Mind the Bad Norms

Revisiting Compressed Oracle-based Quantum Indistinguishability Proofs

Ritam Bhaumik[1], Benoît Cogliati[2], Jordan Ethan[3], and Ashwin Jha[4]

[1] TII, Abu Dhabi, UAE
bhaumik.ritam@gmail.com
[2] Thales DIS France SAS, Meudon, France
benoit.cogliati@gmail.com
[3] CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
jordan.ethan@cispa.de
[4] Ruhr-Universität Bochum, Bochum, Germany
letterstoashwin@gmail.com

Abstract. In this work, we revisit the Hosoyamada-Iwata (HI) proof for the quantum CPA security of the 4-round Luby-Rackoff construction and identify a gap that appears to undermine the security proof. We emphasize that this is *not* an attack, and the construction may still achieve the claimed security level. However, this gap raises concerns about the feasibility of establishing a formal security proof for the 4-round Luby-Rackoff construction. In fact, the issue persists even if the number of rounds is increased arbitrarily. On a positive note, we restore the security of the 4-round Luby-Rackoff construction in the *non-adaptive* setting, achieving security up to $2^{n/6}$ superposition queries. Furthermore, we establish the quantum CPA security of the 4-round MistyR and 5-round MistyL constructions, up to $2^{n/5}$ and $2^{n/7}$ superposition queries, respectively, where n denotes the size of the underlying permutation.

Keywords: quantum security, compressed oracle, recording standard oracle with errors, Luby-Rackoff, Misty

1 Introduction

Quantum Security. In symmetric cryptography, it is generally admitted that a doubling of the key length would be sufficient to deter the threat of quantum computers. Indeed, this corresponds to the lowered cost of exhaustive search from Grover's algorithm. However, in recent years a plethora of results (see for instance [7,8,9,10,11,19,25,27,28,29,30]) have shown that this view is too simplistic, and that more efficient distinguishers can be created. This highlights

An abridged version of this article appears in IACR-ASIACRYPT 2024. The authors would like to thank Akinori Hosoyamada and Tetsu Iwata for their comments on a precursor note that evolved into this paper. Jordan Ethan's research was conducted within the framework of the French-German Center for Cybersecurity, a collaboration between CISPA and LORIA. Ashwin Jha's work was supported by the German Research Foundation (DFG) within the framework of the Excellence Strategy of the Federal Government and the States – EXC 2092 CaSa – 39078197.

the need to study whether existing security proofs for generic constructions and modes of operation can be extended to the quantum setting, which has received a considerable focus in a series of recent works [4,6,15,22,23,24,26,42,43,5].

Pseudorandom Functions and Permutations. Classically, most of the well-known symmetric cryptographic algorithms are constructed as a mode of operation over fixed length primitives that are instantiated with either a pseudorandom[1] permutation (PRP) or function (PRF).

Some well-known examples of generic PRP constructions include the Luby-Rackoff cipher [32], Lai-Massey [31] and the generic Misty ciphers [34,36]. Of these the former two constructions can be instantiated by any primitive (function or permutation), while the latter solely works with permutations. In general, PRP-based constructions are preferred as they can be directly instantiated with well-analyzed block ciphers. On the other hand, PRF based constructions are usually easier to analyze in security proofs. Indeed, many security proofs involve the boilerplate switching lemma [3,41]: replace PRP calls with PRF calls with a factor of $O(q^2/2^n)$ per call, where q and n denote the number of queries and output size, respectively. Thus, all of the above mentioned constructions are classically secure birthday-bound PRFs. On the other hand more recent efforts have focused on building beyond-the-birthday-bound secure PRP-to-PRF constructions, starting with the well-known sum of permutations [2,20] and the truncation of permutation [20] to the more recent encrypted Davis-Meyer [14] and its dual [35]. The analysis of these PRP and PRF constructions lead to a great advancement in the provable security research, mushrooming several new proof techniques such as the H-coefficient technique [39,21], mirror theory [38,40,13] the χ^2-technique [16], and the recent use of Fourier analysis [17] to prove the exact security of sum of permutations.

The Compressed Oracle. In the quantum setting, however, the research on the security of these well-known constructions is still in the rudimentary stage. While there are some generic attacks on Luby-Rackoff [29,22] and Misty [18], on the security proofs front the results are still far from tight even in the birthday-bound[2] regime. Having said that, the situation has changed in recent years, largely due to Zhandry's compressed oracle technique [43] — an elegant way to lazy sample a random function. Indeed most recent security proofs [22,23,24,5] in symmetric cryptography relied on the compressed oracle [43] and its variants respectively introduced by Hosoyamada and Iwata [22] and Chung *et al.* [12].

When proving the indistinguishability of a construction C based on PRFs from a true random function, the proof typically follows these steps:

– Model the random function as a construction with a structure similar to C, but with some of the inputs augmented with adversarial queries to ensure the uniqueness of inputs, thereby guaranteeing the uniformity of outputs.

[1] the fixed-length permutation /function is keyed, efficiently computable, and indistinguishable from a uniform random permutation/function.

[2] Note that, in the quantum setting birthday-bound refers to the cube-root of the output size.

– Identify "bad events" that occur when the output of intermediate function calls leads to input collisions in subsequent calls.
– Upper-bound the probability of such bad events occurring.
– Establish a one-to-one mapping between intermediate values in both constructions, assuming no bad event has occurred.

It is important to note that ensuring these bad events are described only using inputs and outputs recorded by the compressed oracle is critical to the proof. In particular, certain information may be lost in this process, such as the specific adversarial query or the relationship between input-output pairs belonging to the same query.

1.1 Our Contribution

Our contribution is three-fold. Firstly, we identify some critical issues in some of the previous works in this direction. They relate to the aforementioned one-to-one mapping: most notably, in the 4-round Luby-Rackoff security proof [22], the authors cannot prevent bad collisions without relying on information that is not present in the compressed oracle entries. We also spotted similar flaws in [24,5,33].

Secondly, we propose a new security proof for the 4-round Luby-Rackoff construction in the non-adaptive chosen plaintext attack setting: the adversary has to prepare all of its queries in advance, and receive the corresponding outputs at once. By using an artificial dummy database call on all the adversary's inputs, this allows us to mitigate the issue from [22], since now the database contains all the necessary information to handle the bad events.

Finally, we prove the security of Misty schemes in the quantum setting using the two-domain framework from [5]. In more details, we prove that the 4-round MistyR (resp. 5-round MistyL) construction is secure up to $2^{n/5}$ (resp. $2^{n/7}$) chosen plaintext queries, where n denotes the size of the underlying permutation. We note that, in both cases, this corresponds to the minimum number of rounds to achieve an exponential bound in n, since period-finding attacks based on Simon's algorithm exist for the 3-round MistyR (resp. 4-round MistyL) constructions [18].

2 Quantum Computing

Throughout, we assume familiarity with the fundamentals of finite dimensional linear algebra and Quantum computing. A comprehensive exposition on these subjects is given in [37,1]. In this section, we introduce some notation we use later in the paper; an introductory overview of the relevant notions is also available in Appendix A.

2.1 General Notation

The set of all binary strings, including the empty string ε, is denoted $\{0,1\}^*$. For some $x, y \in \{0,1\}^*$, $x\|y$ denotes the concatenation of x and y. For some

positive integer m, $[m]$ denotes the set $\{1, \ldots, m\}$, and $\{0,1\}^m$ denotes the set of all m-bit binary strings.

We use the standard Dirac notations. $\langle \cdot | \cdot \rangle$ denotes the inner product over a k-dimensional Hilbert space $\mathcal{H} := \mathbb{C}^k$, and $\|\cdot\|$ denotes the norm. Given an orthonormal basis $\mathtt{B}$ of $\mathcal{H}$, we sometimes write $\mathbb{C}[\mathtt{B}]$ to emphasize the basis representation of $\mathcal{H}$. $\mathrm{U}(\mathcal{H})$ will denote the set of all unitaries on $\mathcal{H}$. $\mathsf{Tr}(\mathbf{L})$ will denote the trace of a linear operator $\mathbf{L}$. $\mathsf{Tr}_{\mathcal{H}_1}(\mathbf{L})$ will denote the partial trace on $\mathcal{H}_1$ of a linear operator $\mathbf{L}$ over the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$. $\mathrm{D}(\mathcal{H})$ will denote the set of all density operators of $\mathcal{H}$. $\|\mathbf{L}\|_1$ will denote the trace norm of $\mathbf{L}$.

2.2 Quantum (Non-Adaptive) Oracle-Algorithms

In what follows, we define $\mathcal{H}_{in} := \mathbb{C}^{2^m}$, $\mathcal{H}_{out} := \mathbb{C}^{2^n}$. Let $\mathcal{H}_{work}$ and $\mathcal{H}_{state}$ be two finite dimensional complex Hilbert spaces.

Any function $f : \{0,1\}^m \to \{0,1\}^n$ can be realized by the unitary mapping $|x, y\rangle$ to $|x, y \oplus f(x)\rangle$ on $\mathcal{H}_{in} \otimes \mathcal{H}_{out}$. Indeed, the oracle access to f, denoted $\mathbf{O}_f$, is represented by this standard unitary

$$\mathbf{O}_f |x, y\rangle \mapsto |x, y \oplus f(x)\rangle,$$

on the space $\mathcal{H}_{in} \otimes \mathcal{H}_{out}$. To represent a stateful oracle, we simply bestow additional qubits to represent the oracle state. Formally, we define

$$\mathbf{O}_f |x, y, s\rangle \mapsto |x, y + f(x), s'\rangle,$$

on the product space $\mathcal{H}_{\mathbf{O}_f} := \mathcal{H}_{in} \otimes \mathcal{H}_{out} \otimes \mathcal{H}_{state}$, where $\{|x, y, s\rangle\}$ denotes the computational basis of $\mathcal{H}_{\mathbf{O}_f}$. The oracle state space $\mathcal{H}_{state}$ into $\mathcal{H}_{db} \otimes \mathcal{H}_{aux}$, where $\mathcal{H}_{db}$ denotes the internal state which is (possibly transient) and persistent across queries, and $\mathcal{H}_{aux}$ denotes the state space of any ancillary qubits required to compute the function itself. As ancillary qubits are always reset after each query, it is convenient to focus solely on the former (the useful *state*) while disregarding the latter (the ancillary qubits). Indeed, we often drop $\mathcal{H}_{aux}$ from the description and simply consider $\mathcal{H}_{db}$ as the oracle state space.

For any quantum *oracle-algorithm* A that makes q black-box queries to a (possibly stateful) oracle $\mathbf{O}_f$, we define the interactive game $A^{\mathbf{O}_f}$ to be the sequence of $2q+1$ unitaries: $\mathbf{U}_q \mathbf{O}_f \ldots \mathbf{U}_1 \mathbf{O}_f \mathbf{U}_0$ over the product space $\mathcal{H}_{A^{\mathbf{O}_f}} = \mathcal{H}_{in} \otimes \mathcal{H}_{out} \otimes \mathcal{H}_{work} \otimes \mathcal{H}_{state}$, where it is implicitly understood that $\mathbf{U}_i$'s operate on $\mathcal{H}_A = \mathcal{H}_{in} \otimes \mathcal{H}_{out} \otimes \mathcal{H}_{work}$ and $\mathbf{O}_f$ operates on $\mathcal{H}_{\mathbf{O}_f}$.

We write $A^{\mathbf{O}_f}[\rho_A \otimes \rho_{\mathbf{O}_f}] = b$ to denote the event that the oracle-aided algorithm A outputs b after making q queries to oracle $\mathbf{O}_f$, where A and $\mathbf{O}_f$ are initialized in $\rho_A \in \mathrm{D}(\mathcal{H}_A)$ and $\rho_{\mathbf{O}_f} \in \mathrm{D}(\mathcal{H}_{state})$, or jointly as $\rho^0_{A,\mathbf{O}_f} := \rho_A \otimes \rho_{\mathbf{O}_f}$.

Capturing Non-Adaptivity. For any oracle-algorithm A that makes q non-adaptive queries to $\mathbf{O}_f$, we define the non-adaptive interactive game $A^{\mathbf{O}_f^{\otimes q}}$ to be the unitary $\mathbf{U}_1 \mathbf{O}_f^{\otimes q} \mathbf{U}_0$ on the product space $\mathcal{H}_{in}^{\otimes q} \otimes \mathcal{H}_{out}^{\otimes q} \otimes \mathcal{H}_{work} \otimes \mathcal{H}_{state}$ where it is implicitly understood that $\mathbf{O}_f^{\otimes q}$ operates on $\mathcal{H}_{in}^{\otimes q} \otimes \mathcal{H}_{out}^{\otimes q} \times \mathcal{H}_{state}$, while $\mathbf{U}_0$ and $\mathbf{U}_1$ operates on $\mathcal{H}_{in}^{\otimes q} \otimes \mathcal{H}_{out}^{\otimes q} \otimes \mathcal{H}_{work}$.

Indeed the above formalism is analogous to the classical setting, where the non-adaptive algorithm makes all q queries, $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_q) \in (\{0,1\}^m)^q$, together and receives all q responses, $\mathbf{y} = (\mathbf{y}_1, \ldots, \mathbf{y}_q) \in (\{0,1\}^n)^q$, together from the oracle. Analogously, in the quantum setting, we have

$$\mathbf{O}_f^{\otimes q}|\mathbf{x}, \mathbf{y}, s\rangle = |\mathbf{x}, \mathbf{y} + f(\mathbf{x}), s'\rangle,$$

where $f(\mathbf{x}) = (f(\mathbf{x}_1), \ldots, f(\mathbf{x}_q))$ is simply the pointwise application of f on $\mathbf{x}$.

2.3 Quantum Distinguishing Games

For any two quantum oracles $\mathbf{I}$ and $\mathbf{R}$, we define the distinguishing advantage of any quantum distinguisher[3] A by

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathbf{I};\mathbf{R}}(A) := \left|\Pr\left(A^{\mathbf{I}}[\rho^0_{A,\mathbf{I}}] = 1\right) - \Pr\left(A^{\mathbf{R}}[\rho^0_{A,\mathbf{R}}] = 1\right)\right|,$$

where $\rho^0_{A,\mathbf{I}}$ and $\rho^0_{A,\mathbf{R}}$ denote the initial state of $A^{\mathbf{I}}$ and $A^{\mathbf{R}}$, respectively.

The Computationally Unbounded Case. For any computationally-unbounded A, it is well known that

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathbf{I};\mathbf{R}}(A) \leq \frac{1}{2}\|\mathsf{Tr}_{\mathcal{H}_{\mathbf{I}_{db}}}(\rho^q_{A,\mathbf{I}}) - \mathsf{Tr}_{\mathcal{H}_{\mathbf{R}_{db}}}(\rho^q_{A,\mathbf{R}})\|_1,$$

where $\rho^q_{A,\mathbf{O}} := A^{\mathbf{O}}\rho_{A,\mathbf{O}}A^{\mathbf{O}\dagger}$ is the state after q queries to the oracle at-hand $\mathbf{O} \in \{\mathbf{I}, \mathbf{R}\}$. In addition, without loss of generality, we can assume A to be deterministic, and thus, define the initial state of A, $\rho_A = |\psi_A\rangle\langle\psi_A|$ for some fixed unit vector $|\psi_A\rangle \in \mathcal{H}_A$.

The Quantum IND-CPA Game. Let $F = \{F_K : \{0,1\}^m \to \{0,1\}^n\}_{K\in\mathcal{K}}$ be a family of functions. The IND-qCPA advantage of some distinguisher A against F is defined as

$$\mathbf{Adv}^{\mathsf{qcpa}}_F(A) := \mathbf{Adv}^{\mathsf{dist}}_{\mathbf{O}_{F_K};\mathbf{O}_f}(A), \tag{1}$$

where K is uniformly distributed over $\mathcal{K}$, and $f : \{0,1\}^m \to \{0,1\}^n$ is a uniform random function.

For a non-adaptive distinguisher A, the non-adaptive IND-qCPA advantage is defined analogously as:

$$\mathbf{Adv}^{\mathsf{qncpa}}_F(A) := \mathbf{Adv}^{\mathsf{dist}}_{\mathbf{O}^{\otimes q}_{F_K};\mathbf{O}^{\otimes q}_f}(A), \tag{2}$$

3 Zhandry's Compressed Oracle

In [43], Zhandry proposed an elegant solution to implement a restricted form of lazy sampling for quantum random oracle, or simply a uniform random function $f : \{0,1\}^m \to \{0,1\}^n$. We will largely follow the Chung-Fehr-Hunag-Liao (CFHL) intepretation [12] of the compressed oracle, and its refinement by Bhaumik-Cogliati-Ethan-Jha (BCEJ) [5].

[3] An oracle-algorithm with binary output.

3.1 The Chung-Fehr-Huang-Liao Interpretation

Let $\mathcal{Y}$ denote $\{0,1\}^n$ and define $\mathtt{C}_\mathcal{Y}$ to be the computational basis of the n-qubit space $\mathbb{C}^{2^n}$. Let $\widehat{\mathcal{Y}}$ denote the dual group of $\mathcal{Y}$, consisting of all the group homomorphisms $\widehat{y}(z) := (-1)^{y \cdot z}$.It is well-known that $\widehat{\mathcal{Y}}$ is isomorphic to $\mathcal{Y}$. We assume $\widehat{\mathcal{Y}}$ to be an additive group with the group operation $\widehat{y} + \widehat{z} := \widehat{y \oplus z}$. Naturally, $\widehat{0}$ denotes the identity. For each $\widehat{y} \in \widehat{\mathcal{Y}}$ define

$$|\widehat{y}\rangle := \frac{1}{2^{n/2}} \sum_{z \in \mathcal{Y}} \widehat{y}(z)|z\rangle = \frac{1}{2^{n/2}} \sum_{z \in \mathcal{Y}} (-1)^{y \cdot z}|z\rangle,$$

The set $\mathtt{F}_\mathcal{Y} := \{|\widehat{y}\rangle\}$ is referred as the *Fourier* basis of $\mathbb{C}^{2^n}$, and the mapping $|y\rangle \to |\widehat{y}\rangle$ is the well-known Hadamard transformation that maps the computational basis $\mathtt{C}_\mathcal{Y}$ to Fourier basis $\mathtt{F}_\mathcal{Y}$. The reverse basis transformation from $\mathtt{F}_\mathcal{Y}$ to $\mathtt{C}_\mathcal{Y}$ is given by

$$|y\rangle := \frac{1}{2^{n/2}} \sum_{\widehat{z} \in \widehat{\mathcal{Y}}} \widehat{z}(y)|\widehat{z}\rangle = \frac{1}{2^{n/2}} \sum_{\widehat{z} \in \widehat{\mathcal{Y}}} (-1)^{z \cdot y}|\widehat{z}\rangle.$$

Next, let $\mathcal{Z}$ denote the set $\mathcal{Y} \cup \{\perp\}$ for a special symbol $\perp$; similarly $\widehat{\mathcal{Z}}$ will denote $\widehat{\mathcal{Y}} \cup \{\perp\}$. We also choose a corresponding norm-1 vector $|\perp\rangle$ orthogonal to $\mathbb{C}^{2^n}$, so that the span of both $\mathtt{C}_\mathcal{Z} := \{|y\rangle \mid y \in \mathcal{Z}\}$ and $\mathtt{F}_\mathcal{Z} := \{|\widehat{y}\rangle \mid \widehat{y} \in \widehat{\mathcal{Z}}\}$ is $\mathbb{C}^{2^n+1}$; we'll call $\mathtt{C}_\mathcal{Z}$ and $\mathtt{F}_\mathcal{Z}$ the computational basis and Fourier basis respectively of the extended space $\mathbb{C}^{2^n+1}$.

Functions and Databases. Let $\mathcal{X}$ denote $\{0,1\}^m$ for some arbitrary m, and let $\mathcal{F}$ denote the set of m-bit-to-n-bit classical functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$. The *quantum truth table* of f is defined as

$$|f\rangle := \bigotimes_{x \in \mathcal{X}} |x\rangle|f(x)\rangle.$$

Let $\widehat{\mathcal{F}}$ denote the set of *Fourier* functions $\widehat{f} : \mathcal{X} \longrightarrow \widehat{\mathcal{Y}}$. The quantum truth table of $\widehat{f}$ is defined similarly as

$$|\widehat{f}\rangle := \bigotimes_{x \in \mathcal{X}} |x\rangle|\widehat{f}(x)\rangle.$$

For a subset $\mathcal{S} \subseteq \mathcal{X}$, a function $f : \mathcal{S} \longrightarrow \mathcal{Y}$ will be called a *partial function* from $\mathcal{X}$ to $\mathcal{Y}$. A partial function f can be extended to a function $d_f : \mathcal{X} \longrightarrow \mathcal{Z}$ by defining $d_f(y) = \perp$ for all $y \in \mathcal{X} \setminus \mathcal{S}$. We call d_f the *database* representing f, with $\perp$ denoting the cells where f is not defined. (When f is a full function, d_f coincides with f.) The database will also be represented as a quantum truth table

$$|d_f\rangle := \bigotimes_{x \in \mathcal{X}} |x\rangle|d_f(x)\rangle.$$

Similarly we define partial Fourier functions $\widehat{f} : \mathcal{S} \longrightarrow \widehat{\mathcal{Y}}$, databases $d_{\widehat{f}} : \mathcal{X} \longrightarrow \widehat{\mathcal{Z}}$ representing partial Fourier functions, and their quantum truth tables $|d_{\widehat{f}}\rangle$. When f and $\widehat{f}$ are clear from context, we'll find it convenient to drop the subscripts and write d_f and $d_{\widehat{f}}$ simply as d and $\widehat{d}$ respectively. We'll write $\mathcal{D}$ (resp. $\widehat{\mathcal{D}}$) to denote the set of all databases $d : \mathcal{X} \longrightarrow \mathcal{Z}$ (resp. all Fourier databases $\widehat{d} : \mathcal{X} \longrightarrow \widehat{\mathcal{Z}}$). When convenient we will treat a database d as a relation on $\mathcal{X} \times \mathcal{Y}$ and write $(x, y) \in d$ to denote $d(x) = y$; $|d|$ will then denote the size of this relation, i.e., the size of $\{x \in \mathcal{X} \mid d(x) \in \mathcal{Y}\}$.

For any function $f \in \mathcal{F}$, let $\widehat{f} \in \widehat{\mathcal{F}}$ be defined as the map $x \mapsto \widehat{f(x)}$. Then we have

$$|\widehat{f}\rangle = \frac{1}{2^{n2^m/2}} \sum_{g \in \mathcal{F}} (-1)^{f \cdot g} |g\rangle, \tag{3}$$

where $f \cdot g$ is defined as $\sum_{x \in \mathcal{X}} f(x) \cdot g(x)$. Thus, $\{|f\rangle \mid f \in \mathcal{F}\}$ and $\{|\widehat{f}\rangle \mid \widehat{f} \in \widehat{\mathcal{F}}\}$ span the same space (isomorphic to $\mathbb{C}^{2^{n2^m}}$). Similarly we can show that $\{|d\rangle \mid d \in \mathcal{D}\}$ and $\{|\widehat{d}\rangle \mid \widehat{d} \in \widehat{\mathcal{D}}\}$ span the same space isomorphic to $\mathbb{C}^{(2^n+1)^{2^m}}$; we call this space the *database space* $\mathbb{D}$.

Letting $\mathbf{0}$ denote the constant 0^n function and observing that $\mathbf{0} \cdot g = 0$ for any $g \in \mathcal{F}$, we have

$$|\widehat{\mathbf{0}}\rangle = \frac{1}{2^{n2^m/2}} \sum_{g \in \mathcal{F}} |g\rangle,$$

the uniform superposition over all functions in $\mathcal{F}$.

The Standard Oracle. The *standard oracle* is a stateful oracle with $\mathcal{H}_{db} = \mathbb{C}[\mathcal{F}]$. Given a truth-table representation $|f\rangle$ of a function $f \in \mathcal{F}$, it acts on the adversary registers $|x\rangle|y\rangle$ and the truth-table registers $|f\rangle$ as

$$\mathbf{stO}|x\rangle|y\rangle \otimes |f\rangle = |x\rangle|y \oplus f(x)\rangle \otimes |f\rangle. \tag{4}$$

It is obvious to see that $\mathbf{stO}$ is perfectly indistinguishable with a uniform random function, when the truth table register is initialized in $|\widehat{\mathbf{0}}\rangle$.

If we first put the adversary's response register and the truth-table register in the Fourier basis, we have

$$\mathbf{stO}|x\rangle|\widehat{y}\rangle \otimes |\widehat{f}\rangle = |x\rangle|\widehat{y}\rangle \otimes |\widehat{f} + \widehat{\delta}_{xy}\rangle, \tag{5}$$

where δ_{xy} is the function in $\mathcal{F}$ defined as

$$\delta_{xy}(z) = \begin{cases} y & \text{when } z = x, \\ 0 & \text{otherwise,} \end{cases}$$

and the operations $\oplus$ in $\mathcal{F}$ and $+$ in $\widehat{\mathcal{F}}$ are defined point-wise. We define the operator $\mathbf{O}_{x\widehat{y}}$ on the truth-table register as

$$\mathbf{O}_{x\widehat{y}}|\widehat{f}\rangle := |\widehat{f} + \widehat{\delta}_{xy}\rangle.$$

Then we can write $\mathbf{stO}|x\rangle|\widehat{y}\rangle \otimes |\widehat{f}\rangle = |x\rangle|\widehat{y}\rangle \otimes \mathbf{O}_{x\widehat{y}}|\widehat{f}\rangle$.

The Compressed Oracle. For any $x \in \mathcal{X}$, the *cell compression* unitary $\mathbf{comp}_x$ on $\mathbb{C}^{2^n+1}$ is defined on the basis $\mathtt{F}_{\mathcal{Z}}$ as

$$\mathbf{comp}_x := |\perp\rangle\langle\widehat{0}| + |\widehat{0}\rangle\langle\perp| + \sum_{\widehat{y}\in\widehat{\mathcal{Y}}\setminus\{\widehat{0}\}} |\widehat{y}\rangle\langle\widehat{y}|.$$

The *database compression* unitary $\mathbf{comp}$ on $\mathbb{D}$ is defined as

$$\mathbf{comp} := \bigotimes_{x\in\mathcal{X}} \mathbf{comp}_x.$$

The *compressed oracle* $\mathbf{cO}$ is a stateful oracle with $\mathcal{H}_{db} = \mathbb{D}$. It acts on the adversary's registers and the oracle's database registers as

$$\mathbf{cO} := (\mathbf{I}_{\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\widehat{\mathcal{Y}}]} \otimes \mathbf{comp}) \circ \mathbf{stO} \circ (\mathbf{I}_{\mathbb{C}[\mathcal{X}]\otimes\mathbb{C}[\widehat{\mathcal{Y}}]} \otimes \mathbf{comp}).$$

For a database $\widehat{d}$ we have

$$\mathbf{cO}|x\rangle|\widehat{y}\rangle \otimes |\widehat{d}\rangle = |x\rangle|\widehat{y}\rangle \otimes \mathbf{cO}_{x\widehat{y}}|\widehat{d}\rangle,$$

where $\mathbf{cO}_{x\widehat{y}} := \mathbf{comp}_x \circ \mathbf{O}_{x\widehat{y}} \circ \mathbf{comp}_x$.

3.2 The Two-Domain Distance Technique

Bhaumik et al. distilled [5] the Chung et al. interpretation [12] for indistinguishability setting and proposed a generic way to represent both the ideal and real world oracles using a single compressed permutation oracle. In addition, they combined it with a result from Hosoyamada and Iwata to get a quantum analog of "identical-up to-bad", the so-called two-domain distance lemma.

Domain-Restricted Databases. For a subset $\widetilde{\mathcal{X}}$ of $\mathcal{X}$ we will write $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ to denote the set of databases restricted to $\widetilde{\mathcal{X}}$, defined equivalently as $\{d|_{\widetilde{\mathcal{X}}} \mid d \in \mathcal{D}\}$ or the set of databases $d : \widetilde{\mathcal{X}} \longrightarrow \mathcal{Z}$. Since $\mathcal{D}$ is a basis of the database space $\mathbb{D}$, a domain-restricted database space will span a subspace of $\mathbb{D}$ isomorphic to $\mathbb{C}^{(2^n+1)^{|\widetilde{\mathcal{X}}|}}$. We continue to represent elements of $\widetilde{\mathcal{X}}$ as m-bit numbers.

Transition Capacity. For a domain-restricted database-set $\mathcal{D}|_{\widetilde{\mathcal{X}}}$, a subset $\mathcal{P} \subseteq \mathcal{D}|_{\widetilde{\mathcal{X}}}$ will be called a *database property* on $\mathcal{D}|_{\widetilde{\mathcal{X}}}$. We also define the projection

$$\Pi_{\mathcal{P}} := \sum_{d\in\mathcal{P}} |d\rangle\langle d|.$$

For a database $d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}$ and an $x \in \widetilde{\mathcal{X}}$ define

$$d|^x := \{d' \in \mathcal{D}|_{\widetilde{\mathcal{X}}} \mid d'(x') = d(x')\forall x' \in \widetilde{\mathcal{X}} \setminus \{x\}\}.$$

In other words, $d|^x$ is the set of databases in $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ which are identical to d except (possibly) at x. (Note that since d (resp. x) is also in $\mathcal{D}$ (resp. $\mathcal{X}$), $d|^x$ is only

well-defined when we specify $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ as well; however, since $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ will usually be clear from the context, for notational convenience we leave the dependence of $d|^x$ on $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ implicit.)

For two properties $\mathcal{P}$ and $\mathcal{P}'$, the *transition capacity* from $\mathcal{P}$ to $\mathcal{P}'$ is defined as

$$[\![\mathcal{P} \hookrightarrow \mathcal{P}']\!] := \max_{x \in \widetilde{\mathcal{X}}, \widehat{y} \in \widehat{\mathcal{Y}}, d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \|\Pi_{\mathcal{P}' \cap d|^x} \circ \mathbf{cO}_{x\widehat{y}} \circ \Pi_{\mathcal{P} \cap d|^x}\|.$$

The transition capacity $[\![\mathcal{P} \hookrightarrow \mathcal{P}']\!]$ is roughly a measure of an upper bound for how likely it can be that a database in $\mathcal{P}$ will transition into a database in $\mathcal{P}'$ after a single query to $\mathbf{cO}$.

For a property $\mathcal{P} \subseteq \mathcal{D}|_{\widetilde{\mathcal{X}}}$, let $\mathcal{P}^c$ denote its negation, i.e., $\mathcal{D}|_{\widetilde{\mathcal{X}}} \setminus \mathcal{P}$. Then we have the following lemma from [5, Transition Capacity Bound].

Lemma 1. *Let $\mathcal{P}, \mathcal{P}'$ be properties on $\mathcal{D}|_{\widetilde{\mathcal{X}}}$ such that for every $x \in \widetilde{\mathcal{X}}$ and $d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}$, we can find a set $\mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'} \subseteq \mathcal{Y}$ satisfying*

$$\mathcal{P}' \cap d|^x \subseteq \{d' \in d|^x \mid d'(x) \in \mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'}\} \subseteq \mathcal{P} \cap d|^x. \tag{6}$$

In other words, for any database $d' \in d|^x$,

$$d' \in \mathcal{P}' \implies d'(x) \in \mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'} \implies d' \in \mathcal{P}.$$

Then we have

$$[\![\mathcal{P}^c \hookrightarrow \mathcal{P}']\!] \leq \max_{x \in \widetilde{\mathcal{X}}, d \in \mathcal{D}|_{\widetilde{\mathcal{X}}}} \sqrt{\frac{10|\mathcal{S}_{x,d}^{\mathcal{P}^c \hookrightarrow \mathcal{P}'}|}{2^n}}.$$

Size-restricted Properties. For a domain-restricted database-set $\mathcal{D}|_{\widetilde{\mathcal{X}}}$, a property $\mathcal{P} \subseteq \mathcal{D}|_{\widetilde{\mathcal{X}}}$, and some $i \leq |\widetilde{\mathcal{X}}|$, we define

$$\mathcal{P}_{[\leq i]} := \{d \in \mathcal{P} \mid |d| \leq i\}.$$

Then the transition capacity $[\![\mathcal{P}^c_{[\leq i-1]} \hookrightarrow \mathcal{P}_{[\leq i]}]\!]$ is a measure of the maximum probability of a database outside $\mathcal{P}$ with at most $i-1$ entries changing to a database in $\mathcal{P}$ after a single application $\mathbf{cO}_{x\widehat{y}}$. (Note that $\mathcal{P}^c_{[\leq i-1]}$ denotes the size-restriction of $\mathcal{P}^c$, and not the complement of $\mathcal{P}_{[\leq i-1]}$.)

Let $\bot := \{d_\bot\}$ denote the *empty* property (where $d_\bot$ is the empty database, i.e., the constant-$\bot$ function). Then for $\mathcal{P}$ such that $d_\bot \notin \mathcal{P}$, $\bot = \mathcal{P}^c_{[\leq 0]}$. We define

$$\left(\bot \overset{q}{\rightsquigarrow} \mathcal{P}\right) := \sum_{i=1}^{q} [\![\mathcal{P}^c_{[\leq i-1]} \hookrightarrow \mathcal{P}_{[\leq i]}]\!],$$

the *q-query transition bound* from $\bot$ to $\mathcal{P}$. In other words, $\left(\bot \overset{q}{\rightsquigarrow} \mathcal{P}\right)$ is a measure of the probability that the empty database changes into a database in $\mathcal{P}$ *at any point* during q successive queries.

Prefixed Oracle. Fix some $t < m$ and write $\mathcal{X} = \mathcal{T} \times \mathcal{I}$, where $\mathcal{T} = \{0,1\}^{\lceil \log_2 t \rceil}$ and $\mathcal{I} = \{0,1\}^{m - \lceil \log_2 t \rceil}$. Any family of functions $\mathbf{p} = (\mathbf{p}_k : \mathcal{I} \to \mathcal{X})_{k \in [t]}$ is said to be a (t,m)-*domain-separator* if for all $(k,x) \in [t] \times \mathcal{I}$, $\mathbf{p}_k(x) \in \mathcal{I}_k$, where $\mathcal{I}_k = \{\langle k \rangle_{\lceil \log_2 t \rceil} \parallel x : x \in \mathcal{I}\}$. We write $\mathbf{p}_k(\mathcal{I})$ and $\mathbf{p}(\mathcal{I})$ to denote $\{\mathbf{p}_k(x) : x \in \mathcal{I}\}$ and $\cup_{k \in [t]} \mathbf{p}_k(\mathcal{I})$, respectively.

For any (t,m)-domain-separator $\mathbf{p}$, the *prefixed-compressed oracle* $\mathbf{cO}^{\mathbf{p}}$ is defined as a family of oracles $\{\mathbf{cO}^{\mathbf{p}_k}\}_{k \in [t]}$, where $\mathbf{cO}^{\mathbf{p}_k}$ denotes the restriction of $\mathbf{cO}$ to inputs from $\widetilde{\mathcal{X}} := \mathbf{p}(\mathcal{I}) \subset \mathcal{X}$, i.e., for some $k \in [t]$, $x \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$ and $\widehat{d} \in \widehat{\mathcal{D}}$, we have

$$\mathbf{cO}^{\mathbf{p}_k} |x\rangle |\widehat{y}\rangle \otimes |\widehat{d}\rangle = |\mathbf{p}_k(x)\rangle |\widehat{y}\rangle \otimes \mathbf{cO}^{\mathbf{p}_k}_{x\widehat{y}} |\widehat{d}\rangle,$$

where $\mathbf{cO}^{\mathbf{p}_k}_{x\widehat{y}} := \mathbf{comp}_{\mathbf{p}_k(x)} \circ \mathbf{O}_{\mathbf{p}_k(x)\widehat{y}} \circ \mathbf{comp}_{\mathbf{p}_k(x)}$.

Two-Domain Systems. Let $\mathbf{I}$ and $\mathbf{R}$ be two stateful oracles with $\mathcal{H}_{in} = \mathbb{C}[\mathcal{I}]$, $\mathcal{H}_{out} = \mathbb{C}[\mathcal{Z}]$, $\mathcal{H}_{db} = \mathbb{D}$, defined by the sequences of unitaries:

$$\mathbf{I} := \mathbf{F}_t \mathbf{cO}^{\mathbf{I}_t} \dots \mathbf{cO}^{\mathbf{I}_1} \mathbf{F}_0, \qquad \mathbf{R} := \mathbf{F}_t \mathbf{cO}^{\mathbf{R}_t} \dots \mathbf{cO}^{\mathbf{R}_1} \mathbf{F}_0,$$

where with a slight abuse of notations we reuse $\mathbf{I}$ and $\mathbf{R}$ to also denote the corresponding (t,m)-domain-separators, and the unitaries $\mathbf{F}_0, \dots, \mathbf{F}_t$ only operate on the input, output and ancillary qubits, if any, needed to compute the function itself. However, we continue ignoring the ancillary qubits whenever convenient.

Consider a q-query interactive game where a computationally unbounded and deterministic distinguisher A aims to distinguish $\mathbf{R}$ from $\mathbf{I}$. We emphasize that in such an interactive game with $\mathbf{I}$ or $\mathbf{R}$, the compressed oracle $\mathbf{cO}$ is invoked a total of $q' := kq$ times. Fix two domains $\widetilde{\mathcal{X}}_{\mathbf{I}} = \mathbf{I}(\mathcal{I})$, $\widetilde{\mathcal{X}}_{\mathbf{R}} = \mathbf{R}(\mathcal{I})$, and define $\mathcal{D}_{\mathbf{I}} := \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathbf{I}}}$ and $\mathcal{D}_{\mathbf{R}} := \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathbf{R}}}$. Consider properties $\mathcal{B}_{\mathbf{I}} \subseteq \mathcal{D}_{\mathbf{I}} \setminus \perp$ and $\mathcal{B}_{\mathbf{R}} \subseteq \mathcal{D}_{\mathbf{R}} \setminus \perp$, and define $\mathcal{G}_{\mathbf{I}} := \mathcal{D}_{\mathbf{I}} \setminus \mathcal{B}_{\mathbf{I}}$ and $\mathcal{G}_{\mathbf{R}} := \mathcal{D}_{\mathbf{R}} \setminus \mathcal{B}_{\mathbf{R}}$. The central tool of our security proofs will be the following adaptation of [5, Lemma 4]. A proof of this lemma is available in Appendix B.

Lemma 2 (Two-Domain Distance Lemma). *Suppose we can find a map $h : \mathcal{G}_{\mathbf{I}} \longrightarrow \mathcal{G}_{\mathbf{R}}$ such that the following hold:*

- *h is a bijection from $\mathcal{G}_{\mathbf{I}}$ to $\mathcal{G}_{\mathbf{R}}$;*
- *For every $i \in [q'] \cup \{0\}$, $h|_{\mathcal{G}_{\mathbf{I}[\le i]}}$ is a bijection from $\mathcal{G}_{\mathbf{I}[\le i]}$ to $\mathcal{G}_{\mathbf{R}[\le i]}$;*
- *For every $i \in [q']$, $x \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$, $d \in \mathcal{G}_{\mathbf{I}[\le i-1]}$, and $d' \in \mathcal{G}_{\mathbf{I}[\le i]}$,*

$$\langle d' \,|\, \mathbf{cO}^{\mathbf{I}_k}_{x\widehat{y}} \,|\, d \rangle = \langle h(d') \,|\, \mathbf{cO}^{\mathbf{R}_k}_{x\widehat{y}} \,|\, h(d) \rangle.$$

where $k = t$ if $i = 0 \bmod t$, and $k = i \bmod t$ otherwise.

Then, we have

$$\|\mathsf{Tr}_{\mathbb{D}}(\rho^q_{A,\mathbf{I}}) - \mathsf{Tr}_{\mathbb{D}}(\rho^q_{A,\mathbf{R}})\|_1 \le 3\left(\perp \overset{q'}{\rightsquigarrow} \mathcal{B}_{\mathbf{I}}\right)_{\mathbf{I}} + 3\left(\perp \overset{q'}{\rightsquigarrow} \mathcal{B}_{\mathbf{R}}\right)_{\mathbf{R}},$$

where $\rho^q_{A,\mathbf{p}} := A^{\mathbf{p}}|\psi_A, d_\perp\rangle\langle\psi_A, d_\perp|A^{\mathbf{p}\dagger}$ *is the state after* q *queries to the oracle at-hand* $\mathbf{p} \in \{\mathbf{I}, \mathbf{R}\}$ *for some norm-1 vector* $|\psi_A\rangle$ *and the empty database* $|d_\perp\rangle$. *The transition bounds* $\left(\perp \overset{q'}{\rightsquigarrow} \cdot\right)_{\mathbf{I}}$ *and* $\left(\perp \overset{q'}{\rightsquigarrow} \cdot\right)_{\mathbf{R}}$ *are computed for queries to* $\mathbf{cO}^{\mathbf{I}}$ *and* $\mathbf{cO}^{\mathbf{R}}$, *respectively.*

When the oracle in use is clear from the context, we will drop the subscripts for the transition bounds and simply write both as $\left(\perp \overset{q'}{\rightsquigarrow} \cdot\right)$. We'll also keep the domain-separator implicit when there's no scope for ambiguity.

3.3 The Hosoyamada-Iwata Interpretation

Hosoyamada and Iwata proposed a slightly different variant of **stO** with an aim to characterize and analyze databases in an explicit computational basis with an exact definition of $\perp$ with the help of an ancillary flag bit that signifies if the database entry is defined or not.

Let $\mathcal{S} \subseteq \mathcal{X}$ and $\mathcal{Z} = \{0,1\} \times \mathcal{Y}$. For any partial function $f : \mathcal{S} \to \mathcal{Y}$, we associate the database function $d_f : \mathcal{X} \to \mathcal{Z}$ defined as:

$$d_f(x) := \begin{cases} (1, y) & \text{when } f(x) = y \in \mathcal{Y}, \\ (0, 0^n) & \text{if } f(x) \text{ is undefined,} \end{cases}$$

On comparing this with Zhandry's original interpretation, we see that the $\perp$ in original interpretation corresponds to $(0, 0^n)$ in HI interpretation. As before, we drop the subscripts when f is either clear from the context or inconsequential.

We define the database space as the $2^{(n+1)2^m}$-dimensional complex Hilbert space $\mathcal{H}_{db} = \mathbb{C}[\mathcal{Z}]$ which is isomorphic to $\mathbb{C}^{2^{(n+1)2^m}}$. Note that not all $d \in \mathcal{Z}$ can be associated with some partial function f. A database $d = ((b_0, \beta_0), \ldots, (b_{2^m-1}, \beta_{2^m-1}))$ is said to be *valid* if it satisfies that for each $i \in \{0, 1, \ldots, 2^m - 1\}$ such that $b_i = 0$ we have $\beta_i = 0^n$. Indeed, any valid database $((b_0, \beta_0), \ldots, (b_{2^m-1}, \beta_{2^m-1}))$ is identified with the set $\{(i, \beta_i) \mid b_i = 1\}$, which is nothing but the truth table of a partially-defined function from $\{0,1\}^m$ to $\{0,1\}^n$. Accordingly, let Π_{valid} be the orthogonal projection onto the vector space spanned by valid databases.

Any database $|d\rangle \in \mathbb{C}[\mathcal{Z}]$ can be equivalently viewed as an array of 2^m cells $|d[0]\rangle \ldots |d[2^m-1]\rangle$. Writing $|d[i]\rangle$ as $|b_i, \beta_i\rangle$ for each $i \in \{0, 1, \ldots, 2^m-1\}$ (where b_i and β_i are respectively the control qubit and the response register of the i-th cell $|d[i]\rangle$ of $|d\rangle$), the standard oracle **stO** is now defined as:

$$\mathbf{stO}|i, y\rangle|d\rangle := |i, y + \beta_i\rangle|d\rangle$$

for each $|i, y, d\rangle \in \mathcal{H}_{in} \times \mathcal{H}_{out} \times \mathcal{H}_{db}$. For $|d\rangle$ such that $|d[i]\rangle = |0, 0^n\rangle$, we define $|d \cup (i, \beta)\rangle$ to be the database with $|1, \beta\rangle$ as its i-th cell and identical to $|d\rangle$ in all other cells.

Define the following unitary operators on database cells:

$$\mathbf{IH}_0 := \mathbf{I}_1 \otimes \mathbf{H}^{\otimes n} \qquad \mathbf{Tg}_0 := \mathbf{I}_1 \otimes |0^n\rangle\langle 0^n| + \mathbf{X}(\mathbf{I}_{2^n} - |0^n\rangle\langle 0^n|)$$

$$\mathbf{cH}_0 := |0\rangle\langle 0| \otimes \mathbf{I}_{2^n} + |1\rangle\langle 1| \otimes \mathbf{H}^{\otimes n}$$

and databases:

$$\mathbf{IH} := \mathbf{IH}_0^{\otimes 2^m} \qquad \mathbf{Tg} := \mathbf{Tg}_0^{\otimes 2^m} \qquad \mathbf{cH} := \mathbf{cH}_0^{\otimes 2^m}$$

where $\mathbf{X}$ and $\mathbf{H}$ are the well-known flip and Hadamard operators on $\mathbb{C}$, i.e. in the computational basis:

$$\mathbf{X} := |0\rangle\langle 1| + |1\rangle\langle 0| \qquad \mathbf{H} := \frac{1}{2}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right)$$

Note that all these operators are Hermitian. Using these, we define the encode and decode operator **dec** on databases as follows:

$$\mathbf{enc} := \mathbf{cH} \circ \mathbf{Tg} \circ \mathbf{IH};$$
$$\mathbf{dec} := \mathbf{enc}^\dagger = \mathbf{IH} \circ \mathbf{Tg} \circ \mathbf{cH};$$

The recording standard oracle **RStOE**, due to Hosoyamada and Iwata [22], is defined as:

$$\mathbf{RStOE} := (\mathbf{I}_{2^{m+n}} \otimes \mathbf{enc})\mathbf{stO}(\mathbf{I}_{2^{m+n}} \otimes \mathbf{dec})$$

Thus, **RStOE** first decodes the database, then applies **stO** on the adversary's registers and the decoded database, and then encodes the database again. Let $|\mathbf{0}\rangle$ denote the valid empty database.

Hosoyamada and Iwata proved [22,24] the following useful propositions.

Proposition 1 (Proposition 1 in [24]). *Suppose that the oracle state is initialized in $|\mathbf{0}\rangle$. For any $i \geq 1$, if the oracle state register is measured after i queries, then the resulting database d is valid, and contains at most i entries.*

Proposition 2 (Proposition 2 in [24]). *For any valid database d satisfying $d[i] = |0, 0^n\rangle$, we have*

$$\mathbf{RStOE}|i, y\rangle|d \cup (i, \beta)\rangle = |i, y \oplus \beta\rangle|d \cup (i, \beta)\rangle + |\epsilon_1\rangle; \tag{7}$$

$$\mathbf{RStOE}|i, y\rangle|d\rangle = \sum_{\beta \in \{0,1\}^n} \frac{1}{2^{n/2}}|i, y \oplus \beta\rangle|d \cup (i, \beta)\rangle + |\epsilon_2\rangle; \tag{8}$$

for some $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$ such that $\||\epsilon_1\rangle\|, \||\epsilon_2\rangle\| \in O(1/\sqrt{2^n})$.

Although we do not require them in this paper, we remark that [22] gives an exact description of $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$. Intuitively, $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$ can be viewed as the errors introduced in the lazy sampling of a quantum random function due to interference.

Finally, the main technical result used to study the indistinguishability game and bound the advantage is given below.

Proposition 3 (Proposition 3 in [24]). *For each $j \in \{0,1,\ldots,q\}$, let $|\mathbb{R}_j\rangle$ and $|\mathbb{I}_j\rangle$ denote the state vector corresponding to the real and ideal worlds after the j-th query, respectively. Suppose, there exist vectors $|\mathbb{R}_j^{\mathsf{g}}\rangle$, $|\mathbb{R}_j^{\mathsf{b}}\rangle$, $|\mathbb{I}_j^{\mathsf{g}}\rangle$, $|\mathbb{I}_j^{\mathsf{b}}\rangle$ and non-negative reals $\epsilon_{\mathbf{I}}^{(j)}$ and $\epsilon_{\mathbf{R}}^{(j)}$ such that*

1. $|\mathbb{R}_j\rangle = |\mathbb{R}_j^{\mathsf{g}}\rangle + |\mathbb{R}_j^{\mathsf{b}}\rangle$, $|\mathbb{I}_j\rangle = |\mathbb{I}_j^{\mathsf{g}}\rangle + |\mathbb{I}_j^{\mathsf{b}}\rangle$;
2. $|\mathbb{R}_j^{\mathsf{g}}\rangle\langle\mathbb{R}_j^{\mathsf{g}}| = |\mathbb{I}_j^{\mathsf{g}}\rangle\langle\mathbb{I}_j^{\mathsf{g}}|$;
3. $\||\mathbb{I}_j^{\mathsf{b}}\rangle\| \leq \||\mathbb{I}_{j-1}^{\mathsf{b}}\rangle\| + \epsilon_{\mathbf{I}}^{(j)}$, $\||\mathbb{R}_j^{\mathsf{b}}\rangle\| \leq \||\mathbb{R}_{j-1}^{\mathsf{b}}\rangle\| + \epsilon_{\mathbf{R}}^{(j)}$.

Then, for any computationally unbounded and deterministic distinguisher A we have $\|\mathsf{Tr}_{\mathcal{H}_{\mathbf{I}_{db}}}(\rho_{A,\mathbf{I}}^q) - \mathsf{Tr}_{\mathcal{H}_{\mathbf{R}_{db}}}(\rho_{A,\mathbf{R}}^q)\|_1 \leq \sum_{i=1}^q \epsilon_{\mathbf{I}}^{(j)} + \sum_{i=1}^q \epsilon_{\mathbf{R}}^{(j)}$, where $\rho_{A,\mathbf{R}}^q = |\psi_A\rangle\langle\psi_A| \otimes |\mathbf{0_R}\rangle\langle\mathbf{0_R}|$ and $\rho_{A,\mathbf{I}}^q = |\psi_A\rangle\langle\psi_A| \otimes |\mathbf{0_I}\rangle\langle\mathbf{0_I}|$ for some norm-1 vector $\psi_A \in \mathcal{H}_A$ and $|\mathbf{0_R}\rangle$ and $|\mathbf{0_I}\rangle$ denote the all zero database states in the real and ideal worlds respectively.

4 Revisiting IND-qCPA Security of LR_4

4.1 The Luby-Rackoff Construction

For some $r \geq 1$ and $f_1,\ldots,f_r : \{0,1\}^n \to \{0,1\}^n$, we define $g : [r] \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ by the mapping:

$$(i, x_1, x_2) \longmapsto (x_2 \oplus f_i(x_1), x_1),$$

and write $g_i(\cdot,\cdot) := g(i,\cdot,\cdot)$. The r-round Luby-Rackoff construction, denoted LR_r is defined as:

$$(x_1, x_2) \longmapsto g_r \circ \cdots \circ g_1(x_1, x_2). \tag{9}$$

For all $i \in [r]$, we write (also see Fig. 1):

- $x^{i-1} := (x_1^{i-1}, x_2^{i-1})$ to denote the input to g_i, where $x^0 := x = (x_1, x_2)$, denotes the input to LR_r.
- (u_i, v_i) to denote the input-output tuple corresponding to f_i.
- $y = (y_1, y_2) := (x_1^r, x_2^r)$ to denote the output of LR_r.

Hosoyamada and Iwata stated [22] the following IND-qCPA security bound for LR_4.

Theorem 1 (Theorem 3 in [22]). *Suppose $f_1, f_2, f_3, f_4 : \{0,1\}^n \to \{0,1\}^n$ are four mutually independent uniform random functions. Then, for any $q \geq 0$, and any quantum adversary A that makes at most q CPA queries, we have*

$$\mathbf{Adv}_{\mathsf{LR}_4}^{\mathsf{qcpa}}(A) = O\left(\sqrt{\frac{q^3}{2^n}}\right).$$

The proof of this theorem uses the HI interpretation of Zhandry's compressed oracle, the so-called **RStOE**. The high level proof approach is as follows:

1. Simulate the random functions f_1, f_2, f_3, f_4 using independent instances of **RStOE** with the corresponding databases, d_1, d_2, $d_{\mathbf{R}}$, d_4, respectively.
2. The authors then apply a series of hybrids, introducing intermediate constructions between the real construction LR_4, and the ideal construction, a uniform random function $\Gamma : \{0,1\}^{2n} \to \{0,1\}^{2n}$. The first of these intermediate constructions is a length-preserving function, that we refer as $\widetilde{\mathsf{LR}_4}$, defined by the mapping (see also Fig. 1):
$$(x_1, x_2) \mapsto g_4 \circ G_3 \circ g_2 \circ g_1(x_1, x_2), \tag{10}$$
where $G_3(x_1', x_2') := (F_3(x_1', x_2'), x_1')$ for all $(x_1', x_2') \in \{0,1\}^{2n}$. The function $F_3 : \{0,1\}^{2n} \to \{0,1\}^n$ is a uniform random function, to be implemented by an appropriate **RStOE**, say $d_{\mathbf{I}}$.
In this note, we will solely focus on the distance between LR_4 and $\widetilde{\mathsf{LR}_4}$. In fact, showing a negligible distance between the two systems is the technical core of the proof. For the discussion in this paper, it is sufficient to consider the chopped output x_1^3. So, we drop the application of f_4. We write $d^{\mathbf{R}} = (d_1, d_2, d_{\mathbf{R}})$ and $d^{\mathbf{I}} = (d_1, d_2, d_{\mathbf{I}})$.
3. In a bid to use Proposition 3 to bound the advantage, the authors iteratively apply Proposition 2 to study the action of each of f_1, f_2, f_3 (only in the real world), and F_3 (only in the ideal world) in that order, followed by the respective uncomputation steps for f_2 and f_1 in that order.
4. The key idea in the proof is the observation that LR_4 and $\widetilde{\mathsf{LR}_4}$ are indistinguishable as long as the inputs to f_3 (res. F_3 in the ideal world) are pairwise distinct across all queries, i.e., the database triple $d^{\mathbf{R}} = (d_1, d_2, d_{\mathbf{R}})$ (res. $d^{\mathbf{I}} = (d_1, d_2, d_{\mathbf{I}})$ in the ideal world) is considered to be *good* if and only if there does not exists distinct database entries $(u_1, v_1), (u_1', v_1') \in d_1$, $(u_2, v_2), (u_2', v_2') \in d_2$, and $(u_3, v_3) \in d_{\mathbf{R}}$ (res. $(u_3, x_2^2, v_3) \in d_{\mathbf{I}}$ in the real world) such that $u_1 \oplus v_2 = u_1' \oplus v_2' = u_3'$. All other database triples are considered *bad*. Let Π_{bad} denote the projection onto the space spanned by bad databases. A key property of good database triples is the fact that they enable a one-to-one correspondence $d^{\mathbf{R}} \mapsto [d^{\mathbf{R}}]_{\mathbf{I}}$ between the real and ideal databases, i.e., the two worlds can be easily shown to behave identically when the databases remain good throughout the execution. Thus, by setting $|\mathbb{R}_j^{\mathsf{b}}\rangle = \Pi_{bad}|\mathbb{R}_j\rangle$, $|\mathbb{R}_j^{\mathsf{g}}\rangle = |\mathbb{R}_j\rangle - |\mathbb{R}_j^{\mathsf{b}}\rangle$, $|\mathbb{I}_j^{\mathsf{b}}\rangle = \Pi_{bad}|\mathbb{I}_j\rangle$, and $|\mathbb{I}_j^{\mathsf{g}}\rangle = |\mathbb{I}_j\rangle - |\mathbb{I}_j^{\mathsf{b}}\rangle$, we satisfy condition 1 and 2 in Proposition 3.
Now, all that remains is to study the action of each function call, and bound the norm of the bad vectors after each application, assuming that the state is spanned by good databases before the action. In particular, we concentrate on the application of f_1 in the next section, uncovering a flaw in the argumentation that breaks the proof.

4.2 Action of f_1 and the Trivialization of Norm

For any unit vector $|\psi\rangle$ and an arbitrary projection operator Π, we say that $\|\Pi|\psi\rangle\|$ is *trivially bounded* when we simply use the fact that $\|\Pi|\psi\rangle\| \leq 1$.

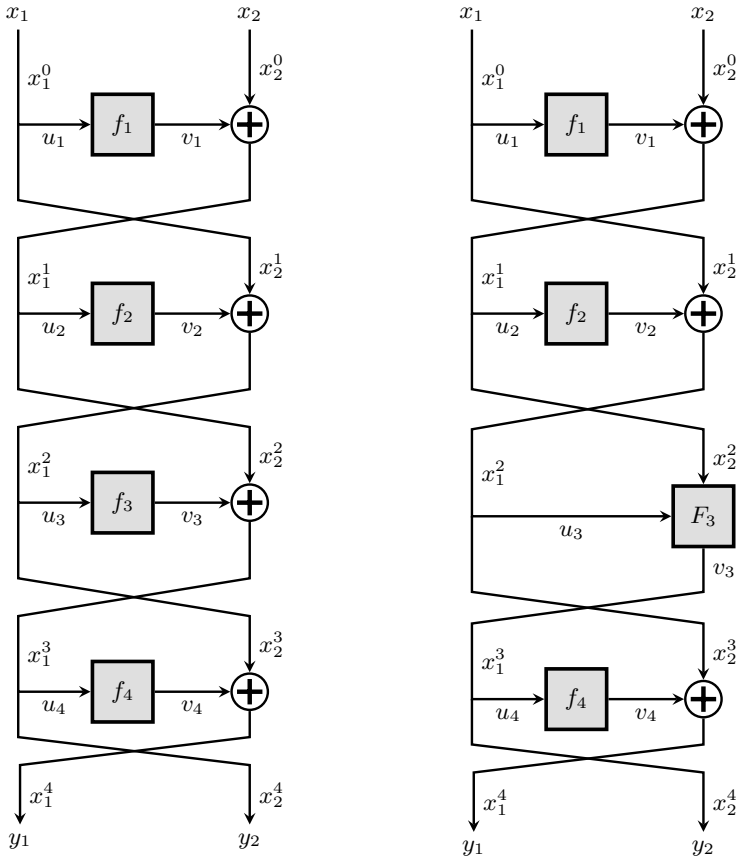

Fig. 1. 4-round Luby-Rackoff (left) and 4-round Luby-Rackoff with a BIG function (right).

We will study the action in the ideal world, although the same issue lies in the real world application as well. For brevity we assume that the output of f_1 is written on some ancillary register to be used in later actions. By a recursive application of Proposition 2, there exists vectors $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$ such that

$$\begin{aligned}\mathbf{O}_{f_1}|\mathbb{I}^{\mathbf{g}}_{j-1}\rangle := &\sum_{\substack{x,y,z,d^{\mathbf{I}}\\ d^{\mathbf{I}}:\mathsf{good}\\ d_1(x_1)\neq\perp}} \alpha^{(j-1)}_{x,y,z,d^{\mathbf{I}}}|x,y,z\rangle\otimes|d_1(x_1)\rangle\otimes|d^{\mathbf{I}}\rangle\\ &+\sum_{\substack{x,y,z,\beta,d^{\mathbf{I}}\\ d^{\mathbf{I}}:\mathsf{good}\\ d_1(x_1)=\perp}} \frac{\alpha^{(j-1)}_{x,y,z,d^{\mathbf{I}}}}{2^{n/2}}|x,y,z\rangle\otimes|\beta\rangle\otimes|d^{\mathbf{I}}\cup(x_1,\beta)_1\rangle\\ &+|\epsilon_1\rangle+|\epsilon_2\rangle,\end{aligned}$$

where $|d^{\mathbf{I}} \cup (x_1, \beta)_1\rangle = |d_1 \cup (x_1, \beta)\rangle \otimes |d_2\rangle \otimes |d_{\mathbf{I}}\rangle$ denotes the database that is same as $|d^{\mathbf{I}}\rangle$ except for $d_1(x_1)$ which has been newly defined as β.

In this note we are only concerned with the second summand, denoted $|\mathbb{I}_j^{g,1}\rangle$, which gives the state transition on a fresh input to f_1 starting with a good state. Roughly speaking, a new entry (x_1, β) is recorded in d_1 at the cost of an amplitude factor of $2^{-n/2}$.

Formally, we are interested in the following norm, which is an equivalent representation of [22, (51)]:

$$\|\Pi_{bad}|\mathbb{I}_j^{g,1}\rangle\|^2 = \Big\| \sum_{\substack{x,y,z,\beta,d^{\mathbf{I}} \\ d^{\mathbf{I}}:\mathsf{good} \\ d_1(x_1)=\perp \\ d^{\mathbf{I}}\cup(x_1,\beta)_1:\mathsf{bad}}} \frac{\alpha^{(j-1)}_{x,y,z,d^{\mathbf{I}}}}{2^{n/2}} |x,y,z\rangle \otimes |\beta\rangle \otimes |d^{\mathbf{I}} \cup (x_1,\beta)_1\rangle \Big\|^2$$

$$= \sum_{\substack{x,y,z,\beta,d^{\mathbf{I}} \\ d^{\mathbf{I}}:\mathsf{good} \\ d_1(x_1)=\perp \\ d^{\mathbf{I}}\cup(x_1,\beta)_1:\mathsf{bad}}} \left| \frac{\alpha^{(j-1)}_{x,y,z,d^{\mathbf{I}}}}{2^{n/2}} \right|^2 \tag{11}$$

$$= \sum_{\substack{x,y,z,d^{\mathbf{I}} \\ d^{\mathbf{I}}:\mathsf{good} \\ d_1(x_1)=\perp}} \left|\alpha^{(j-1)}_{x,y,z,d^{\mathbf{I}}}\right|^2 \sum_{\substack{\beta \\ d^{\mathbf{I}}\cup(x_1,\beta)_1:\mathsf{bad}}} \frac{1}{2^n} \tag{12}$$

$$\leq O\left(\frac{j}{2^n}\right) \sum_{\substack{x,y,z,d^{\mathbf{I}} \\ d^{\mathbf{I}}:\mathsf{good} \\ d_1(x_1)=\perp}} \left|\alpha^{(j-1)}_{x,y,z,d^{\mathbf{I}}}\right|^2 \tag{13}$$

$$\leq O\left(\frac{j}{2^n}\right), \tag{14}$$

where (13) to (14) follows from the fact that $\||\mathbb{I}_{j-1}\rangle\| \leq 1$. However, there is no supporting argument in [22] for (12) to (13). In fact, we claim that

$$\sum_{\substack{\beta \\ d^{\mathbf{I}}\cup(x_1,\beta)_1:\mathsf{bad}}} \frac{1}{2^n} = O(1). \tag{15}$$

To bound the summation, we have to estimate the size of the set $\{\beta : d^{\mathbf{I}} \cup (x_2, \beta)_1$ is $\mathsf{bad}\}$. Now, $d^{\mathbf{I}} \cup (x_1, \beta)_1$ is bad if and only if there exists distinct database entries $(u_1', v_1') \in d_1$, $(u_2, v_2), (u_2', v_2') \in d_2$, and $(u_1' \oplus v_2', u_2', v_3') \in d_{\mathbf{I}}$ such that

$$x_1 \oplus v_2 = u_1' \oplus v_2'.$$

Note that, the above predicate is independent of β! Thus, in the worst case, the predicate is true for all possible values of β which immediately establishes the

claim. Once we plug in the bound from (15) in (12), we get

$$\|\Pi_{bad}|\mathbb{I}_j^{g,1}\rangle\|^2 = O(1), \tag{16}$$

which clearly trivializes the norm. This completely breaks the security proof, as this revised bound leads to a trivial bound of O(1) on the PRF advantage.

4.3 Do Additional Rounds Help?

One might think that, while this approach does not work for three rounds, maybe it will if we add more rounds, i.e., by considering r-round Luby-Rackoff for $r \geq 4$. Unfortunately, as we show in this section, the "trivialization of norm" seems to be a fundamental issue. We will argue this further for input collision at f_i for any odd $i \in \{1, \ldots, r\}$. A similar argument can also be given for any even i.

Consider the database snapshot after $j \geq 2$ queries. Suppose, the adversary makes a query (x_1, x_2), such that $d_1(x_1) = \perp$, i.e., the database entry corresponding to x_1 is empty, and a new entry (x_1, β) is to be created. Now, if we have distinct $(u'_1, v'_1) \in d_1$, $(u_2, v_2), (u'_2, v'_2) \in d_2, \ldots, (u_{i-1}, v_{i-1}), (u'_{i-1}, v'_{i-1}) \in d_{i-1}$, $(u'_i, v'_i) \in d_i$, such that

$$\begin{aligned} u'_i &= u'_1 \oplus v'_2 \oplus \cdots \oplus v'_{i-1}, \text{ and} \\ x_1 \oplus v_2 \oplus \cdots \oplus v_{i-1} &= u'_1 \oplus v'_2 \oplus \cdots \oplus v'_{i-1}, \end{aligned}$$

then there is a possibility[4] that this query leads to a collision at the input of f_i. And what's more, this condition is independent[5] of β, and thus, a similar trivialization of norms as in (15) would occur in this case as well, rendering this line of argumentation effectively useless.

5 Non-Adaptive IND-qCPA Security of LR_4

The main reason that the existing Luby-Rackoff proof fails is a lack of global knowledge of adversarial query pattern. At any instant, the compressed oracle only has the information recorded in the database and the current input. Thus, one has to argue as if every possible combination of global inputs are possible which as we showed in Section 4 leads to a trivialization of norm in case of LR_4. At the same time, for several other constructions, like TNT and LRWQ, one can still try to reconstruct a moderately global view to achieve some security bound.

[4] We are obviously overcounting by considering all possible combinations of queries. In fact, most of these combinations are never queried by the adversary. However, as of now, there is no effective way to find out the query ordering from database entries.

[5] This independence only holds corresponding to the badness condition. In a typical execution of LR_r, these variables will obviously depend on β. However, due to the badness condition and the ignorance of query ordering (see the above point), this dependence is lost.

The Dummy Call Idea: In the non-adaptive setting, the adversary makes a single query of the form $x^q = (x_1, \ldots, x_q)$. We can employ a single dummy compressed oracle call to record x^q, and then implement the oracle at-hand. Note that the compressed oracle in both the dummy call and actual oracle evaluation can be implemented by a single compressed oracle using the prefixed oracle technique. More formally, fix some $1 < t < m$ and suppose $\mathbf{O}_f$ denote the stateful oracle corresponding to the function $f : \{0,1\}^m \to \{0,1\}^n$, defined as follows:

$$\mathbf{O} \coloneqq \mathcal{O}_{t-1}\mathbf{cO}^{\mathbf{p}_{t-1}} \ldots \mathbf{cO}^{\mathbf{p}_1}\mathcal{O}_0,$$

where $\mathbf{p}$ is a (t,ℓ)-domain-separator, with $\ell \gg m$. Then, the q-query variant of $\mathbf{O}$ with dummy call is defined to be the sequence

$$(\mathbf{cO}^{\mathbf{p}_t})^\dagger \circ \mathbf{O}^{\otimes q} \circ \mathbf{cO}^{\mathbf{p}_t},$$

where the database space is $\mathbb{D} = \mathbb{C}^{(2^n+1)^{2^\ell}}$, with $\ell \geq mq + \lceil \log_2 t \rceil$. In other words, we enclose the original non-adaptive oracle between two compressed oracle calls, which record and erase the global input $(x^q, \widehat{y}^q)$. Note that erasing the dummy call entries is crucial; otherwise, this perturbs the state.

In what follows, we assume the actions of the dummy call are implicit and do not analyze them explicitly. Consequently, we will often focus only on the relevant subspace of the database used in the other actions.

We prove the following IND-qNCPA bound for LR_4.

Theorem 2. *Suppose $f_1, f_2, f_3, f_4 : \{0,1\}^n \to \{0,1\}^n$ are three mutually independent uniform random functions. Then, for any $q \geq 0$, and any quantum adversary $\mathscr{A}$ that makes at most q qNCPA queries, we have*

$$\mathbf{Adv}^{\mathsf{qncpa}}_{\mathsf{LR}_4}(\mathscr{A}) = 3\sqrt{\frac{q^6}{2^n}} + 6\sqrt{\frac{q^5}{2^n}}.$$

Proof. Our goal is to bound the distinguishing advantage for any non-adaptive adversary trying to distinguish LR_4 from a uniform random function. First, let $F_3, F_4 : \{0,1\}^{3n} \to \{0,1\}^n$ be two uniform random functions. For $i \in \{3,4\}$, define

$$G_i(x_1, x_2, x_1', x_2') \coloneqq (x_2' \oplus F_i(x_1, x_2, x_1'), x_1'),$$

for any $(x_1, x_2, x_1', x_2') \in \{0,1\}^{4n}$. We define the hybrid random function $\widetilde{\mathsf{LR}}_4$ as (see also Fig. 2):

$$\widetilde{\mathsf{LR}}_4(x_1, x_2) \coloneqq G_4(x_1, x_2, G_3(x_1, x_2, \mathsf{LR}_2(x_1, x_2))).$$

Then, it is easy to see that $\widetilde{\mathsf{LR}}_4$ is indistinguishable to a uniform random function $\Gamma : \{0,1\}^{2n} \to \{0,1\}^{2n}$. So, it is sufficient to bound the distance between LR_4 and $\widetilde{\mathsf{LR}}_4$. Let $\mathcal{X} = \{0,1\}^{4+2nq}$, $\mathcal{Y} = \{0,1\}^n$ and $\Gamma : \mathcal{X} \to \mathcal{Y}$ be a uniform random function. For each $x_1, x_2, x_3 \in \{0,1\}^n$, we define

$$f_1(x_1) \coloneqq \Gamma(1001 \| x_1 \| 0^{2nq-n})$$

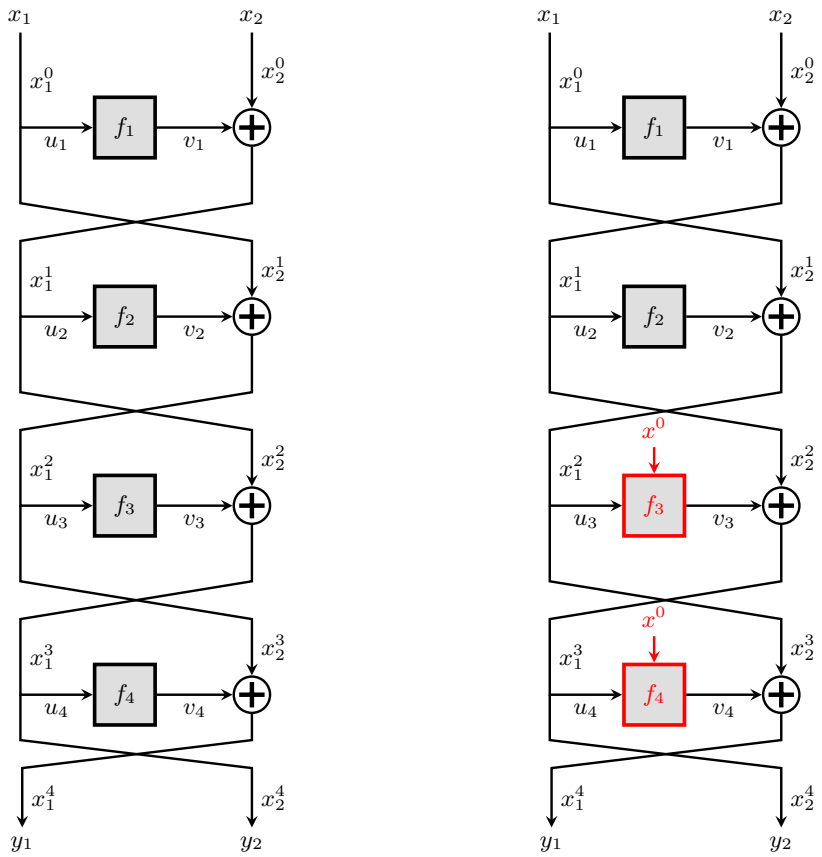

Fig. 2. LR_4 (left) vs the hybrid random function, $\widetilde{\mathsf{LR}}_4$ (right).

$$
\begin{aligned}
f_2(x_1) &\coloneqq \Gamma(1010 \| x_1 \| 0^{2nq-n}) \\
f_3(x_1) &\coloneqq \Gamma(1011 \| x_1 \| 0^{2nq-n}) \\
f_4(x_1) &\coloneqq \Gamma(1100 \| x_1 \| 0^{2nq-n}) \\
F_3(x_1, x_2, x_3) &\coloneqq \Gamma(1101 \| x_1 \| x_2 \| x_3 \| 0^{2nq-3n}) \\
F_4(x_1, x_2, x_3) &\coloneqq \Gamma(1110 \| x_1 \| x_2 \| x_3 \| 0^{2nq-3n})
\end{aligned}
$$

In addition, we implicitly define the dummy call, denoted dummy, to operate over a disjoint[6] subspace of the database, mapping $2qn$-bit inputs to n-bit outputs. The exact description of the dummy call is not necessary as the output is never used.

The distinctness of the first four bits ensures that $f_1, f_2, f_3, f_4, F_3, F_4$ are all independent, and they are independent of dummy by definition.

[6] Disjoint from the other functions due to the first bit.

The database in the real world is denoted $d_{\mathbf{R}}$ (tracking dummy, f_1, f_2, f_3, f_4) and $d_{\mathbf{I}}$ in the ideal world (tracking dummy, f_1, f_2, F_3, F_4). Let $\mathcal{D}_{\mathbf{R}}$ (resp. $\mathcal{D}_{\mathbf{I}}$) be the set of all possible choices for $d_{\mathbf{R}}$ (resp. $d_{\mathbf{I}}$).
For some $x = (x_1, x_2, \ldots, x_{2q}) \in \mathcal{Y}^{2q}$, let

$$\begin{aligned} [x]_0 &\coloneqq 0000\|x & [x_1]_1 &\coloneqq 1001\|x_1\|0^{2nq-n} \\ [x_1,x_2,x_3]_5 &\coloneqq 1101\|x_1\|x_2\|x_3\|0^{2nq-3n} & [x_1]_2 &\coloneqq 1010\|x_1\|0^{2nq-n} \\ [x_1,x_2,x_3]_6 &\coloneqq 1110\|x_1\|x_2\|x_3\|0^{2nq-3n} & [x_1]_3 &\coloneqq 1011\|x_1\|0^{2nq-n} \\ & & [x_1]_4 &\coloneqq 1100\|x_1\|0^{2nq-n} \end{aligned}$$

In addition, for all $k \in [q]$, we write $[x_{2k-1}, x_{2k}]_{0\|k}$ to denote the k-th diblock coordinate (x_{2k-1}, x_{2k}) of x. We will mostly use this view, and thus, view the $2qn$-bit entry as q separate entries of size $2n$-bit each, and thus, $d_{\mathbf{R}}([x_{2k-1}, x_{2k}]_{0\|k}) \neq \perp$ (or $d_{\mathbf{I}}([x_{2k-1}, x_{2k}]_{0\|k}) \neq \perp$) is well-defined as long as $d_{\mathbf{R}}([x]_0) \neq \perp$ (res. $d_{\mathbf{I}}([x]_0) \neq \perp$ for some $x = (z, (x_{2k-1}, x_{2k}), z')$ where z and z' are $2(k-1)n$-bit and $2(q-k)n$-bit strings.
Define

$$\begin{aligned} \widetilde{\mathcal{X}}_{\mathbf{R}} &\coloneqq \{[x]_0, [x_1]_1, [x_1]_2, [x_1]_3, [x_1]_4 : x = (x_1, \ldots, x_{2q}) \in \mathcal{Y}^{2q}\} \\ \widetilde{\mathcal{X}}_{\mathbf{I}} &\coloneqq \{[x]_0, [x_1]_1, [x_1]_2, [x_1,x_2,x_3]_5, [x_1,x_2,x_3]_6 : x = (x_1, \ldots, x_{2q}) \in \mathcal{Y}^{2q}\} \end{aligned}$$

Then it is easy to see that $\mathcal{D}_{\mathbf{R}} = \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathbf{R}}}$ and $\mathcal{D}_{\mathbf{I}} = \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathbf{I}}}$.

5.1 Bad and Good Databases

Let $\mathcal{B}_{\mathbf{R}}$ be the set of databases $d_{\mathbf{R}}$ satisfying one of the following condition: we can find $(x_1, x_2) \neq (x_1', x_2') \in \mathcal{Y}^2$ and $v_1, v_2, v_1', v_2' \in \mathcal{Y}$ such that

- for some $k \notin k' \in [q]$, $d_{\mathbf{R}}([x_1, x_2]_{0\|k}) \neq \perp, d_{\mathbf{R}}([x_1', x_2']_{0\|k'}) \neq \perp$;
- $([x_1]_1, v_1), ([x_1']_1, v_1) \in d_{\mathbf{R}}$;
- $([x_2 \oplus v_1]_2, v_2), ([x_2' \oplus v_1']_2, v_2') \in d_{\mathbf{R}}$;
- $x_1 \oplus v_2 = x_1' \oplus v_2'$;

or we can find $(x_1, x_2) \neq (x_1', x_2') \in \mathcal{Y}^2$ and $v_1, v_2, v_3, v_1', v_2', v_3' \in \mathcal{Y}$ such that

- for some $k \notin k' \in [q]$, $d_{\mathbf{R}}([x_1, x_2]_{0\|k}) \neq \perp, d_{\mathbf{R}}([x_1', x_2']_{0\|k'}) \neq \perp$;
- $([x_1]_1, v_1), ([x_1']_1, v_1) \in d_{\mathbf{R}}$;
- $([x_2 \oplus v_1]_2, v_2), ([x_2' \oplus v_1']_2, v_2') \in d_{\mathbf{R}}$;
- $([x_1 \oplus v_2]_3, v_3), ([x_1' \oplus v_2']_3, v_3) \in d_{\mathbf{R}}$;
- $x_2 \oplus v_1 \oplus v_3 = x_2' \oplus v_1' \oplus v_3'$;

Next, let $\mathcal{B}_{\mathbf{I}}$ be the set of databases $d_{\mathbf{I}}$ satisfying one of the the following condition: we can find $(x_1, x_2) \neq (x_1', x_2') \in \mathcal{Y}^2$ and $v_1, v_2, v_1', v_2' \in \mathcal{Y}$

- for some $k \notin k' \in [q]$, $d_{\mathbf{I}}([x_1, x_2]_{0\|k}) \neq \perp, d_{\mathbf{I}}([x_1', x_2']_{0\|k'}) \neq \perp$;
- $([x_1]_1, v_1), ([x_1']_1, v_1) \in d_{\mathbf{I}}$;
- $([x_2 \oplus v_1]_2, v_2), ([x_2' \oplus v_1']_2, v_2') \in d_{\mathbf{I}}$;

– $x_1 \oplus v_2 = x'_1 \oplus v'_2$;

or we can find $(x_1, x_2) \neq (x'_1, x'_2) \in \mathcal{Y}^2$ and $v_1, v_2, v_3, v'_1, v'_2, v'_3 \in \mathcal{Y}$ such that

– for some $k \notin k' \in [q]$, $d_{\mathbf{I}}([x_1, x_2]_{0\|k}) \neq \perp, d_{\mathbf{I}}([x'_1, x'_2]_{0\|k'}) \neq \perp$;
– $([x_1]_1, v_1), ([x'_1]_1, v_1) \in d_{\mathbf{I}}$;
– $([x_2 \oplus v_1]_2, v_2), ([x'_2 \oplus v'_1]_2, v'_2) \in d_{\mathbf{I}}$;
– $([x_1, x_2, x_1 \oplus v_2]_5, v_5), ([x'_1, x'_2, x'_1 \oplus v'_2]_5, v_5) \in d_{\mathbf{I}}$;
– $x_2 \oplus v_1 \oplus v_3 = x'_2 \oplus v'_1 \oplus v'_3$;

Let $\mathcal{G}_{\mathbf{R}} \coloneqq \mathcal{D}_{\mathbf{R}} \setminus \mathcal{B}_{\mathbf{R}}$ and $\mathcal{G}_{\mathbf{I}} \coloneqq \mathcal{D}_{\mathbf{I}} \setminus \mathcal{B}_{\mathbf{I}}$. The above definitions mean that in both $\mathcal{G}_{\mathbf{R}}$ and $\mathcal{G}_{\mathbf{I}}$, each u_3 and u_4 is associated with a unique pair (x_1, x_2). Then it is easy to see that $\mathcal{G}_{\mathbf{R}}$ and $\mathcal{G}_{\mathbf{I}}$ have an obvious bijection $h : \mathcal{G}_{\mathbf{R}} \longrightarrow \mathcal{G}_{\mathbf{I}}$ as follows: for each $d_{\mathbf{R}}$ we define $d_{\mathbf{I}} \coloneqq h(d_{\mathbf{R}})$ such that

– for each $x \in \mathcal{Y}^{2q}$, $d_{\mathbf{I}}([x]_0) = d_{\mathbf{R}}([x]_0)$. Note that, by definition of the oracle, there will be only one entry of this type in both the worlds;
– for each $u_1 \in \mathcal{Y}$, $d_{\mathbf{I}}([u_1]_1) = d_{\mathbf{R}}([u_1]_1)$;
– for each $u_2 \in \mathcal{Y}$, $d_{\mathbf{I}}([u_2]_2) = d_{\mathbf{R}}([u_2]_2)$;
– for each $u_3, u_4 \in \mathcal{Y}$ such that $d_{\mathbf{R}}([u_3]_3) \neq \perp$ and $d_{\mathbf{R}}([u_4]_4) \neq \perp$, find the unique $(x_1, x_2) \in \mathcal{Y}^2$, and define $d_{\mathbf{I}}([x_1, x_2, u_3]_5) = d_{\mathbf{R}}([u_3]_3)$ and $d_{\mathbf{I}}([x_1, x_2, u_4]_6) = d_{\mathbf{R}}([u_4]_4)$.

Then h satisfies the conditions of Lemma 2. To complete the proof, we show that

$$\left(\perp \overset{4q+2}{\rightsquigarrow} \mathcal{B}_{\mathbf{R}}\right) + \left(\perp \overset{4q+2}{\rightsquigarrow} \mathcal{B}_{\mathbf{I}}\right) \leq 2\sqrt{\frac{q^6}{2^n}} + 4\sqrt{\frac{q^5}{2^n}}.$$

5.2 Sequence of Actions

We ignore the dummy call actions, as the transition from a good to bad database is independent of the output of this operator.

Recall that the q non-adaptive queries can be represented by a single q-fold query to be evaluated sequentially.

Action of f_1. For $i \in \{4k + 2 : 0 \leq k \leq q - 1\}$, we bound the the transition capacity $[\![\mathcal{B}^c_{\mathbf{R}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\leq i]}]\!]$. For any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \leq i - 1$ and any $x \in \mathcal{Y}$, we have

$$\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \{d_{\mathbf{R}}([x'_1]_1) \oplus d_{\mathbf{R}}([u'_3]_3) \oplus d_{\mathbf{R}}([u_3]_3) \oplus x_2 \oplus x'_2 \mid \mathtt{E}\},$$

where $\mathtt{E}$ denotes the predicate $d_{\mathbf{R}}([u_3]_3) \neq \perp, d_{\mathbf{R}}([u'_3]_3) \neq \perp, d_{\mathbf{R}}([x, x_2]_{0\|*}) \neq \perp, d_{\mathbf{R}}([x'_1, x'_2]_{0\|*}) \neq \perp$.

There are at most q choices for (x'_1, x'_2), $\lceil i - 1/4 \rceil$ choices for each of u_3 and u'_3, and at most q choices for x_2, so $|\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d}| \leq q^2 \lceil (i-1)/3 \rceil^2 \leq q^4$, and from there using Lemma 1 we have

$$[\![\mathcal{B}^c_{\mathbf{R}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\leq i]}]\!] \leq \sqrt{\frac{10q^4}{2^n}}, \qquad \forall\, i \in \{4k + 2 : 0 \leq k \leq q - 1\}. \tag{17}$$

By the same arguments we can also show that

$$[\![\mathcal{B}^c_{\mathbf{I}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\le i]}]\!] \le \sqrt{\frac{10q^4}{2^n}}, \qquad \forall\, i \in \{4k+2 : 0 \le k \le q-1\}. \tag{18}$$

Action of f_2. Next consider the transition capacity $[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!]$ for $i \in \{4k+3 : 0 \le k \le q-1\}$. For any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \le i-1$ and any $x \in \mathcal{Y}$, we have

$$\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \{d_{\mathbf{R}}([u'_2]_2) \oplus x_1 \oplus x'_1 \mid \mathtt{E}\},$$

where $\mathtt{E}$ denotes the predicate $d_{\mathbf{R}}([u'_2]_2) \neq \perp$, $d_{\mathbf{R}}([x_1, x_2]_{0\|*}) \neq \perp$, $d_{\mathbf{R}}([x'_1, x'_2]_{0\|*}) \neq \perp$. Again, there are at most $\lceil (i-1)/4 \rceil$ choices for u'_2 and at most q^2 choices for (x_1, x'_1). Thus, from Lemma 1, we have

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] \le \sqrt{\frac{10q^3}{2^n}}, \qquad \forall\, i \in \{4k+3 : 0 \le k \le q-1\}. \tag{19}$$

Action of f_3 (resp. F_3): For $i \in \{4k+4 : 1 \le k \le q-1\}$, for any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \le i-1$ and any $x \in \mathcal{Y}$, we have

$$\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \{d_{\mathbf{R}}([x_1]_1) \oplus d_{\mathbf{R}}([x'_1]_1) \oplus d_{\mathbf{R}}([u'_3]_3) \oplus x_2 \oplus x'_2 \mid \mathtt{E}\},$$

where $\mathtt{E}$ denotes the predicate $d_{\mathbf{R}}([x_1]_1), d_{\mathbf{R}}([x'_1]_1), d_{\mathbf{R}}([u_3]_3) \neq \perp, d_{\mathbf{R}}([x_1, x_2]_{0\|*}) \neq \perp, d_{\mathbf{R}}([x'_1, x'_2]_{0\|*}) \neq \perp$. There are at most $\lceil (i-1)/4 \rceil$ choices for u'_3 and at most q^2 choices for $((x_1, x_2), (x'_1, x'_2))$. Since the analysis is identical in both the worlds, by using Lemma 1, we have

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] \le \sqrt{\frac{10q^3}{2^n}}, \qquad \forall\, i \in \{4k+4 : 0 \le k \le q-1\} \tag{20}$$

$$[\![\mathcal{B}^c_{\mathbf{I}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\le i]}]\!] \le \sqrt{\frac{10q^3}{2^n}}, \qquad \forall\, i \in \{4k+4 : 0 \le k \le q-1\} \tag{21}$$

Action of f_4 (resp. F_4): Since the property $\mathcal{B}_{\mathbf{R}}$ (resp. $\mathcal{B}_{\mathbf{I}}$) is independent of the output of f_4 (resp. F_4) and the database is good right before the action, we have $\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \emptyset$. Thus,

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] = 0, \qquad \forall\, i \in \{4k+5 : 0 \le k \le q-1\} \tag{22}$$

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] = 0, \qquad \forall\, i \in \{4k+5 : 0 \le k \le q-1\} \tag{23}$$

Summing over the $4q+2$ actions using (17)-(23) gives

$$\left(\perp \overset{4q+2}{\rightsquigarrow} \mathcal{B}_{\mathbf{R}}\right) \le 2\sqrt{\frac{10q^5}{2^n}} + \sqrt{\frac{10q^6}{2^n}}, \qquad \left(\perp \overset{4q+2}{\rightsquigarrow} \mathcal{B}_{\mathbf{I}}\right) \le 2\sqrt{\frac{10q^5}{2^n}} + \sqrt{\frac{10q^6}{2^n}}. \tag{24}$$

Adding the two inequalities completes the proof of Theorem 2.

5.3 The Problem with the Adaptive Setting

A closer look at the non-adaptive proof serves to show why a similar proof is difficult to achieve in the adaptive setting. The dummy call is used to record all the q non-adaptive queries of the adversary in the database, before LR_4 is applied to each of them sequentially. This enables us to argue that the oracle knows all q queries at the time of each of the subsequent actions (f_1, f_2, f_3 etc.) which in turn helps in upper bounding the bad norm to a non-trivial value.

The proof hinges on the characterisation as bad of any database which has a 'collision' on the f input in either of the last two rounds, i.e., collisions on $x_1 \oplus v_2$ or $x_2 \oplus v_1 \oplus v_3$ for different database entries. Specifically, this implies that certain later values of x_1 or x_2 can always make the database go bad irrespective of earlier choices of v_1, v_2, or v_3. As a concrete example, recall (from Section 5.1) that a database is (also) considered bad if:

- for some $k \neq k \in [q]$, $d_{\mathbf{R}}([x_1, x_2]_{0\|k})$, $d_{\mathbf{R}}([x'_1, x'_2]_{0\|k'}) \neq \perp$ (i.e. the adversary has made these two queries).
- $([x_1]_1, v_1), ([x'_1]_1, v'_1) \in d_{\mathbf{R}}$; ($f_1$ has been evaluated over x_1 and x'_1)
- $([x_2 \oplus v_1]_2, v_2), ([x'_2 \oplus v'_1]_2, v'_2) \in d_{\mathbf{R}}$; ($f_2$ has been evaluated over $x_2 \oplus v_1$ and $x'_2 \oplus v'_1$)
- $x_1 \oplus v_2 = x'_1 \oplus v'_2$; (there is an input-collision on f_3)

Now, in the context of f_1's action, comparing the above definition with the previous proofs (specifically see the discussion around (15) and (16)), one can see that conditions 1 and 3 are missing in previous proofs. This is because it is impossible for the oracle to detect the queries made by the adversary, as at any given instant, it can only see the database entries, nothing less and nothing more. As a result, the norm bound becomes trivial. On the other hand, in our case, specifically because condition 1 can be checked at all times (once the dummy call is executed), condition 3 is also well-defined. As a result, as shown in (17) and (18), the norm bound is non-trivial.

At the same time, the dummy call must be erased before the oracle returns an output to the adversary. Otherwise, this perturbs the state, which can be detected by the adversary. So, this approach only works in non-adaptive games which can be modelled as an adversary making a single "big" query (consisting of q usual queries) to the oracle and the oracle returning a single "big" output (consisting of q usual outputs). An adaptive game, on the other hand, does not adhere to such simplifications. More specifically, since future values of x_1 and x_2 are directly under the adversary's control and are not known to the oracle in advance, the amplitude of such events cannot be bounded using known techniques. In the HI framework, this problem appears as the trivialization of the norm (see Section 4). In the BCEJ framework, this observation implies that databases can go bad *between* two actions, something that the framework does not account for. In the non-adaptive setting, however, the oracle knows in advance the future values of x_1 and x_2, and the outputs of f can accordingly be classified as 'bad' and bounded at the time of the action of f.

Lastly, we remark that this is not a problem specific to Luby-Rackoff, but is inherent to any proof for which the definition of bad databases is in terms of an input that the adversary can adaptively choose. We have also noticed this error in other proofs. For example, in [5], the security proofs of TNT, LRWQ and LRQ suffer from this problem, and do not hold in the adaptive setting. While for TNT and LRWQ this seems to be more of a definitional problem, since the bad events can be defined directly in terms of the database entries (though possibly leading to a slightly worse bound), for the LRQ proof this looks like a more fundamental issue that does not admit an easy fix. We spotted similar flaws in other works like the proof of LRWQ in [24] and the tight security proof for TNT [33]. While the former seems to be fixable, the latter is again a fundamental issue.

6 IND-qCPA Security of Misty

6.1 The Misty Constructions

For some $r \geq 1$ and $f_1, \ldots, f_r : \{0,1\}^n \to \{0,1\}^n$, we define

- $g^L : [r] \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ by the mapping:

$$(i, x_1, x_2) \longmapsto (x_2, x_2 \oplus f_i(x_1)),$$

- $g^R : [r] \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ by the mapping:

$$(i, x_1, x_2) \longmapsto (x_2 \oplus f_i(x_1), f_i(x_1)),$$

and write $g_i^L(\cdot,\cdot) := g^L(i,\cdot,\cdot)$ and $g_i^R(\cdot,\cdot) := g^R(i,\cdot,\cdot)$.

MistyL Construction: The r-round MistyL, denoted MistyL_r is defined as:

$$(x_1, x_2) \longmapsto g_r^L \circ \cdots \circ g_1^L(x_1, x_2). \tag{25}$$

MistyR Construction: The r-round MistyR construction, denoted MistyR_r is defined as:

$$(x_1, x_2) \longmapsto g_r^R \circ \cdots \circ g_1^R(x_1, x_2). \tag{26}$$

For all $i \in [r]$, we write:

- $x^{i-1} := (x_1^{i-1}, x_2^{i-1})$ to denote the input to g_i, where $x^0 := x = (x_1, x_2)$, denotes the input to $\mathsf{Misty}\{\mathsf{L}|\mathsf{R}\}_r$.
- (u_i, v_i) to denote the input-output tuple corresponding to f_i.
- $y = (y_1, y_2) := (x_1^r, x_2^r)$ to denote the output of $\mathsf{Misty}\{\mathsf{L}|\mathsf{R}\}_r$.

6.2 IND-qCPA Security of MistyR

We prove the following IND-qCPA bound for MistyR_4.

Theorem 3. *Suppose $f_1, f_2, f_3, f_4 : \{0,1\}^n \to \{0,1\}^n$ are four mutually independent uniform random functions. Then, for any $q \geq 0$, and any quantum adversary $\mathscr{A}$ that makes at most q queries, we have*

$$\mathbf{Adv}^{\mathsf{qcpa}}_{\mathsf{MistyR}_4}(\mathscr{A}) = O\left(\sqrt{\frac{q^5}{2^n}}\right).$$

Proof. Let $F_3, F_4 : \{0,1\}^{3n} \to \{0,1\}^n$ be two uniform random functions. Define

$$G_3^R(x_1, x_2, x_1', x_2') := (x_2' \oplus F_3(x_1, x_2, x_1'), F_3(x_1, x_2, x_1'))$$
$$G_4^R(x_1, x_2, x_1', x_2') := (x_2' \oplus F_4(x_1, x_2, x_1'), F_4(x_1, x_2, x_1'))$$

for any $(x_1, x_2, x_1', x_2') \in \{0,1\}^{4n}$. We define the hybrid random function $\widetilde{\mathsf{MistyR}}_4$ as (see also Fig. 3):

$$\widetilde{\mathsf{MistyR}}_4(x_1, x_2) := G_4^L(x_1, x_2, G_3^L(x_1, x_2, \mathsf{MistyR}_2(x_1, x_2))).$$

Then, it is easy to see that $\widetilde{\mathsf{MistyR}}_4$ is indistinguishable to a uniform random function $\Gamma : \{0,1\}^{2n} \to \{0,1\}^{2n}$. So, it is sufficient to bound the distance between MistyR_4 and $\widetilde{\mathsf{MistyR}}_4$.

Let $\mathcal{X} := \{0,1\}^{3n+3}$, and let $f : \mathcal{X} \longrightarrow \mathcal{Y}$ be a $(3n+3)$-bit-to-n-bit uniform random function. We implement f through $\mathbf{cO}$ defined over $\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}] \otimes \mathbb{D}$. For each $x, y, z \in \mathcal{Y}$,

$$f_1(x) = f(000\|x\|0^{2n}) \qquad f_4(x) = f(011\|x\|0^{2n})$$
$$f_2(x) = f(001\|x\|0^{2n}) \qquad F_3(x,y,z) = f(100\|x\|y\|z)$$
$$f_3(x) = f(010\|x\|0^{2n}) \qquad F_4(x,y,z) = f(101\|x\|y\|z).$$

The distinctness of the first three bits ensures that $f_1, f_2, f_3, f_4, F_3, F_4$ are all independent, and they can be implemented by the prefix oracle. We do not give the implementation explicitly as it is obvious. This setup allows us to use a single database $d_f : \mathcal{X} \longrightarrow \mathcal{Z}$ to keep track of f_1, f_1, f_2, f_3, f_4, F_3 and F_4; we refer to this database as $d_{\mathbf{R}}$ in the real world (tracking f_1, f_2, f_3 and f_4) and $d_{\mathbf{I}}$ in the ideal world (tracking f_1, f_2, F_3 and F_4). Let $\mathcal{D}_{\mathbf{R}}$ (resp. $\mathcal{D}_{\mathbf{I}}$) be the set of all possible choices for $d_{\mathbf{R}}$ (resp. $d_{\mathbf{I}}$). Let

$$[x]_1 := 000\|x\|0^{2n}, [x]_2 := 001\|x\|0^{2n},$$
$$[x]_3 := 010\|x\|0^{2n}, [x]_4 := 011\|x\|0^{2n}.$$

and define the sets

$$\widetilde{\mathcal{X}}_{\mathbf{R}} := \{[x]_1, [x]_2, [x]_3, [x]_4 \mid x \in \mathcal{Y}\},$$
$$\widetilde{\mathcal{X}}_{\mathbf{I}} := \{[x]_1, [x]_2, (100\|x\|x'\|y), (101\|x\|x'\|y) \mid x, x', y \in \mathcal{Y}\}.$$

Then it is easy to see that $\mathcal{D}_{\mathbf{R}} = \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathbf{R}}}$ and $\mathcal{D}_{\mathbf{I}} = \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathbf{I}}}$.

Let $\mathcal{B}_{\mathbf{R}}$ be the set of databases $d_{\mathbf{R}}$ satisfying one of the two following conditions: we can find $u_1, u_1', u_2, u_2', v_1, v_1', v_2, v_2' \in \mathcal{Y}$ such that

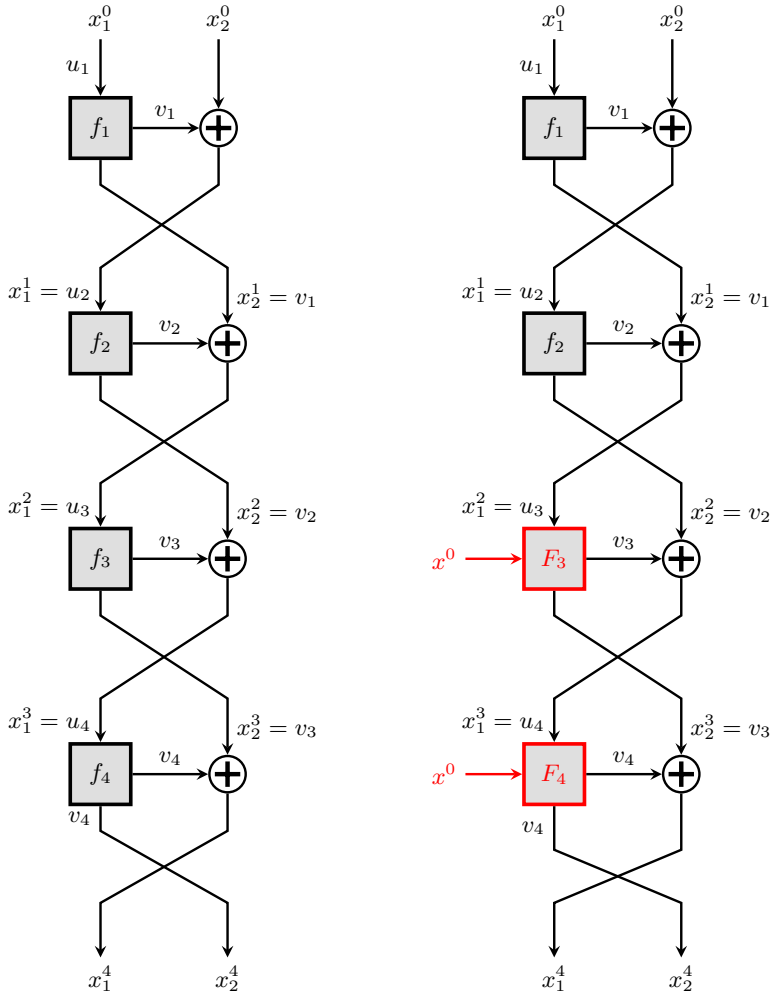

Fig. 3. MistyR_4 (left) vs the hybrid random function, $\widetilde{\mathsf{MistyR}}_4$ (right).

1. $([u_1]_1, v_1), ([u_1']_1, v_1'), ([u_2]_2, v_2), ([u_2']_2, v_2') \in d_{\mathbf{R}}$;
2. $v_2 \oplus v_1 = v_2' \oplus v_1'$;

or we can find $u_1, u_1', u_2, u_2', v_1, v_1', v_2, v_2', v_3, v_3' \in \mathcal{Y}$ such that

1. $([u_1]_1, v_1), ([u_1']_1, v_1'), ([u_2]_2, v_2), ([u_2']_2, v_2'),$
   $([v_2 \oplus v_1]_3, v_3), ([v_2' \oplus v_1']_3, v_3') \in d_{\mathbf{R}}$;
2. $v_3 \oplus v_2 = v_3' \oplus v_2'$;

Next, let $\mathcal{B}_{\mathbf{I}}$ be the set of databases $d_{\mathbf{I}}$ satisfying one of the two following conditions: we can find $u_1, u_1', u_2, u_2', v_1, v_1', v_2, v_2' \in \mathcal{Y}$ such that

1. $([u_1]_1, v_1), ([u_1']_1, v_1'), ([u_2]_2, v_2), ([u_2']_2, v_2') \in d_{\mathbf{I}}$;

2. $v_2 \oplus v_1 = v_2' \oplus v_1'$;

or we can find $u_1, u_1', u_2, u_2', v_1, v_1', v_2, v_2', v_3, v_3' \in \mathcal{Y}$ such that

1. $([u_1]_1, v_1), ([u_1']_1, v_1'), ([u_2]_2, v_2), ([u_2']_2, v_2')$, $(100\|u_1\|v_1 \oplus u_2\|v_2 \oplus v_1, v_3), (100\|u_1'\|v_1' \oplus u_2'\|v_2' \oplus v_1', v_3') \in d_{\mathbf{I}}$;
2. $v_3 \oplus v_2 = v_3' \oplus v_2'$;

Let $\mathcal{G}_{\mathbf{R}} := \mathcal{D}_{\mathbf{R}} \setminus \mathcal{B}_{\mathbf{R}}$ and $\mathcal{G}_{\mathbf{I}} := \mathcal{D}_{\mathbf{I}} \setminus \mathcal{B}_{\mathbf{I}}$. Suppose $d_{\mathbf{R}} \in \mathcal{G}_{\mathbf{R}}$ and $d_{\mathbf{I}} \in \mathcal{G}_{\mathbf{I}}$. Then each u_3 for which there exists v_3 such that $([u_3]_3, v_3) \in d_{\mathbf{R}}$ is associated with a unique pair $([u_1]_1, v_1), ([u_2]_2, v_2) \in d_{\mathbf{R}}$ such that $u_3 = v_1 \oplus v_2$, and each u_4 for which there exists v_4 such that $([u_4]_4, v_4) \in d_{\mathbf{R}}$ is associated with a unique triple $([u_1]_1, v_1), ([u_2]_2, v_2), ([u_3]_3, v_3) \in d_{\mathbf{R}}$ such that $u_3 = v_1 \oplus v_2$ and $u_4 = v_2 \oplus v_3$.

Similarly, each u_3 for which there exist x_1, x_2, v_3 such that $(100\|x_1\|x_2\|u_3, v_3) \in d_{\mathbf{I}}$ is associated with a unique pair $([u_1]_1, v_1), ([u_2]_2, v_2) \in d_{\mathbf{I}}$ such that $u_3 = v_1 \oplus v_2$, and this pair also satisfies $x_1 = u_1, x_2 = v_1 \oplus u_2$; and each u_4 for which there exist x_1, x_2, v_4 such that $(101\|x_1\|x_2\|u_4, v_4) \in d_{\mathbf{I}}$ is associated with a unique triple $([u_1]_1, v_1), ([u_2]_2, v_2), (100\|x_1\|x_2\|u_3, v_3) \in d_{\mathbf{I}}$ such that $u_3 = v_1 \oplus v_2$ and $u_4 = v_2 \oplus v_3$, and this triple also satisfies $x_1 = u_1, x_2 = v_1 \oplus u_2$.

Then we can define the bijection $h : \mathcal{G}_{\mathbf{R}} \longrightarrow \mathcal{G}_{\mathbf{I}}$ as follows: for each $d_{\mathbf{R}}$ we define $d_{\mathbf{I}} := h(d_{\mathbf{R}})$ such that

- for each $u_1 \in \mathcal{Y}$, $d_{\mathbf{I}}([u_1]_1) = d_{\mathbf{R}}([u_1]_1)$;
- for each $u_2 \in \mathcal{Y}$, $d_{\mathbf{I}}([u_2]_2) = d_{\mathbf{R}}([u_2]_2)$;
- for each $x_1, x_2 \in \mathcal{Y}$ and the associated (u_3, u_4), $d_{\mathbf{I}}(100\|x_1\|x_2\|u_3) = d_{\mathbf{R}}([u_3]_3)$ and $d_{\mathbf{I}}(101\|x_1\|x_2\|u_4) = d_{\mathbf{R}}([u_4]_4)$.

Then h satisfies the conditions of Lemma 2. To complete the proof of Theorem 3, we just need to show that $\left(\perp \overset{4q}{\rightsquigarrow} \mathcal{B}_{\mathbf{R}}\right) + \left(\perp \overset{4q}{\rightsquigarrow} \mathcal{B}_{\mathbf{I}}\right) \leq (4 + 2\sqrt{2})\sqrt{10q^5/2^n}$.

Sequence of Actions. Each query by the adversary to its oracle results in a sequence of four queries to f, one each to f_1, f_2, and one to f_3 and f_4 in the real world or F_3 and F_4 in the ideal world, in that order. We view the query response phase as a sequence of $4q$ (possibly duplicate) *actions* and analyze the transition capacity at each action.

Action of f_1: For $i \in \{4k+1 : 0 \leq k \leq q-1\}$, we first look at the transition capacity $[\![\mathcal{B}^c_{\mathbf{R}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\leq i]}]\!]$. For any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \leq i-1$ and any $x \in \mathcal{Y}$, we have

$$\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \{d_{\mathbf{R}}([u_1]_1) \oplus d_{\mathbf{R}}([u_2]_2) \oplus d_{\mathbf{R}}([u_2']_2) \mid d_{\mathbf{R}}([u_1]_1) \neq \perp,$$
$$d_{\mathbf{R}}([u_2]_2) \neq \perp, d_{\mathbf{R}}([u_2']_2) \neq \perp\}.$$

There are at most $\lceil (i-1)/4 \rceil^3$ choices for the triple (u_2, u_1', u_2'), so $|\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d}| \leq \lceil (i-1)/4 \rceil^3 \leq q^3$, and from there using Lemma 1 we have

$$[\![\mathcal{B}^c_{\mathbf{R}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\leq i]}]\!] \leq \sqrt{\frac{10q^3}{2^n}}, \qquad \forall\, i \in \{4k+1 : 0 \leq k \leq q-1\}. \tag{27}$$

By the same arguments we can also show that

$$[\![\mathcal{B}^c_{\mathbf{I}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\le i]}]\!] \le \sqrt{\frac{10q^3}{2^n}}, \qquad \forall\ i \in \{4k+1 : 0 \le k \le q-1\}. \tag{28}$$

Action of f_2: Next we look at the transition capacity $[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!]$ for $i \in \{4k+2 : 0 \le k \le q-1\}$. For any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \le i-1$ and any $x \in \mathcal{Y}$, we have

$$\begin{aligned}\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \{&d_{\mathbf{R}}([u_1]_1) \oplus d_{\mathbf{R}}([u'_1]_1) \oplus d_{\mathbf{R}}([u'_2]_2) \mid d_{\mathbf{R}}([u_1]_1) \neq \perp, d_{\mathbf{R}}([u'_1]_1) \neq \perp,\\ &d_{\mathbf{R}}([u'_2]_2) \neq \perp\} \cup \{d_{\mathbf{R}}([u_3]_3) \oplus d_{\mathbf{R}}([u'_3]_3) \oplus d_{\mathbf{R}}([u'_2]_2) \mid\\ &d_{\mathbf{R}}([u_3]_3) \neq \perp, d_{\mathbf{R}}([u'_3]_3) \neq \perp, d_{\mathbf{R}}([u'_2]_2) \neq \perp\}.\end{aligned}$$

Again, there are at most $\lceil (i-1)/4 \rceil^3$ choices for each of the triples (u_2, u'_1, u'_2) and (u_3, u'_2, u'_3), and arguing as before we have

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] \le \sqrt{\frac{20q^3}{2^n}}, \qquad \forall\ i \in \{4k+2 : 0 \le k \le q-1\}. \tag{29}$$

By the same arguments we can also show that

$$[\![\mathcal{B}^c_{\mathbf{I}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\le i]}]\!] \le \sqrt{\frac{20q^3}{2^n}}, \qquad \forall\ i \in \{4k+2 : 0 \le k \le q-1\}. \tag{30}$$

Action of f_3 (resp. F_3): Next we look at the transition capacity $[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!]$ for $i \in \{4k+3 : 0 \le k \le q-1\}$. For any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \le i-1$ and any $x \in \mathcal{Y}$, we have

$$\begin{aligned}\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \{&d_{\mathbf{R}}([u_2]_2) \oplus d_{\mathbf{R}}([u'_2]_2) \oplus d_{\mathbf{R}}([u'_3]_3) \mid d_{\mathbf{R}}([u_2]_2) \neq \perp,\\ &d_{\mathbf{R}}([u'_2]_2) \neq \perp, d_{\mathbf{R}}([u'_3]_3) \neq \perp\}.\end{aligned}$$

Again, there are at most $\lceil (i-1)/4 \rceil^3$ choices for the pair (u_2, u'_2, u'_3), and arguing as before we have

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] \le \sqrt{\frac{10q^3}{2^n}}, \qquad \forall\ i \in \{4k+3 : 0 \le k \le q-1\}. \tag{31}$$

By the same arguments we can also show that

$$[\![\mathcal{B}^c_{\mathbf{I}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\le i]}]\!] \le \sqrt{\frac{10q^3}{2^n}}, \qquad \forall\ i \in \{4k+3 : 0 \le k \le q-1\}. \tag{32}$$

Action of f_4(resp. F_4): Finally, for $i \in \{4k : 1 \le k \le q\}$, for any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \le i-1$ (resp. any $d_{\mathbf{I}}$ with $|d_{\mathbf{I}}| \le i-1$) and any $x \in \mathcal{Y}$, since the property $\mathcal{B}_{\mathbf{R}}$ (resp. $\mathcal{B}_{\mathbf{I}}$) does not depend on $d_{\mathbf{R}}([x]_4)$ (resp. $d_{\mathbf{I}}(101\|x_1\|x_2\|x)$), we have $\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \emptyset$ (resp. $\mathcal{S}^{\mathcal{B}^c_{\mathbf{I}} \hookrightarrow \mathcal{B}_{\mathbf{I}}}_{x,d} = \emptyset$). Thus,

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] = 0, \qquad \forall\ i \in \{4k : 0 \le k \le q-1\}, \tag{33}$$

and also,

$$[\![\mathcal{B}^{c}_{\mathbf{I}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\leq i]}]\!] = 0, \qquad \forall\ i \in \{4k : 0 \leq k \leq q-1\}. \tag{34}$$

Summing over the $4q$ actions using (27)-(34) gives

$$\left(\perp \overset{4q}{\rightsquigarrow} \mathcal{B}_{\mathbf{R}}\right) \leq (2+\sqrt{2})\sqrt{\frac{10q^5}{2^n}}, \qquad \left(\perp \overset{4q}{\rightsquigarrow} \mathcal{B}_{\mathbf{I}}\right) \leq (2+\sqrt{2})\sqrt{\frac{10q^5}{2^n}}. \tag{35}$$

Adding the two inequalities completes the proof of Theorem 3.

6.3 IND-qCPA Security of MistyL

We prove the following IND-qCPA bound for MistyL_5.

Theorem 4. *Suppose $f_1, f_2, f_3, f_4, f_5 : \{0,1\}^n \to \{0,1\}^n$ are five mutually independent uniform random functions. Then, for any $q \geq 0$, and any quantum adversary $\mathscr{A}$ that makes at most q queries, we have*

$$\mathbf{Adv}^{\mathsf{qcpa}}_{\mathsf{MistyL}_5}(\mathscr{A}) = O\left(\sqrt{\frac{q^7}{2^n}}\right).$$

A proof of this theorem is available in Appendix C.

7 Conclusion

In this work, we uncover a flaw in the proof of quantum security for the Luby-Rackoff, TNT, LRWQ and LRQ constructions. While TNT and LRWQ might still be proven secure (most likely with a degraded bound), the issue in the other cases seems inherent to the proof techniques that were used. In particular, for the technique to work, it is critical that bad databases are only described with information that is actually present in the database. For some constructions, notably the Luby-Rackoff and LRQ constructions, a part of the input to the construction will never appear in the database directly which means that it cannot be used to characterize bad databases. On a positive note, we restore the security of the 4-round Luby-Rackoff construction in the *non-adaptive* setting, and prove the security of the 4-round MistyR and 5-round MistyL constructions.

References

1. A. Ramachandra Rao, P.B.: Linear Algebra. Hindustan Book Agency (2000). https://doi.org/10.1007/978-93-86279-01-9
2. Bellare, M., Krovetz, T., Rogaway, P.: Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In: Nyberg, K. (ed.) Advances in Cryptology - EUROCRYPT '98, Proceeding. Lecture Notes in Computer Science, vol. 1403, pp. 266–280. Springer (1998). https://doi.org/10.1007/BFB0054132

3. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) Advances in Cryptology - EUROCRYPT 2006, Proceedings. Lecture Notes in Computer Science, vol. 4004, pp. 409–426. Springer (2006). https://doi.org/10.1007/11761679_25
4. Bhaumik, R., Bonnetain, X., Chailloux, A., Leurent, G., Naya-Plasencia, M., Schrottenloher, A., Seurin, Y.: QCB: Efficient quantum-secure authenticated encryption. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part I. LNCS, vol. 13090, pp. 668–698. Springer, Heidelberg (Dec 2021). https://doi.org/10.1007/978-3-030-92062-3_23
5. Bhaumik, R., Cogliati, B., Ethan, J., Jha, A.: On quantum secure compressing pseudorandom functions. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023, Part III. LNCS, vol. 14440, pp. 34–66. Springer, Heidelberg (Dec 2023). https://doi.org/10.1007/978-981-99-8727-6_2
6. Boneh, D., Zhandry, M.: Quantum-secure message authentication codes. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 592–608. Springer, Heidelberg (May 2013). https://doi.org/10.1007/978-3-642-38348-9_35
7. Bonnetain, X., Naya-Plasencia, M.: Hidden shift quantum cryptanalysis and implications. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part I. LNCS, vol. 11272, pp. 560–592. Springer, Heidelberg (Dec 2018). https://doi.org/10.1007/978-3-030-03326-2_19
8. Bonnetain, X., Naya-Plasencia, M., Schrottenloher, A.: On quantum slide attacks. In: Paterson, K.G., Stebila, D. (eds.) SAC 2019. LNCS, vol. 11959, pp. 492–519. Springer, Heidelberg (Aug 2019). https://doi.org/10.1007/978-3-030-38471-5_20
9. Bonnetain, X., Naya-Plasencia, M., Schrottenloher, A.: Quantum security analysis of AES. IACR Trans. Symm. Cryptol. **2019**(2), 55–93 (2019). https://doi.org/10.13154/tosc.v2019.i2.55-93
10. Bonnetain, X., Schrottenloher, A., Sibleyras, F.: Beyond quadratic speedups in quantum attacks on symmetric schemes. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022, Part III. LNCS, vol. 13277, pp. 315–344. Springer, Heidelberg (May / Jun 2022). https://doi.org/10.1007/978-3-031-07082-2_12
11. Chailloux, A., Naya-Plasencia, M., Schrottenloher, A.: An efficient quantum collision search algorithm and implications on symmetric cryptography. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part II. LNCS, vol. 10625, pp. 211–240. Springer, Heidelberg (Dec 2017). https://doi.org/10.1007/978-3-319-70697-9_8
12. Chung, K.M., Fehr, S., Huang, Y.H., Liao, T.N.: On the compressed-oracle technique, and post-quantum security of proofs of sequential work. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part II. LNCS, vol. 12697, pp. 598–629. Springer, Heidelberg (Oct 2021). https://doi.org/10.1007/978-3-030-77886-6_21
13. Cogliati, B., Dutta, A., Nandi, M., Patarin, J., Saha, A.: Proof of mirror theory for a wide range of $\xi _{\max }$. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology - EUROCRYPT 2023, Proceedings, Part IV. Lecture Notes in Computer Science, vol. 14007, pp. 470–501. Springer (2023). https://doi.org/10.1007/978-3-031-30634-1_16
14. Cogliati, B., Seurin, Y.: EWCDM: An efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 121–149. Springer, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53018-4_5
15. Czajkowski, J., Hülsing, A., Schaffner, C.: Quantum indistinguishability of random sponges. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019,

Part II. LNCS, vol. 11693, pp. 296–325. Springer, Heidelberg (Aug 2019). https://doi.org/10.1007/978-3-030-26951-7_11
16. Dai, W., Hoang, V.T., Tessaro, S.: Information-theoretic indistinguishability via the chi-squared method. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 497–523. Springer, Heidelberg (Aug 2017). https://doi.org/10.1007/978-3-319-63697-9_17
17. Dinur, I.: Tight indistinguishability bounds for the XOR of independent random permutations by fourier analysis. In: Joye, M., Leander, G. (eds.) Advances in Cryptology - EUROCRYPT 2024, Proceedings, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 33–62. Springer (2024). https://doi.org/10.1007/978-3-031-58716-0_2
18. Gouget, A., Patarin, J., Toulemonde, A.: (Quantum) cryptanalysis of misty schemes. In: Hong, D. (ed.) ICISC 20. LNCS, vol. 12593, pp. 43–57. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-68890-5_3
19. Grassi, L., Naya-Plasencia, M., Schrottenloher, A.: Quantum algorithms for the k-xor problem. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part I. LNCS, vol. 11272, pp. 527–559. Springer, Heidelberg (Dec 2018). https://doi.org/10.1007/978-3-030-03326-2_18
20. Hall, C., Wagner, D.A., Kelsey, J., Schneier, B.: Building prfs from prps. In: Krawczyk, H. (ed.) Advances in Cryptology - CRYPTO '98, Proceedings. Lecture Notes in Computer Science, vol. 1462, pp. 370–389. Springer (1998). https://doi.org/10.1007/BFB0055742
21. Hoang, V.T., Tessaro, S.: Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 3–32. Springer, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53018-4_1
22. Hosoyamada, A., Iwata, T.: 4-round Luby-Rackoff construction is a qPRP. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 145–174. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-34578-5_6
23. Hosoyamada, A., Iwata, T.: On tight quantum security of HMAC and NMAC in the quantum random oracle model. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part I. LNCS, vol. 12825, pp. 585–615. Springer, Heidelberg, Virtual Event (Aug 2021). https://doi.org/10.1007/978-3-030-84242-0_21
24. Hosoyamada, A., Iwata, T.: Provably quantum-secure tweakable block ciphers. IACR Trans. Symm. Cryptol. **2021**(1), 337–377 (2021). https://doi.org/10.46586/tosc.v2021.i1.337-377
25. Hosoyamada, A., Sasaki, Y., Xagawa, K.: Quantum multicollision-finding algorithm. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part II. LNCS, vol. 10625, pp. 179–210. Springer, Heidelberg (Dec 2017). https://doi.org/10.1007/978-3-319-70697-9_7
26. Hosoyamada, A., Yasuda, K.: Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part I. LNCS, vol. 11272, pp. 275–304. Springer, Heidelberg (Dec 2018). https://doi.org/10.1007/978-3-030-03326-2_10
27. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 207–237. Springer, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53008-5_8

28. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Quantum differential and linear cryptanalysis. IACR Trans. Symm. Cryptol. **2016**(1), 71–94 (2016). https://doi.org/10.13154/tosc.v2016.i1.71-94, https://tosc.iacr.org/index.php/ToSC/article/view/536
29. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round feistel cipher and the random permutation. In: IEEE International Symposium on Information Theory, ISIT 2010, Proceedings. pp. 2682–2685. IEEE (2010). https://doi.org/10.1109/ISIT.2010.5513654
30. Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: International Symposium on Information Theory and its Applications, ISITA 2012, Proceedings. pp. 312–316. IEEE (2012), https://ieeexplore.ieee.org/document/6400943/
31. Lai, X.: On the Design and Security of Block Ciphers. Ph.D. thesis, ETH Zürich (1992)
32. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput. **17**(2), 373–386 (1988). https://doi.org/10.1137/0217022
33. Mao, S., Zhang, Z., Hu, L., Li, L., Wang, P.: Quantum security of tnt. Cryptology ePrint Archive, Paper 2023/1280 (2023), https://eprint.iacr.org/2023/1280, https://eprint.iacr.org/2023/1280
34. Matsui, M.: The first experimental cryptanalysis of the data encryption standard. In: Desmedt, Y. (ed.) CRYPTO'94. LNCS, vol. 839, pp. 1–11. Springer, Heidelberg (Aug 1994). https://doi.org/10.1007/3-540-48658-5_1
35. Mennink, B., Neves, S.: Encrypted Davies-Meyer and its dual: Towards optimal security using mirror theory. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 556–583. Springer, Heidelberg (Aug 2017). https://doi.org/10.1007/978-3-319-63697-9_19
36. Nachef, V., Patarin, J., Treger, J.: Generic attacks on misty schemes. In: Abdalla, M., Barreto, P.S.L.M. (eds.) Progress in Cryptology - LATINCRYPT 2010, Proceedings. Lecture Notes in Computer Science, vol. 6212, pp. 222–240. Springer (2010). https://doi.org/10.1007/978-3-642-14712-8_14
37. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information (10th Anniversary edition). Cambridge University Press (2010)
38. Patarin, J.: Security of random feistel schemes with 5 or more rounds. In: Franklin, M.K. (ed.) Advances in Cryptology - CRYPTO 2004, Proceedings. Lecture Notes in Computer Science, vol. 3152, pp. 106–122. Springer (2004). https://doi.org/10.1007/978-3-540-28628-8_7
39. Patarin, J.: The "coefficients h" technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) Selected Areas in Cryptography - SAC 2008, Revised Selected Papers. Lecture Notes in Computer Science, vol. 5381, pp. 328–345. Springer (2008). https://doi.org/10.1007/978-3-642-04159-4_21
40. Patarin, J.: A proof of security in o(2n) for the xor of two random permutations. In: Safavi-Naini, R. (ed.) Information Theoretic Security - ICITS 2008, Proceedings. Lecture Notes in Computer Science, vol. 5155, pp. 232–248. Springer (2008). https://doi.org/10.1007/978-3-540-85093-9_22
41. Shoup, V.: OAEP reconsidered. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 239–259. Springer, Heidelberg (Aug 2001). https://doi.org/10.1007/3-540-44647-8_15
42. Song, F., Yun, A.: Quantum security of NMAC and related constructions - PRF domain extension against quantum attacks. In: Katz, J., Shacham, H. (eds.)

CRYPTO 2017, Part II. LNCS, vol. 10402, pp. 283–309. Springer, Heidelberg (Aug 2017). https://doi.org/10.1007/978-3-319-63715-0_10
43. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 239–268. Springer, Heidelberg (Aug 2019). https://doi.org/10.1007/978-3-030-26951-7_9

Appendix

A Basics in Linear Algebra and Quantum Computing

A.1 Hilbert Space, Operators and Norms

We use the standard Dirac notations. Fix a positive integer k. A k-dimensional *complex Hilbert space* $\mathcal{H}$ is simply the vector space $\mathbb{C}^k$ over the complex field $\mathbb{C}$ with the natural choice of inner product $\langle\cdot|\cdot\rangle$ defined as follows:

$$\langle\phi|\psi\rangle = \sum_{i,j} \alpha_i^* \beta_j,$$

for any $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ represented in some arbitrary basis $\{|\gamma_i\rangle\}$ as:

$$|\phi\rangle = \sum_i \alpha_i |\gamma_i\rangle \qquad\qquad |\psi\rangle = \sum_j \beta_j |\gamma_j\rangle,$$

where α_i, β_j are complex numbers and α_i^* is simply the complex conjugate of α_i. We emphasize that the inner product definition is independent of the choice of basis. This inner product satisfies the properties of an inner product space, including

- *Linearity:* $\langle\alpha\phi_1 + \beta\phi_2|\psi\rangle = \alpha\langle\phi_1|\psi\rangle + \beta\langle\phi_2|\psi\rangle$,
- *Conjugate symmetry:* $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$,
- *Positive-definiteness:* $\langle\phi|\phi\rangle > 0$ for all non-zero $|\phi\rangle$.

The *norm* of any vector $|\phi\rangle \in \mathcal{H}$ is defined as $\||\phi\rangle\| := \sqrt{\langle\phi|\phi\rangle}$.

Orthonormal Bases, Tensor Product. An *orthonormal basis* for $\mathcal{H}$ is a set of vectors $\{|\gamma_i\rangle\}$ such that $\langle\gamma_i|\gamma_j\rangle = \delta_{ij}$ for all $i, j \in \{1, \ldots, k\}$, where δ_{ij} is the Kronecker delta function. Given an orthonormal basis $\mathtt{B}$ of $\mathcal{H}$, we sometimes write $\mathbb{C}[\mathtt{B}]$ to emphasize the basis representation of $\mathcal{H}$.

For any two finite-dimensional complex Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ of dimensions k_1 and k_2, respectively, the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ is another complex Hilbert space of dimension $k_1 k_2$, where the inner product is defined as:

$$\langle\phi_1 \otimes \phi_2|\psi_1 \otimes \psi_2\rangle = \langle\phi_1|\psi_1\rangle\langle\phi_2|\psi_2\rangle.$$

It is also well-known that $\mathcal{H}_1 \otimes \mathcal{H}_2$ is isomorphic to the canonical $k_1 k_2$-dimensional complex Hilbert space $\mathbb{C}^{k_1 k_2}$.

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two complex Hilbert spaces of dimensions k_1 and k_2, respectively. It is well-known that any linear operator $\mathbf{L} : \mathcal{H}_1 \to \mathcal{H}_2$ can be represented by a $k_2 \times k_1$ complex matrix relative to the chosen basis for representing $\mathcal{H}_1$ and $\mathcal{H}_2$. Consequently, we use operators and matrices interchangeably as long as the bases are either fixed or clear from the context.

Unitary Operators. A linear operator $\mathbf{U}$ on $\mathcal{H}$ is said to be unitary if and only if $\mathbf{U}^\dagger\mathbf{U} = \mathbf{I}_\mathcal{H}$, where $\mathbf{U}^\dagger$ is the adjoint[7] of $\mathbf{U}$ and $\mathbf{I}_\mathcal{H}$ denotes the identity operator on $\mathcal{H}$. Let $\mathrm{U}(\mathcal{H})$ denote the set of all unitaries on $\mathcal{H}$.

Trace. For any linear operator $\mathbf{L}$ on $\mathcal{H}_1$ we define the *trace* as the sum of diagonal elements of $\mathbf{L}$, i.e.

$$\mathsf{Tr}(\mathbf{L}) := \sum_i \mathbf{L}_{ii}, \tag{36}$$

where $\mathbf{L}_{ii}$ denotes the (i,i)-th element of $\mathbf{L}$.

Partial Trace. For any linear operator $\mathbf{L}$ on $\mathcal{H}_1(\mathtt{B}_1) \otimes \mathcal{H}_2(\mathtt{B}_2)$, we define the *partial trace* of $\mathbf{L}$ on $\mathcal{H}_1$ as a linear operator from $\mathcal{H}_1(\mathtt{B}_1) \otimes \mathcal{H}_2(\mathtt{B}_2)$ to $\mathcal{H}_2(\mathtt{B}_2)$,

$$\mathsf{Tr}_{\mathcal{H}_1}(\mathbf{L}) := \sum_{|b_1'\rangle \in \mathtt{B}_1} \left(\langle b_1'| \otimes \mathbf{I}_{\mathcal{H}_2}\right) \mathbf{L} \left(|b_1'\rangle \otimes \mathbf{I}_{\mathcal{H}_2}\right), \tag{37}$$

where $\mathbf{I}_{\mathcal{H}_2}$ denotes the identity operator on $\mathcal{H}_2$.

Density Operators. Any linear operator $\mathbf{D}$ on $\mathcal{H}$ is said to be a density operator if and only if it is

- *Hermitian*: $\mathbf{D}^\dagger = \mathbf{D}$,
- *Positive Semi-definite*: $\langle \phi \,|\, \mathbf{D} \,|\, \phi \rangle \geq 0$, for every non-zero $|\phi\rangle \in \mathcal{H}$,
- *Trace-1*: $\mathsf{Tr}(\mathbf{D}) = 1$.

Let $\mathrm{D}(\mathcal{H})$ denote the set of all density operators of $\mathcal{H}$.

Trace Norm. For any linear operator $\mathbf{L}$ on some finite-dimensional complex Hilbert space $\mathcal{H}$, we define the *trace norm* of $\mathbf{L}$ as

$$\|\mathbf{L}\|_1 = \mathsf{Tr}\left(\sqrt{\mathbf{L}^\dagger\mathbf{L}}\right) = \sum_{i=1}^{r} \sigma_i, \tag{38}$$

where $\mathbf{L}^\dagger$ denotes the conjugate transpose of $\mathbf{L}$, and $\sigma_1, \ldots, \sigma_r$ denote the singular values of $\mathbf{L}$, where r denotes the rank of $\mathbf{L}$. Note that, $\mathbf{L}^\dagger\mathbf{L}$ is a positive semi-definite matrix, and thus, its square root is well-defined.

[7] This is equivalent to the conjugate transpose of the $2^n \times 2^n$ complex matrix $\mathbf{U}$ of $\mathcal{H}(\mathtt{B})$ for some orthonormal bases $\mathtt{B}$.

A.2 Quantum System, State, Measurement and Algorithm

Any n-qubit quantum system Q is the 2^n-dimensional complex Hilbert space $\mathcal{H} = \mathbb{C}^{2^n}$ with inner product $\langle\cdot|\cdot\rangle$. The state of Q is given by a *density operator* ρ_Q of $\mathcal{H}$. A state ρ is said to be *pure* if it can be expressed as $|\psi\rangle\langle\psi|$ for some $|\psi\rangle \in \mathcal{H}$ of unit norm (i.e., $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle} = 1$), and *mixed* otherwise. Indeed, pure states are often (equivalently) represented by a unit vector $|\psi\rangle_Q \in \mathcal{H}$, where the subscript Q is used to make the concerned quantum register explicit. We will also prefer this latter (simplified) representation whenever possible.

For any finite set $\mathcal{X} = \{x_1, \ldots, x_k\}$, let $\mathtt{C}_\mathcal{X} = \{|x_1\rangle, \ldots, |x_k\rangle\}$ denote an arbitrarily fixed basis of the k-dimensional complex Hilbert space $\mathcal{H}$ that we refer as the canonical *computational* basis pf $\mathcal{H}$ with respect to $\mathcal{X}$. Since the mapping $x \mapsto |x\rangle$ is an obvious bijection from $\mathcal{X}$ to $\mathtt{C}_\mathcal{X}$, we simply write $\mathbb{C}[\mathcal{X}]$ to mean $\mathbb{C}[\mathtt{C}_\mathcal{X}]$. Furthermore we often simplify this to $\mathbb{C}^{|\mathcal{X}|}$ since it is isomorphic to $\mathbb{C}[\mathcal{X}]$. Unless stated otherwise, we always assume a computational basis representation of the underlying space, where the computational basis will be clear from the context.

Given a pure quantum state $|\psi\rangle_Q$ and an orthonormal bases $\mathtt{B} = \{|b_0\rangle, \ldots, |b_{2^n-1}\rangle\}$ of $\mathcal{H}$, a measurement of $|\psi\rangle_Q$ in the bases $\mathtt{B}$ collapses the state to $|b_i\rangle$ (or simply the label $b_i \in \{b_0, \ldots, b_{2^n-1}\}$) with probability $|\langle b_i|\psi\rangle|^2$. Although we do not explicitly use it in this paper, we remark that the probabilistic behavior of measurements can be analogously extended to mixed states using the notion of positive operator-valued measurements.

Given two quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$, the joint quantum system is given by the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$. Given $\rho_1 \in \mathrm{D}(\mathcal{H}_1)$ (res. $|\psi_1\rangle \in \mathcal{H}_1$) and $\rho_2 \in \mathrm{D}(\mathcal{H}_2)$ (res. $|\psi_2\rangle \in \mathcal{H}_2$), the product state is given by $\rho_1 \otimes \rho_2$ (res. $|\psi_1, \psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ when the state is pure).

Barring measurements, all other quantum operations are unitary. Any quantum algorithm A of depth q can be defined as a sequence of unitary operators $\mathbf{U}_1, \ldots, \mathbf{U}_q$ on the space $\mathcal{H}_{in} \otimes \mathcal{H}_{out} \times \mathcal{H}_{work}$, followed by an optional measurement in the computational[8] basis. Here $\mathcal{H}_{in}$, $\mathcal{H}_{out}$, and $\mathcal{H}_{work}$ denote the input space, output space and workspace of A. If the algorithm is initialized in the state ρ_0 then the final state (before measurement), say ρ_q, is given by $\mathbf{U}_q \ldots \mathbf{U}_1 \rho_0 \mathbf{U}_1^\dagger \ldots \mathbf{U}_q^\dagger$. At this stage, ρ_q is measured and by convention the output is written in the register corresponding to $\mathcal{H}_{out}$.

B Proof of Lemma 2

We mimic the proof approach of [5, Lemma 4]. Let $\mathbf{U}_0, \ldots, \mathbf{U}_q$ denote A's unitaries. Define:

- $\mathbf{V}_0 \coloneqq \mathbf{F}_0 \circ \mathbf{U}_0$,
- $\mathbf{V}_{it+j} \coloneqq \mathbf{F}_j$, for all $i \in [q-1] \cup \{0\}$, $j \in [t-1]$,

[8] By our convention, the computational bases can be fixed arbitrarily to suit the measurement basis of the algorithm.

– $\mathbf{V}_{it} \coloneqq \mathbf{U}_0 \circ \mathbf{U}_i \circ \mathbf{F}_t$, for all $i \in [q-1]$,
– $\mathbf{V}_{qt} \coloneqq \mathbf{U}_q \circ \mathbf{F}_t$.

This defines a sequence of $q'+1$ unitaries, $\mathbf{V}_0, \ldots, \mathbf{V}_{q'}$, where $q' = qt$. For each $i \in [q']$, $\mathbf{p} \in \{\mathbf{I}, \mathbf{R}\}$, define $\mathbf{W}_{i,\mathbf{p}} \coloneqq \mathbf{cO}^{\mathbf{p}_{i_t}} \circ \mathbf{V}_{i-1}$, where

$$i_t \coloneqq \begin{cases} t & \text{if } i = 0 \bmod t, \\ i \bmod t & \text{otherwise.} \end{cases}$$

Let $|\psi_\perp\rangle = |\psi_A\rangle \otimes |d_\perp\rangle$. Then, for all $\mathbf{p} \in \{\mathbf{I}, \mathbf{R}\}$, we can write $\rho^q_{A,\mathbf{p}} = |\psi_{q',\mathbf{p}}\rangle\langle\psi_{q',\mathbf{p}}|$, where

$$|\psi_{q',\mathbf{p}}\rangle = \mathbf{V}_{q'} \circ \mathbf{W}_{q',\mathbf{p}} \circ \mathbf{W}_{q'-1,\mathbf{p}} \circ \ldots \circ \mathbf{W}_{1,\mathbf{p}}|\psi_\perp\rangle.$$

Let $\mathbf{W}^b_{i,\mathbf{p}} \coloneqq \Pi_{\mathcal{B}_{\mathbf{p}[\le i]}} \circ \mathbf{W}_{i,\mathbf{p}}$ and $\mathbf{W}^g_{i,\mathbf{p}} \coloneqq \Pi_{\mathcal{G}_{\mathbf{p}[\le i]}} \circ \mathbf{W}_{i,\mathbf{p}}$. Then we have $\mathbf{W}_{i,\mathbf{p}} = \mathbf{W}^b_{i,\mathbf{p}} + \mathbf{W}^g_{i,\mathbf{p}}$. Further, let $|\psi_{i,\mathbf{p}}\rangle \coloneqq \mathbf{W}_{i,\mathbf{p}} \circ \ldots \circ \mathbf{W}_{1,\mathbf{p}}|\psi_\perp\rangle$, and $|\psi^g_{i,\mathbf{p}}\rangle \coloneqq \mathbf{W}^g_{i,\mathbf{p}} \circ \ldots \circ \mathbf{W}^g_{1,\mathbf{p}}|\psi_\perp\rangle$.

Claim. For every $i \in [q']$ and each $\mathbf{p} \in \{\mathbf{I}, \mathbf{R}\}$:

$$\||\psi_{i,\mathbf{p}}\rangle - |\psi^g_{i,\mathbf{p}}\rangle\| \le \left(\perp \overset{i}{\rightsquigarrow} \mathcal{B}_{\mathbf{p}}\right)_{\mathbf{p}}. \tag{39}$$

Proof. Fix some $\mathbf{p} \in \{\mathbf{I}, \mathbf{R}\}$. First consider $i = 1$, we have

$$\||\psi_{1,\mathbf{p}}\rangle - |\psi^g_{1,\mathbf{p}}\rangle\| = \|\mathbf{W}_{1,\mathbf{p}}|\psi_\perp\rangle - \mathbf{W}^g_{1,\mathbf{p}}|\psi_\perp\rangle\| = \|\mathbf{W}^b_{1,\mathbf{p}}|\psi_\perp\rangle\|.$$

Since $d_\perp \in \mathcal{G}_{\mathbf{p}}$ and $\mathbf{V}_0$ commutes with $\Pi_{\mathcal{G}_{\mathbf{p}[\le 0]}}$, we have

$$\begin{aligned} \|\mathbf{W}^b_{1,\mathbf{p}}|\psi_\perp\rangle\| &= \|\Pi_{\mathcal{B}_{\mathbf{p}[\le 1]}} \circ \mathbf{W}_{1,\mathbf{p}} \circ \Pi_{\mathcal{G}_{\mathbf{p}[\le 0]}}|\psi_\perp\rangle\| \\ &= \|\Pi_{\mathcal{B}_{\mathbf{p}[\le 1]}} \circ \mathbf{cO}^{\mathbf{p}_1} \circ \mathbf{V}_0 \circ \Pi_{\mathcal{G}_{\mathbf{p}[\le 0]}}|\psi_\perp\rangle\| \\ &= \|\Pi_{\mathcal{B}_{\mathbf{p}[\le 1]}} \circ \mathbf{cO}^{\mathbf{p}_1} \circ \Pi_{\mathcal{G}_{\mathbf{p}[\le 0]}} \circ \mathbf{V}_0|\psi_\perp\rangle\| \\ &\le \|\Pi_{\mathcal{B}_{\mathbf{p}[\le 1]}} \circ \mathbf{cO}^{\mathbf{p}_1} \circ \Pi_{\mathcal{G}_{\mathbf{p}[\le 0]}}\| \\ &\le [\![\mathcal{G}_{\mathbf{p}[\le 0]} \hookrightarrow \mathcal{B}_{\mathbf{p}[\le 1]}]\!]_{\mathbf{p}} = \left(\perp \overset{1}{\rightsquigarrow} \mathcal{B}_{\mathbf{p}}\right)_{\mathbf{p}}, \end{aligned}$$

where the last inequality follows from [5, Proposition 4]. This proves the $i = 1$ case. Suppose for some $i \ge 2$:

$$\||\psi_{i-1,\mathbf{p}}\rangle - |\psi^g_{i-1,\mathbf{p}}\rangle\| \le \left(\perp \overset{i-1}{\rightsquigarrow} \mathcal{B}_{\mathbf{p}}\right)_{\mathbf{p}}.$$

Then we have

$$\begin{aligned} \||\psi_{i,\mathbf{p}}\rangle - |\psi^g_{i,\mathbf{p}}\rangle\| &= \|\mathbf{W}_{i,\mathbf{p}}|\psi_{i-1,\mathbf{p}}\rangle - \mathbf{W}^g_{i,\mathbf{p}}|\psi^g_{i-1,\mathbf{p}}\rangle\| \\ &= \|\mathbf{W}_{i,\mathbf{p}}|\psi_{i-1,\mathbf{p}}\rangle - \mathbf{W}_{i,\mathbf{p}}|\psi^g_{i-1,\mathbf{p}}\rangle + \mathbf{W}_{i,\mathbf{p}}|\psi^g_{i-1,\mathbf{p}}\rangle - \mathbf{W}^g_{i,\mathbf{p}}|\psi^g_{i-1,\mathbf{p}}\rangle\| \\ &= \|\mathbf{W}_{i,\mathbf{p}}(|\psi_{i-1,\mathbf{p}}\rangle - |\psi^g_{i-1,\mathbf{p}}\rangle) + (\mathbf{W}_{i,\mathbf{p}} - \mathbf{W}^g_{i,\mathbf{p}})|\psi^g_{i-1,\mathbf{p}}\rangle\| \end{aligned}$$

$$\begin{aligned}&\leq \|\mathbf{W}_{i,\mathbf{p}}(|\psi_{i-1,\mathbf{p}}\rangle - |\psi^g_{i-1,\mathbf{p}}\rangle)\| + \|\mathbf{W}^b_{i,\mathbf{p}}|\psi^g_{i-1,\mathbf{p}}\rangle\| \\ &\leq \||\psi_{i-1,\mathbf{p}}\rangle - |\psi^g_{i-1,\mathbf{p}}\rangle\| + \|\Pi_{\mathcal{B}_{\mathbf{p}[\leq i]}} \circ \mathbf{W}_{i,\mathbf{p}}|\psi^g_{i-1,\mathbf{p}}\rangle\|.\end{aligned}$$

Since $|\psi^g_{i-1,\mathbf{p}}\rangle$ is in the column space of $\Pi_{\mathcal{G}_{\mathbf{p}[\leq i-1]}}$. Thus, by reasoning as in the $i = 1$ case, we have

$$\begin{aligned}\|\Pi_{\mathcal{B}_{\mathbf{p}[\leq i]}} \circ \mathbf{W}_{i,\mathbf{p}}|\psi^g_{i-1,\mathbf{p}}\rangle\| &\leq \|\Pi_{\mathcal{B}_{\mathbf{p}[\leq i]}} \circ \mathbf{cO}^{\mathbf{p}_{i_t}} \circ \Pi_{\mathcal{G}_{\mathbf{p}[\leq i-1]}}\| \\ &\leq [\![\mathcal{G}_{\mathbf{p}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{p}[\leq i]}]\!]_{\mathbf{p}}.\end{aligned}$$

Using induction on $i \in [q']$ we get

$$\begin{aligned}\||\psi_{i,\mathbf{p}}\rangle - |\psi^g_{i,\mathbf{p}}\rangle\| &\leq \||\psi_{i-1,\mathbf{p}}\rangle - |\psi^g_{i-1,\mathbf{p}}\rangle\| + \|\Pi_{\mathcal{B}_{\mathbf{p}[\leq i]}} \circ \mathbf{W}_{i,\mathbf{p}}|\psi^g_{i-1,\mathbf{p}}\rangle\| \\ &\leq \left(\perp \overset{i-1}{\rightsquigarrow} \mathcal{B}_{\mathbf{p}}\right)_{\mathbf{p}} + [\![\mathcal{G}_{\mathbf{p}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{p}[\leq i]}]\!]_{\mathbf{p}} = \left(\perp \overset{i}{\rightsquigarrow} \mathcal{B}_{\mathbf{p}}\right)_{\mathbf{p}},\end{aligned}$$

thus completing the proof of the claim. □

Claim. For any $x \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$, any $i \in [q']$, and any $d \in \mathcal{G}_{\mathbf{I}[\leq i]}$,

$$\langle x, \widehat{y}, d|\psi^g_{i,\mathbf{I}}\rangle = \langle x, \widehat{y}, h(d)|\psi^g_{i,\mathbf{R}}\rangle. \tag{40}$$

Proof. For the case of $i = 1$, considering some $d \in \mathcal{G}_{\mathbf{I}[\leq 1]}$, we have

$$|\psi^g_{1,\mathbf{I}}\rangle = \mathbf{W}^g_{1,\mathbf{I}}|\psi_\perp\rangle = \Pi_{\mathcal{G}_{\mathbf{I}[\leq 1]}} \circ \mathbf{cO}^{\mathbf{I}_1} \circ \mathbf{V}_0|\psi_\perp\rangle.$$

Let $|\gamma_{x,\widehat{y}}\rangle$ denote the basis state $|x\rangle|\widehat{y}\rangle$. Then we have

$$\begin{aligned}\mathbf{cO}^{\mathbf{I}_1} \circ \mathbf{V}_0|\psi_\perp\rangle &= \mathbf{cO}^{\mathbf{I}_1} \circ \mathbf{V}_0|\psi_A\rangle \otimes |d_\perp\rangle \\ &= \sum_{x,\widehat{y}} \langle\gamma_{x,\widehat{y}} \,|\, \mathbf{V}_0 \,|\, \psi_A\rangle \; \mathbf{cO}^{\mathbf{I}_1}|\gamma_{x,\widehat{y}}\rangle \otimes |d_\perp\rangle \\ &= \sum_{x,\widehat{y}} \langle\gamma_{x,\widehat{y}} \,|\, \mathbf{V}_0 \,|\, \psi_A\rangle \left(|\gamma_{x,\widehat{y}}\rangle \otimes \mathbf{cO}^{\mathbf{I}_1}_{x\widehat{y}}|d_\perp\rangle\right) \\ &= \sum_{\substack{x,\widehat{y} \\ d \in \mathcal{D}_{\mathbf{I}}}} \langle\gamma_{x,\widehat{y}} \,|\, \mathbf{V}_0 \,|\, \psi_A\rangle \; \langle d \,|\, \mathbf{cO}^{\mathbf{I}_1}_{x\widehat{y}} \,|\, d_\perp\rangle \; |\gamma_{x,\widehat{y}}\rangle \otimes |d\rangle \\ &= \sum_{\substack{x,\widehat{y} \\ d \in \mathcal{D}_{\mathbf{I}}}} \langle\gamma_{x,\widehat{y}} \,|\, \mathbf{V}_0 \,|\, \psi_A\rangle \; \langle d \,|\, \mathbf{cO}^{\mathbf{I}_1}_{x\widehat{y}} \,|\, d_\perp\rangle \; |\gamma_{x,\widehat{y}}\rangle \otimes |d\rangle,\end{aligned}$$

where $x \in \mathcal{I}$, and $\widehat{y} \in \widehat{\mathcal{Y}}$ in all the sums. Thus,

$$\Pi_{\mathcal{G}_{\mathbf{I}[\leq 1]}} \circ \mathbf{cO}^{\mathbf{I}_1} \circ \mathbf{V}_0|\psi_\perp\rangle = \sum_{\substack{x,\widehat{y} \\ d \in \mathcal{G}_{\mathbf{I}[\leq 1]}}} \langle\gamma_{x,\widehat{y}} \,|\, \mathbf{V}_0 \,|\, \psi_A\rangle \; \langle d \,|\, \mathbf{cO}^{\mathbf{I}_1}_{x\widehat{y}} \,|\, d_\perp\rangle \; |\varphi_{x,\widehat{y},d}\rangle,$$

where $\varphi_{x,\widehat{y},d}$ denotes the basis state $|x, \widehat{y}, d\rangle$. This gives, for any $x \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$, and $d \in \mathcal{G}_{\mathbf{I}[\leq 1]}$,

$$\langle\varphi_{x,\widehat{y},d}|\psi^g_{1,\mathbf{I}}\rangle = \langle\gamma_{x,\widehat{y}} \,|\, \mathbf{V}_0 \,|\, \psi_A\rangle \; \langle d \,|\, \mathbf{cO}^{\mathbf{I}_1}_{x\widehat{y}} \,|\, d_\perp\rangle.$$

Similarly, we can show that

$$\langle \varphi_{x,\widehat{y},h(d)} | \psi^g_{1,\mathbf{R}} \rangle = \langle \gamma_{x,\widehat{y}} \,|\, \mathbf{V}_0 \,|\, \psi_A \rangle \, \langle h(d) \,|\, \mathbf{cO}^{\mathbf{R}_1}_{x\widehat{y}} \,|\, d_\perp \rangle.$$

Since $\mathcal{G}_{\mathbf{I}[\leq 0]} = \mathcal{G}_{\mathbf{R}[\leq 0]} = \{d_\perp\}$, we have $d_\perp = h(d_\perp)$, and the third condition of the lemma gives us $\langle \varphi_{x,\widehat{y},d} | \psi^g_{1,\mathbf{I}} \rangle = \langle \varphi_{x,\widehat{y},h(d)} | \psi^g_{1,\mathbf{R}} \rangle$, thus establishing the $i = 1$ case. For some $i \geq 2$, for all $x, \in \mathcal{I}$, $\widehat{y} \in \widehat{\mathcal{Y}}$, and $d \in \mathcal{G}_{\mathbf{I}[\leq i-1]}$, suppose

$$\alpha_{x,\widehat{y},d} = \langle \varphi_{x,\widehat{y},d} | \psi^g_{i-1,\mathbf{I}} \rangle = \langle \varphi_{x,\widehat{y},h(d)} | \psi^g_{i-1,\mathbf{R}} \rangle.$$

Then (since $h|_{\mathcal{G}_{\mathbf{I}[\leq i-1]}}$ is bijective) we have

$$|\psi^g_{i-1,\mathbf{I}}\rangle = \sum_{\substack{x,\widehat{y} \\ d \in \mathcal{G}_{\mathbf{I}[\leq i-1]}}} \alpha_{x,\widehat{y},d} |\gamma_{x,\widehat{y}}\rangle \otimes |d\rangle,$$

$$|\psi^g_{i-1,\mathbf{R}}\rangle = \sum_{\substack{x,\widehat{y} \\ d \in \mathcal{G}_{\mathbf{I}[\leq i-1]}}} \alpha_{x,\widehat{y},d} |\gamma_{x,\widehat{y}}\rangle \otimes |h(d)\rangle.$$

This gives

$$\begin{aligned}
|\psi^g_{i,\mathbf{I}}\rangle &= \mathbf{W}^g_{i,\mathbf{I}} |\psi^g_{i-1,\mathbf{I}}\rangle \\
&= \mathit{\Pi}_{\mathcal{G}_{\mathbf{I}[\leq i]}} \circ \mathbf{cO}^{\mathbf{I}_{i_t}} \circ \mathbf{V}_{i-1} |\psi^g_{i-1,\mathbf{I}}\rangle \\
&= \sum_{\substack{x,\widehat{y} \\ d \in \mathcal{G}_{\mathbf{I}[\leq i-1]}}} \alpha_{x,\widehat{y},d} \, \mathit{\Pi}_{\mathcal{G}_{\mathbf{I}[\leq i]}} \circ \mathbf{cO}^{\mathbf{I}_{i_t}} \circ \mathbf{V}_{i-1} |\gamma_{x,\widehat{y}}\rangle \otimes |d\rangle \\
&= \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}' \\ d \in \mathcal{G}_{\mathbf{I}[\leq i-1]}}} \alpha_{x,\widehat{y},d} \, \langle \gamma_{x',\widehat{y}'} \,|\, \mathbf{V}_{i-1} \,|\, \gamma_{x,\widehat{y}} \rangle \, \mathit{\Pi}_{\mathcal{G}_{\mathbf{I}[\leq i]}} \circ \mathbf{cO}^{\mathbf{I}_{i_t}} |\gamma_{x',\widehat{y}'}\rangle \otimes |d\rangle \\
&= \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}' \\ d \in \mathcal{G}_{\mathbf{I}[\leq i-1]}}} \alpha_{x,\widehat{y},d} \, \langle \gamma_{x',\widehat{y}'} \,|\, \mathbf{V}_{i-1} \,|\, \gamma_{x,\widehat{y}} \rangle \, \mathit{\Pi}_{\mathcal{G}_{\mathbf{I}[\leq i]}} \left(|\gamma_{x',\widehat{y}'}\rangle \otimes \mathbf{cO}^{\mathbf{I}_{i_t}}_{x'\widehat{y}'} |d\rangle \right) \\
&= \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}' \\ d \in \mathcal{G}_{\mathbf{I}[\leq i-1]} \\ d' \in \mathcal{D}_{\mathbf{I}}}} \alpha_{x,\widehat{y},d} \, \langle \gamma_{x',\widehat{y}'} \,|\, \mathbf{V}_{i-1} \,|\, \gamma_{x,\widehat{y}} \rangle \, \langle d' \,|\, \mathbf{cO}^{\mathbf{I}_{i_t}}_{x'\widehat{y}'} \,|\, d \rangle \, \mathit{\Pi}_{\mathcal{G}_{\mathbf{I}[\leq i]}} \left(|\gamma_{x',\widehat{y}'}\rangle \otimes |d'\rangle \right) \\
&= \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}' \\ d \in \mathcal{G}_{\mathbf{I}[\leq i-1]} \\ d' \in \mathcal{G}_{\mathbf{I}[\leq i]}}} \alpha_{x,\widehat{y},d} \, \langle \gamma_{x',\widehat{y}'} \,|\, \mathbf{V}_{i-1} \,|\, \gamma_{x,\widehat{y}} \rangle \, \langle d' \,|\, \mathbf{cO}^{\mathbf{I}_{i_t}}_{x'\widehat{y}'} \,|\, d \rangle \, |\varphi_{x',\widehat{y}',d'}\rangle,
\end{aligned}$$

so that for any $x' \in \mathcal{I}$, $\widehat{y}' \in \widehat{\mathcal{Y}}$, and $d' \in \mathcal{G}_{\mathbf{I}[\leq i]}$, we have

$$\langle \varphi_{x',\widehat{y}',d'} | \psi^g_{i,\mathbf{I}} \rangle = \sum_{\substack{x,\widehat{y} \\ d \in \mathcal{G}_{\mathbf{I}[\leq i-1]}}} \alpha_{x,\widehat{y},d} \, \langle \gamma_{x',\widehat{y}'} \,|\, \mathbf{V}_{i-1} \,|\, \gamma_{x,\widehat{y}} \rangle \, \langle d' \,|\, \mathbf{cO}^{\mathbf{I}_{i_t}}_{x\widehat{y}} \,|\, d \rangle.$$

Similarly, we can show that

$$\langle \varphi_{x',\widehat{y}',h(d')} | \psi^g_{i,\mathbf{R}} \rangle = \sum_{\substack{x,\widehat{y} \\ d \in \mathcal{G}_{\mathbf{I}[\leq i-1]}}} \alpha_{x,\widehat{y},h(d)} \, \langle \gamma_{x',\widehat{y}'} \,|\, \mathbf{V}_{i-1} \,|\, \gamma_{x,\widehat{y}} \rangle \, \langle h(d') \,|\, \mathbf{cO}^{\mathbf{R}_{i_t}}_{x\widehat{y}} \,|\, h(d) \rangle.$$

Then the third condition of Lemma 2 proves the claim. □

Using (40) observation, for any $i \in [q']$, we have

$$\begin{aligned}
\mathsf{Tr}_{\mathbb{D}} \left(|\psi^g_{i,\mathbf{I}}\rangle\langle\psi^g_{i,\mathbf{I}}| \right) &= \sum_{d \in \mathcal{D}} \langle d \,|\, \psi^g_{i,\mathbf{I}} \rangle \langle\, \psi^g_{i,\mathbf{I}} \,|\, d \rangle \\
&= \sum_{d \in \mathcal{G}_{\mathbf{I}[\leq i]}} \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}'}} \alpha_{x,\widehat{y},d} \alpha_{x',\widehat{y}',d} |x,\widehat{y}\rangle\langle x',\widehat{y}'| \\
&= \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}'}} \left(\sum_{d \in \mathcal{G}_{\mathbf{I}[\leq i]}} \alpha_{x,\widehat{y},d} \alpha_{x',\widehat{y}',d} \right) |x,\widehat{y}\rangle\langle x',\widehat{y}'| \\
&= \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}'}} \left(\sum_{d \in \mathcal{G}_{\mathbf{I}[\leq i]}} \alpha_{x,\widehat{y},h(d)} \alpha_{x',\widehat{y}',h(d)} \right) |x,\widehat{y}\rangle\langle x',\widehat{y}'| \\
&= \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}'}} \left(\sum_{h(d) \in \mathcal{G}_{\mathbf{R}[\leq i]}} \alpha_{x,\widehat{y},h(d)} \alpha_{x',\widehat{y}',h(d)} \right) |x,\widehat{y}\rangle\langle x',\widehat{y}'| \\
&= \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}'}} \left(\sum_{d' \in \mathcal{G}_{\mathbf{R}[\leq i]}} \alpha_{x,\widehat{y},d'} \alpha_{x',\widehat{y}',d'} \right) |x,\widehat{y}\rangle\langle x',\widehat{y}'| \\
&= \sum_{d' \in \mathcal{G}_{\mathbf{R}[\leq i]}} \sum_{\substack{x,x' \\ \widehat{y},\widehat{y}'}} \alpha_{x,\widehat{y},d'} \alpha_{x',\widehat{y}',d'} |x,\widehat{y}\rangle\langle x',\widehat{y}'| \\
&= \sum_{d' \in \mathcal{D}} \langle d' \,|\, \psi^g_{i,\mathbf{R}} \rangle \langle\, \psi^g_{i,\mathbf{R}} \,|\, d' \rangle \\
&= \mathsf{Tr}_{\mathbb{D}} \left(|\psi^g_{i,\mathbf{R}}\rangle\langle\psi^g_{i,\mathbf{R}}| \right). \qquad (41)
\end{aligned}$$

Now, for each $\mathbf{p} \in \{\mathbf{I}, \mathbf{R}\}$, let $|\psi^b_{q',\mathbf{p}}\rangle := |\psi_{q',\mathbf{p}}\rangle - |\psi^g_{q',\mathbf{p}}\rangle$. Then, we have

$$\begin{aligned}
\| \mathsf{Tr}_{\mathbb{D}}(\rho^q_{A,\mathbf{I}}) - \mathsf{Tr}_{\mathbb{D}}(\rho^q_{A,\mathbf{R}}) \|_1 &= \| \mathsf{Tr}_{\mathbb{D}}(|\psi_{q',\mathbf{I}}\rangle\langle\psi_{q',\mathbf{I}}|) - \mathsf{Tr}_{\mathbb{D}}(|\psi_{q',\mathbf{R}}\rangle\langle\psi_{q',\mathbf{R}}|) \|_1 \\
&\leq \| \mathsf{Tr}_{\mathbb{D}}(|\psi^g_{q',\mathbf{I}}\rangle\langle\psi^b_{q',\mathbf{I}}|) \|_1 + \| \mathsf{Tr}_{\mathbb{D}}(|\psi^b_{q',\mathbf{I}}\rangle\langle\psi^g_{q',\mathbf{I}}|) \|_1 \\
&\quad + \| \mathsf{Tr}_{\mathbb{D}}(|\psi^b_{q',\mathbf{I}}\rangle\langle\psi^b_{q',\mathbf{I}}|) \|_1 + \| \mathsf{Tr}_{\mathbb{D}}(|\psi^b_{q',\mathbf{R}}\rangle\langle\psi^b_{q',\mathbf{R}}|) \|_1 \\
&\quad + \| \mathsf{Tr}_{\mathbb{D}}(|\psi^b_{q',\mathbf{R}}\rangle\langle\psi^g_{q',\mathbf{R}}|) \|_1 + \| \mathsf{Tr}_{\mathbb{D}}(|\psi^g_{q',\mathbf{R}}\rangle\langle\psi^b_{q',\mathbf{R}}|) \|_1
\end{aligned}$$

$$
\begin{aligned}
&\leq \|\!|\psi^g_{q',\mathbf{I}}\rangle\langle\psi^b_{q',\mathbf{I}}|\|\!|_1 + \|\!|\psi^b_{q',\mathbf{I}}\rangle\langle\psi^g_{q',\mathbf{I}}|\|\!|_1 \\
&\quad + \|\!|\psi^b_{q',\mathbf{I}}\rangle\langle\psi^b_{q',\mathbf{I}}|\|\!|_1 + \|\!|\psi^b_{q',\mathbf{R}}\rangle\langle\psi^b_{q',\mathbf{R}}|\|\!|_1 \\
&\quad + \|\!|\psi^b_{q',\mathbf{R}}\rangle\langle\psi^g_{q',\mathbf{R}}|\|\!|_1 + \|\!|\psi^g_{q',\mathbf{R}}\rangle\langle\psi^b_{q',\mathbf{R}}|\|\!|_1 \\
&\leq 3\|\!|\psi^b_{q',\mathbf{I}}\rangle\|\!| + 3\|\!|\psi^b_{q',\mathbf{R}}\rangle\|\!| \\
&\leq 3\left(\perp \overset{q'}{\rightsquigarrow} \mathcal{B}_{\mathbf{I}}\right)_{\mathbf{I}} + 3\left(\perp \overset{q'}{\rightsquigarrow} \mathcal{B}_{\mathbf{R}}\right)_{\mathbf{R}},
\end{aligned}
$$

where

- the first inequality follows from the linearity of the partial trace map with the observation (41), and the triangle inequality;
- the second inequality follows from the fact that partial trace is a completely positive and trace-preserving map;
- the third inequality follows from repeated applications of [5, Proposition 5]; and
- the final inequality follows from (39).

This completes the proof.

C Proof of Theorem 4

Let $F_4, F_5 : \{0,1\}^{3n} \to \{0,1\}^n$ be two uniform random functions. Define

$$
\begin{aligned}
G^L_4(x_1, x_2, x'_1, x'_2) &:= (x'_2, x'_2 \oplus F_4(x_1, x_2, x'_1)) \\
G^L_5(x_1, x_2, x'_1, x'_2) &:= (x'_2, x'_2 \oplus F_5(x_1, x_2, x'_1))
\end{aligned}
$$

for any $(x_1, x_2, x'_1, x'_2) \in \{0,1\}^{4n}$. We define the hybrid random function $\widetilde{\mathsf{MistyL}}_5$ as (see also Fig. 4):

$$
\widetilde{\mathsf{MistyL}}_5(x_1, x_2) := G^L_5(x_1, x_2, G^L_4(x_1, x_2, \mathsf{MistyL}_3(x_1, x_2))).
$$

Then, it is easy to see that $\widetilde{\mathsf{MistyL}}_5$ is indistinguishable to a uniform random function $\Gamma : \{0,1\}^{2n} \to \{0,1\}^{2n}$. So, it is sufficient to bound the distance between MistyL_5 and $\widetilde{\mathsf{MistyL}}_5$.

Let $\mathcal{X} := \{0,1\}^{3n+3}$, and let $f : \mathcal{X} \longrightarrow \mathcal{Y}$ be a $(3n+3)$-bit-to-n-bit uniform random function. We implement f through $\mathbf{cO}$ defined over $\mathbb{C}[\mathcal{X}] \otimes \mathbb{C}[\mathcal{Y}] \otimes \mathbb{D}$. For each $x, y, z \in \mathcal{Y}$,

$$
\begin{aligned}
f_1(x) &= f(000\|x\|0^{2n}), \\
f_2(x) &= f(001\|x\|0^{2n}), \\
f_3(x) &= f(010\|x\|0^{2n}), \\
f_4(x) &= f(011\|x\|0^{2n}), \\
f_5(x) &= f(100\|x\|0^{2n}),
\end{aligned}
$$

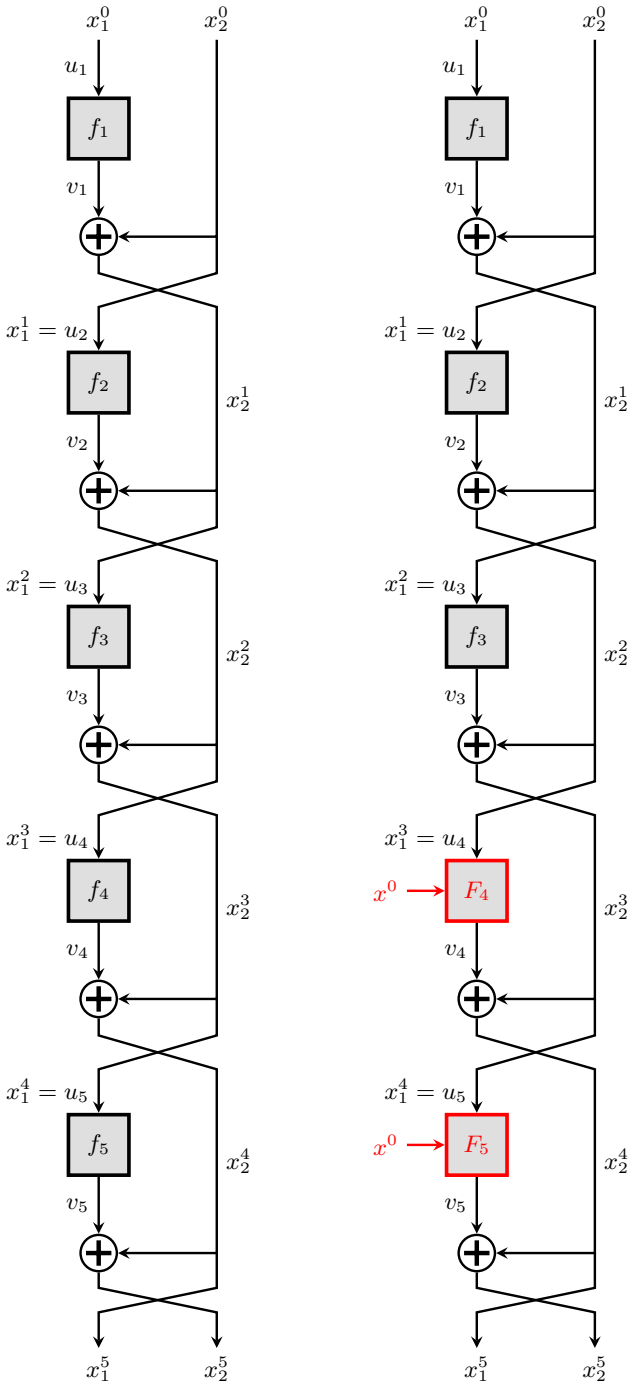

Fig. 4. MistyL_5 (left) vs the hybrid random function, $\widetilde{\mathsf{MistyL}}_5$ (right).

$$F_4(x,y,z) = f(101\|x\|y\|z),$$
$$F_5(x,y,z) = f(110\|x\|y\|z).$$

The distinctness of the first three bits ensures that $f_1, f_2, f_3, f_4, f_5, F_4, F_5$ are all independent, and they can be implemented by the prefix oracle. We do not give the implementation explicitly as it is obvious. This setup allows us to use a single database $d_f : \mathcal{X} \longrightarrow \mathcal{Z}$ to keep track of f_1, $f_1, f_2, f_3, f_4, f_5 F_4$ and F_5; we refer to this database as $d_{\mathbf{R}}$ in the real world (tracking f_1, f_2, f_3, f_4 and f_5) and $d_{\mathbf{I}}$ in the ideal world (tracking f_1, f_2, f_3, F_4 and F_5). Let $\mathcal{D}_{\mathbf{R}}$ (resp. $\mathcal{D}_{\mathbf{I}}$) be the set of all possible choices for $d_{\mathbf{R}}$ (resp. $d_{\mathbf{I}}$). Let

$$[x]_1 := 000\|x\|0^{2n}, [x]_2 := 001\|x\|0^{2n},$$
$$[x]_3 := 010\|x\|0^{2n}, [x]_4 := 011\|x\|0^{2n},$$
$$[x]_5 := 100\|x\|0^{2n}.$$

and define the sets

$$\widetilde{\mathcal{X}}_{\mathbf{R}} := \{[x]_1, [x]_2, [x]_3, [x]_4, [x]_5 \mid x \in \mathcal{Y}\},$$
$$\widetilde{\mathcal{X}}_{\mathbf{I}} := \{[x]_1, [x]_2, [x]_3 \left(101\|x\|x'\|y\right), \left(110\|x\|x'\|y\right) \mid x, x', y \in \mathcal{Y}\}.$$

Then it is easy to see that $\mathcal{D}_{\mathbf{R}} = \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathbf{R}}}$ and $\mathcal{D}_{\mathbf{I}} = \mathcal{D}|_{\widetilde{\mathcal{X}}_{\mathbf{I}}}$.

Let $\mathcal{B}_{\mathbf{R}}$ be the set of databases $d_{\mathbf{R}}$ satisfying one of the two following conditions: we can find $u_1, u_1', u_2, u_2', v_1, v_1', v_2, v_2' \in \mathcal{Y}$ such that

1. $([u_1]_1, v_1), ([u_1']_1, v_1'), ([u_2]_2, v_2), ([u_2']_2, v_2') \in d_{\mathbf{R}}$;
2. $v_2 \oplus v_1 \oplus u_2 = v_2' \oplus v_1' \oplus u_2'$;

or we can find $u_1, u_1', u_2, u_2', v_1, v_1', v_2, v_2', v_3, v_3' \in \mathcal{Y}$ such that

1. $([u_1]_1, v_1), ([u_1']_1, v_1'), ([u_2]_2, v_2), ([u_2']_2, v_2')$, $([v_1 \oplus u_2]_3, v_3), ([v_1' \oplus u_2']_3, v_3') \in d_{\mathbf{R}}$;
2. $v_3 \oplus v_2 \oplus v_1 \oplus u_2 = v_3' \oplus v_2' \oplus v_1' \oplus u_2$;

Next, let $\mathcal{B}_{\mathbf{I}}$ be the set of databases $d_{\mathbf{I}}$ satisfying one of the two following conditions: we can find $u_1, u_1', u_2, u_2', v_1, v_1', v_2, v_2' \in \mathcal{Y}$ such that

1. $([u_1]_1, v_1), ([u_1']_1, v_1'), ([u_2]_2, v_2), ([u_2']_2, v_2') \in d_{\mathbf{I}}$;
2. $v_2 \oplus v_1 \oplus u_2 = v_2' \oplus v_1' \oplus u_2'$;

or we can find $u_1, u_1', u_2, u_2', v_1, v_1', v_2, v_2', v_3, v_3' \in \mathcal{Y}$ such that

1. $([u_1]_1, v_1), ([u_1']_1, v_1'), ([u_2]_2, v_2), ([u_2']_2, v_2')$, $([v_1 \oplus u_2]_3, v_3), ([v_1' \oplus u_2']_3, v_3') \in d_{\mathbf{I}}$;
2. $v_3 \oplus v_2 \oplus v_1 \oplus u_2 = v_3' \oplus v_2' \oplus v_1' \oplus u_2$;

Let $\mathcal{G}_{\mathbf{R}} := \mathcal{D}_{\mathbf{R}} \setminus \mathcal{B}_{\mathbf{R}}$ and $\mathcal{G}_{\mathbf{I}} := \mathcal{D}_{\mathbf{I}} \setminus \mathcal{B}_{\mathbf{I}}$. Thus the above definitions mean that in both $\mathcal{G}_{\mathbf{R}}$ and $\mathcal{G}_{\mathbf{I}}$, each pair of values $(u_4 := v_2 \oplus v_1 \oplus u_2, u_5 := v_3 \oplus v_2 \oplus v_1 \oplus u_2)$ is associated with a unique pair (x_1, x_2). Then we can define the bijection $h : \mathcal{G}_{\mathbf{R}} \longrightarrow \mathcal{G}_{\mathbf{I}}$ as follows: for each $d_{\mathbf{R}}$ we define $d_{\mathbf{I}} := h(d_{\mathbf{R}})$ such that

- for each $x_L \in \mathcal{Y}$, $d_{\mathbf{I}}([u_1]_1) = d_{\mathbf{R}}([u_1]_1)$;
- for each $u_2 \in \mathcal{Y}$, $d_{\mathbf{I}}([u_2]_2) = d_{\mathbf{R}}([u_2]_2)$;
- for each $u_3 \in \mathcal{Y}$, $d_{\mathbf{I}}([u_3]_3) = d_{\mathbf{R}}([u_3]_3)$;
- for each $x_1, x_2 \in \mathcal{Y}$ and the associated (u_4, u_5), $d_{\mathbf{I}}(101\|x_1\|x_2\|u_4) = d_{\mathbf{R}}([u_4]_4)$ and $d_{\mathbf{I}}(110\|x_1\|x_2\|u_5) = d_{\mathbf{R}}([u_5]_5)$.

Then h satisfies the conditions of Lemma 2. To complete the proof of Theorem 4, we just need to show that

$$\left(\perp \overset{5q}{\rightsquigarrow} \mathcal{B}_{\mathbf{R}}\right) + \left(\perp \overset{5q}{\rightsquigarrow} \mathcal{B}_{\mathbf{I}}\right) \leq (2 + 4\sqrt{2})\sqrt{\frac{10q^5}{2^n}}.$$

Sequence of Actions. Each query by the adversary to its oracle results in a sequence of four queries to f, one each to f_1, f_2, f_3 and one to f_4 and f_5 in the real world or F_4 and F_5 in the ideal world, in that order. We view the query response phase as a sequence of $5q$ (possibly duplicate) *actions* and analyze the transition capacity at each action.

Action of f_1: For $i \in \{5k+1 : 0 \leq k \leq q-1\}$, we first look at the transition capacity $[\![\mathcal{B}^c_{\mathbf{R}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\leq i]}]\!]$. Note that any two consecutive rounds of MistyL are independent (can be executed in parallel). So, without loss of generality, we assume that f_2 is applied first followed by f_1. Hence, for any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \leq i-1$ and any $x \in \mathcal{Y}$, we have

$$\begin{aligned}
\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \{&u_2 \oplus u_2' \oplus d_{\mathbf{R}}([u_1]_1) \oplus d_{\mathbf{R}}([u_2]_2) \oplus d_{\mathbf{R}}([u_2']_2) \\
&\mid d_{\mathbf{R}}([u_1]_1) \neq \perp, d_{\mathbf{R}}([u_2]_2) \neq \perp, d_{\mathbf{R}}([u_2']_2) \neq \perp\} \\
\cup \{&u_2 \oplus u_2' \oplus d_{\mathbf{R}}([u_1]_1) \oplus d_{\mathbf{R}}([u_2]_2) \oplus d_{\mathbf{R}}([u_2']_2) \oplus d_{\mathbf{R}}([u_3]_3) \oplus d_{\mathbf{R}}([u_3']_3) \\
&\mid d_{\mathbf{R}}([u_1]_1) \neq \perp, d_{\mathbf{R}}([u_2]_2) \neq \perp, d_{\mathbf{R}}([u_2']_2) \neq \perp, d_{\mathbf{R}}([u_3]_3) \neq \perp, \\
&d_{\mathbf{R}}([u_3']_3) \neq \perp\}.
\end{aligned}$$

There are respectively at most $\lceil (i-1)/5 \rceil^3$ and $\lceil (i-1)/5 \rceil^5$ choices for the tuples (u_1, u_2, u_2') and $(u_1, u_2, u_2', u_3, u_3')$, so $|\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d}| \leq 2\lceil (i-1)/5 \rceil^5 \leq 2q^5$, and from there using Lemma 1 we have

$$[\![\mathcal{B}^c_{\mathbf{R}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\leq i]}]\!] \leq \sqrt{\frac{20q^5}{2^n}}, \qquad \forall\ i \in \{5k+1 : 0 \leq k \leq q-1\}. \tag{42}$$

By the same arguments we can also show that

$$[\![\mathcal{B}^c_{\mathbf{I}[\leq i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\leq i]}]\!] \leq \sqrt{\frac{20q^5}{2^n}}, \qquad \forall\ i \in \{5k+1 : 0 \leq k \leq q-1\}. \tag{43}$$

ACTION OF f_2: For $i \in \{5k+2 : 1 \le k \le q\}$, for any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \le i-1$ (resp. any $d_{\mathbf{I}}$ with $|d_{\mathbf{I}}| \le i-1$) and any $x \in \mathcal{Y}$, we have

$$\begin{aligned}\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}} = \{&x \oplus u_2 \oplus d_{\mathbf{R}}([u_1]_1) \oplus d_{\mathbf{R}}([u'_1]_1) \oplus d_{\mathbf{R}}([u_2]_2) \\ &\mid d_{\mathbf{R}}([u_1]_1) \neq \perp, d_{\mathbf{R}}([u'_1]_1) \neq \perp, d_{\mathbf{R}}([u_2]_2) \neq \perp\} \\ \cup \{&x \oplus u_2 \oplus d_{\mathbf{R}}([u_1]_1) \oplus d_{\mathbf{R}}([u'_1]_1) \oplus d_{\mathbf{R}}([u_2]_2) \oplus d_{\mathbf{R}}([u_3]_3) \oplus d_{\mathbf{R}}([u'_3]_3) \\ &\mid d_{\mathbf{R}}([u_1]_1) \neq \perp, d_{\mathbf{R}}([u'_1]_1) \neq \perp, d_{\mathbf{R}}([u_2]_2) \neq \perp, d_{\mathbf{R}}([u_3]_3) \neq \perp, \\ &d_{\mathbf{R}}([u'_3]_3) \neq \perp\}.\end{aligned}$$

There are respectively at most $\lceil (i-1)/5 \rceil^3$ and $\lceil (i-1)/5 \rceil^5$ choices for the tuples (u_1, u_2, u'_1) and $(u_1, u'_1, u_2, u_3, u'_3)$, so $|\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}| \le 2q^5$, and from there using Lemma 1 we have

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] = \sqrt{\frac{20q^5}{2^n}}, \qquad \forall\, i \in \{5k+2 : 1 \le k \le q\}, \tag{44}$$

and also,

$$[\![\mathcal{B}^c_{\mathbf{I}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\le i]}]\!] = \sqrt{\frac{20q^5}{2^n}}, \qquad \forall\, i \in \{5k+2 : 1 \le k \le q\}. \tag{45}$$

ACTION OF f_3: Next we look at the transition capacity $[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!]$ for $i \in \{5k+3 : 0 \le k \le q-1\}$. For any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \le i-1$ and any $x \in \mathcal{Y}$, we have

$$\begin{aligned}\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}} = \{&u_2 \oplus u'_2 \oplus d_{\mathbf{R}}([u_1]_1) \oplus d_{\mathbf{R}}([u'_1]_1) \oplus d_{\mathbf{R}}([u_2]_2) \oplus d_{\mathbf{R}}([u_2]_2) \oplus \\ &d_{\mathbf{R}}([u_3]_3) \mid d_{\mathbf{R}}([u_1]_1) \neq \perp, d_{\mathbf{R}}([u'_1]_1) \neq \perp, d_{\mathbf{R}}([u_2]_2) \neq \perp, \\ &d_{\mathbf{R}}([u'_2]_2) \neq \perp, d_{\mathbf{R}}([u_3]_3) \neq \perp\}.\end{aligned}$$

There are at most $\lceil (i-1)/5 \rceil^5$ choices for the tuple $(u_1, u'_1, u_2, u'_2, u_3)$, so $|\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}| \le \lceil (i-1)/5 \rceil^5 \le q^5$, and from there using Lemma 1 we have

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] \le \sqrt{\frac{10q^5}{2^n}}, \qquad \forall\, i \in \{5k+3 : 0 \le k \le q-1\}. \tag{46}$$

By the same arguments we can also show that

$$[\![\mathcal{B}^c_{\mathbf{I}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\le i]}]\!] \le \sqrt{\frac{10q^5}{2^n}}, \qquad \forall\, i \in \{5k+3 : 0 \le k \le q-1\}. \tag{47}$$

ACTION OF f_4 (RESP. F_4): Finally, for $i \in \{5k : 1 \le k \le q\}$, for any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \le i-1$ (resp. any $d_{\mathbf{I}}$ with $|d_{\mathbf{I}}| \le i-1$) and any $x \in \mathcal{Y}$, since the property $\mathcal{B}_{\mathbf{R}}$ (resp. $\mathcal{B}_{\mathbf{I}}$) does not depend on $d_{\mathbf{R}}([x]_4)$ (resp. $d_{\mathbf{I}}(101\|x_1\|x_2\|x)$), we have $\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}} = \emptyset$ (resp. $\mathcal{S}_{x,d}^{\mathcal{B}^c_{\mathbf{I}} \hookrightarrow \mathcal{B}_{\mathbf{I}}} = \emptyset$). Thus,

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] = 0, \qquad \forall\, i \in \{5k+4 : 0 \le k \le q-1\}, \tag{48}$$

and also,

$$[\![\mathcal{B}^c_{\mathbf{I}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\le i]}]\!] = 0, \qquad \forall\, i \in \{5k+4 : 0 \le k \le q-1\}. \tag{49}$$

Action of f_5(resp. F_5): Finally, for $i \in \{5k : 1 \le k \le q\}$, for any $d_{\mathbf{R}}$ with $|d_{\mathbf{R}}| \le i-1$ (resp. any $d_{\mathbf{I}}$ with $|d_{\mathbf{I}}| \le i-1$) and any $x \in \mathcal{Y}$, since the property $\mathcal{B}_{\mathbf{R}}$ (resp. $\mathcal{B}_{\mathbf{I}}$) does not depend on $d_{\mathbf{R}}([x]_5)$ (resp. $d_{\mathbf{I}}(110\|x_1\|x_2\|x)$), we have $\mathcal{S}^{\mathcal{B}^c_{\mathbf{R}} \hookrightarrow \mathcal{B}_{\mathbf{R}}}_{x,d} = \emptyset$ (resp. $\mathcal{S}^{\mathcal{B}^c_{\mathbf{I}} \hookrightarrow \mathcal{B}_{\mathbf{I}}}_{x,d} = \emptyset$). Thus,

$$[\![\mathcal{B}^c_{\mathbf{R}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{R}[\le i]}]\!] = 0, \qquad \forall\, i \in \{5k : 0 \le k \le q-1\}, \tag{50}$$

and also,

$$[\![\mathcal{B}^c_{\mathbf{I}[\le i-1]} \hookrightarrow \mathcal{B}_{\mathbf{I}[\le i]}]\!] = 0, \qquad \forall\, i \in \{5k : 0 \le k \le q-1\}. \tag{51}$$

Summing over the $5q$ actions using (42)-(51) gives

$$\left(\perp \overset{5q}{\rightsquigarrow} \mathcal{B}_{\mathbf{R}}\right) \le (1+2\sqrt{2})\sqrt{\frac{10q^7}{2^n}}, \qquad \left(\perp \overset{5q}{\rightsquigarrow} \mathcal{B}_{\mathbf{I}}\right) \le (1+2\sqrt{2})\sqrt{\frac{10q^7}{2^n}}. \tag{52}$$

Adding the two inequalities completes the proof of Theorem 4.