frac{a_r C_{2,2}(\gamma) + b_r E(\gamma) + c_r C_4(\gamma)}{(N-1)_3^r}$$

where $a_r = (N-6)^r - (-6)^r$, $b_r = (3N-6)^r - 3(N-6)^r + 2(-6)^r$, $c_r = (-6)^r$.

Now we compute $\mu_{\mathbf{XOP}[r]}^{\bar{4}}(f)$. Observe that $C_{2,2} = X + Y + Z$ terms can be computed as follows, where $8 = 4!/3$ comes from the order of x_1, x_2, x_3, x_4 ($4!$) and the symmetry of X, Y, Z (3),

$$\begin{aligned} \sum_{|\gamma|=4} C_{2,2}(\gamma) \chi_\gamma(f) &= \frac{1}{8} \sum_{\text{supp}(\gamma)=\{x_1, x_2, x_3, x_4\}} \llbracket y_1 = y_2 \rrbracket \llbracket y_3 = y_4 \rrbracket \chi_\gamma(f) \\ &= \frac{1}{8} \sum_{\substack{\text{supp}(\gamma)=\{x_1, x_2, x_3, x_4\} \\ y_1 \neq 0^n, y_3 \neq 0^n}} \chi_{y_1}(f(x_1) + f(x_2)) \chi_{y_3}(f(x_3) + f(x_4)) \\ &= \frac{1}{8} \sum_{\substack{x_1, x_2, x_3, x_4 \\ \text{distinct}}} (N \llbracket f(x_1) = f(x_2) \rrbracket - 1)(N \llbracket f(x_3) = f(x_4) \rrbracket - 1) \\ &= \frac{(N)_4}{8} ((\mu_{\mathbf{PC},2}(f) - 1) - 2(\mu_{\mathbf{PC}}(f) - 1)). \end{aligned}$$

Here, the last term can be interpreted as a linear sum of distinguishing advantage between random functions with planted collision(s) and uniformly random functions. [Lemmas 6.6](#) and [6.10](#) gives the bound $\left| \langle \sum_{|\gamma|=4} C_{2,2}(\gamma) \chi_\gamma, P_{\mathcal{A}} \rangle \right| = O(q^3 N^2)$.

For the E term, we have

$$\begin{aligned} \sum_{|\gamma|=4} E(\gamma) \chi_\gamma(f) &= \sum_{\text{supp}(\gamma)=\{x_1, x_2, x_3, x_4\}} \llbracket y_1 = y_2 = y_3 = y_4 \rrbracket \chi_\gamma(f) \\ &= \sum_{\substack{\text{supp}(\gamma)=\{x_1, x_2, x_3, x_4\} \\ y \neq 0^n}} \chi_y(f(x_1) + f(x_2) + f(x_3) + f(x_4)) = \frac{(N)_4}{24} (\mu_{4\mathbf{X}}(f) - 1), \end{aligned}$$

which gives $\left| \langle \sum_{|\gamma|=4} E(\gamma) \chi_\gamma, P_{\mathcal{A}} \rangle \right| = O(q^3 N^2)$ because of [Lemma 6.11](#).

For the last term with C_4 , we can directly bound

$$\left| \langle \sum_{|\gamma|=4} C_4(\gamma) \chi_\gamma, P_{\mathcal{A}} \rangle \right| \leq \left\| \sum_{|\gamma|=4} C_4(\gamma) \chi_\gamma \right\|_2 = O(N^4).$$

Plugging three bounds on the expansion of $\langle \mu_{\text{XoP}[r]}^{\bar{4}}, P_{\mathcal{A}} \rangle$ gives

$$|\langle \mu_{\text{XoP}[r]}^{\bar{4}}, P_{\mathcal{A}} \rangle| = O\left(\frac{N^r \cdot q^3 N^2 + N^r \cdot q^3 N^2 + N^4}{N^{3r}}\right) = O\left(\frac{q^3}{N^{2r-2}}\right)$$

which is $O(q^3/N^r)$ because $r \geq 2$, as desired. $\square$

6.5 Degree-6 component as planted three collisions plus small terms

We use the following lemma.

Lemma 6.13. For $x, y \in \mathbb{R}$, $|(x+y)^r - x^r| \leq r|y|(|x| + |y|)^{r-1}$.

Proof. Noting that $\binom{r}{k} \leq k \binom{r}{k-1} = r \binom{r-1}{k-1}$ for $1 \leq k \leq r$, we have

$$|(x+y)^r - x^r| \leq \sum_{k=1}^r \binom{r}{k} |x^{r-k} y^k| \leq r|y| \sum_{k=1}^r \binom{r-1}{k-1} |x|^{r-k} |y|^{k-1}$$

which equals to $r|y|(|x| + |y|)^{r-1}$. $\square$

Lemma 6.14. $|\langle \mu_{\text{XoP}[r]}^{\bar{6}}, P_{\mathcal{A}} \rangle| = O\left(\frac{q^3}{N^r}\right)$.

Proof. We need to compute $\hat{\mu}_{\mathbf{P}}$ first. Let us define $Z_{2,2,2}, Z_{2,4}, Z_{3,3}, Z_6$ by

$$\begin{aligned} Z_{2,2,2} &:= \sum_{M \text{ perfect matching of } [6]} \prod_{\{i,j\} \in M} \llbracket z_i = z_j \rrbracket, \\ Z_{2,4} &:= \sum_{\substack{\{i,j\} \subset [6] \\ \{i,j\} \cap \{g,h,k,\ell\} = \emptyset}} \llbracket z_i = z_j \rrbracket \llbracket z_g = z_h = z_k = z_\ell \rrbracket, \\ Z_{3,3} &:= \sum_{\substack{1 \in \{i,j,k\} \subset [6] \\ \{i,j,k\} \cap \{g,h,\ell\} = \emptyset}} \llbracket z_i = z_j = z_k \rrbracket \llbracket z_g = z_h = z_\ell \rrbracket, \\ Z_6 &:= \llbracket z_1 = z_2 = z_3 = z_4 = z_5 = z_6 \rrbracket. \end{aligned}$$

By the inclusion-exclusion principle for the fifteen events $E_{ij} = [z_i = z_j]$ gives,

$$\llbracket z_1, \dots, z_6 \text{ distinct} \rrbracket = 1 - \dots - Z_{2,2,2} + 6Z_{2,4} + 4Z_{3,3} - 120Z_6,$$

where the omitted terms correspond to partitions containing at least one singleton block, which will be vanished.

Similarly, we define $C_{2,2,2}, C_{2,4}, C_{3,3}, C_6$ by

$$\begin{aligned} C_{2,2,2}(\gamma) &:= \sum_{M \text{ perfect matching of } [6]} \prod_{\{i,j\} \in M} \llbracket y_i = y_j \rrbracket, \\ C_{2,4}(\gamma) &:= \sum_{\substack{\{i,j\} \subset [6] \\ \{i,j\} \cap \{g,h,k,\ell\} = \emptyset}} \llbracket y_i = y_j \rrbracket \llbracket y_g + y_h + y_k + y_\ell = 0^n \rrbracket, \\ C_{3,3}(\gamma) &:= \sum_{\substack{1 \in \{i,j,k\} \subset [6] \\ \{i,j,k\} \cap \{g,h,\ell\} = \emptyset}} \llbracket y_i + y_j + y_k = 0^n \rrbracket \llbracket y_g + y_h + y_\ell = 0^n \rrbracket, \\ C_6(\gamma) &:= \llbracket y_1 + y_2 + y_3 + y_4 + y_5 + y_6 = 0^n \rrbracket. \end{aligned}$$

By applying Eq. (16) and simplifying, we obtain

$$\widehat{\mu}_{\mathbf{P}}(\gamma) = \frac{-N^2 C_{2,2,2}(\gamma) + 6NC_{2,4}(\gamma) + 4NC_{3,3}(\gamma) - 120C_6(\gamma)}{(N-1)_5}.$$

set $R(\gamma) = 6NC_{2,4}(\gamma) + 4NC_{3,3}(\gamma) - 120C_6(\gamma)$. Note that $R(\gamma) = O(N)$. We rewrite

$$\begin{aligned} (\widehat{\mu}_{\mathbf{P}}(\gamma)(N-1)_5 \chi_\gamma)^r &= (-N^2 C_{2,2,2}(\gamma) + R(\gamma))^r \chi_\gamma \\ &= S(\gamma) \chi_\gamma + (-N^2)^r C_{2,2,2}(\gamma) \chi_\gamma, \end{aligned}$$

where $S(\gamma) = (-N^2 C_{2,2,2}(\gamma) + R(\gamma))^r - (-N^2)^r C_{2,2,2}(\gamma)$. For the second term, we have

$$\begin{aligned} &\sum_{\text{supp}(\gamma)=\{x_1 < \dots < x_6\}} C_{2,2,2}(\gamma) \chi_\gamma(f) \\ &= \frac{15}{6!} \sum_{\text{supp}(\gamma)=\{x_1, \dots, x_6\}} \llbracket y_1 = y_2 \rrbracket \llbracket y_3 = y_4 \rrbracket \llbracket y_5 = y_6 \rrbracket(\gamma) \chi_\gamma(f) \\ &= \frac{1}{48} \sum_{\substack{x_1, \dots, x_6 \\ \text{distinct}}} \prod_{s=1}^3 (N \llbracket f(x_{2s-1}) = f(x_{2s}) \rrbracket - 1) \\ &= \frac{(N)_6}{48} (\mu_{\text{PC},3} - 3\mu_{\text{PC},2} + 3\mu_{\text{PC}} - 1) \\ &= \frac{(N)_6}{48} ((\mu_{\text{PC},3} - 1) - 3(\mu_{\text{PC},2} - 1) + 3(\mu_{\text{PC}} - 1)). \end{aligned}$$

This will be routinely bounded using Lemmas 6.6 and 6.10 below.

Now let us bound $S(\gamma)$. Partition the degree-six characters into

$$\begin{aligned} \Gamma_0 &:= \{\gamma : C_{2,2,2}(\gamma) = 0\}, \\ \Gamma_1 &:= \{\gamma : C_{2,2,2}(\gamma) = 1\}, \\ \Gamma_{\geq 2} &:= \{\gamma : C_{2,2,2}(\gamma) \geq 2\}. \end{aligned}$$

For $J \in \{0, 1, \geq 2\}$, let $B_J := \sum_{\gamma \in \Gamma_J} S(\gamma) \chi_\gamma$. Then we have

$$\left| \left\langle \sum_{|\gamma|=6} S(\gamma) \chi_\gamma, P_{\mathcal{A}} \right\rangle \right| \leq |\langle B_0, P_{\mathcal{A}} \rangle| + |\langle B_1, P_{\mathcal{A}} \rangle| + |\langle B_{\geq 2}, P_{\mathcal{A}} \rangle|$$

and using Cauchy-Schwarz inequality

$$|\langle B_J, P_{\mathcal{A}} \rangle| \leq \|B_J\|_2 \|P_{\mathcal{A}}\|_2 \leq \|B_J\|_2 \leq \left(\sum_{\gamma \in \Gamma_J} |S(\gamma)|^2 \right)^{1/2}.$$

If $\gamma \in \Gamma_0$, then $S(\gamma) = R(\gamma)^r = O(N^r)$.

$$\begin{aligned} |\langle B_0, P_{\mathcal{A}} \rangle| &\leq \left(\sum_{\substack{|\gamma|=6 \\ C_{2,2,2}(\gamma)=0}} |S(\gamma)|^2 \right)^{1/2} \\ &\leq (O(N^{12}) O(N^{2r}))^{1/2} = O(N^{r+6}). \end{aligned}$$

If $\gamma \in \Gamma_1$, we apply [Lemma 6.13](#), which gives

$$\begin{aligned} |S(\gamma)| &= |(-N^2 C_{2,2,2}(\gamma) + R(\gamma))^r - (-N^2)^r C_{2,2,2}(\gamma)| \\ &= |(-N^2 + R(\gamma))^r - (-N^2)^r| = O(N^{2r-1}). \end{aligned}$$

Since $C_{2,2,2}(\gamma) = 1$, we have at most $O(N^3)$ choices of labels per support. Hence,

$$\begin{aligned} |\langle B_1, P_A \rangle| &\leq \left(\sum_{\substack{|\gamma|=6 \\ C_{2,2,2}(\gamma)=1}} |S(\gamma)|^2 \right)^{1/2} \\ &\leq \left(O(N^{3+6}) O(N^{(2r-1) \cdot 2}) \right)^{1/2} = O(N^{2r+3.5}). \end{aligned}$$

If $\gamma \in \Gamma_{\geq 2}$, then

$$\begin{aligned} |S(\gamma)| &= |(-N^2 C_{2,2,2}(\gamma) + R(\gamma))^r - (-N^2)^r C_{2,2,2}(\gamma)| \\ &= |O(N^2)^r - (-N^2)^r O(1)| = O(N^{2r}). \end{aligned}$$

Since $C_{2,2,2}(\gamma) \geq 2$, there exist indices i, j and g, h, k, l such that $y_i = y_j$ and $y_g = y_h = y_k = y_l$. Hence, we have at most $O(N^2)$ choices of labels per support. Hence,

$$\begin{aligned} |\langle B_{\geq 2}, P_A \rangle| &\leq \left(\sum_{\substack{|\gamma|=6 \\ C_{2,2,2}(\gamma) \geq 2}} |S(\gamma)|^2 \right)^{1/2} \\ &\leq (O(N^{2+6}) O(N^{2r \cdot 2}))^{1/2} = O(N^{2r+4}) \end{aligned}$$

Finally,

$$\begin{aligned} |\langle \mu_{\text{XoP}[r]}^{\leq 6}, P_A \rangle| &\leq \frac{N^{2r} \left| \langle \sum_{|\gamma|=6} C_{2,2,2}(\gamma) \chi_\gamma, P_A \rangle \right| + \sum_{J \in \{0,1,\geq 2\}} |\langle B_J, P_A \rangle|}{(N-1)_5^r} \\ &\leq \frac{O(q^3 N^{2r+4}) + O(N^{r+6}) + O(N^{2r+3.5}) + O(N^{2r+4})}{\Theta(N^{5r})} \\ &= O\left(\frac{q^3}{N^{3r-4}}\right) + O\left(\frac{1}{N^{4r-6}}\right) + O\left(\frac{1}{N^{3r-3.5}}\right) + O\left(\frac{1}{N^{3r-4}}\right) \\ &= O\left(\frac{q^3}{N^r}\right). \end{aligned}$$

This concludes the proof. □

7 Middle Quantum Query Security via Improved Small-range Indistinguishability

In this section, we prove the following theorem. As in [Theorem 4.1](#), the asymptotic notation may hide a constant depending on r .

Lemma 7.1. *If $n \geq 5, r \leq \frac{N}{16}$, and $q \leq \frac{N}{57774}$, then*

$$\text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{XoP}[r]}, \mathcal{D}_{\mathbf{F}}) = O\left(\frac{q^{3/2}}{N^{r-1/2}}\right).$$

The main result of this section is the following bound for the planted collision pseudorandomness. Compared to q^3/N^2 bound in [Lemma 6.6](#), the following lemma gives a better bound for $q^3 \geq N$.

Lemma 7.2. *Let $N = 2^n \geq 2$. For every integer $q \geq 0$, it holds that $\text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\text{F}}) = O(q^{3/2}/N^{3/2})$.*

This lemma can be used to give an alternative bound for the small-range indistinguishability [\[58\]](#) for the large-range regime. This improves the bound in [Theorem 6.4](#) when $q^3 \gg N$ and R is sufficiently large, or more precisely for $q^3 \gg N$ and $R \gg N^4/q^3$.

Corollary 7.3. *Let $N = 2^n \geq 4$, $q \geq 1$, and $R \geq N^2$ be integers. Then*

$$\text{Adv}_q^{\text{dist}}(\mathcal{S}_R, \mathcal{S}_\infty) = O\left(\frac{q^{3/2}\sqrt{N}}{R} + \frac{N^4}{R^2}\right).$$

In particular, if $R \geq N^{7/2}/q^{3/2}$, then $\text{Adv}_q^{\text{dist}}(\mathcal{S}_R, \mathcal{S}_\infty) = O\left(\frac{q^{3/2}\sqrt{N}}{R}\right)$.

Proof. We use the fact from the proof of [Lemma 6.6](#) that the acceptance probability of the small-range distribution can be decomposed into the random functions and the random functions with a planted collision as in [Eq. \(28\)](#). Using [Lemma 6.5](#), the coefficient $\Pr[C_f = 1]$ of the planted collision part satisfies $\Pr[C_f = 1] \leq \mathbb{E}[C_f] = \binom{N}{2}/R$. By [Lemma 7.2](#), we have

$$\text{Adv}_q^{\text{dist}}(\mathcal{S}_R, \mathcal{S}_\infty) \leq \frac{\binom{N}{2}}{R} \text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\text{F}}) + \frac{N^4}{8R^2} = O\left(\frac{q^{3/2}\sqrt{N}}{R} + \frac{N^4}{R^2}\right).$$

The last claim follows from $N^4/R^2 \leq q^{3/2}\sqrt{N}/R$ when $R \geq N^{7/2}/q^{3/2}$. $\square$

We prove the main result. The remainder of this section is devoted to prove the above lemma.

Proof of Lemma 7.1. If $q \leq N^{1/3}$, then [Lemma 6.1](#) proves the desired result. We therefore assume $q \geq N^{1/3}$. Fix a q -query algorithm $\mathcal{A}$. Recall from the proof of [Lemma 6.7](#) that

$$\mu_{\text{XoP}[r]}^{\overline{2}} = \frac{(-1)^r N}{2(N-1)^{r-1}} (\mu_{\text{PC}} - \mathbf{1}).$$

Applying [Lemma 7.2](#), we have

$$\left| \langle \mu_{\text{XoP}[r]}^{\overline{2}}, P_{\mathcal{A}} \rangle \right| \leq \frac{N}{2(N-1)^{r-1}} \text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\text{F}}) = O\left(\frac{q^{3/2}}{N^{r-1/2}}\right).$$

For the remaining components, [Lemma 5.2](#) with $d_{\max} = 2q$ gives

$$\sum_{d=3}^{2q} \|\mu_{\text{XoP}[r]}^{\overline{d}}\|_2^2 = O\left(\frac{1}{N^{4r-5}} + \frac{1}{N^{4r-6}} + \frac{1}{N^{6r-9}} + \frac{1}{N^{6r-8}}\right) = O\left(\frac{1}{N^{4r-6}}\right).$$

The conditions of that lemma follow from $q \geq N^{1/3}$, $q \leq N/57774$, and $N \geq 16r$. Since $\|P_{\mathcal{A}}\|_2 \leq 1$, the Cauchy-Schwarz inequality bounds the contribution of these components by

$$\left| \sum_{d=3}^{2q} \langle \mu_{\text{XoP}[r]}^{\overline{d}}, P_{\mathcal{A}}^{\overline{d}} \rangle \right| \leq \left(\sum_{d=3}^{2q} \|\mu_{\text{XoP}[r]}^{\overline{d}}\|_2^2 \right)^{1/2} = O\left(\frac{1}{N^{2r-3}}\right).$$

Finally, $r \geq 2$ and $q \geq N^{1/3}$ imply

$$\frac{1}{N^{2r-3}} \leq \frac{1}{N^{r-1}} \leq \frac{q^{3/2}}{N^{r-1/2}}.$$

Combining the above bounds with $\mu_{\text{XoP}[r]}^{\overline{1}} = \mathbf{0}$ and [Theorem 3.6](#) proves the theorem. $\square$

7.1 Planted collisions in the compressed oracle

Fix a q -query algorithm $\mathcal{A}$. By Eq. (27), we immediately have

$$\langle \mu_{\text{PC}} - \mathbf{1}, P_{\mathcal{A}} \rangle = \frac{2}{N-1} \mathbb{E}_{f \leftarrow \mathbf{F}} \left[P_{\mathcal{A}}(f) \sum_{x < y} \left(\mathbb{I}[f(x) = f(y)] - \frac{1}{N} \right) \right]. \quad (29)$$

We express the expectation on the right-hand side using the compressed oracle [57]. We follow the formalization of [22].

The compressed oracle. We briefly explain the compressed oracle for random functions, which is perfectly indistinguishable from a quantum random oracle. The database consists of one register for each input x , with basis $\{|\perp\rangle\} \cup \{|v\rangle : v \in \{0,1\}^n\}$. Write $|+\rangle = N^{-1/2} \sum_{v \in \{0,1\}^n} |v\rangle$, and let the compression operator **Comp** be the unitary that swaps $|\perp\rangle$ and $|+\rangle$ while fixing their orthogonal complement. For the compressed representation of v , we use the notation

$$|\widehat{v}\rangle := \text{Comp} |v\rangle = |v\rangle - \frac{|+\rangle}{\sqrt{N}} + \frac{|\perp\rangle}{\sqrt{N}}.$$

The vectors $\{|\widehat{v}\rangle\}_v$ are orthonormal. Their span is the orthogonal complement of $|+\rangle$ in the database register. Throughout the execution, each database register remains supported on this span. For $f \in \mathbf{F}$, write $|\widehat{f}\rangle := \bigotimes_x |\widehat{f(x)}\rangle$. The empty database and a compressed query O satisfy

$$|\emptyset\rangle = |\perp\rangle^{\otimes N} = N^{-N/2} \sum_{f \in \mathbf{F}} |\widehat{f}\rangle, \quad O |x, y\rangle |\widehat{f}\rangle = |x, y + f(x)\rangle |\widehat{f}\rangle.$$

A compressed query applies **Comp** to the database register indexed by the query input, performs the usual quantum random oracle query, and applies **Comp** again. In particular, $O^\dagger = O$, and a query on input x acts only on database register x .

Define the collision operators

$$\text{Col}_{xy} := \sum_v (|\widehat{v}\rangle\langle\widehat{v}|)_x \otimes (|\widehat{v}\rangle\langle\widehat{v}|)_y, \quad \Delta\text{Col} := \sum_{x < y} \left(\text{Col}_{xy} - \frac{1}{N} I \right). \quad (30)$$

They satisfy the following equations; see the similarity between the second equation and Eq. (29):

$$\text{Col}_{xy} |\widehat{f}\rangle = \mathbb{I}[f(x) = f(y)] |\widehat{f}\rangle, \quad \Delta\text{Col} |\widehat{f}\rangle = \sum_{x < y} \left(\mathbb{I}[f(x) = f(y)] - \frac{1}{N} \right) |\widehat{f}\rangle.$$

Let $|\psi_q^f\rangle$ be the final state of the purified algorithm $\mathcal{A}$ with oracle f . Let $\Pi_{\mathcal{A}} = |1\rangle\langle 1|_Z \otimes I_{\text{rest}}$ be its acceptance projector on the output qubit Z , so $P_{\mathcal{A}}(f) = \langle \psi_q^f | \Pi_{\mathcal{A}} | \psi_q^f \rangle$. On the joint algorithm–database space, write $\Pi = \Pi_{\mathcal{A}} \otimes I_{\text{db}}$. The final state of the compressed execution is

$$|\Psi_q\rangle = N^{-N/2} \sum_{f \in \mathbf{F}} |\psi_q^f\rangle |\widehat{f}\rangle.$$

Expanding its acceptance expectation and using the orthogonality of $\{|\widehat{f}\rangle\}_f$, we obtain

$$\begin{aligned} \langle \Psi_q | \Pi \Delta\text{Col} | \Psi_q \rangle &= \frac{1}{N^N} \sum_{f, g \in \mathbf{F}} \langle \psi_q^g | \Pi_{\mathcal{A}} | \psi_q^f \rangle \langle \widehat{g} | \Delta\text{Col} | \widehat{f} \rangle \\ &= \mathbb{E}_{f \leftarrow \mathbf{F}} \left[P_{\mathcal{A}}(f) \sum_{x < y} \left(\mathbb{I}[f(x) = f(y)] - \frac{1}{N} \right) \right] \\ &= \frac{N-1}{2} \langle \mu_{\text{PC}} - \mathbf{1}, P_{\mathcal{A}} \rangle. \end{aligned} \quad (31)$$

Thus, it suffices to bound the left-hand side by $O(q^{3/2}/\sqrt{N})$ to prove Lemma 7.2.

7.2 The number of collisions in the database

For a database $D \in (\{0, 1\}^n \cup \{\perp\})^{\{0, 1\}^n}$, define the two diagonal operators

$$\begin{aligned} D_{\text{cnt}} |D\rangle &:= |\{x : D(x) \neq \perp\}| |D\rangle, \\ \text{Col}_{\text{cnt}} |D\rangle &:= \sum_{x < y} \llbracket D(x) = D(y) \neq \perp \rrbracket |D\rangle. \end{aligned}$$

These count the queried inputs and collision pairs in the database, respectively. We prove the following bound in [Appendix C](#); the second bound is not tight but sufficient for our purpose.

Lemma 7.4. *Let $|\Xi_t\rangle$ be the final state over the algorithm and database registers outputted by some algorithm after making $t \leq N$ queries to the compressed oracle O . Then*

$$\langle \Xi_t | D_{\text{cnt}} | \Xi_t \rangle \leq t, \quad \langle \Xi_t | \text{Col}_{\text{cnt}} | \Xi_t \rangle \leq 129t.$$

Write the compressed execution of $\mathcal{A}$ as

$$W = U_q O U_{q-1} \cdots U_1 O U_0, \quad |\Psi_q\rangle = W |\Omega\rangle,$$

where $|\Omega\rangle = |0\rangle |\emptyset\rangle$ is the initial algorithm state and the U_i are oracle-independent unitaries acting only on the algorithm registers. On each database register, define

$$Q := I - |\perp\rangle\langle\perp|.$$

Observe the following identities

$$Q_x Q_y \text{Col}_{xy} |\emptyset\rangle = \left(\text{Col}_{xy} - \frac{1}{N} I \right) |\emptyset\rangle, \quad \text{Col}_{xy} Q_x Q_y |\emptyset\rangle = 0$$

followed by expanding $\text{Col}_{xy} |\perp, \perp\rangle = N^{-1} \sum_v |\hat{v}, \hat{v}\rangle$. Define, using the commutator $[A, B] = AB - BA$,

$$T := \sum_{x < y} [Q_x Q_y, \text{Col}_{xy}], \quad R := \Delta \text{Col} - T \tag{32}$$

that acts on the database registers. The two identities above gives

$$T |\emptyset\rangle = \sum_{x < y} (Q_x Q_y \text{Col}_{xy} |\emptyset\rangle - \text{Col}_{xy} Q_x Q_y |\emptyset\rangle) = \sum_{x < y} \left(\text{Col}_{xy} - \frac{1}{N} I \right) |\emptyset\rangle = \Delta \text{Col} |\emptyset\rangle.$$

Since $R = \Delta \text{Col} - T$ acts only on the database registers, we also have $R |\Omega\rangle = 0$. Using $RW = WR + [R, W]$, we therefore obtain

$$\begin{aligned} RW |\Omega\rangle &= WR |\Omega\rangle + [R, W] |\Omega\rangle = [R, W] |\Omega\rangle \\ &= \sum_{j=1}^q (U_q O \cdots O U_j) [R, O] (U_{j-1} O \cdots O U_0) |\Omega\rangle. \end{aligned} \tag{33}$$

The last equality uses $[R, U_i] = 0$ and the product rule for commutators. The first and last products are interpreted as U_q when $j = q$ and U_0 when $j = 1$, respectively.

We further observe that $[R, O] = -[T, O]$. The query O preserves each database state $|\hat{f}\rangle$, while Col_{xy} acts on it by multiplication by $\llbracket f(x) = f(y) \rrbracket$. This gives

$$\text{Col}_{xy} O |z, w\rangle |\hat{f}\rangle = \llbracket f(x) = f(y) \rrbracket |z, w + f(z)\rangle |\hat{f}\rangle = O \text{Col}_{xy} |z, w\rangle |\hat{f}\rangle.$$

Thus $[\text{Col}_{xy}, O] = 0$ for every $x < y$, and hence $[\Delta\text{Col}, O] = 0$. Since $R = \Delta\text{Col} - T$, it follows that

$$[R, O] = [\Delta\text{Col}, O] - [T, O] = -[T, O].$$

Define the states immediately before a query and the corresponding backward states by

$$|\Psi_j^-\rangle := U_{j-1}O \cdots OU_0|\Omega\rangle, \quad |\Phi_j\rangle := U_j^\dagger O \cdots OU_q^\dagger \Pi |\Psi_q\rangle.$$

Note also that $T^\dagger = -T$ and $[\Pi, T] = 0$ because T acts on the database while Π acts on the algorithm's register. This shows that the expectation of ΠT is purely imaginary. Therefore,

$$\langle \Psi_q | \Pi \Delta\text{Col} | \Psi_q \rangle = \text{Re} \langle \Psi_q | \Pi R | \Psi_q \rangle.$$

Combining the preceding identities gives

$$\begin{aligned} \langle \Psi_q | \Pi \Delta\text{Col} | \Psi_q \rangle &= \text{Re} \langle \Psi_q | \Pi R W | \Omega \rangle = \text{Re} \langle \Psi_q | \Pi [R, W] | \Omega \rangle \\ &= \sum_{j=1}^q \text{Re} \langle \Phi_j | [R, O] | \Psi_j^- \rangle \\ &= - \sum_{j=1}^q \text{Re} \langle \Phi_j | [T, O] | \Psi_j^- \rangle \end{aligned} \tag{34}$$

7.3 Proof of the planted-collision bound

Proof of Lemma 7.2. The cases $q = 0$ and $q > N/2$ are immediate. We assume $1 \leq q \leq N/2$.

Define

$$B_x := |\perp\rangle\langle\perp|_x \sum_{y \neq x} Q_y \text{Col}_{xy}, \quad B := \sum_x |x\rangle\langle x| \otimes B_x,$$

where the first register in B is the query input register. For a fixed query input x , we have

$$[Q_x Q_y, \text{Col}_{xy}] = [Q_y, \text{Col}_{xy}] - |\perp\rangle\langle\perp|_x Q_y \text{Col}_{xy} + \text{Col}_{xy} Q_y |\perp\rangle\langle\perp|_x.$$

The first term commutes with the query. The last two terms, summed over $y \neq x$, give $-B_x + B_x^\dagger$. All terms not involving x also commute with the query. Hence

$$[T, O] = OB - BO + B^\dagger O - OB^\dagger. \tag{35}$$

We show in [Appendix C](#) that every joint algorithm-database state $|\Xi\rangle$ whose database registers are supported on $\text{span}\{|\hat{f}\rangle : f \in \mathbf{F}\}$ satisfies

$$\|B^\dagger |\Xi\rangle\|^2 \leq \frac{4}{N} \langle \Xi | (\text{D}_{\text{cnt}} + \text{Col}_{\text{cnt}}) | \Xi \rangle. \tag{36}$$

Each of the four vectors $|\Phi_j\rangle, O|\Phi_j\rangle, |\Psi_j^-\rangle, O|\Psi_j^-\rangle$ has norm at most one. Recall the states $|\Psi_j^-\rangle$ and $O|\Psi_j^-\rangle$ are obtained after $j-1$ and j queries to O , respectively.

To apply [Lemma 7.4](#) to $|\Phi_j\rangle$, consider an algorithm that runs W , copies its output bit to an auxiliary qubit using a CNOT gate, and then applies $U_j^\dagger O \cdots OU_q^\dagger$ to the original registers. The component of the resulting state in which the auxiliary qubit is 1 is precisely $|\Phi_j\rangle$. This algorithm makes $2q-j$ queries, since $O^\dagger = O$. One additional query gives the component $O|\Phi_j\rangle$ and uses $2q-j+1 \leq 2q$ queries in total. Both count operators are positive and act only on the database registers, so their expectations in either component are at most their expectations in the corresponding full state. Thus, since $2q \leq N$, [Lemma 7.4](#) gives

$$\langle \Xi | \text{D}_{\text{cnt}} | \Xi \rangle \leq 2q, \quad \langle \Xi | \text{Col}_{\text{cnt}} | \Xi \rangle \leq 258q$$

for each of the four vectors $|\Xi\rangle$ above. Applying Eq. (36), we obtain

$$\|B^\dagger |\Xi\rangle\|^2 \leq \frac{4}{N}(2q + 258q) = \frac{1040q}{N}.$$

By the Cauchy-Schwarz inequality, each of the four terms in Eq. (35), between $\langle\Phi_j|$ and $|\Psi_j^-\rangle$, has absolute value at most $\sqrt{1040q/N}$. For example,

$$|\langle\Phi_j|OB|\Psi_j^-\rangle| \leq \|B^\dagger O|\Phi_j\rangle\| \| |\Psi_j^-\rangle \| \leq \sqrt{\frac{1040q}{N}}.$$

It follows that

$$|\langle\Phi_j|[T,O]|\Psi_j^-\rangle| \leq 4\sqrt{\frac{1040q}{N}}.$$

Using Eq. (34), we obtain

$$|\langle\Psi_q|\Pi\Delta\text{Col}|\Psi_q\rangle| \leq \sum_{j=1}^q |\langle\Phi_j|[T,O]|\Psi_j^-\rangle| \leq 4q\sqrt{\frac{1040q}{N}} = 16\sqrt{65} \frac{q^{3/2}}{\sqrt{N}}.$$

Finally, Eq. (31) concludes the proof of the lemma. $\square$

References

- [1] Advanced Encryption Standard (AES). National Institute of Standards and Technology, NIST FIPS PUB 197, U.S. Department of Commerce, November 2001. 3
- [2] Akshima, Tyler Besselman, Kai-Min Chung, Siyao Guo, and Tzu-Yi Yang. Tight quantum time-space tradeoffs for permutation inversion. In Joan Daemen and Emmanuel Thomé, editors, *Advances in Cryptology - EUROCRYPT 2026 - 45th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Rome, Italy, May 10-14, 2026, Proceedings, Part I*, volume 16541 of *Lecture Notes in Computer Science*, pages 431–456. Springer, 2026. 3, 4
- [3] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantum-access-secure message authentication via blind-unforgeability. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 788–817. Springer, Cham, May 2020. 3
- [4] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 208–236. Springer, Cham, August 2022. 3
- [5] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald De Wolf. Quantum lower bounds by polynomials. *Journal of the ACM (JACM)*, 48(4):778–797, 2001. 4, 13, 45
- [6] Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible. In Kaisa Nyberg, editor, *EUROCRYPT’98*, volume 1403 of *LNCS*, pages 266–280. Springer, Berlin, Heidelberg, May / June 1998. 3
- [7] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523, 1997. 4, 9
- [8] Daniel J. Bernstein. Stronger security bounds for Wegman-Carter-Shoup authenticators. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 164–180. Springer, Berlin, Heidelberg, May 2005. 3

- [9] Srimanta Bhattacharya and Mridul Nandi. Full indifferentiable security of the xor of two or more random permutations using the χ^2 method. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 387–412. Springer, Cham, April / May 2018. [3](#)
- [10] Srimanta Bhattacharya and Mridul Nandi. Luby-Rackoff backwards with more users and more security. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part III*, volume 13092 of *LNCS*, pages 345–375. Springer, Cham, December 2021. [3](#)
- [11] Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 592–608. Springer, Berlin, Heidelberg, May 2013. [3](#)
- [12] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 361–379. Springer, Berlin, Heidelberg, August 2013. [3](#)
- [13] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, 46(4-5):493–505, 1998. [4](#)
- [14] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Quantum Information: A Millennium Volume*, volume 305 of *Contemporary Mathematics*, pages 53–74. American Mathematical Society, 2002. [42](#)
- [15] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum algorithm for the collision problem. arXiv:quant-ph/9705002, 1997. [3](#), [8](#), [42](#)
- [16] Joseph Carolan. Compressed permutation oracles. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing*, pages 150–161. ACM, 2026. [3](#)
- [17] Yu Long Chen, Wonseok Choi, and Changmin Lee. Improved multi-user security using the squared-ratio method. In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part II*, volume 14082 of *LNCS*, pages 694–724. Springer, Cham, August 2023. [3](#), [8](#)
- [18] Yu Long Chen, Eran Lambooi, and Bart Mennink. How to build pseudorandom functions from public random permutations. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 266–293. Springer, Cham, August 2019. [3](#), [8](#)
- [19] Wonseok Choi, Hwigeom Kim, Jooyoung Lee, and Yeongmin Lee. Multi-user security of the sum of truncated random permutations. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part II*, volume 13792 of *LNCS*, pages 682–710. Springer, Cham, December 2022. [3](#), [8](#)
- [20] Wonseok Choi, ByeongHak Lee, and Jooyoung Lee. Indifferentiability of truncated random permutations. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 175–195. Springer, Cham, December 2019. [3](#)
- [21] Wonseok Choi, Jooyoung Lee, and Yeongmin Lee. Building PRFs from TPRPs: Beyond the block and the tweak length bounds. *IACR Trans. Symm. Cryptol.*, 2024(1):35–70, 2024. [8](#)
- [22] Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. On the compressed-oracle technique, and post-quantum security of proofs of sequential work. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 598–629. Springer, Cham, October 2021. [6](#), [35](#), [47](#)
- [23] Benoit Cogliati, Rodolphe Lampe, and Jacques Patarin. The indistinguishability of the XOR of k permutations. In Carlos Cid and Christian Rechberger, editors, *FSE 2014*, volume 8540 of *LNCS*, pages 285–302. Springer, Berlin, Heidelberg, March 2015. [8](#)

- [24] Alexandru Cojocaru, Minki Hhan, Qipeng Liu, Takashi Yamakawa, and Aaram Yun. Quantum lifting for invertible permutations and ideal ciphers. In *CRYPTO 2025, Part II*, LNCS, pages 481–512. Springer, Cham, August 2025. [3](#)
- [25] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 497–523. Springer, Cham, August 2017. [3](#), [8](#)
- [26] Nilanjan Datta, Avijit Dutta, Sougata Mandal, Hrithik Nandi, and Amlan Sinha. Post-quantum security of keyed sum of permutations and its siblings. In *Advances in Cryptology – ASIACRYPT 2026*. Springer, 2026. To appear. [9](#)
- [27] Data encryption standard. National Bureau of Standards, NBS FIPS PUB 46, U.S. Department of Commerce, January 1977. [3](#)
- [28] Itai Dinur. Tight indistinguishability bounds for the XOR of independent random permutations by Fourier analysis. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part I*, volume 14651 of *LNCS*, pages 33–62. Springer, Cham, May 2024. [3](#), [4](#), [5](#), [8](#), [11](#)
- [29] Itai Dinur. Combining outputs of a random permutation: New constructions and tight security bounds by fourier analysis. In *EUROCRYPT 2025, Part I*, LNCS, pages 244–273. Springer, Cham, June 2025. [3](#), [4](#)
- [30] Avijit Dutta, Mridul Nandi, and Abishanka Saha. Proof of Mirror Theory for $\xi_{\max} = 2$. *IEEE Transactions on Information Theory*, 68(9):6218–6232, 2022. [3](#), [8](#)
- [31] Sean Eberhard. More on additive triples of bijections. arXiv:1704.02407, 2017. [3](#), [4](#), [8](#)
- [32] Sean Eberhard, Freddie Manners, and Rudi Mrazović. Additive triples of bijections, or the toroidal semiqueens problem. *Journal of the European Mathematical Society*, 21(2):441–463, 2019. [4](#)
- [33] Hartmut Ehlich and Karl Zeller. Schwankung von polynomen zwischen gitterpunkten. *Mathematische Zeitschrift*, 86:41–44, 1964. [45](#)
- [34] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Limit on the speed of quantum computation in determining parity. *Phys. Rev. Lett.*, 81:5442–5444, Dec 1998. [8](#), [44](#)
- [35] Ben Foxman, Alex Lombardi, Fermi Ma, Barak Nehoran, and John Wright. Quantum lazy sampling and path recording for any group, 2026. [3](#)
- [36] Shoni Gilboa, Shay Gueron, and Ben Morris. How many queries are needed to distinguish a truncated random permutation from a random function? *Journal of Cryptology*, 31(1):162–171, January 2018. [3](#)
- [37] Aldo Gensing and Bart Mennink. The summation-truncation hybrid: Reusing discarded bits for free. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 187–217. Springer, Cham, August 2020. [3](#)
- [38] Chris Hall, David Wagner, John Kelsey, and Bruce Schneier. Building PRFs from PRPs. In Hugo Krawczyk, editor, *CRYPTO’98*, volume 1462 of *LNCS*, pages 370–389. Springer, Berlin, Heidelberg, August 1998. [3](#)
- [39] Yu-Hsuan Huang, Andreas Hülsing, Varun Maram, Silvia Ritsch, and Abishanka Saha. Feistel tools: Reprogramming and query-recording for QRPs. Cryptology ePrint Archive, Paper 2026/146, 2026. [3](#)
- [40] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152. Springer, Cham, August 2018. [3](#)

- [41] Stefan Lucks. The sum of PRPs is a secure PRF. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 470–484. Springer, Berlin, Heidelberg, May 2000. 3, 8
- [42] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. In *57th ACM STOC*, pages 806–809. ACM Press, June 2025. 3
- [43] Avradip Mandal, Jacques Patarin, and Valérie Nachev. Indifferentiability beyond the birthday bound for the xor of two public random permutations. In Guang Gong and Kishan Chand Gupta, editors, *INDOCRYPT 2010*, volume 6498 of *LNCS*, pages 69–81. Springer, Berlin, Heidelberg, December 2010. 3
- [44] Bart Mennink and Alan Szepieniec. XOR of PRPs in a quantum world. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017*, pages 367–383. Springer, Cham, 2017. 8
- [45] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. In *65th FOCS*, pages 485–492. IEEE Computer Society Press, October 2024. 3
- [46] Ryan O’Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014. 5, 12
- [47] Jacques Patarin. A proof of security in $O(2n)$ for the xor of two random permutations. In Reihaneh Safavi-Naini, editor, *ICITS 08*, volume 5155 of *LNCS*, pages 232–248. Springer, Berlin, Heidelberg, August 2008. 3, 8
- [48] Jacques Patarin. Generic attacks for the xor of k random permutations. In Michael J. Jacobson, Jr., Michael E. Locasto, Payman Mohassel, and Reihaneh Safavi-Naini, editors, *ACNS 13 International Conference on Applied Cryptography and Network Security*, volume 7954 of *LNCS*, pages 154–169. Springer, Berlin, Heidelberg, June 2013. 5, 8
- [49] Theodore J. Rivlin and Elliott W. Cheney. A comparison of uniform approximations on an interval and a finite subset thereof. *SIAM Journal on Numerical Analysis*, 3(2):311–320, 1966. 45
- [50] Ansis Rosmanis. Tight bounds for inverting permutations via compressed oracle arguments, 2021. 3, 4
- [51] Adrian She and Henry Yuen. Unitary property testing lower bounds by polynomials. In Yael Tautman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference, ITCS 2023, MIT, Cambridge, Massachusetts, USA, January 10-13, 2023*, volume 251 of *LIPIcs*, pages 96:1–96:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. 4
- [52] Kazuo Shinagawa and Tetsu Iwata. Quantum attacks on sum of Even–Mansour pseudorandom functions. *Information Processing Letters*, 173:106172, 2022. 9
- [53] Victor Shoup. On fast and provably secure message authentication based on universal hashing. In Neal Koblitz, editor, *CRYPTO’96*, volume 1109 of *LNCS*, pages 313–328. Springer, Berlin, Heidelberg, August 1996. 3
- [54] Fang Song and Aaram Yun. Quantum security of NMAC and related constructions - PRF domain extension against quantum attacks. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 283–309. Springer, Cham, August 2017. 3
- [55] Mark N. Wegman and Larry Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265–279, 1981. 3
- [56] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Information and Computation*, 15(7&8):557–567, 2015. 3

- [57] Mark Zhandry. How to record quantum queries, and applications to quantum indistinguishability. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 239–268. Springer, Cham, August 2019. [3](#), [4](#), [6](#), [35](#)
- [58] Mark Zhandry. How to construct quantum random functions. *Journal of the ACM (JACM)*, 68(5):1–43, 2021. [3](#), [4](#), [6](#), [26](#), [34](#)

A Collision Bias and Heuristic Attacks

We present a heuristic outline of the quantum attacks described in [Section 1.3](#). Throughout, $r \geq 2$ is fixed, and the oracle O is either a uniformly random function ($O = \text{rf}$) or the $\text{XoP}[r]$ construction ($O = \text{XoP}$). The collision statistic calculations below are intended to explain the expected scalings of advantages.

Recall the collision probability of $\text{XoP}[r]$

$$\Pr[\text{XoP}[r](x) = \text{XoP}[r](x')] = \frac{1}{N} + \frac{(-1)^r}{N(N-1)^{r-1}}, \quad \delta_r := \frac{(-1)^r}{N(N-1)^{r-1}}$$

where δ_r is the difference between the collision probabilities of $\text{XoP}[r]$ and a random function, and $|\delta_r| = \Theta(N^{-r})$.

All attacks except the last one are based on the collision finding attack [\[15\]](#). We actually *count* the number of the (parts of) collisions in the following way:

1. For an appropriate set $S \subset \{0, 1\}^n$, compute the table $T_S := \{O(x) : x \in S\}$, the set of distinct outputs obtained from the inputs in S . Define the indicator function $f_S(z) = \llbracket O(z) \in T_S \rrbracket$ for $z \in \{0, 1\}^n \setminus S$.
2. Approximately count the number of $z \in \{0, 1\}^n \setminus S$ such that $f_S(z) = 1$.

Note that $f_S(z) = \llbracket O(z) \in T_S \rrbracket$ indicates that z is a part of the *cross collision* $O(z) = O(x)$ for some $x \in S$. The first step makes $s := |S|$ queries to the oracle O . Let $K = |\{z \in \{0, 1\}^n \setminus S : f_S(z) = 1\}|$ be the number of inputs outside S whose outputs collide with one of the stored values in T_S . Using quantum counting [\[14\]](#) with t queries to O , we can obtain an estimate $\tilde{K}$ satisfying

$$\left| \frac{\tilde{K}}{N-s} - \frac{K}{N-s} \right| = O\left(\frac{\sqrt{K/(N-s)}}{t} + \frac{1}{t^2}\right)$$

with a constant probability. In other words, if $s, t = \Theta(q)$ and $K = \Theta(s)$, the additive error $|\tilde{K} - K|$ is bounded by

$$O\left(\sqrt{\frac{N}{q}} + \frac{N}{q^2}\right).$$

We first compare the distribution of K under the two oracle choices. If $O = \text{rf}$, then conditioned on T_S , the values $O(z)$ for $z \notin S$ are independent and uniform. Therefore,

$$K \mid T_S \sim \text{Bin}\left(N-s, \frac{|T_S|}{N}\right).$$

In particular, for $s = \Theta(q)$ and $s \leq cN$ for a fixed constant $c < 1$, we have

$$\mathbb{E}_{\text{rf}}[K] = \Theta(q), \quad \text{std}_{\text{rf}}(K) = \Theta(\sqrt{q}). \quad (37)$$

For $\text{XoP}[r]$, the collision probability between every pair of distinct inputs differs from that of a random function by δ_r . As a heuristic approximation, we expect the number of cross collisions to differ by

$$|\mathbb{E}_{\text{XoP}}[K] - \mathbb{E}_{\text{rf}}[K]| \approx (N-s)s|\delta_r| = \Theta\left(\frac{q}{N^{r-1}}\right),$$

where we use $s = \Theta(q)$ and $N-s = \Theta(N)$. We use this heuristic estimate below to derive the expected advantage of the collision-based attacks.

Small-query regime: $q \lesssim N^{1/3}$. In this regime, it suffices to search for a collision rather than estimate K accurately. The algorithm first constructs T_S using $s = \Theta(q)$ queries and then uses $t = \Theta(q)$ further queries to search for a $z \notin S$ satisfying $f_S(z) = 1$.

For a fixed value of K , Grover search using t queries finds such a z with probability

$$\Theta\left(\frac{t^2 K}{N}\right)$$

which coincides with $\Theta\left(\frac{q^3}{N}\right)$ for our parameter choice when $K = \Theta(q)$.

Using the heuristic estimate above for the difference in $\mathbb{E}[K]$, we expect the difference between the acceptance probabilities under the two oracle choices to be of order

$$\Theta\left(\frac{t^2}{N} |\mathbb{E}_{\text{XoP}}[K] - \mathbb{E}_{\text{rf}}[K]|\right) = \Theta\left(\frac{q^3}{N^r}\right).$$

Thus the collision-finding attack is expected to achieve advantage $\Theta(q^3/N^r)$ in this regime.

Moderate-query regime: $N^{1/3} \lesssim q \lesssim N^{1/2}$. We now use quantum counting to estimate K . Let $\tilde{K}$ be the estimate obtained using $t = \Theta(q)$ queries in the second step. The counting error discussed above (obtained with constant probability) is

$$|\tilde{K} - K| = O\left(\sqrt{\frac{N}{q}} + \frac{N}{q^2}\right) = O\left(\sqrt{\frac{N}{q}}\right)$$

since $q \gtrsim N^{1/3}$. Also note that the standard deviation $\Theta(\sqrt{q})$ of K in [Eq. \(37\)](#) is relatively smaller than this error in this regime. This comparison will be important in the next regime.

Using the heuristic estimate above, we expect

$$|\mathbb{E}_{\text{XoP}}[K] - \mathbb{E}_{\text{rf}}[K]| = \Theta\left(\frac{q}{N^{r-1}}\right).$$

Comparing this difference with the quantum-counting error $\Theta(\sqrt{N/q})$ heuristically suggests distinguishing advantage of order

$$\Theta\left(\frac{q/N^{r-1}}{\sqrt{N/q}}\right) = \Theta\left(\frac{q^{3/2}}{N^{r-1/2}}\right).$$

Large-query regime: $N^{1/2} \lesssim q \lesssim N$. Continue to use $s = \Theta(q)$ queries to construct the table and $t = \Theta(q)$ queries for quantum counting. The additive error of the estimate is, given $q \gtrsim N^{1/2}$,

$$O\left(\sqrt{\frac{N}{q}} + \frac{N}{q^2}\right) = O(\sqrt{q}).$$

Note that the standard deviation of K in [Eq. \(37\)](#) is already $\Theta(\sqrt{q})$. This means that the values of K for two different random oracles may be of order $\Theta(\sqrt{q})$, which is no smaller than the estimation error.

Using the heuristic estimate above, we expect

$$|\mathbb{E}_{\text{XoP}}[K] - \mathbb{E}_{\text{rf}}[K]| = \Theta\left(\frac{q}{N^{r-1}}\right).$$

Comparing this difference with the above typical difference $\sqrt{q}$ of two random oracles suggests distinguishing advantage of order, heuristically,

$$\Theta\left(\frac{q/N^{r-1}}{\sqrt{q}}\right) = \Theta\left(\frac{\sqrt{q}}{N^{r-1}}\right).$$

At $q = \Theta(N)$, this heuristic scaling becomes $\Theta(N^{3/2-r})$, matching the second bound of [Theorem 4.1](#).

Parity attack ($q \geq N/2$). Finally, suppose that $q \geq N/2$. Fix a nonzero $a \in \{0,1\}^n$ and define the Boolean function $g_O(x) := \langle a, O(x) \rangle$ for the oracle O , which can be computed by a single query to O . For the XoP $[r]$ construction, assuming $n \geq 2$, the parity of $g_{\text{XoP}[r]}$, i.e., $\bigoplus_{x \in \{0,1\}^n} g_{\text{XoP}[r]}(x)$ becomes 0 because

$$\left\langle a, \bigoplus_{x \in \{0,1\}^n} \text{XoP}[r](x) \right\rangle = \left\langle a, \bigoplus_{i=1}^r \bigoplus_{x \in \{0,1\}^n} P_i(x) \right\rangle = \left\langle a, \bigoplus_{i=1}^r \bigoplus_{y \in \{0,1\}^n} y \right\rangle = 0.$$

For a random function, this parity is a uniformly random bit. The parity of g_O can be computed exactly with $N/2$ quantum queries by pairing up the N inputs and computing the XOR of each pair with Deutsch's algorithm, which is optimal [34]. The distinguisher that outputs the parity thus has advantage $1/2$.

B Reductions between Planted Distributions

B.1 Several planted collisions

We recall the statement of the lemma for convenience.

Lemma 6.10. $\text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{PC},k}, \mathcal{D}_{\mathbf{F}}) = O(q^3/N^2)$ for $k = 2, 3$.

Proof of Lemma 6.10. Fix $i \in \{1, 2, 3\}$ and a q -query algorithm $\mathcal{A}$.

Let g be an oracle from $\mathcal{D}_{\mathbf{F}}$ or $\mathcal{D}_{\text{PC}}$. Given the oracle g , we will construct another oracle h as follows. Sample $2i - 2$ distinct points $z_1, \dots, z_{2i-2} \in [N]$ uniformly and sample independent uniform values $v_1, \dots, v_{i-1} \in [N]$. Let $T = [N] \setminus \{z_1, \dots, z_{2i-2}\}$. Define

$$h(x) = \begin{cases} v_j & x \in \{z_{2j-1}, z_{2j}\}, \\ g(x) & x \in T. \end{cases}$$

We define an algorithm $\mathcal{B}_i$ given the oracle g for $i \in \{1, 2, 3\}$ as follows.

$\mathcal{B}_i$: It defines h as above, and executes $\mathcal{A}$ with oracle h .

Note that one quantum query to h can be simulated using at most two queries to g . In more detail, for every $x, z \in \{0,1\}^n$, the simulation acts as follows:

$$\begin{aligned} |x, 0^n, z\rangle &\xrightarrow{\text{query to } g} |x, g(x), z\rangle \\ &\xrightarrow{\text{unitary}} |x, g(x), z + h(x)\rangle \\ &\xrightarrow{\text{query to } g} |x, 0^n, z + h(x)\rangle. \end{aligned}$$

If $g \sim \mathcal{D}_{\mathbf{F}}$, then $h \sim \mathcal{D}_{\text{PC},i-1}$ because of newly planted collisions. On the other hand, if $g \sim \mathcal{D}_{\text{PC}}$, both inputs of the original planted collision pair of g is contained in T with probability

$$p_i = \frac{(N - 2i + 2)_2}{(N)_2} \geq \frac{1}{5}.$$

On this event, $h \sim \mathcal{D}_{\text{PC},i}$ as there are i pairs of the planted collisions. If any of the inputs of the original planted collision of g is not contained in T , we can observe that $g|_T$ is a uniform random function (without planted collisions), as well as $h|_T$. Also note that $h|_{[N] \setminus T}$ consists of $i - 1$ collisions, which shows that $h \sim \mathcal{D}_{\text{PC},i-1}$ in this case.

Consequently, the distributions of h in the two cases, $g \sim \mathcal{D}_{\mathbf{F}}$ and $g \sim \mathcal{D}_{\text{PC}}$, are exactly

$$\mathcal{D}_{\text{PC},i-1} \quad \text{and} \quad p_i \mathcal{D}_{\text{PC},i} + (1 - p_i) \mathcal{D}_{\text{PC},i-1}.$$

Taking the difference of the two acceptance probabilities of $\mathcal{B}_i$ for the two cases gives

$$p_i \text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{PC},i}, \mathcal{D}_{\text{PC},i-1}; \mathcal{A}) = \text{Adv}^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\mathbf{F}}; \mathcal{B}_i) \leq \text{Adv}_{2q}^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\mathbf{F}}).$$

We can use the hybrid argument (or the triangle inequality) to show, using $\mathcal{D}_{\text{PC},0} = \mathcal{D}_{\mathbf{F}}$, the following for $k \in \{2, 3\}$:

$$\begin{aligned} \text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{PC},k}, \mathcal{D}_{\mathbf{F}}) &\leq \sum_{i=1}^k p_i^{-1} \text{Adv}_{2q}^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\mathbf{F}}) \\ &\leq 5k \text{Adv}_{2q}^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\mathbf{F}}) = O(q^3/N^2). \end{aligned} \quad \square$$

B.2 A planted triple from a planted pair

We first prove the decisional version of the quantum search bound using the polynomial method [5].

Claim B.1. Let $\mathcal{Z}_M$ be the distribution that always outputs the all-zero function $b_\emptyset(j) = 0$ for all $j \in [M]$. Let $\mathcal{S}_M$ be a distribution obtained by sampling $z \leftarrow [M]$ uniformly at random, and outputting the indicator function $b_z(j) = \mathbb{I}[j = z]$. Then, for every q , it holds that

$$\text{Adv}_q^{\text{dist}}(\mathcal{S}_M, \mathcal{Z}_M) \leq \frac{16q^2}{M}$$

Proof. Fix a q -query quantum algorithm $\mathcal{A}$ having access to an oracle $b : [M] \rightarrow \{0, 1\}$. Write $x = (x_1, \dots, x_M) \in \{0, 1\}^M$ be an alternative representation of b by choosing $x_i = b(i)$. Let $P(x) = \Pr[\mathcal{A}^x \rightarrow 1]$ be the acceptance probability of $\mathcal{A}$ given oracle x . It is clear that $0 \leq P(x) \leq 1$ for all $x \in \{0, 1\}^M$.

The polynomial method for quantum query algorithms [5] shows that P can be written as a real multilinear polynomial of degree at most $2q$ on input x .

We use the standard symmetrization argument in the original polynomial method paper [5, Section 3.1] by taking the average of all inputs. This shows that there exists a univariate real polynomial p of degree at most $2q$ such that for every $k \in \{0, \dots, M\}$, it holds that

$$p(k) = \frac{1}{\binom{M}{k}} \sum_{x \in \{0, 1\}^M, |x|=k} P(x).$$

In other words, $p(k)$ is the average acceptance probability of $\mathcal{A}$ over all Boolean functions of Hamming weight k . In particular, it holds that $p(0)$ and $p(1)$ correspond to the acceptance probability of $\mathcal{A}$ with oracle from $\mathcal{Z}_M$ and $\mathcal{S}_M$, respectively.

It remains to give an upper bound of $\delta := |p(1) - p(0)|$. By the mean value theorem, there exists $z \in (0, 1)$ such that $|p'(z)| = \delta$. Since the degree of p is at most $2q$ and $0 \leq p(k) \leq 1$ for every $k \in \{0, \dots, M\}$, the results from [33, 49] show that

$$4q^2 \geq \deg(p)^2 \geq \frac{\delta M}{1 + \delta}.$$

If $16q^2/M \geq 1$, there is nothing to prove. Otherwise, rearranging above gives

$$\delta \leq \frac{4q^2}{M - 4q^2} \leq \frac{16q^2}{M}$$

which proves the desired upper advantage bound. $\square$

Lemma 6.8. $\text{Adv}_q^{\text{dist}}(\mathcal{D}_{3\text{PC}}, \mathcal{D}_{\mathbf{F}}) = O(q^2/N)$.

Proof of Lemma 6.8. Fix a q -query algorithm $\mathcal{A}$. We first prove the intermediate bound

$$\text{Adv}_q^{\text{dist}}(\mathcal{D}_{3\text{PC}}, \mathcal{D}_{\text{PC}}) \leq \frac{64q^2}{N - 2}$$

using the above lemma. Define an algorithm $\mathcal{B}$ with a Boolean oracle $b : [N] \rightarrow \{0, 1\}$ as follows.

1. Sample uniformly distinct inputs a_1, a_2 , a uniform output v , and $R \leftarrow \mathbf{F}$, all independently.
2. Define $h_b : [N] \rightarrow [N]$ by

$$h_b(x) := \begin{cases} v & \text{if } x \in \{a_1, a_2\} \text{ or } b(x) = 1, \\ R(x) & \text{otherwise.} \end{cases}$$

3. Run $\mathcal{A}$ with the oracle O_{h_b} .

As one query to O_{h_b} is simulated by two queries to O_b , $\mathcal{B}$ makes at most $2q$ queries to b .

Suppose $b \leftarrow \mathcal{Z}_N$. As $b(x) = 0$ always, we have $h_b(a_1) = h_b(a_2) = v$ and $h_b(x) = R(x)$ for $x \notin \{a_1, a_2\}$. Since v and the values $R(x)$ for $x \notin \{a_1, a_2\}$ are independent and uniform, h_b is a uniform random function conditioned on $h_b(a_1) = h_b(a_2)$. Since (a_1, a_2) is chosen uniformly, $h_b \sim \mathcal{D}_{\text{PC}}$.

Suppose $b \sim \mathcal{S}_N$. Then we have $b(x) = \llbracket x = z \rrbracket$ for a randomly sampled $z \leftarrow [N]$. Let E be the event $z \in \{a_1, a_2\}$. Note that $\Pr[E] = 2/N$. If E occurs, since $b(x) = 1$ implies $z \in \{a_1, a_2\}$, $h_b \sim \mathcal{D}_{\text{PC}}$ by the above argument. If E does not occur, we have $h_b(a_1) = h_b(a_2) = h_b(z) = v$ and $h_b(x) = R(x)$ for $x \notin \{a_1, a_2, z\}$. Since v and R are independent and uniform, h_b is a uniform random function conditioned on $h_b(a_1) = h_b(a_2) = h_b(z)$. Since (a_1, a_2, z) is chosen uniformly, $h_b \sim \mathcal{D}_{3\text{PC}}$.

Consequently, a q -query distinguisher for $\frac{N-2}{N}\mathcal{D}_{3\text{PC}} + \frac{2}{N}\mathcal{D}_{\text{PC}}$ and $\mathcal{D}_{\text{PC}}$ gives a $2q$ -query distinguisher for $\mathcal{S}_N$ and $\mathcal{Z}_N$. By the claim, we have

$$\begin{aligned} \text{Adv}_q^{\text{dist}}(\mathcal{D}_{3\text{PC}}, \mathcal{D}_{\text{PC}}; \mathcal{A}) &= \frac{N}{N-2} \text{Adv}_q^{\text{dist}}\left(\frac{N-2}{N}\mathcal{D}_{3\text{PC}} + \frac{2}{N}\mathcal{D}_{\text{PC}}, \mathcal{D}_{\text{PC}}; \mathcal{A}\right) \\ &= \frac{N}{N-2} \text{Adv}_{2q}^{\text{dist}}(\mathcal{S}_N, \mathcal{Z}_N; \mathcal{B}) \leq \frac{64q^2}{N-2}. \end{aligned}$$

The triangle inequality now gives exactly the desired comparison:

$$\begin{aligned} \text{Adv}_q^{\text{dist}}(\mathcal{D}_{3\text{PC}}, \mathcal{D}_{\mathbf{F}}) &\leq \text{Adv}_q^{\text{dist}}(\mathcal{D}_{3\text{PC}}, \mathcal{D}_{\text{PC}}) + \text{Adv}_q^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\mathbf{F}}) \\ &= O\left(\frac{q^2}{N} + \frac{q^3}{N^2}\right) = O\left(\frac{q^2}{N}\right), \end{aligned}$$

where we use $q \leq N$ in last equality. □

B.3 Planted 4-XOR by splitting outputs

Lemma 6.11. $\text{Adv}_q^{\text{dist}}(\mathcal{D}_{4\text{X}}, \mathcal{D}_{\mathbf{F}}) = O(q^3/N^2)$.

Proof of Lemma 6.11. Fix $\mathcal{A}$ be a q -query algorithm.

Let $g : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be either a uniform random function (from $\mathcal{D}_{\mathbf{F}}$) or a random function with a single planted collision (from $\mathcal{D}_{\text{PC}}$). We define a function h using g that is either a uniform random function or a random function with a planted 4-xor tuple with a certain probability.

Formally, we define $h : \{0, 1\}^n \rightarrow \{0, 1\}^n$ as follows. Let $M = N/2 = 2^{n-1}$. Sample a uniform random permutation π of $\{0, 1\}^n$ and independent and uniform random $R_1, \dots, R_M \in \{0, 1\}^n$. For each $j \in \{0, 1\}^{n-1}$, set

$$h(\pi(j\|0)) = R_j, \quad h(\pi(j\|1)) = R_j + g(j\|0)$$

where $\|$ denotes the concatenation. Let $\mathcal{B}$ be an algorithm that defines h as above, and executes $\mathcal{A}$ with oracle h . As noted before, each query to h requires at most two queries to g .

We analyze two cases. If $g \sim \mathcal{D}_{\mathbf{F}}$, then it is not hard to see that $h \sim \mathcal{D}_{\mathbf{F}}$. Consider $g \sim \mathcal{D}_{\text{PC}}$ and let $\{u, v\}$ be the planted collision pair of g . Define E by the event that both of u, v are included in $\{(j\|0) : j \in \{0, 1\}^{n-1}\}$. This event occurs with probability at least

$$p = \frac{(M)_2}{(N)_2} = \frac{N-2}{4(N-1)} \geq \frac{1}{6}.$$

Conditioned on E , write $v = v_0\|0$ and $u = u_0\|0$. The restriction of g to $\{(j\|0) : j \in \{0,1\}^{n-1}\}$ is uniform subject to $g(u) = g(v)$. For h , this gives

$$h(\pi(u_0\|0)) + h(\pi(u_0\|1)) + h(\pi(v_0\|0)) + h(\pi(v_0\|1)) = 0^n.$$

The outputs of h on those inputs $\pi(u_0\|0), \pi(u_0\|1), \pi(v_0\|0), \pi(v_0\|1)$ are uniform conditioned on the sum being 0^n , meaning that they become the planted 4-xor tuple. All other outputs are uniformly and randomly distributed. In other words, $h \sim \mathcal{D}_{4X}$ in this case. On the other hand, conditioned on $\neg E$, we can see that the $h \sim \mathcal{D}_{\mathbf{F}}$.

Therefore, the distribution of the oracles given to $\mathcal{A}$ in this execution become $\mathcal{D}_{\mathbf{F}}$ and $p\mathcal{D}_{4X} + (1-p)\mathcal{D}_{\mathbf{F}}$, respectively. Subtracting acceptance probabilities gives

$$p\text{Adv}^{\text{dist}}(\mathcal{D}_{4X}, \mathcal{D}_{\mathbf{F}}; \mathcal{A}) = \text{Adv}^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\mathbf{F}}; \mathcal{B}) \leq \text{Adv}_{2q}^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\mathbf{F}}).$$

Taking the maximum over $\mathcal{A}$ proves

$$\text{Adv}_q^{\text{dist}}(\mathcal{D}_{4X}, \mathcal{D}_{\mathbf{F}}) \leq 6\text{Adv}_{2q}^{\text{dist}}(\mathcal{D}_{\text{PC}}, \mathcal{D}_{\mathbf{F}}) = O(q^3/N^2). \quad \square$$

C Missing Proofs for the Compressed Oracles

Lemma 7.4. *Let $|\Xi_t\rangle$ be the final state over the algorithm and database registers outputted by some algorithm after making $t \leq N$ queries to the compressed oracle O . Then*

$$\langle \Xi_t | D_{\text{cnt}} | \Xi_t \rangle \leq t, \quad \langle \Xi_t | \text{Col}_{\text{cnt}} | \Xi_t \rangle \leq 129t.$$

Proof. After s queries, the state is supported on databases D satisfying $|\{x : D(x) \neq \perp\}| \leq s$. Since the state has norm at most one, this proves the first inequality.

We now bound the increase in the collision count caused by a query. Write

$$\chi_b(v) := (-1)^{b \cdot v}, \quad |\chi_b\rangle := \frac{1}{\sqrt{N}} \sum_v \chi_b(v) |v\rangle$$

for the Fourier basis of the response register. In particular, $|\chi_0\rangle = |+\rangle$. Fix a query input x and a response state $|\chi_b\rangle$. For $b \neq 0$, the query acts on database register x by the operator

$$O_b = Z_b + |+\rangle\langle+| - |+\rangle\langle\chi_b| - |\chi_b\rangle\langle+| + |\chi_b\rangle\langle\perp| + |\perp\rangle\langle\chi_b|, \quad Z_b := \sum_v \chi_b(v) |v\rangle\langle v|,$$

as follows from [22, Lemma 4.3]. For $b = 0$, the query is the identity.

Also fix the computational-basis values of the database registers other than x , and put

$$m_v := |\{y \neq x : D(y) = v\}|, \quad \ell := \sum_v m_v, \quad c := \sum_v \binom{m_v}{2}.$$

Thus, ℓ is the number of inputs $y \neq x$ with $D(y) \neq \perp$, and c is the number of collision pairs not involving x . In particular,

$$\sum_v m_v^2 = \ell + 2c.$$

On this subspace, the collision-count operator is $cI + A$, where

$$A := \sum_v m_v |v\rangle\langle v|$$

acts on database register x and counts collision pairs involving x . We have

$$\|A|+\rangle\|^2 = \|A|\chi_b\rangle\|^2 = \frac{\ell + 2c}{N}.$$

Moreover, $[A, Z_b] = 0$ and $A|\perp\rangle = 0$. In the expansion of O_b , the commutator with each of $|+\rangle\langle+|$, $|+\rangle\langle\chi_b|$, and $|\chi_b\rangle\langle+|$ has norm at most $2\sqrt{(\ell + 2c)/N}$. The commutator with each of the remaining two terms has norm at most $\sqrt{(\ell + 2c)/N}$. Therefore,

$$\|[A, O_b]\| \leq 8\sqrt{\frac{\ell + 2c}{N}}.$$

Since O_b is unitary, the change in the collision-count operator satisfies

$$\|O_b^\dagger A O_b - A\| = \|O_b^\dagger [A, O_b]\| \leq 8\sqrt{\frac{\ell + 2c}{N}}.$$

The same bound holds for $b = 0$, since the change is zero.

Let $|\Xi_s\rangle$ denote the state after s queries and the subsequent algorithm operations, just before the next query, and put

$$k_s := \langle \Xi_s | \text{Col}_{\text{cnt}} | \Xi_s \rangle.$$

Both O and Col_{cnt} preserve the subspaces specified by the query input x , the Fourier-basis response b , and the values of the other database registers. Index these mutually orthogonal subspaces by λ . Let p_λ be the squared norm of the component of $|\Xi_s\rangle$ in subspace λ , and let ℓ_λ, c_λ be the corresponding values of ℓ, c . Then

$$\sum_\lambda p_\lambda = \|\Xi_s\|^2 \leq 1, \quad \ell_\lambda \leq s, \quad \sum_\lambda p_\lambda c_\lambda \leq k_s.$$

The last inequality holds because c_λ counts only collision pairs not involving the queried input. Applying the preceding operator bound in each subspace and then the Cauchy–Schwarz inequality gives

$$\begin{aligned} & \langle \Xi_s | O^\dagger \text{Col}_{\text{cnt}} O | \Xi_s \rangle - k_s \\ & \leq \frac{8}{\sqrt{N}} \sum_\lambda p_\lambda \sqrt{\ell_\lambda + 2c_\lambda} \\ & \leq \frac{8}{\sqrt{N}} \left(\sum_\lambda p_\lambda \right)^{1/2} \left(\sum_\lambda p_\lambda (\ell_\lambda + 2c_\lambda) \right)^{1/2} \\ & \leq 8\sqrt{\frac{s + 2k_s}{N}}. \end{aligned}$$

A unitary acting only on the algorithm's registers leaves the expectation of Col_{cnt} unchanged. An orthogonal projection on those registers cannot increase this expectation, provided that the resulting state is not renormalized. Indeed, such a projection commutes with the positive operator Col_{cnt} . Consequently,

$$k_{s+1} \leq k_s + 8\sqrt{\frac{s + 2k_s}{N}}. \tag{38}$$

Starting from $k_0 = 0$, we prove $k_s \leq 129s$ by induction. If $k_s \leq 129s$ and $s < N$, then

$$k_{s+1} \leq 129s + 8\sqrt{\frac{259s}{N}} \leq 129s + 8\sqrt{259} \leq 129(s+1).$$

This proves the second inequality. □

Proof of Eq. (36). We will prove that for every joint algorithm-database state $|\Xi\rangle$ whose database registers are supported on $\text{span}\{|\hat{f}\rangle : f \in \mathbf{F}\}$, it holds that

$$\|B^\dagger |\Xi\rangle\|^2 \leq \frac{4}{N} \langle \Xi | (\text{D}_{\text{cnt}} + \text{Col}_{\text{cnt}}) |\Xi\rangle.$$

Put $|z_v\rangle := |\hat{v}\rangle - |\perp\rangle / \sqrt{N}$. Then $\langle z_v | z_w \rangle = \llbracket v = w \rrbracket - 1/N$ and $\sum_v |z_v\rangle\langle z_v| = Q$ on $\text{span}\{|\hat{v}\rangle : v \in \{0,1\}^n\}$. For a fixed query input x , define

$$n_v := \sum_{y \neq x} (|z_v\rangle\langle z_v|)_y, \quad b_v := \frac{1}{\sqrt{N}} \sum_{y \neq x} (|\perp\rangle\langle z_v|)_y.$$

The identities for $|z_v\rangle$ give

$$\begin{aligned} B_x B_x^\dagger &= \frac{|\perp\rangle\langle\perp|_x}{N} \sum_v (n_v + b_v)^\dagger (n_v + b_v), \\ \sum_v \|n_v |\Xi\rangle\|^2 &= \left(1 - \frac{1}{N}\right) \langle \Xi | \text{D}_{\text{cnt}, \neq x} |\Xi\rangle + 2 \langle \Xi | \text{Col}_{\text{cnt}, \neq x} |\Xi\rangle, \\ \sum_v \|b_v |\Xi\rangle\|^2 &\leq \frac{N-1}{N} \langle \Xi | \text{D}_{\text{cnt}, \neq x} |\Xi\rangle. \end{aligned}$$

Here the subscript $\neq x$ means that database register x is omitted from the count, and the last line follows from the Cauchy–Schwarz inequality over the $N-1$ database registers. Using $\|a+b\|^2 \leq 2\|a\|^2 + 2\|b\|^2$, dropping the projector $|\perp\rangle\langle\perp|_x$, and summing over the blocks corresponding to the query inputs proves Eq. (36).