4-Round Luby-Rackoff Construction is a qPRP: Tight Quantum Security Bound

Akinori Hosoyamada[1,2] and Tetsu Iwata[2]

[1] NTT Secure Platform Laboratories, Tokyo, Japan
akinori.hosoyamada.bh@hco.ntt.co.jp
[2] Nagoya University, Nagoya, Japan
{hosoyamada.akinori,tetsu.iwata}@nagoya-u.jp

Abstract. The Luby-Rackoff construction, or the Feistel construction, is one of the most important approaches to construct secure block ciphers from secure pseudorandom functions. The 3-round and 4-round Luby-Rackoff constructions are proven to be secure against chosen-plaintext attacks (CPAs) and chosen-ciphertext attacks (CCAs), respectively, in the classical setting. However, Kuwakado and Morii showed that a quantum superposed chosen-plaintext attack (qCPA) can distinguish the 3-round Luby-Rackoff construction from a random permutation in polynomial time. In addition, Ito et al. showed a quantum superposed chosen-ciphertext attack (qCCA) that distinguishes the 4-round Luby-Rackoff construction. Since Kuwakado and Morii showed the result, a problem of much interest has been how many rounds are sufficient to achieve provable security against quantum query attacks. This paper answers this fundamental question by showing that 4-rounds suffice against qCPAs. Concretely, we prove that the 4-round Luby-Rackoff construction is secure up to $O(2^{n/6})$ quantum queries. We also prove that the bound is tight by showing an attack that distinguishes the 4-round Luby-Rackoff construction from a random permutation with $O(2^{n/6})$ quantum queries. Our result is the first to demonstrate the tight security of a typical block-cipher construction against quantum query attacks, without any algebraic assumptions. To give security proofs, we use an alternative formalization of Zhandry's compressed oracle technique.

Keywords: symmetric-key cryptography · post-quantum cryptography · provable security · quantum security · the compressed oracle technique · quantum chosen plaintext attacks · Luby-Rackoff constructions.

1 Introduction

Post-quantum public-key cryptography has been one of the most actively researched areas in cryptography since Shor developed the polynomial-time integer factoring quantum algorithm [31]. NIST is working on a standardization process for post-quantum public-key schemes such as public-key encryption, key-establishment, and digital signature schemes [28].

On the other hand, for symmetric key cryptography, it was said that the security of symmetric-key schemes would not be much affected by quantum computers. However, a series of recent results has shown that some symmetric key schemes are also broken in polynomial time by using Simon's algorithm [32] if quantum adversaries have access to quantum circuits that implement keyed primitives [20,21,9,7,22,30,14,13,12,19], although they are proven or assumed to be secure in the classical setting. These examples illustrate the need of evaluating the post-quantum security of symmetric-key schemes.

Although many quantum query attacks on symmetric-key schemes have been proposed, only a little progress has been made on the *post-quantum provable security* of symmetric-key schemes. There are two possible post-quantum security notions for symmetric-key schemes: *standard security* and *quantum security* [34]. The standard security assumes adversaries have quantum computers, but have access to keyed oracles in a classical manner. On the other hand, the quantum security assumes adversaries can make queries to keyed primitives in quantum superpositions. If a scheme is proven to have quantum security, then it will remain secure even in a far future where all computations and communications are done in quantum superpositions. Therefore, it is a problem of much interest whether a classically secure symmetric-key scheme also has quantum security.

The Luby-Rackoff construction. The Luby-Rackoff construction, or the Feistel construction, is one of the most important approaches to construct efficient and secure block ciphers, which are pseudorandom permutations (PRPs), from efficient and secure pseudorandom functions (PRFs). A significant number of block ciphers including commonly used ones such as DES [26] and Camellia [4] were designed on the basis of this construction.

For families of functions $f_i := \{f_{i,k} : \{0,1\}^{n/2} \to \{0,1\}^{n/2}\}_{k \in \mathcal{K}}$ that are parameterized by k in a key space $\mathcal{K}$ $(1 \le i \le r)$, the r-round Luby-Rackoff construction $\mathsf{LR}_r(f_1, \ldots, f_r)$ is defined as follows: First, keys $k_1, \ldots, k_r$ are chosen independently and uniformly at random from $\mathcal{K}$. For each input $x_0 = x_{0L} \| x_{0R}$, where $x_{0L}, x_{0R} \in \{0,1\}^{n/2}$, the state is updated as

$$x_{(i-1)L} \| x_{(i-1)R} \mapsto x_{iL} \| x_{iR} := x_{(i-1)R} \oplus f_{i,k_i}(x_{(i-1)L}) \| x_{(i-1)L} \tag{1}$$

for $i = 1, \ldots, r$ in a sequential order (see Fig. 1). The output is the final state $x_r = x_{rL} \| x_{rR}$. Then the resulting function becomes a keyed permutation over $\{0,1\}^n$ with keys in $(\mathcal{K})^r$.

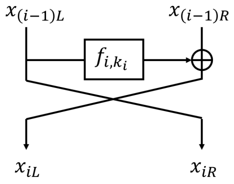

Fig. 1. The i-th round state update.

In the classical setting, if each f_i is a secure PRF, LR_r becomes a secure PRP against chosen-plaintext attacks (CPAs) for $r \ge 3$ and a secure PRP against chosen-ciphertext attacks (CCAs) for $r \geq 4$ [24], i.e., LR_r becomes a strong PRP. However, in the quantum setting, Kuwakado and Morii showed that LR_3 can be distinguished in polynomial time from a truly random permutation by a quantum superposed chosen-plaintext attack [21] (qCPA).[3] Moreover, Ito et al. showed that LR_4 can be distinguished in polynomial time by a quantum superposed chosen-ciphertext attack (qCCA) [19]. On the other hand, for any r, no post-quantum security proof of LR_r is known. A very natural question is then whether such a proof is feasible for some r, and if so, to determine the minimum number of r such that we can prove the post-quantum security of LR_r.

1.1 Our Contributions

As the first step to giving post-quantum security proofs for the Luby-Rackoff constructions, this paper shows that the 4-round Luby-Rackoff construction LR_4 is secure against qCPAs. In particular, we give a security bound of LR_4 against qCPAs when all round functions are truly random functions. We also prove that the bound is tight by showing a matching attack. Concretely, we show the following theorems.

Theorem 1 (Lower bound and upper bound, informal). *If all round functions are truly random functions, then the following claims hold.*

1. LR_4 *cannot be distinguished from a truly random permutation by qCPAs up to* $O(2^{n/6})$ *quantum queries.*
2. *A quantum algorithm exists that distinguishes* LR_4 *from a truly random permutation with a constant probability by making* $O(2^{n/6})$ *quantum chosen-plaintext queries.*

Theorem 2 (Construction of qPRP from qPRF, informal). *Suppose that each* f_i *is a secure PRF against efficient quantum query attacks, for* $1 \leq i \leq 4$. *Then* $\mathsf{LR}_4(f_1, f_2, f_3, f_4)$ *is a secure PRP against efficient qCPAs.*

See Table 1 for a summary of security proofs and attacks for LR_4. Observe that the provable security bound of $O(2^{n/6})$ quantum queries is tight in that we have a matching attack, and our result fills the gap to obtain complete characterization of LR_4 against quantum query adversaries.

Technical details. To give a quantum security proof for LR_4 in the case that all round functions are truly random, we use the *compressed oracle technique* developed by Zhandry [39]. To be precise, we give an alternative formalization of the technique and use it in our proofs.

One challenging obstacle to giving security proofs against quantum superposed query adversaries is that we cannot record *transcripts* of quantum queries and answers. Although it is trivial to store query-answer records in the classical setting, it is highly non-trivial to store them in the quantum setting, since measuring or copying (parts of) quantum states will lead to perturbing them, which may be detected by adversaries.

[3] Strictly speaking, the attack by Kuwakado and Morii works only when all round functions are keyed permutations. Kaplan et al. [20] showed that the attack works for more general cases.

Attack setting	Classical CPA	Classical CCA	Quantum CPA	Quantum CCA
Security proof	Secure up to $O(2^{n/4})$ queries [24]	Secure up to $O(2^{n/4})$ queries [24]	Secure up to $O(2^{n/6})$ queries **[Ours]** (Section 4)	No proofs (Insecure)
Distinguishing attack	$O(2^{n/4})$ queries [29]	$O(2^{n/4})$ queries [29]	$O(2^{n/6})$ queries **[Ours]** (Section 5)	$O(n)$ queries [19]

Table 1. Summary of security proofs and attacks for the 4-round Luby-Rackoff construction LR_4 when all round functions are truly random. In the quantum CPA/CCA settings, adversaries can make quantum superposed queries.

Zhandry's compressed oracle technique enables us to overcome the obstacle when oracles are truly random functions. The technique is so powerful that it can be used to show quantum indifferentiability of the Merkle-Damgård domain extender and quantum security for the Fujisaki-Okamoto transformation [39], in addition to the (tight) lower bounds for the multicollision-finding problems [23]. His crucial observation is that we can record queries and answers without affecting quantum states by appropriately forgetting previous records. In addition, he observed that transcripts of queries can be recorded in an compressed manner, which enables us to simulate random functions (random oracles) extremely efficiently.

The compressed oracle technique is a powerful tool, although the formalization of the technique is (necessarily) somewhat complex. A simpler alternative formalization would be better to have when we apply the technique to complex schemes that use multiple random functions, such as the Luby-Rackoff construction.

Zhandry's formalization enables us to both record transcripts and compress recorded data. We need the compression to efficiently simulate random functions but not when we focus on information theoretic security of cryptographic schemes.

With this in mind, we modify the construction of Zhandry's *compressed standard oracle* and give an alternative formalization of Zhandry's technique without compression of the database. Moreover, we scrutinize the properties of our modified oracle and observe that its behaviors can be described in an intuitively clear manner by introducing some *error terms*. We also explicitly describe error terms, which enables us to give mathematically rigorous proofs. We name our alternative oracle the *recording standard oracle with errors*, because it records transcripts of queries and its behavior is described with error terms. We believe that our alternative formalization and analyses for our oracle's behavior help us understand Zhandry's technique better, which will lead to the technique being applied even more widely. See Section 3 for details on our alternative formalization.

By heavily using our recording standard oracle with errors, we complete the security proof of LR_4 against quantum superposed query attacks, taking advantage of classical proof intuitions to some extent. First, we consider LR_3, the 3-round Luby-Rackoff construction, which is easy to distinguish from a truly random permutation, and a slightly modified version of it, where the last-round state update of LR_3 is modified.

Our observation is that even quantum (chosen-plaintext) query adversaries seem to have difficulty noticing the modification, and we are actually able to show that this is indeed the case. Intuitively, the proof is possible since even quantum query adversaries cannot feasibly produce collisions on the input of the third round. Second, we prove that a modified version of the 2-round Luby-Rackoff construction is hard to distinguish from a truly random permutation. Intuitively, we show the hardness by proving it is hard even for quantum adversaries to produce collisions on the input of the second round of the modified 2-round Luby-Rackoff construction. To show the hardness results, we use our recording standard oracle with errors. Once we prove these two hardness results, the rest of the proof follows easily without any argument specific to the quantum setting. Our proof is much more complex than the classical one, though, we give rigorous and careful analyses. See Section 4 for details on the security proof of LR_4.

In contrast to the high complexity of the provable security result, our quantum distinguishing attack is a simple quantum polynomial speed-up of existing classical attacks. See Section 5 for details on the quantum distinguishing attack.

1.2 Related Works

Other than the ones introduced above, security proofs against quantum query adversaries for symmetric key schemes include a proof for standard modes of operations by Targhi et al. [3], one for the Carter-Wegman message authentication codes (MACs) by Boneh and Zhandry [6], one for NMAC by Song and Yun [33], and one for Davies-Meyer and Merkle-Damgård constructions by Hosoyamada and Yasuda [18]. Zhandry showed the PRP-PRF switching lemma in the quantum setting [36] and demonstrated that quantum-secure PRPs can be constructed from quantum-secure PRFs by using a technique of format preserving encryption [37]. Czajkowski et al. showed that the sponge construction is *collapsing* (collapsing is a quantum extension of the classical notion of collision-resistance) when round functions are one-way random permutations or functions [10].[4] Alagic and Russell proved that polynomial-time attacks against symmetric-key schemes that use Simon's algorithm can be prevented by replacing XOR operations with modular additions on the basis of an algebraic hardness assumption [1]. However, Bonnetain and Naya-Plasecia showed that the countermeasure is not practical [8]. For standard security proofs (against quantum adversaries that make only classical queries) for symmetric-schemes, Mennink and Szepieniec proved security for XOR of PRPs [25]. Czajkowski et al. [11] recently showed that the compressing technique can be extended to quantum oracles with non-uniform distributions such as a random permutation, and showed quantum indifferentiability of the sponge construction.

1.3 Updates from the Conference Version

The preliminary version of this paper was presented at Asiacrypt 2019 [15,16]. The security was proven only up to $O(2^{n/12})$ quantum queries in the preliminary version, while the current version proves the tight bound of $O(2^{n/6})$. Roughly speaking, the

[4] Note that the condition in which the round function of the sponge construction is one-way is unusual in the context of classical symmetric-key provable security.

previous version showed the main proposition in Section 4.2 (Proposition 6 in the current version) by using previous proof techniques. On the other hand, the current version shows the proposition by using the recording standard oracle with errors, which leads to the tight security bound. Section 4.3 is changed accordingly because it uses the result in Section 4.2.

We emphasize that obtaining tight security bounds is very important in the symmetric key setting: The security parameter n is often fixed to a concrete value, and unlike in the public key setting, n cannot be scaled easily. For instance, we cannot increase the block length of the Advanced Encryption Standard (AES), and even if we can define a block cipher with a larger block length as in Rijndael, the deployment is often impractical. More concretely, when $n = 128$ (which is a usual concrete parameter used for instance in the Camellia block cipher [4]), the $O(2^{n/12})$ bound does not exclude the possibility of an attack with (for instance) $2^{128/12} < 2^{11}$ quantum complexity, which could be a real threat in the foreseeable future. Given the current stage of development in quantum computers, clarifying the (non-)existence of such an attack is a very interesting problem from a practical view point as well.

In addition, the previous version contains an error in Section 4.1 (see Section A in Appendix for the details on the error in the preliminary version). The current version fixes the error, and we changed details on the proof strategy of Proposition 4. The contents of Section 4.1 before Proposition 5 are not significantly changed, while most of the remaining parts of Section 4.1 in the preliminary version are modified and integrated as Proposition 5. The proof of Proposition 5 is written from scratch. To correct the error, we showed an additional proposition, which are added into Section 3 as Proposition 3.

Proposition 2 in the preliminary version contains an additional claim, but it is removed in this version since it is not used in security proofs.

1.4 Paper Organization

Section 2 gives basic notations and definitions used throughout the paper. Section 3 gives an overview on Zhandry's compressed oracle technique and our alternative formalization. Section 4 gives the security proof, and Section 5 shows the matching upper bound. Section 6 concludes the paper.

2 Preliminaries

This section describes notations and definitions. In this paper, all algorithms (or adversaries) are assumed to be quantum algorithms, and make quantum superposed queries to oracles. For any finite sets X and Y, let $\mathsf{Func}(X, Y)$ denote the set of all functions from X to Y. For any n-bit string x, we denote the left-half $n/2$-bits of x by x_L and the right-half $n/2$-bits by x_R, respectively. We identify the set $\{0, 1\}^m$ with the set of the integers $\{0, 1, \ldots, 2^m - 1\}$.

2.1 Quantum Computation

Throughout this paper, we assume that readers have basic knowledge about quantum computation and finite dimensional linear algebra (see textbooks such as [27] for an introduction). We use the quantum circuit model for the model of quantum computation. We measure complexity of quantum algorithms by the number of queries they make and the number of quantum gates required to implement the algorithms. When we take the number of gates into account as the complexity of a quantum algorithm, we assume that quantum circuits are composed of quantum gates that are chosen from a fixed universal gate set (e.g., Clifford+T gates). If a quantum adversary $\mathcal{A}$ is allowed to make quantum queries to an oracle O, we assume that a special oracle gate to make queries to O is available to $\mathcal{A}$ in addition to Clifford+T gates. Let $\|\cdot\|$ and $\|\cdot\|_{\mathsf{tr}}$ denote the norm of vectors and the trace norm of operators, respectively. In addition, let $\mathsf{td}(\cdot,\cdot)$ denote the trace distance. For Hermitian operators ρ,σ on a Hilbert space $\mathcal{H}$, $\mathsf{td}(\rho,\sigma)=\frac{1}{2}\|\rho-\sigma\|_{\mathsf{tr}}$ holds. For a mixed state ρ of a joint quantum system $\mathcal{H}_A\otimes\mathcal{H}_B$, let $\mathsf{tr}_B(\rho)$ (resp., $\mathsf{tr}_A(\rho)$) denote the partial trace of ρ over $\mathcal{H}_B$ (resp., $\mathcal{H}_A$). For an integer $n\geq 1$, I_n and $H^{\otimes n}$ denote the identity operator on n-qubit systems and the n-qubit Hadamard operator, respectively. If n is clear from the context, we just write I instead of I_n, for concision. By abuse of notation, for an operator V, we sometimes use the same notation V to denote $V\otimes I$ or $I\otimes V$ for simplicity, when it will cause no confusion. In addition, for a vector $|\phi\rangle$ and a positive integer m, we sometimes use the same notation $|\phi\rangle$ to denote $|\phi\rangle\otimes|0^m\rangle$ or $|0^m\rangle\otimes|\phi\rangle$ for simplicity, when it will cause no confusion.

Quantum oracle query algorithms. Following previous works (see [5], for example), any quantum oracle query algorithm $\mathcal{A}$ that makes at most q queries to oracles is modeled as a sequence of unitary operators $(U_0,\dots,U_q)$, where each U_i is a unitary operator on an ℓ-qubit quantum system, for some integer ℓ. Here, U_0 can be regarded as the initialization process, and for $1\leq i\leq q-1$, U_i is the process after the i-th query. U_q can be regarded as the finalization process. We only consider quantum algorithms that take no inputs and assume that the initial state of $\mathcal{A}$ is $|0^\ell\rangle$.

Stateless oracles. For a function $f:\{0,1\}^m\rightarrow\{0,1\}^n$, the quantum oracle of f is defined as the unitary operator $O_f:|x,y\rangle\mapsto|x,y\oplus f(x)\rangle$. When we run $\mathcal{A}$ relative to the oracle O_f, the unitary operators $U_0,O_f,\dots,U_{q-1},O_f,U_q$ act sequentially on the initial state $|0^\ell\rangle$, the resulting quantum state $U_qO_fU_{q-1}\cdots O_fU_0\,|0^\ell\rangle$ is measured, and finally $\mathcal{A}$ returns the measurement result as the output. f may be chosen in accordance with a distribution at the beginning of each game. We consider that O_f acts on the first $(m+n)$-qubits of $\mathcal{A}$'s quantum states. In other words, we assume that $\mathcal{A}$'s quantum state is a vector of a Hilbert space $\mathcal{H}_{\mathcal{A}}=\mathcal{H}_{\mathrm{query}}\otimes\mathcal{H}_{\mathrm{answer}}\otimes\mathcal{H}_{\mathrm{work}}$ such that $\dim\mathcal{H}_{\mathrm{query}}=2^m$, $\dim\mathcal{H}_{\mathrm{answer}}=2^n$, and $\dim\mathcal{H}_{\mathrm{work}}=2^{\ell-m-n}$, and O_f acts on $\mathcal{H}_{\mathrm{query}}\otimes\mathcal{H}_{\mathrm{answer}}$. (We regard that $\mathcal{H}_{\mathrm{query}}$, $\mathcal{H}_{\mathrm{answer}}$, and $\mathcal{H}_{\mathrm{work}}$ correspond to $\mathcal{A}$'s register to send queries to the oracle O_f, receive answers from O_f, and perform offline computations, respectively.) Let us denote the event that $\mathcal{A}$ runs relative to the oracle O_f and returns an output α by $\alpha\leftarrow\mathcal{A}^{O_f}()$ or by $\mathcal{A}^{O_f}()\rightarrow\alpha$.

Stateful oracles. In this paper, we also consider more general cases in which quantum oracles are stateful, i.e., oracles have ℓ'-qubit quantum states for an integer $\ell' \geq 0$.[5] In these cases, an oracle O is modeled as a sequence of unitary operators $(O_1, \ldots, O_q)$ that acts on the first $(m+n)$-qubits of $\mathcal{A}$'s quantum states in addition to O's quantum states. That is, we assume that each O_i acts on $\mathcal{H}_{\text{query}} \otimes \mathcal{H}_{\text{answer}} \otimes \mathcal{H}_O$, where $\mathcal{H}_O$ is the Hilbert space of the oracle O's quantum states. The entire quantum state of $\mathcal{A}$ and O is a vector of $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_O = \left(\mathcal{H}_{\text{query}} \otimes \mathcal{H}_{\text{answer}} \otimes \mathcal{H}_{\text{work}}\right) \otimes \mathcal{H}_O$. When we run $\mathcal{A}$ relative to the oracle O, the unitary operators $(U_0 \otimes I_{\ell'}), O_1, \ldots, (U_{q-1} \otimes I_{\ell'}), O_q, (U_q \otimes I_{\ell'})$ act in a sequential order on the initial state $|0^\ell\rangle \otimes |\mathsf{init}_O\rangle$, where $|\mathsf{init}_O\rangle \in \mathcal{H}_O$ is the initial state of O. Finally, $\mathcal{A}$ measures the resulting quantum state $(U_q \otimes I_{\ell'})O_q(U_{q-1} \otimes I_{\ell'}) \cdots O_1(U_0 \otimes I_{\ell'})\,|0^\ell\rangle \otimes |\mathsf{init}_O\rangle$, and returns the measurement result as the output. If O has no state and $O_i = O_f$ holds for each i, the behavior of $\mathcal{A}$ relative to O precisely matches that of $\mathcal{A}$ relative to the stateless oracle O_f. Thus, our model of stateful oracles is an extension of the typical model of stateless oracles described above. O may be chosen in accordance with a distribution at the beginning of each game. We denote the event that $\mathcal{A}$ runs relative to the oracle O and returns an output α by $\alpha \leftarrow \mathcal{A}^O()$ or by $\mathcal{A}^O() \to \alpha$.

Quantum distinguishing advantages. Let $\mathcal{A}$ be a quantum algorithm that makes at most q queries and outputs 0 or 1 as the final output, and let O_1 and O_2 be some oracles. We consider the situation in which O_1 and O_2 are chosen randomly in accordance with some distributions. We define the *quantum distinguishing advantage* of $\mathcal{A}$ by

$$\mathbf{Adv}^{\text{dist}}_{O_1,O_2}(\mathcal{A}) := \left|\Pr_{O_1}\left[\mathcal{A}^{O_1}() \to 1\right] - \Pr_{O_2}\left[\mathcal{A}^{O_2}() \to 1\right]\right|. \tag{2}$$

When we are interested only in the number of queries and do not consider other complexities such as the number of gates (i.e., we focus on information theoretic adversaries), we use the notation

$$\mathbf{Adv}^{\text{dist}}_{O_1,O_2}(q) := \max_{\mathcal{A}} \left\{\mathbf{Adv}^{\text{dist}}_{O_1,O_2}(\mathcal{A})\right\}, \tag{3}$$

where the maximum is taken over all quantum algorithms that make at most q quantum queries.

Quantum PRF advantages. Let RF denote the quantum oracle of random functions, i.e., the oracle such that a function $f \in \mathsf{Func}(\{0,1\}^m, \{0,1\}^n)$ is chosen uniformly at random, and adversaries are given oracle access to O_f.

Let $\mathcal{F} = \{F_k : \{0,1\}^m \to \{0,1\}^n\}_{k \in \mathcal{K}}$ be a family of functions. Let us use the same symbol $\mathcal{F}$ to denote the oracle such that k is chosen uniformly at random, and adversaries are given oracle access to O_{F_k}. In addition, let $\mathcal{A}$ be an oracle query algorithm that outputs 0 or 1. Then we define the quantum pseudorandom-function

[5] Here we do not mean that our model captures all reasonable stateful quantum oracles. We use our model of stateful quantum oracles just for intermediate arguments to prove our main results, and the claims of the main results are described in the typical model of stateless oracles.

(qPRF) advantage by $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(\mathcal{A}) := \mathbf{Adv}^{\mathrm{dist}}_{\mathcal{F},\mathsf{RF}}(\mathcal{A})$. Similarly, we define $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(q)$ by $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(q) := \max_{\mathcal{A}} \left\{\mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(\mathcal{A})\right\}$, where the maximum is taken over all quantum algorithms $\mathcal{A}$ that make at most q quantum queries.

Quantum PRP advantages. By RP we denote the quantum oracle of random permutations, i.e., the oracle such that a permutation $P \in \mathsf{Perm}(\{0,1\}^n)$ is chosen uniformly at random, and adversaries are given oracle access to O_P.

Let $\mathcal{P} = \{P_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\mathcal{K}}$ be a family of permutations. We use the same symbol $\mathcal{P}$ to denote the oracle such that k is chosen uniformly at random, and adversaries are given oracle access to O_{P_k}. Let $\mathcal{A}$ be an oracle query algorithm that outputs 0 or 1, and we define the quantum pseudorandom-permutation (qPRP) advantage by $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(\mathcal{A}) := \mathbf{Adv}^{\mathrm{dist}}_{\mathcal{P},\mathsf{RP}}(\mathcal{A})$. Similarly, we define $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(q)$ by $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(q) := \max_{\mathcal{A}} \left\{\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(\mathcal{A})\right\}$, where the maximum is taken over all quantum algorithms $\mathcal{A}$ that make at most q quantum queries.

The following lemma is a quantum version of the PRP-PRF switching lemma.

Proposition 1 (Theorem 2 in of [36]). *For any quantum query adversary $\mathcal{A}$ that makes at most q quantum queries, $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RP}}(\mathcal{A}) \leq O(q^3/2^n)$ holds. (Here we consider a random permutation over $\{0,1\}^n$.)*

Security against efficient adversaries. An algorithm $\mathcal{A}$ is called *efficient* if it can be realized as a quantum circuit that has a polynomial number of quantum gates in n. A set of functions $\mathcal{F}$ (resp., a set of permutations $\mathcal{P}$) is a *quantumly secure PRF* (resp., a *quantumly secure PRP*) if the following properties are satisfied:

1. Uniform sampling $f \xleftarrow{\$} \mathcal{F}$ (resp., $P \xleftarrow{\$} \mathcal{P}$) and evaluation of each f (resp., each P) can be implemented on quantum circuits that have a polynomial number of quantum gates in n.
2. $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(\mathcal{A})$ (resp., $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(\mathcal{A})$) is *negligible* (i.e., for any positive integer c, it is upper bounded by n^{-c} for all sufficiently large n) for any efficient algorithm $\mathcal{A}$.

2.2 The Luby-Rackoff Constructions

The Luby-Rackoff construction [24] is a construction of n-bit permutations from $n/2$-bit functions by using the Feistel network.

Fix $r \geq 1$, and for $1 \leq i \leq r$, let $f_i := \{f_{i,k} : \{0,1\}^{n/2} \to \{0,1\}^{n/2}\}_{k\in\mathcal{K}}$ be a family of functions parameterized by key k in a key space $\mathcal{K}$. Then, the Luby-Rackoff construction for $f_1,\dots,f_r$ is defined as a family of n-bit permutations $\mathsf{LR}_r(f_1,\dots,f_r) := \{\mathsf{LR}_r(f_{1,k_1},\dots,f_{r,k_r})\}_{k_1,\dots,k_r\in\mathcal{K}}$ with the key space $(\mathcal{K})^r$. For each fixed key $(k_1,\dots,k_r)$, $\mathsf{LR}_r(f_{1,k_1},\dots,f_{r,k_r})$ is defined by the following procedure: First, given an input $x_0 \in \{0,1\}^n$, divide it into $n/2$-bit strings x_{0L} and x_{0R}. Second, iteratively update n-bit states as

$$(x_{(i-1)L}, x_{(i-1)R}) \mapsto (x_{iL}, x_{iR}) := (x_{(i-1)R} \oplus f_{i,k_i}(x_{(i-1)L}), x_{(i-1)L}) \tag{4}$$

for $1 \leq i \leq r$. Finally, return the final state $x_r := x_{rL} \| x_{rR}$ as the output (see Fig. 2).

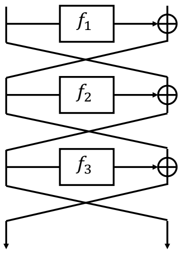

Fig. 2. The 3-round Luby-Rackoff construction.

The resulting function $\mathsf{LR}_r(f_{1,k_1}, \ldots, f_{r,k_r}) : x_0 \mapsto x_r$ becomes an n-bit permutation owing to the property of the Feistel network. Each f_{i,k_i} is called the i-th round function. When we say that an adversary is given oracle access to $\mathsf{LR}_r(f_1, \ldots, f_r)$, we consider the situation in which keys $k_1, \ldots, k_r$ are first chosen independently and uniformly at random, and then the adversary runs relative to the stateless oracle $O_{\mathsf{LR}_r(f_{1,k_1},\ldots,f_{r,k_r})}$: $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus \mathsf{LR}_r(f_{1,k_1}, \ldots, f_{r,k_r})(x)\rangle$. When each round function is chosen from $\mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$ uniformly at random (i.e., each f_i is the set of all functions $\mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$ for all i), we use the notation LR_r for short.

3 An Alternative Formalization for the Compressed Oracle Technique

Many security proofs in the *classical* random oracle model (ROM) implicitly rely on the fact that transcripts of queries and answers can be recorded. However, such proofs do not necessarily work in the *quantum random oracle model* (QROM) [5], since recording transcripts may significantly perturb quantum states, which might be detected by adversaries. To solve this issue, Zhandry introduced the "compressed oracle technique" [39] to enable us to record transcripts of queries and answers even in QROM. In addition to recording transcripts, Zhandry's technique enables us to simulate the random oracle extremely efficiently by compressing databases of transcripts.

Zhandry's technique was originally developed for QROM, in which adversaries can make direct queries to random functions, but it can also be applied when adversaries can make queries to random functions only indirectly. In particular, one may think that the technique is applicable to giving a security proof for the Luby-Rackoff constructions when all round functions are truly random.

The compressed oracle technique is very insightful and promising, but its formal description is somewhat (necessarily) complex. A simpler formalization would be better to have when we want to apply the technique to complex schemes that use multiple random functions, such as the Luby-Rackoff construction.

Security proofs of symmetric-key mode of operations often involve the analysis of information theoretic adversaries. When we are interested in such information theoretic security, we do not care about efficient simulation of a random oracle, and thus do not have to compress databases. With this in mind, we modify the construction of Zhandry's *compressed standard oracle* and give an alternative formalization of his technique without compressing databases that can be used when we focus on (quantum) information theoretic security.

We also study the behavior of our oracle in detail and show that its properties can be described intuitively by introducing the notion of error terms. Since our oracle records transcripts of queries and its behavior is described with error terms, we call our oracle *recording standard oracle with errors* and denote it by RstOE.

In Section 3.1 we give an overview of the original technique by Zhandry, and describe which part of it can be improved. Then, in Section 3.2 we describe our alternative formalization for the technique.

3.1 An Overview of the Original Technique

First, Zhandry observed that the oracle O_f can be implemented with an encoding of f and an operator stO that is independent of f. In this subsection, we consider that each function $f : \{0,1\}^m \to \{0,1\}^n$ is encoded into the $(n2^m)$-qubit state $|f\rangle = |f(0)\|f(1)\|\cdots\|f(2^m-1)\rangle$. The operator stO is the unitary operator that acts on $(n+m+n2^m)$-qubit states defined as

$$\mathsf{stO} : |x\rangle|y\rangle \otimes |\alpha_0\rangle\cdots|\alpha_{2^m-1}\rangle \mapsto |x\rangle|y \oplus \alpha_x\rangle \otimes |\alpha_0\rangle\cdots|\alpha_{2^m-1}\rangle, \tag{5}$$

where $\alpha_x \in \{0,1\}^n$ for each $0 \leq x \leq 2^m - 1$. We can easily confirm that $\mathsf{stO}\,|x\rangle|y\rangle|f\rangle = |x\rangle|y \oplus f(x)\rangle|f\rangle$ holds. Here, we consider that $|x\rangle|y\rangle$ corresponds to the first $(m+n)$-qubits of adversaries' registers.

When f is chosen uniformly at random and $\mathcal{A}$ runs relative to stO and $|f\rangle$ (i.e., $\mathcal{A}$ runs relative to the quantum oracle of a random function), the whole quantum state before $\mathcal{A}$ makes the $(i+1)$-st quantum query becomes

$$|\phi_{f,i+1}\rangle = (U_i \otimes I)\mathsf{stO}(U_{i-1} \otimes I)\mathsf{stO}\cdots\mathsf{stO}(U_0 \otimes I)\,|0^\ell\rangle|f\rangle \tag{6}$$

with probability $1/2^{n2^m}$. Here, we assume that $\mathcal{A}$ has ℓ-qubit quantum states.

Random choice of f can be implemented by first making the uniform superposition of functions $\sum_f \frac{1}{\sqrt{2^{n2^m}}}|f\rangle = H^{\otimes n2^m}|0^{n2^m}\rangle$ and then measuring the state with the computational basis. So far we have considered that a random function f is chosen at the beginning of games, but the output distribution of $\mathcal{A}$ will not be changed even if we measure the $|f\rangle$ register at the same time as we measure $\mathcal{A}$'s register. Thus, below we consider that all quantum registers including those of functions are measured only once at the end of each game.

Then the whole quantum state before $\mathcal{A}$ makes the $(i+1)$-st quantum query becomes

$$|\phi_{i+1}\rangle = \sum_f |\phi_{f,i+1}\rangle = (U_i \otimes I)\mathsf{stO}\cdots\mathsf{stO}(U_0 \otimes I)\left(|0^\ell\rangle \otimes \sum_f \frac{1}{\sqrt{2^{n2^m}}}|f\rangle\right). \tag{7}$$

Next, we change the basis of the y register and α_i registers in (5) from the standard computational basis $\{|u\rangle\}_{u\in\{0,1\}^n}$ to one called the *Fourier basis* $\{H^{\otimes n}|u\rangle\}_{u\in\{0,1\}^n}$[6] by

[6] Note that the Hadamard operator $H^{\otimes n}$ corresponds to the Fourier transformation over the group $(\mathbb{Z}/2\mathbb{Z})^{\oplus n}$.

Zhandry [39]. In what follows, we use the symbol "$\widehat{\ }$" to denote the encoding of classical bit strings into quantum states by using the Fourier basis instead of the computational basis, and we ambiguously denote $H^{\otimes n}|u\rangle$ by $|\widehat{u}\rangle$ for each $u \in \{0,1\}^n$. Then, it can be easily confirmed that

$$\mathsf{stO}\,|x\rangle|\widehat{y}\rangle \otimes |\widehat{\alpha_0}\rangle \cdots |\widehat{\alpha_{2^m-1}}\rangle = |x\rangle|\widehat{y}\rangle \otimes |\widehat{\alpha_0}\rangle \cdots |\widehat{\alpha_x \oplus y}\rangle \cdots |\widehat{\alpha_{2^m-1}}\rangle \tag{8}$$

holds. Intuitively, the direction of data writing changes when we change the basis: When we use the standard computational basis, data is written from the function registers to adversaries' registers as in (5). On the other hand, when we use the Fourier basis, data is written in the opposite direction as in (8). With the Fourier basis, $|\phi_{i+1}\rangle$ can be written as

$$|\phi_{i+1}\rangle = (U_i \otimes I)\mathsf{stO}(U_{i-1} \otimes I)\mathsf{stO} \cdots \mathsf{stO}(U_0 \otimes I)\left(|0^\ell\rangle \otimes |\widehat{0^{n2^m}}\rangle\right). \tag{9}$$

Here, note that $\sum_f |f\rangle = H^{\otimes n2^m}|0^{n2^m}\rangle = |\widehat{0^{n2^m}}\rangle$ holds. In particular, the register of the functions are initially set as $|\widehat{0^{n2^m}}\rangle$, and at most one data is written (in superpositions) when an adversary makes a query. Thus

$$|\phi_{i+1}\rangle = \sum_{xyz\widehat{D}} a'_{xyz\widehat{D}} |xyz\rangle \otimes |\widehat{D}\rangle \tag{10}$$

holds for some complex numbers $a'_{xyz\widehat{D}}$ such that $\sum_{xyz\widehat{D}} |a'_{xyz\widehat{D}}|^2 = 1$, where each x is an m-bit string that corresponds to $\mathcal{A}$'s register to send queries to oracles, y is an n-bit string that corresponds to $\mathcal{A}$'s register to receive answers from oracles, z corresponds to $\mathcal{A}$'s remaining register to perform offline computations, and $\widehat{D} = \widehat{\alpha_0}\|\cdots\|\widehat{\alpha_{2^m-1}}$ is a concatenation of 2^m many n-bit strings.

Zhandry's key observation is that, since stO adds at most one data to the $\widehat{D}$-register in each query, $\widehat{\alpha}_x \neq 0^n$ holds for at most i many x, and thus $\widehat{D}$ can be regarded as a database with at most i many non-zero entries. (Note that $\widehat{D}$ may contain fewer than i non-zero entries. For example, if a state $|x\rangle|\widehat{y}\rangle$ is successively queried to stO twice, then the database will remain unchanged since $\mathsf{stO} \cdot \mathsf{stO} = I$.) We use the same notation $\widehat{D}$ to denote the database and call it the *Fourier database* since now we are using the Fourier basis for $\widehat{D}$. Each entry of the database $\widehat{D}$ has the form $(x, \widehat{\alpha}_x)$, where $x \in \{0,1\}^m$, $\widehat{\alpha}_x \in \{0,1\}^n$, and $\widehat{\alpha}_x \neq 0^n$.

Intuitively, if the Fourier database $\widehat{D}$ contains an entry $(x, \widehat{\alpha}_x)$, it means that $\mathcal{A}$ has queried x to a random function f and holds some information about the value $f(x)$. Hence $\widehat{D}$ can be seen as a record of transcripts for queries and answers. However, it is still not clear what kind of information $\mathcal{A}$ has about the value $f(x)$, since we are now using the Fourier basis. To clarify this information, let the Hadamard operator $H^{\otimes n}$ act on each $\widehat{\alpha}_x$ in $\widehat{D}$ and obtain another (superposition of) database D. Then, intuitively, D satisfies the condition in which "$(x, \alpha_x) \in D$ corresponds to the condition that $\mathcal{A}$ has queried x to the oracle and received the value α_x in response." We call D a *standard database*.

In summary, Zhandry observed that the quantum random oracle can be described as a stateful quantum oracle CstO. The whole quantum state of an adversary $\mathcal{A}$ and the oracle just before the $(i+1)$-st query is

$$|\phi_{i+1}\rangle = \sum_{xyzD} a_{xyzD} |xyz\rangle \otimes |D\rangle, \tag{11}$$

where each D is a standard database that contains at most i entries. Initially, the database D is empty. Intuitively, when $\mathcal{A}$ makes a query $|x, y\rangle$ to the oracle, CstO does the following three-step procedure[7].

The three-step procedure of CstO.

1. Look for a tuple $(x, \alpha_x) \in D$. If one is found, respond with $|x, y \oplus \alpha_x\rangle$.
2. If no tuple is found, create new registers initialized to the state $\frac{1}{\sqrt{2^n}} \sum_{\alpha_x} |\alpha_x\rangle$. Add the registers (x, α_x) to D. Then respond with $|x, y \oplus \alpha_x\rangle$.
3. Finally, regardless of whether the tuple was found or added, there is now a tuple (x, α_x) in D, which may have to be removed. To do so, test whether the registers containing α_x contain 0^n in the Fourier basis. If so, remove the tuple from D. Otherwise, leave the tuple in D.

Intuitively, the first and second steps correspond to the classical *lazy sampling*, which do the following procedure: When an adversary makes a query x to the oracle, look for a tuple (x, α_x) in the database. If one is found, respond with α_x (this part corresponds to the first procedure of CstO). If no tuple is found, *choose α_x uniformly at random from* $\{0, 1\}^n$ (this part corresponds to creating the superposition $\frac{1}{\sqrt{2^n}} \sum_{\alpha_x} |\alpha_x\rangle$ in the second step of CstO), respond with α_x, and add (x, α_x) to the database.

The third "test and forget" step is crucial and specific to the quantum setting. Intuitively, the third step forgets data that is no longer used by the adversary from the database. By appropriately forgetting information, we can record transcripts of queries and answers without perturbing quantum states.

Formalization with compression. On the basis of above clever intuitions, Zhandry gave a formalized description of the compressed standard oracle CstO (although we do not give the explicit description here). Note that, since each database D has at most i entries before the $(i+1)$-st query, D can be encoded in a compressed manner by using only $O(i(m+n))$ qubits. With this observation, CstO is formalized in such a way that it has $O(i(m+n))$-qubit states before the $(i+1)$-st query for each i, which enables us to simulate a random oracle very efficiently on the fly, without an a priori bound on the number of queries (which required computational assumption before Zhandry's work).

3.2 Our Alternative Formalization

Next we give our alternative formalization. The original oracle CstO maintains only an $O(i(m+n))$-qubit state by compressing databases. On the other hand, in our alternative

[7] Note that this three-step procedure is a quoted verbatim from a preliminary full version of the original paper [38] on IACR Cryptology ePrint archive, except that the symbol y' and 0 are used instead of α_x and 0^n, respectively, in the original procedure.

formalization, we do not consider any compression to focus on recording transcripts of queries, and our oracle always has $(n+1)2^m$-qubit states.

From now on, we represent each function $f : \{0,1\}^m \to \{0,1\}^n$ as an $(n+1)2^m$-bit string $(0\|f(0))\|(0\|f(1))\|\cdots\|(0\|f(2^m-1))$. Remember that the whole quantum state after $\mathcal{A}$ makes the i-th query is described as

$$|\tilde{\phi}_i\rangle = \mathsf{stO}(U_{i-1}\otimes I)\mathsf{stO}\cdots\mathsf{stO}(U_0\otimes I)\left(|0^\ell\rangle \otimes \sum_f \frac{1}{\sqrt{2^{n2^m}}}|f\rangle\right). \tag{12}$$

At each query, unlike the original technique that adds/deletes at most one entry to/from each database, we first "decode" superpositions of databases to superpositions of functions when an adversary makes a query, then respond to the adversary, and finally "encode" again superpositions of functions to superpositions of databases. Below we describe our encoding.

Encoding functions to databases: Intuitive descriptions. Modifying the idea of Zhandry, we apply the following operations to the $|f\rangle$-register of $|\tilde{\phi}_i\rangle$ (i.e., just after the i-th query).

1. Let the Hadamard operator $H^{\otimes n}$ act on the $f(x)$ register for all x. Now the state becomes
$$\sum_{xyz\widetilde{D}} a'_{xyz\widetilde{D}} |xyz\rangle \otimes |\widetilde{D}\rangle \tag{13}$$
for some complex numbers $a'_{xyz\widetilde{D}}$, where each $\widetilde{D} = (0\|\widehat{\alpha}_0)\|\cdots\|(0\|\widehat{\alpha}_{2^m-1})$ is a concatenation of 2^m many $(n+1)$-bit strings, and $\widehat{\alpha}_x \neq 0^n$ at most i-many x.
2. For each x, if $\widehat{\alpha}_x \neq 0^n$, flip the bit just before $\widehat{\alpha}_x$. Now each $\widetilde{D}$ changes to the bit string $(b_0\|\widehat{\alpha}_0)\|\cdots\|(b_{2^m-1}\|\widehat{\alpha}_{2^m-1})$, where $b_x \in \{0,1\}$, and $b_x = 1$ if and only if $\widehat{\alpha}_x \neq 0^n$.
3. For each $x \in \{0,1\}^n$, let the n-bit Hadamard transformation $H^{\otimes n}$ act on $|\widehat{\alpha}_x\rangle$ if and only if $b_x = 1$. Then the quantum state becomes
$$|\tilde{\psi}_i\rangle := \sum_{xyzD} a_{xyzD} |xyz\rangle \otimes |D\rangle \tag{14}$$
for some complex numbers a_{xyzD}, where each D is a concatenation of 2^m many $(n+1)$-bit strings $(b_0\|\alpha_0)\|\cdots\|(b_{2^m-1}\|\alpha_{2^m-1})$ such that $b_x \neq 0$ holds for at most i many x, and intuitively $b_x \neq 0$ means that $\mathcal{A}$ has queried x to a random function f and has information that $f(x) = \alpha_x$.

Encoding functions to databases: Formal descriptions. The above three operations can be formally realized as actions of unitary operators on $|f\rangle$-registers. The first one is realized as $\mathsf{IH} := (I_1 \otimes H^{\otimes n})^{\otimes 2^m}$. The second one is realized as $U_{\text{toggle}} := (I_1 \otimes |0^n\rangle\langle 0^n| + X \otimes (I_n - |0^n\rangle\langle 0^n|))^{\otimes 2^m}$, where X is the 1-qubit operator such that $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$. The third one is realized by the operator $\mathsf{CH} := (CH^{\otimes n})^{\otimes 2^m}$, where $CH := |0\rangle\langle 0| \otimes I_n + |1\rangle\langle 1| \otimes H^{\otimes n}$.

We call the action of unitary operator $U_{\text{enc}} := \mathsf{CH} \cdot U_{\text{toggle}} \cdot \mathsf{IH}$ and its conjugate U^*_{enc} *encoding* and *decoding*, respectively. By using our encoding and decoding, the recording standard oracle with errors is defined as follows.

Definition 1 (Recording standard oracle with errors). *The* recording standard oracle with errors *is the stateful quantum oracle such that queries are processed with the unitary operator* RstOE *defined by* $\mathsf{RstOE} := (I \otimes U_{\text{enc}}) \cdot \mathsf{stO} \cdot (I \otimes U^*_{\text{enc}})$.

Note that $|\tilde{\psi}_i\rangle = \mathsf{RstOE}(U_{i-1} \otimes I)\mathsf{RstOE} \cdots \mathsf{RstOE}(U_0 \otimes I)(|0^\ell\rangle \otimes |0^{(n+1)2^m}\rangle)$ and $|\tilde{\phi}_i\rangle = (I \otimes U^*_{\text{enc}})\,|\tilde{\psi}_i\rangle$ hold for each i.

Next, we introduce notations related to our recording standard oracle with errors that are required to describe properties of RstOE.

Notations related to RstOE. We call a bit string $D = (b_0||\alpha_0)|| \cdots || (b_{2^m-1}||\alpha_{2^m-1})$, where $b_x \in \{0,1\}$ and $\alpha_x \in \{0,1\}^n$ for each $x \in \{0,1\}^m$, is a *valid database* if $\alpha_x \neq 0^n$ holds only if $b_x = 1$. We call D an *invalid database* if it is not a valid database. Note that, in a valid database, b_x can be 0 or 1 if $\alpha_x = 0^n$. We identify a valid database D with the partially defined function from $\{0,1\}^m$ to $\{0,1\}^n$ of which the value on $x \in \{0,1\}^m$ is defined to be y if and only if $b_x = 1$ and $\alpha_x = y$. We use the same notation D for this function. If x is in the domain of D, we write $D(x) \neq \perp$, and otherwise write $D(x) = \perp$. Moreover, we identify D with the set $\{(x, D(x))\}_{x \in \mathrm{dom}(D)} \subset \{0,1\}^m \times \{0,1\}^n$, and we use the notations $D \cup (x,\alpha)$ and $D \setminus (x', \alpha')$ to denote the insertion of (x,α) into D and the deletion of (x', α') from D. For a valid database D that corresponds to the bit string $(b_0||\alpha_0)|| \cdots ||(b_{2^m-1}||\alpha_{2^m-1})$ such that $D(x) = \perp$ (i.e., $b_x = 0$ and $\alpha_x = 0^n$) and $\gamma \neq 0^n$, we denote the invalid database that corresponds to the bit string $(b_0||\alpha_0)|| \cdots ||(b_{x-1}||\alpha_{x-1})||(1||\gamma)||(b_{x+1}||\alpha_{x+1})|| \cdots ||(b_{2^m-1}||\alpha_{2^m-1})$ by $D \cup [\![x, \gamma]\!]$. Unless otherwise noted, we always assume that D is valid.

The following proposition describes the core properties of RstOE.

Proposition 2 (Core Properties). *Let D be a valid database and suppose that n is sufficiently large ($n \geq 6$ suffices). Then, the following properties hold.*

1. *Suppose that $D(x) = \perp$. Then, for any y and α, there exists a vector $|\epsilon\rangle$ such that*

$$\mathsf{RstOE}\,|x\rangle\,|y\rangle \otimes |D \cup (x,\alpha)\rangle = |x\rangle\,|y \oplus \alpha\rangle \otimes |D \cup (x,\alpha)\rangle + |\epsilon\rangle$$

and $\|\,|\epsilon\rangle\,\| \leq 5/\sqrt{2^n}$. More precisely,

$$\begin{aligned}
|\epsilon\rangle = {} & \frac{1}{\sqrt{2^n}}\,|x, y \oplus \alpha\rangle \left(|D\rangle - \left(\sum_{\gamma \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|D \cup (x,\gamma)\rangle \right) \right) \\
& - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}}\,|x, y \oplus \gamma\rangle \otimes \left(|D \cup (x,\gamma)\rangle - |D^{\mathsf{invalid}}_{\gamma}\rangle \right) \\
& + \frac{1}{2^n}\,|x\rangle\,|\widehat{0^n}\rangle \otimes \left(2 \sum_{\delta \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|D \cup (x,\delta)\rangle - |D\rangle \right)
\end{aligned} \tag{15}$$

holds, where $|D_\gamma^{\mathsf{invalid}}\rangle$ is a superposition of invalid databases defined by

$$|D_\gamma^{\mathsf{invalid}}\rangle := \sum_{\delta \neq 0^n} \frac{(-1)^{\gamma\cdot\delta}}{\sqrt{2^n}} |D \cup [\![x, \delta]\!]\rangle$$

for each γ, and $|\widehat{0^n}\rangle = H^{\otimes n}|0^n\rangle$.

2. *Suppose that $D(x) = \bot$. Then, for any y, there exists a vector $|\epsilon'\rangle$ such that*

$$\mathsf{RstOE}\,|x\rangle|y\rangle \otimes |D\rangle = \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle|y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle + |\epsilon'\rangle$$

and $\| \, |\epsilon'\rangle \, \| \leq 2/\sqrt{2^n}$. To be more precise,

$$|\epsilon'\rangle = \frac{1}{\sqrt{2^n}} |x\rangle|\widehat{0^n}\rangle \otimes \left(|D\rangle - \sum_{\gamma \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) \qquad (16)$$

holds, where $|\widehat{0^n}\rangle = H^{\otimes n}|0^n\rangle$.

An intuitive interpretation of Proposition 2. The proposition shows that, when the adversary's state is not superposed, we can intuitively capture time evolutions of databases with only the (classical) lazy-sampling-like arguments by ignoring the error terms $|\epsilon\rangle$ and $|\epsilon'\rangle$: When an adversary makes a query x to the oracle, RstOE looks for a tuple (x, α) in the database. If one is found, respond with α (the first property in the above proposition). If no tuple is found, create the superposition $\frac{1}{\sqrt{2^n}} \sum_{\alpha_x} |\alpha_x\rangle$, respond with α_x, and add (x, α_x) to the database (the second property in the above proposition).

Note that this intuition for the classical lazy-sampling does not necessarily work when the adversary's state is superposed. In particular, the error term $|\epsilon\rangle$ in the first property may become non-negligible, which means that a record (x, α) in a database may be deleted or overwritten by another record (x, γ) with non-negligible probability (in a quantum sense) when a quantum query is made. When (x, α) is overwritten with another record (x, γ), intuitively, the new value γ is chosen uniformly at random.

On the other hand, basically we can ignore invalid databases in security proofs since, when we measure the database register while an adversary runs relative to the recording standard oracle with errors, we always obtain a valid database.

Proof (of Proposition 2). Recall that RstOE is decomposed as

$$\mathsf{RstOE} = (I \otimes \mathsf{CH}) \cdot (I \otimes U_{\text{toggle}}) \cdot (I \otimes \mathsf{IH})\mathsf{stO}(I \otimes \mathsf{IH}^*) \cdot (I \otimes U_{\text{toggle}}^*) \cdot (I \otimes \mathsf{CH}^*), \quad (17)$$

and that each D is described as a bit string $(b_0 \| \alpha_0) \| \cdots \| (b_{2^m-1} \| \alpha_{2^m-1})$, where $b_x \in \{0, 1\}$ and $\alpha_x \in \{0, 1\}^n$ for each $x \in \{0, 1\}^m$.

We begin with showing the first property. Since now the operator RstOE does not affect the registers of entry of x' in D for $x' \neq x$, it suffices to show that the claim holds when D is empty. In addition, without loss of generality, we can assume that $x = 0^m$.

Now $D \cup (x, \alpha)$ corresponds to the bit string $(1\|\alpha)\|(0\|0^n)\| \cdots \|(0\|0^n)$. We have that $U^*_{\mathrm{enc}} = \mathsf{IH}^* U^*_{\mathrm{toggle}} \mathsf{CH}^* = \mathsf{IH} U_{\mathrm{toggle}} \mathsf{CH}$ and

$$\begin{aligned}
U^*_{\mathrm{enc}} \left| D \cup (x, \alpha) \right\rangle &= \mathsf{IH} U_{\mathrm{toggle}} \left(\sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} \left| 1 \| u \right\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} \left| 0 \| 0^n \right\rangle \right) \\
&= \mathsf{IH} \left(\sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} \left| 0 \| u \right\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} \left| 0 \| 0^n \right\rangle \right) \\
&\quad + \mathsf{IH} \left(\frac{1}{\sqrt{2^n}} \left(\left| 1 \| 0^n \right\rangle - \left| 0 \| 0^n \right\rangle \right) \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} \left| 0 \| 0^n \right\rangle \right) \\
&= \left| 0 \| \alpha \right\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} \left| 0 \right\rangle \left| \widehat{0^n} \right\rangle \right) + \left| \epsilon_1 \right\rangle, \qquad (18)
\end{aligned}$$

where $|\widehat{0^n}\rangle := H^{\otimes n} |0^n\rangle$ and $|\epsilon_1\rangle = \frac{1}{\sqrt{2^n}}(|1\rangle - |0\rangle) |\widehat{0^n}\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right)$. Thus, we have that

$$\begin{aligned}
&\mathsf{stO} \left(I \otimes U^*_{\mathrm{enc}} \right) |x, y\rangle \otimes |D \cup (x, \alpha)\rangle \\
&\quad = |x, y \oplus \alpha\rangle \otimes |0\|\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right) + \mathsf{stO}(|x, y\rangle \otimes |\epsilon_1\rangle). \qquad (19)
\end{aligned}$$

Note that, from (18), it follows that

$$U_{\mathrm{enc}} \left(|0\|\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right) + |\epsilon_1\rangle \right) = |D \cup (x, \alpha)\rangle. \qquad (20)$$

Therefore,

$$\begin{aligned}
&(I \otimes U_{\mathrm{enc}}) \, \mathsf{stO} \left(I \otimes U^*_{\mathrm{enc}} \right) |x, y\rangle \otimes |D \cup (x, \alpha)\rangle \\
&\quad = (I \otimes U_{\mathrm{enc}}) \left(|x, y \oplus \alpha\rangle \otimes |0\|\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right) + \mathsf{stO}(|x, y\rangle \otimes |\epsilon_1\rangle) \right) \\
&\quad = (I \otimes U_{\mathrm{enc}}) \left(|x, y \oplus \alpha\rangle \otimes |0\|\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right) + |x, y \oplus \alpha\rangle \otimes |\epsilon_1\rangle \right) \\
&\qquad - (I \otimes U_{\mathrm{enc}}) \left(|x, y \oplus \alpha\rangle \otimes |\epsilon_1\rangle \right) + (I \otimes U_{\mathrm{enc}}) \mathsf{stO}(|x, y\rangle \otimes |\epsilon_1\rangle) \\
&\quad = |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle + |\epsilon_2\rangle \qquad (21)
\end{aligned}$$

holds, where $|\epsilon_2\rangle = -(I \otimes U_{\mathrm{enc}}) \left(|x, y \oplus \alpha\rangle \otimes |\epsilon_1\rangle \right) + (I \otimes U_{\mathrm{enc}}) \mathsf{stO}(|x, y\rangle \otimes |\epsilon_1\rangle)$. Now we have that

$$\begin{aligned}
&(I \otimes U_{\mathrm{enc}}) \mathsf{stO}(|x, y\rangle \otimes |\epsilon_1\rangle) \\
&\quad = (I \otimes \mathsf{CH} \cdot U_{\mathrm{toggle}} \cdot \mathsf{IH}) \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes (|1\rangle - |0\rangle)
\end{aligned}$$

$$
\begin{aligned}
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \otimes |\gamma\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |\widehat{0^n}\rangle \right) \\
&= (I \otimes \mathsf{CH} \cdot U_{\text{toggle}}) \frac{1}{\sqrt{2^n}} \sum_{\gamma,\delta} \frac{(-1)^{\gamma\cdot\delta}}{2^n} |x, y \oplus \gamma\rangle \otimes (|1\rangle - |0\rangle) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \otimes |\delta\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right) \\
&= (I \otimes \mathsf{CH}) \frac{1}{\sqrt{2^n}} \sum_{\gamma,\delta} \frac{(-1)^{\gamma\cdot\delta}}{2^n} |x, y \oplus \gamma\rangle \otimes (|0\rangle - |1\rangle) \otimes |\delta\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right) \\
&\quad + (I \otimes \mathsf{CH}) \frac{2}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{2^n} |x, y \oplus \gamma\rangle \otimes (|1\rangle - |0\rangle) \otimes |0^n\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes \Big(|0\rangle \otimes \left(H^{\otimes n} |\gamma\rangle \right) - |1\rangle \otimes |\gamma\rangle \Big) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right) \\
&\quad + \frac{2}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{2^n} |x, y \oplus \gamma\rangle \otimes \Big(|1\rangle \otimes \left(H^{\otimes n} |0^n\rangle \right) - |0\rangle \otimes |0^n\rangle \Big) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right)
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |0\rangle \otimes \left(H^{\otimes n} |\gamma\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right) \\
&\quad - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |1\rangle \otimes |\gamma\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right) \\
&\quad + \frac{2}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{2^n} |x, y \oplus \gamma\rangle \otimes \left(\sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |0\rangle \otimes \left(\sum_{\delta} \frac{(-1)^{\gamma\cdot\delta}}{\sqrt{2^n}} |\delta\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right) \\
&\quad - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |1\rangle \otimes |\gamma\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right) \\
&\quad + \frac{2}{2^n} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes \left(\sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |0\rangle \otimes \left(\sum_{\delta \neq 0^n} \frac{(-1)^{\gamma\cdot\delta}}{\sqrt{2^n}} |\delta\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right) \\
&\quad + \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |0\rangle \otimes \left(\frac{1}{\sqrt{2^n}} |0^n\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle \, |0^n\rangle \right)
\end{aligned}
$$

$$
\begin{aligned}
&- \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \gamma\right\rangle \otimes \left|1\right\rangle \otimes \left|\gamma\right\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} \left|0\right\rangle \left|0^n\right\rangle \right) \\
&+ \frac{2}{2^n} \sum_{\gamma} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \gamma\right\rangle \otimes \left(\sum_{\delta} \frac{1}{\sqrt{2^n}} \left|D \cup (x, \delta)\right\rangle - \left|D\right\rangle \right) \\
={}& \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \gamma\right\rangle \otimes \left|D_{\gamma}^{\mathsf{invalid}}\right\rangle \\
&+ \frac{1}{2^n} \sum_{\gamma} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \gamma\right\rangle \otimes \left|D\right\rangle \\
&- \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \gamma\right\rangle \otimes \left|D \cup (x, \gamma)\right\rangle \\
&+ \frac{2}{2^n} \left|x\right\rangle \left|\widehat{0^n}\right\rangle \otimes \left(\sum_{\delta} \frac{1}{\sqrt{2^n}} \left|D \cup (x, \delta)\right\rangle - \left|D\right\rangle \right) \\
={}& -\frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \gamma\right\rangle \otimes \left(\left|D \cup (x, \gamma)\right\rangle - \left|D_{\gamma}^{\mathsf{invalid}}\right\rangle \right) \\
&+ \frac{1}{2^n} \left|x\right\rangle \left|\widehat{0^n}\right\rangle \otimes \left(2 \sum_{\delta} \frac{1}{\sqrt{2^n}} \left|D \cup (x, \delta)\right\rangle - \left|D\right\rangle \right), \qquad (22)
\end{aligned}
$$

where

$$
\begin{aligned}
\left|D_{\gamma}^{\mathsf{invalid}}\right\rangle &= \left(\sum_{\delta \neq 0^n} \frac{(-1)^{\gamma \cdot \delta}}{\sqrt{2^n}} \left|0\right\rangle \left|\delta\right\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} \left|0\right\rangle \left|0^n\right\rangle \right) \\
&= \sum_{\delta \neq 0^n} \frac{(-1)^{\gamma \cdot \delta}}{\sqrt{2^n}} \left|D \cup \llbracket x, \delta \rrbracket\right\rangle
\end{aligned}
$$

for each γ.

In addition, we have that

$$
\begin{aligned}
U_{\text{enc}} \left|\epsilon_1\right\rangle &= (\mathsf{CH} U_{\text{toggle}} \mathsf{IH}) \frac{1}{\sqrt{2^n}} (\left|1\right\rangle - \left|0\right\rangle) \left|\widehat{0^n}\right\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} \left|0\right\rangle \left|\widehat{0^n}\right\rangle \right) \\
&= \mathsf{CH} \frac{1}{\sqrt{2^n}} (\left|1\right\rangle - \left|0\right\rangle) \left|0^n\right\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} \left|0\right\rangle \left|0^n\right\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} (\left|1\right\rangle \left|\widehat{0^n}\right\rangle - \left|0\right\rangle \left|0^n\right\rangle) \otimes \left(\bigotimes_{i=1}^{2^m-1} \left|0\right\rangle \left|0^n\right\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} \left|D \cup (x, \gamma)\right\rangle - \frac{1}{\sqrt{2^n}} \left|D\right\rangle \qquad (23)
\end{aligned}
$$

holds. Thus,

$$(I \otimes U_{\mathrm{enc}}) |x, y \oplus \alpha\rangle \otimes |\epsilon_1\rangle = \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \left(\left(\sum_{\gamma} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) - |D\rangle \right) \tag{24}$$

holds. Therefore,

$$\begin{aligned}
&\mathsf{RstOE} |x, y\rangle \otimes |D \cup (x, \alpha)\rangle \\
&\quad = |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle \\
&\qquad + \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \left(|D\rangle - \left(\sum_{\gamma} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) \right) \\
&\qquad - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes \left(|D \cup (x, \gamma)\rangle - |D_{\gamma}^{\mathsf{invalid}}\rangle \right) \\
&\qquad + \frac{1}{2^n} |x\rangle |\widehat{0^n}\rangle \otimes \left(2 \sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right)
\end{aligned} \tag{25}$$

holds, and this proves the first property.

Next, we show the second property. Since now the operator RstOE does not affect the registers of entry of x' in D for $x' \neq x$, it suffices to show that the claim holds when D has no entry. In addition, we can without loss of generality assume that $x = 0^m$. Now D corresponds to the bit string $(0\|0^n)\|(0\|0^n)\| \cdots \|(0\|0^n)$, and we have that

$$\begin{aligned}
U_{\mathrm{enc}}^{*} |D\rangle &= \mathsf{IH} U_{\mathrm{toggle}} \mathsf{CH} |D\rangle \\
&= \left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |0\rangle |\alpha\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m - 1} |0\rangle |\widehat{0^n}\rangle \right).
\end{aligned} \tag{26}$$

Hence, it holds that

$$\mathsf{stO}(I \otimes U_{\mathrm{enc}}^{*}) |x, y\rangle \otimes |D\rangle = \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \otimes |0\rangle |\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m - 1} |0\rangle |\widehat{0^n}\rangle \right). \tag{27}$$

In addition, we have that

$$\begin{aligned}
&(I \otimes U_{\mathrm{enc}}) \mathsf{stO} (I \otimes U_{\mathrm{enc}}^{*}) |x, y\rangle \otimes |D\rangle \\
&\quad = (I \otimes (\mathsf{CH} U_{\mathrm{toggle}} \mathsf{IH})) \left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \otimes |0\rangle |\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m - 1} |0\rangle |\widehat{0^n}\rangle \right) \right) \\
&\quad = (I \otimes (\mathsf{CH} U_{\mathrm{toggle}})) \left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \right. \\
&\qquad\qquad \left. \otimes \left(\sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} |0\rangle |u\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m - 1} |0\rangle |0^n\rangle \right) \right)
\end{aligned}$$

$$
\begin{aligned}
&= (I \otimes \mathsf{CH})\left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \right. \\
&\qquad\qquad \left. \otimes \left(\sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} |1\rangle |u\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |0^n\rangle \right) \right) \\
&\quad + (I \otimes \mathsf{CH})\left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \right. \\
&\qquad\qquad \left. \otimes \left(\frac{1}{\sqrt{2^n}} (|0\rangle - |1\rangle) \otimes |0^n\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |0^n\rangle \right) \right) \\
&= \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \otimes |1\rangle |\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |0^n\rangle \right) \\
&\quad + \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \otimes \left(\frac{1}{\sqrt{2^n}} (|0\rangle |0^n\rangle - |1\rangle |\widehat{0^n}\rangle) \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |0^n\rangle \right) \\
&= \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle \\
&\quad + \frac{1}{\sqrt{2^n}} |x\rangle |\widehat{0^n}\rangle \otimes \left(|D\rangle - \sum_{\gamma} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) \qquad (28)
\end{aligned}
$$

holds. Therefore, the second property also holds. □

Let RstOE be the recording oracle with errors for a random function $f : \{0,1\}^m \to \{0,1\}^n$. We also show the following lemma for later use.

Proposition 3. *Let y be a fixed n-bit string, and*

$$
\begin{aligned}
|\psi\rangle = &\sum_{\substack{x \in \{0,1\}^m, \alpha \in \{0,1\}^n, D \\ D(x) = \perp}} c_{x,\alpha,D} |x, y\rangle \otimes |D \cup (x, \alpha)\rangle \otimes |\psi_{x,\alpha,D}\rangle \\
&+ \sum_{\substack{x \in \{0,1\}^m, D \\ D(x) = \perp}} c'_{x,D} |x, y\rangle \otimes |D\rangle \otimes |\psi'_{x,D}\rangle
\end{aligned}
$$

be a vector such that $\| |\psi\rangle \| \le 1$, $\| |\psi_{x,D}\rangle \| \le 1$, and $\| |\psi'_{x,\alpha,D}\rangle \| \le 1$ for each x, α, and D. Here, $|x\rangle$ and $|y\rangle$ are the registers to send queries to f and receive the responses, respectively, and $|\psi_{x,\alpha,D}\rangle$, $|\psi'_{x,D}\rangle$ correspond to an additional quantum system on which RstOE *does not affect. In addition, $c_{x,\alpha,D}$ and $c'_{x,D}$ are complex numbers such that*

$$
\sum_{\substack{x \in \{0,1\}^m, \alpha \in \{0,1\}^n, D \\ D(x) = \perp}} |c_{x,\alpha,D}|^2 \le 1
$$

and

$$
\sum_{\substack{x \in \{0,1\}^m, D \\ D(x) = \perp}} |c'_{x,D}|^2 \le 1.
$$

Let Π_{valid} *be the orthogonal projection onto the vector space spanned by valid databases. Then there exists a vector* $|\epsilon\rangle$ *such that* $\| \, |\epsilon\rangle \, \| \leq 10/\sqrt{2^n}$ *and*

$$\begin{aligned}
\Pi_{\mathsf{valid}}\mathsf{RstOE}\,|\psi\rangle = &\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\perp}} c_{x,\alpha,D}\,|x, y\oplus\alpha\rangle\otimes|D\cup(x,\alpha)\rangle\otimes|\psi_{x,\alpha,D}\rangle\\
&-\sum_{\substack{x\in\{0,1\}^m,\alpha,\gamma\in\{0,1\}^n,D\\ D(x)=\perp}} \frac{1}{2^n}c_{x,\alpha,D}\,|x, y\oplus\gamma\rangle\otimes|D\cup(x,\gamma)\rangle\otimes|\psi_{x,\alpha,D}\rangle\\
&+\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\perp}} c'_{x,D}\frac{1}{\sqrt{2^n}}\,|x, y\oplus\alpha\rangle\otimes|D\cup(x,\alpha)\rangle\otimes|\psi'_{x,D}\rangle\\
&+|\epsilon\rangle
\end{aligned}$$

hold.

An intuitive interpretation of Proposition 3. Intuitively, this proposition shows that, when an adversary's register to receive responses from the oracle (i.e., the $|y\rangle$ register) is not superposed, we can ignore the effect that an existing record (x,α) will be deleted from a database. (Nevertheless, we cannot ignore the effect that an existing record (x,α) will be overwritten with another record (x,γ).)

Proof (of Proposition 3). Let

$$\begin{aligned}
|\phi_0\rangle := &\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\perp}} c_{x,\alpha,D}\,|x, y\oplus\alpha\rangle\otimes|D\cup(x,\alpha)\rangle\otimes|\psi_{x,\alpha,D}\rangle,\\
|\phi_1\rangle := &\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\perp}} c_{x,\alpha,D}\frac{1}{\sqrt{2^n}}\,|x, y\oplus\alpha\rangle\\
&\qquad\otimes\left(|D\rangle-\left(\sum_{\gamma\in\{0,1\}^n}\frac{1}{\sqrt{2^n}}\,|D\cup(x,\gamma)\rangle\right)\right)\otimes|\psi_{x,\alpha,D}\rangle,\\
|\phi_2\rangle := -&\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\perp}} c_{x,\alpha,D}\frac{1}{\sqrt{2^n}}\sum_{\gamma}\frac{1}{\sqrt{2^n}}\,|x, y\oplus\gamma\rangle\\
&\qquad\otimes\Big(|D\cup(x,\gamma)\rangle-|D^{\mathsf{invalid}}_{\gamma}\rangle\Big)\otimes|\psi_{x,\alpha,D}\rangle,\\
|\phi_3\rangle := &\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\perp}} c_{x,\alpha,D}\frac{1}{2^n}\,|x\rangle\,|\widehat{0^n}\rangle\\
&\qquad\otimes\left(2\sum_{\delta\in\{0,1\}^n}\frac{1}{\sqrt{2^n}}\,|D\cup(x,\delta)\rangle-|D\rangle\right)\otimes|\psi_{x,\alpha,D}\rangle,\\
|\phi'_0\rangle := &\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\perp}} c'_{x,D}\frac{1}{\sqrt{2^n}}\,|x, y\oplus\alpha\rangle\otimes|D\cup(x,\alpha)\rangle\otimes|\psi'_{x,D}\rangle
\end{aligned}$$

$$|\phi'_1\rangle := \sum_{\substack{x\in\{0,1\}^m, D\\ D(x)=\bot}} c'_{x,D} \frac{1}{\sqrt{2^n}} |x\rangle |\widehat{0^n}\rangle \otimes \left(|D\rangle - \sum_{\gamma\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |D \cup (x,\gamma)\rangle \right) \otimes |\psi'_{x,D}\rangle$$

Then

$$\mathsf{RstOE}\,|\psi\rangle = \sum_{0\le i\le 3} |\phi_i\rangle + \sum_{0\le i\le 1} |\phi'_i\rangle$$

follows from Proposition 2.

Upper bounding $\| |\phi_1\rangle \|$.

First, for distinct tuples $(x,\alpha,D) \neq (x',\alpha',D')$ such that $D(x)=\bot$ and $D(x')=\bot$,

$$|x, y\oplus\alpha\rangle \otimes \left(|D\rangle - \left(\sum_{\gamma\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |D\cup(x,\gamma)\rangle \right) \right)$$

is orthogonal to

$$|x', y\oplus\alpha'\rangle \otimes \left(|D'\rangle - \left(\sum_{\gamma\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |D'\cup(x',\gamma)\rangle \right) \right).$$

Thus

$$\| |\phi_1\rangle \|^2 \le (2/2^n)\cdot \sum_{\substack{x\in\{0,1\}^m, \alpha\in\{0,1\}^n, D\\ D(x)=\bot}} |c_{x,\alpha,D}|^2 \le 2/2^n \tag{29}$$

holds.

Upper bounding $\| |\phi_3\rangle \|$.

We have that

$$\begin{aligned} \| |\phi_3\rangle \|^2 &\le 5\cdot \sum_{\substack{x\in\{0,1\}^m, D\\ D(x)=\bot}} \left(\sum_{\alpha} \frac{|c_{x,\alpha,D}|}{2^n} \right)^2 \\ &\le 5\cdot \sum_{\substack{x\in\{0,1\}^m, D\\ D(x)=\bot}} \frac{\sum_\alpha |c_{x,\alpha,D}|^2}{2^n} \\ &\le \frac{5}{2^n} \end{aligned} \tag{30}$$

holds, where we used the convexity of the function $X \mapsto X^2$ for the second inequality.

Upper bounding $\| |\phi'_1\rangle \|$.

We have that

$$\left\| |\phi'_1\rangle \right\|^2 \le \frac{2}{2^n} \sum_{\substack{x\in\{0,1\}^m, D\\ D(x)=\bot}} |c'_{x,D}|^2 \le \frac{2}{2^n} \tag{31}$$

holds.

Now the claim of the lemma holds by setting $|\epsilon\rangle := |\phi_1\rangle + |\phi_3\rangle + |\phi'_1\rangle$. □

4 Security Proofs

The goal of this section is to show the following theorem, which gives the quantum query lower bound for the problem of distinguishing the 4-round Luby-Rackoff construction LR_4 from random permutations RP, when all round functions are truly random functions.

Theorem 3. *Let q be a positive integer. Let $\mathcal{A}$ be an adversary that makes at most q quantum queries. Then, $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathsf{LR}_4}(\mathcal{A})$ is in $O\left(\sqrt{q^3/2^{n/2}}\right)$.*

Since we can efficiently simulate truly random functions against efficient quantum adversaries [35], the following corollary follows from Theorem 3.

Corollary 1. *Let f_i be a quantumly secure PRF for each $1 \leq i \leq 4$. Then, the 4-round Luby-Rackoff construction $\mathsf{LR}_4(f_1, f_2, f_3, f_4)$ is a quantumly secure PRP.*

In the rest of this section, we assume that all round functions in the Luby-Rackoff constructions are truly random functions, and we focus on the number of queries when we consider computational resources of adversaries. To have a good intuition on our proof in the quantum setting, it would be better to intuitively capture how LR_3 is proven to be secure against classical CPAs, how the quantum attack on LR_3 works, and what problem will be hard even for quantum adversaries. Thus, before giving a formal proof for the above theorem, in what follows we give some observations about these questions, and then explain where to start.

An overview of a classical security proof for LR_3. Here we give an overview of a *classical* proof for the security of LR_3 against chosen plaintext attacks in the classical setting. For simplicity, we consider a proof for PRF security of LR_3.

Let bad_2 be the event that an adversary makes two distinct plaintext queries $(x_{0L}, x_{0R}) \neq (x'_{0L}, x'_{0R})$ to the real oracle LR_3 such that the corresponding inputs x_{1L} and x'_{1L} to the second round function f_2 are equal, i.e., inputs to f_2 collide. In addition, let bad_3 be the event that inputs to f_3 collide, and define $\mathsf{bad} := \mathsf{bad}_2 \vee \mathsf{bad}_3$.

If bad_2 (resp., bad_3) does not occur, then the right-half (resp., left-half) $n/2$ bits of LR_3's outputs cannot be distinguished from truly random $n/2$-bit strings. Thus, unless the event bad occurs, adversaries cannot distinguish LR_3 from random functions.

If the number of queries of an adversary $\mathcal{A}$ is at most q, we can show that the probability that the event bad occurs when $\mathcal{A}$ runs relative to the oracle LR_3 is in $O(q^2/2^{n/2})$. Thus we can deduce that LR_3 is indistinguishable from a random function up to $O(2^{n/4})$ queries.

Quantum chosen plaintext attack on LR_3. Next, we give an overview of the quantum chosen plaintext attack on LR_3 by Kuwakado and Morii [21]. Note that we consider the setting in which adversaries can make quantum superposition queries. The attack distinguishes LR_3 from a random permutation with only $O(n)$ queries.

Fix $\alpha_0 \neq \alpha_1 \in \{0,1\}^{n/2}$ and for $i = 0, 1$, define $g_i : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ by $g_i(x) = (\mathsf{LR}_3(\alpha_i, x))_R \oplus \alpha_i$, where $(\mathsf{LR}_3(\alpha_i, x))_R$ denote the right half $n/2$-bits of $\mathsf{LR}_3(\alpha_i, x)$. In addition, define $G : \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ by $G(b, x) = g_b(x)$.

Then, $g_0(x) = g_1(x \oplus s)$ can be easily confirmed to hold for any $x \in \{0,1\}^{n/2}$, where $s = f_1(\alpha_0) \oplus f_1(\alpha_1)$. Thus $G(b,x) = G((b,x) \oplus (1,s))$ holds for any b and x, i.e., the function G has the period $(1,s)$.

If we can make quantum superposed queries to G, then we can find the period $(1,s)$ by using Simon's period finding algorithm [32], making $O(n)$ queries to G. In fact G can be implemented on an oracle-aided quantum circuit C^{LR_3} by making $O(1)$ queries to LR_3.[8]

Roughly speaking, Simon's algorithm outputs the periods with a high probability by making $O(n)$ queries if applied to periodic functions, and outputs the result that "this function is not periodic" if applied to functions without periods.

If we are given the oracle of a random permutation RP, the circuit C^{RP} will implement an almost random function, which does not have any period with a high probability. Thus, if we run Simon's algorithm on C^{RP}, with a high probability, it does not output any period. Therefore, we can distinguish LR_3 from RP by checking if Simon's period finding algorithm outputs a period.

Observation: Why the classical proof does not work? Here we give an observation about why quantum adversaries can distinguish LR_3 from random permutations even though LR_3 is proven to be indistinguishable from a random permutation in the classical setting.

We observe that quantum adversaries can make the event bad_2 occur: Once we find the period $1\|s = 1\|f_1(\alpha_0) \oplus f_2(\alpha_1)$ given the real oracle LR_3, we can force collisions on the input of f_2. Concretely, take $x \in \{0,1\}^{n/2}$ arbitrarily and set $(x_{0L}, x_{0R}) := (\alpha_0, x)$, $(x'_{0L}, x'_{0R}) := (\alpha_1, x \oplus s)$. Then the corresponding inputs to f_2 become $f_1(\alpha_0) \oplus x$ for both plaintexts. Thus the classical proof idea does not work in the quantum setting.

Quantum security proof for LR_4: The idea. As we explained above, the essence of the quantum attack on LR_3 is finding collisions for inputs to the second round function f_2. On the other hand, finding collisions for inputs to the third round function f_3 seems difficult even for quantum (chosen-plaintext) query adversaries.

Having these observations, our idea is that even quantum adversaries would have difficulty in noticing that the third state update $(x_{2L}, x_{2R}) \mapsto (x_{2R} \oplus f_3(x_{2L}), x_{2L})$ of LR_3 is modified as $(x_{2L}, x_{2R}) \mapsto (F(x_{2L}, x_{2R}), x_{2L})$, where $F : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ is a random function. We denote this modified function by LR'_3 (see Fig. 3) and begin by showing that it is hard to distinguish LR'_3 from LR_3.

We will show this by combining the classical proof idea and our recording standard oracle with errors. Roughly speaking, we define "bad" databases as the ones that contain "collisions at left-half inputs to the third round function". Then we show that the probability that we measure bad databases is very small, and that adversaries cannot distinguish LR'_3 from LR_3 when databases are not bad.

Next, let LR''_2 denote a modified version of the 2-round Luby-Rackoff construction such that the first and second state update operations are modified as $(x_{0L}, x_{0R}) \mapsto$

[8] Here we have to truncate outputs of O without destroying quantum states, which is pointed out to be non-trivial in the quantum setting [20]. However, this "truncation" issue can be overcome by using a technique described in [17].

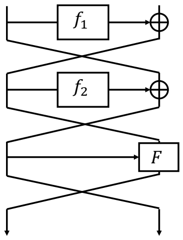

Fig. 3. LR_3'

$(F_1(x_{0L}, x_{0R}), x_{0L})$ and $(x_{1L}, x_{1R}) \mapsto (F_2(x_{1L}, x_{1R}), x_{1L})$, respectively, where $F_1, F_2 : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2}$ are independent random functions (see Fig. 4). Then, we intuitively see that LR_2'' is hard to distinguish from a random function RF from $\{0,1\}^n$ to $\{0,1\}^n$. We also show this by combining a classical proof idea and the recording standard oracle with errors. Roughly speaking, here we define "bad" databases as the ones that contain "collisions at left-half inputs to F_2". Then we show that the probability that we measure bad databases is very small, and that adversaries cannot distinguish LR_2'' from RF when databases are not bad.

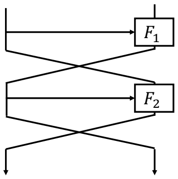

Fig. 4. LR_2''

Once we show the above two properties, i.e.,

1. LR_3' is hard to distinguish from LR_3, and
2. LR_2'' is hard to distinguish from RF,

we can prove Theorem 3 with simple and easy arguments. In other words, those two properties are technically the most difficult parts to show in our proof for Theorem 3.

Organization of the rest of Section 4. Section 4.1 shows that LR_3' is hard to distinguish from LR_3. Section 4.2 shows that LR_2'' is hard to distinguish from RF. Section 4.3 proves Theorem 3 by combining the results in Sections 4.1 and 4.2.

4.1 Hardness of Distinguishing LR_3' from LR_3

Here we show the following proposition.

Proposition 4. *Let q be a positive integer. Let $\mathcal{A}$ be an adversary that makes at most q quantum queries. Then,* $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_3,\mathsf{LR}_3'}(\mathcal{A})$ *is in* $O\left(\sqrt{q^3/2^{n/2}}\right)$.

First, let us discuss the behavior of the quantum oracles of LR_3 and LR_3'.

Quantum oracle of LR_3. Let O_{f_i} denote the quantum oracle of each round function f_i. In addition, let us define the unitary operator $O_{\mathrm{UP}.i}$ that computes the state update of the i-th round by

$$\begin{aligned} O_{\mathrm{UP}.i} : &\left|x_{(i-1)L}, x_{(i-1)R}\right\rangle \left|y_L, y_R\right\rangle \\ &\mapsto \left|x_{(i-1)L}, x_{(i-1)R}\right\rangle \left|(y_L, y_R) \oplus (f_i(x_{(i-1)L}) \oplus x_{(i-1)R}, x_{(i-1)L})\right\rangle . \end{aligned}$$

$O_{\mathrm{UP}.i}$ can be implemented by making one query to f_i (see Fig. 5).

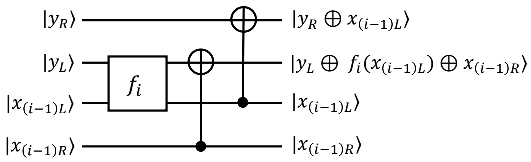

Fig. 5. Implementation of $O_{\mathrm{UP}.i}$. f_i will be implemented by using the recording standard oracle with errors.

Now O_{LR_3} can be implemented as follows by using $\{O_{\mathrm{UP}.i}\}_{1\le i\le 3}$:

1. Take $|x\rangle|y\rangle = |x_{0L}, x_{0R}\rangle|y_L, y_R\rangle$ as an input.
2. Compute the state (x_{1L}, x_{1R}) by querying $|x_{0L}, x_{0R}\rangle|0^n\rangle$ to $O_{\mathrm{Up}.1}$, and obtain
$$|x_{0L}, x_{0R}\rangle|y_L, y_R\rangle \otimes |x_{1L}, x_{1R}\rangle . \tag{32}$$
3. Compute the state (x_{2L}, x_{2R}) by querying $|x_{1L}, x_{1R}\rangle|0^n\rangle$ to $O_{\mathrm{Up}.2}$, and obtain
$$|x_{0L}, x_{0R}\rangle|y_L, y_R\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle . \tag{33}$$
4. Query $|x_{2L}, x_{2R}\rangle|y_L, y_R\rangle$ to $O_{\mathrm{Up}.3}$, and obtain
$$|x\rangle|y \oplus \mathsf{LR}_3(x)\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle . \tag{34}$$
5. Uncompute Steps 2 and 3 to obtain
$$|x\rangle|y \oplus \mathsf{LR}_3(x)\rangle . \tag{35}$$
6. Return $|x\rangle|y \oplus \mathsf{LR}_3(x)\rangle$.

The above implementation is illustrated in Fig. 6.

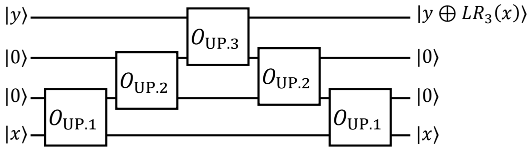

Fig. 6. Implementation of LR_3.

Quantum oracle of LR_3'. The quantum oracle of LR_3' is implemented in the same way as LR_3, except that the third round state update oracle $O_{\mathrm{UP}.3}$ is replaced with another oracle $O_{\mathrm{UP}.3}'$ defined as

$$O_{\mathrm{UP}.3}' : |x_{2L}, x_{2R}\rangle\,|y_L, y_R\rangle \mapsto |x_{2L}, x_{2R}\rangle\,|(y_L, y_R) \oplus (F(x_{2L}, x_{2R}) \oplus x_{2R}, x_{2L})\rangle\,.$$

$O_{\mathrm{UP}.3}'$ is implemented by making one query to O_F, i.e., the quantum oracle of F (see Fig. 7).

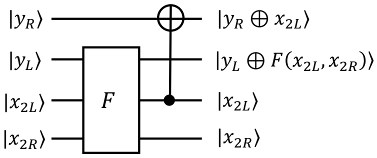

Fig. 7. Implementation of $O_{\mathrm{UP}.3}'$. F will be implemented by using the recording standard oracle with errors.

In what follows, we consider that the oracles of the functions f_i and F are implemented as the recording standard oracle with errors, and we use D_1, D_2, D_3, and D_F to denote (valid) databases for f_1, f_2, f_3, and F, respectively. In particular, after the i-th query of an adversary to LR_3, the joint quantum states of the adversary and functions can be described as

$$\sum_{x,y,z,D_1,D_2,D_3} a_{x,y,z,D_1,D_2,D_3}\,|x, y, z\rangle \otimes |D_1\rangle\,|D_2\rangle\,|D_3\rangle \tag{36}$$

for some complex numbers a_{x,y,z,D_1,D_2,D_3} such that $\sum_{x,y,z,D_1,D_2,D_3} |a_{x,y,z,D_1,D_2,D_3}|^2 = 1$. Here, x, y, and z correspond to the adversary's register to send queries to oracles, receive answers from oracles, and perform offline computations, respectively. (If the oracle is LR_3', then the register $|D_3\rangle$, which corresponds to f_3, is replaced with $|D_F\rangle$, which corresponds to F.)

Next, we define good and bad databases for LR_3 and LR_3'. Intuitively, we say that a tuple (D_1, D_2, D_3) (resp., (D_1, D_2, D_F)) for LR_3 (resp., LR_3') is bad if and only if it contains the information that some inputs to f_3 (resp., the left halves of some inputs to F) collide. Roughly speaking, we define good and bad databases in such a way that a one-to-one correspondence exists between good databases for LR_3 and those for LR'_3, so that adversaries will not be able to distinguish LR'_3 from LR_3 as long as databases are good.

Good and bad databases for LR_3. Here we introduce the notion of *good* and *bad* for each tuple (D_1, D_2, D_3) of valid database for LR_3. We say that (D_1, D_2, D_3) is good if, for each entry $(x_{2L}, \gamma) \in D_3$, there exists exactly one pair $((x_{0L}, \alpha), (x_{1L}, \beta)) \in D_1 \times D_2$ such that $\beta \oplus x_{0L} = x_{2L}$. We say that (D_1, D_2, D_3) is bad if it is not good.

Good and bad databases for LR'_3. Next we introduce the notion of *good* and *bad* for each tuple (D_1, D_2, D_F) of valid database for LR'_3. We say that a valid database D_F is *without overlap* if each pair of distinct entries (x_{2L}, x_{2R}, γ) and $(x'_{2L}, x'_{2R}, \gamma')$ in D_F satisfies $x_{2L} \neq x'_{2L}$. We say that (D_1, D_2, D_F) is good if D_F is without overlap, and for each entry $(x_{2L}, x_{2R}, \gamma) \in D_F$, there exists exactly one pair $((x_{0L}, \alpha), (x_{1L}, \beta)) \in D_1 \times D_2$ such that $\beta \oplus x_{0L} = x_{2L}$ and $x_{2R} = x_{1L}$. We say that (D_1, D_2, D_F) is bad if it is not good.

Compatibility of D_F with D_3. Let D_F be a valid database for F without overlap and D_3 be a valid database for f_3. We say that D_F is compatible with D_3 if the following conditions are satisfied:

1. If $(x_{2L}, x_{2R}, \gamma) \in D_F$, then $(x_{2L}, x_{2R} \oplus \gamma) \in D_3$.
2. If $(x_{2L}, \gamma) \in D_3$, there is a unique x_{2R} such that $(x_{2L}, x_{2R}, x_{2R} \oplus \gamma) \in D_F$.

For each valid D_F without overlap, the unique valid database exists for f_3, which we denote by $[D_F]_3$.

Remark 1. For each good database (D_1, D_2, D_3) for LR_3, a unique D_F without overlap exists such that $[D_F]_3 = D_3$ and (D_1, D_2, D_F) is a good database for LR'_3, by the definition of good databases. Similarly, for each good database (D_1, D_2, D_F) for LR'_3, $(D_1, D_2, [D_F]_3)$ becomes a good database for LR_3. That is, there exists a one-to-one correspondence between good databases for LR_3 and those for LR'_3.

Here we prove the following lemma for later use, which shows that the behavior of $O'_{\mathrm{UP}.3}$ for D_F without overlap is the same as that of $O_{\mathrm{UP}.3}$ for $[D_F]_3$.

Lemma 1. *It holds that*

$$\begin{aligned} &\langle x'_{2L}, x'_{2R}, y'_L, y'_R| \otimes \langle D'_F|\, O'_{\mathrm{UP}.3}\, |x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |D_F\rangle \\ &\quad = \langle x'_{2L}, x'_{2R}, y'_L, y'_R| \otimes \langle [D'_F]_3|\, O_{\mathrm{UP}.3}\, |x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |[D_F]_3\rangle \end{aligned} \tag{37}$$

for any $x_{2L}, x_{2R}, y_L, y_R, x'_{2L}, x'_{2R}, y'_L, y'_R \in \{0,1\}^{n/2}$ and any valid databases D_F and D'_F without overlap.

Proof. It suffices to consider the case that $x'_{2L} = x_{2L}$, $x'_{2R} = x_{2R}$, and $y'_R = y_R$. Since the database $O'_{\mathrm{UP}.3}$ affects only the entry of (x_{2L}, x_{2R}) in D_F when it acts on $|x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |D_F\rangle$, it suffices to show the claim for the cases that (1) D_F has only a single entry (x_{2L}, x_{2R}, α), or (2) D_F has no entry (i.e., $D_F = \emptyset$).

First, we show the claim for the first case where $D_F = \{(x_{2L}, x_{2R}, \alpha)\}$. In this case, by the first property of Proposition 2 we have that

$$\begin{aligned}
&O'_{\mathrm{UP}.3}\, |x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |D_F\rangle \\
&\quad = |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, x_{2R}, \alpha)\rangle \\
&\qquad + \frac{1}{\sqrt{2^{n/2}}}\, |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left(|\emptyset\rangle - \left(\sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}}\, |(x_{2L}, x_{2R}, \gamma)\rangle \right) \right) \\
&\qquad - \frac{1}{\sqrt{2^{n/2}}} \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}}\, |x_{2L}, x_{2R}, y_L \oplus \gamma, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, x_{2R}, \gamma)\rangle \\
&\qquad + \frac{1}{2^{n/2}}\, |x_{2L}, x_{2R}\rangle\, |\widehat{0^n}\rangle\, |y_R \oplus x_{2L}\rangle \otimes \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}}\, |(x_{2L}, x_{2R}, \delta)\rangle - |\emptyset\rangle \right) \\
&\qquad + |\mathsf{invalid}\rangle \qquad (38)
\end{aligned}$$

holds, where $\emptyset$ is the empty database and $|\mathsf{invalid}\rangle$ is a vector containing invalid databases. In addition, we have that $[D_F]_3 = \{(x_{2L}, \alpha \oplus x_{2R})\}$, and

$$\begin{aligned}
&O_{\mathrm{UP}.3}\, |x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |[D_F]_3\rangle \\
&\quad = |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, \alpha \oplus x_{2R})\rangle \\
&\qquad + \frac{1}{\sqrt{2^{n/2}}}\, |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left(|\emptyset\rangle - \left(\sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}}\, |(x_{2L}, \gamma)\rangle \right) \right) \\
&\qquad - \frac{1}{\sqrt{2^{n/2}}} \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}}\, |x_{2L}, x_{2R}, y_L \oplus \gamma \oplus x_{2R}, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, \gamma)\rangle \\
&\qquad + \frac{1}{2^{n/2}}\, |x_{2L}, x_{2R}\rangle\, |\widehat{0^n}\rangle\, |y_R \oplus x_{2L}\rangle \otimes \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}}\, |(x_{2L}, \delta)\rangle - |\emptyset\rangle \right) \\
&\qquad + |\mathsf{invalid}'\rangle
\end{aligned}$$

$$\begin{aligned}
&= |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \alpha)]_3\rangle \\
&\quad + \frac{1}{\sqrt{2^{n/2}}}\, |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left(|\emptyset\rangle - \left(\sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}}\, |[(x_{2L}, x_{2R}, \gamma \oplus x_{2R})]_3\rangle \right) \right) \\
&\quad - \frac{1}{\sqrt{2^{n/2}}} \sum_{\gamma} \frac{1}{\sqrt{2^{n}}}\, |x_{2L}, x_{2R}, y_L \oplus \gamma \oplus x_{2R}, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \gamma \oplus x_{2R})]_3\rangle \\
&\quad + \frac{1}{2^{n/2}}\, |x_{2L}, x_{2R}\rangle\, |\widehat{0^n}\rangle\, |y_R \oplus x_{2L}\rangle \otimes \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}}\, |[(x_{2L}, x_{2R}, \delta \oplus x_{2R})]\rangle - |\emptyset\rangle \right)
\end{aligned}$$

$$
\begin{aligned}
&+ |\mathsf{invalid}'\rangle \\
&= |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \alpha)]_3\rangle \\
&\quad + \frac{1}{\sqrt{2^{n/2}}} |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left(|\emptyset\rangle - \left(\sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |[(x_{2L}, x_{2R}, \gamma)]_3\rangle \right)\right) \\
&\quad - \frac{1}{\sqrt{2^{n/2}}} \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |x_{2L}, x_{2R}, y_L \oplus \gamma, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \gamma)]_3\rangle \\
&\quad + \frac{1}{2^{n/2}} |x_{2L}, x_{2R}\rangle |\widehat{0^n}\rangle |y_R \oplus x_{2L}\rangle \otimes \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}} |[(x_{2L}, x_{2R}, \delta)]_3\rangle - |\emptyset\rangle \right) \\
&\quad + |\mathsf{invalid}'\rangle, \qquad (39)
\end{aligned}
$$

where $|\mathsf{invalid}'\rangle$ is a vector containing invalid databases. From (38) and (39), the claim immediately follows for the first case that $D_F = \{(x_{2L}, x_{2R}, \alpha)\}$.

We can similarly show that the claim holds for the second case where D_F is empty by straightforward calculations using the second property of Proposition 2. □

Technical core to prove the indistinguishability of LR_3 and LR_3'. Let $|\psi_i\rangle$ and $|\psi_i'\rangle$ be the joint quantum states of the adversary $\mathcal{A}$ and the oracle just before making the i-th query when $\mathcal{A}$ runs relative to LR_3 and LR_3', respectively. In addition, by $|\psi_{q+1}\rangle$ and $|\psi_{q+1}'\rangle$ we similarly denote the states just before the final measurement, by abuse of notation. Then

$$
|\psi_j\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_3 \\ (D_1,D_2,D_3)\,:\,\text{valid database}}} c_{x,y,z,D_1,D_2,D_3} \, |x, y, z\rangle \otimes |D_1\rangle |D_2\rangle |D_3\rangle
$$

holds for some complex number c_{x,y,z,D_1,D_2,D_3} such that

$$
\sum_{\substack{x,y,z,D_1,D_2,D_3 \\ (D_1,D_2,D_3)\,:\,\text{valid database}}} |c_{x,y,z,D_1,D_2,D_3}|^2 = 1.
$$

Here, $x = x_{0L} \| x_{0R}$, $y = y_L \| y_R$, and z correspond to $\mathcal{A}$'s registers to send queries, receive answers, and perform offline computations, respectively ($x_{0L}, x_{0R}, y_L, y_R \in \{0,1\}^{n/2}$). Note that $|D_1|, |D_2| \le 2(j-1)$ and $|D_3| \le j-1$ hold for each summand of $|\psi_j\rangle$, since each query to the recording standard oracle with errors RstOE affects only the qubits that correspond to a single entry of each database. $|\psi_j'\rangle$ can be decomposed on the computational basis in the same way.

Showing the following proposition is the technical core to prove Proposition 4.

Proposition 5. *For each $j = 1, \ldots, q+1$, there exist vectors $|\psi_j^{\mathsf{good}}\rangle$, $|\psi_j^{\mathsf{bad}}\rangle$, $|\psi_j'^{\mathsf{good}}\rangle$, $|\psi_j'^{\mathsf{bad}}\rangle$, and complex number $a^{(j)}_{x,y,z,D_1,D_2,D_F}$ such that*

$$
|\psi_j\rangle = |\psi_j^{\mathsf{good}}\rangle + |\psi_j^{\mathsf{bad}}\rangle, \quad |\psi_j'\rangle = |\psi_j'^{\mathsf{good}}\rangle + |\psi_j'^{\mathsf{bad}}\rangle,
$$

$$|\psi_j^{\mathsf{good}}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,good}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x,y,z\rangle \otimes |D_1,D_2,[D_F]_3\rangle, \tag{40}$$

$$|\psi_j'^{\mathsf{good}}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,good}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x,y,z\rangle \otimes |D_1,D_2,D_F\rangle, \tag{41}$$

the vector $|D_1,D_2,D_F\rangle$ in $|\psi_j'^{\mathsf{good}}\rangle$ (resp., $|D_1,D_2,[D_F]_3\rangle$ in $|\psi_j^{\mathsf{good}}\rangle$) has non-zero quantum amplitude only if $|D_1| \leq 2(j-1)$, $|D_2| \leq 2(j-1)$, and $|D_F| \leq j-1$, and

$$\|\,|\psi_j^{\mathsf{bad}}\rangle\,\| \leq \left\||\psi_{j-1}^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \quad \|\,|\psi_j'^{\mathsf{bad}}\rangle\,\| \leq \left\||\psi_{j-1}'^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{42}$$

hold (we set $|\psi_0^{\mathsf{bad}}\rangle = 0$ and $|\psi_0'^{\mathsf{bad}}\rangle = 0$).

Proof intuition. Recall that a database (D_1,D_2,D_3) for LR_3 (resp., (D_1,D_2,D_F) for LR_3') is defined to be bad if and only if inputs to D_3 collide (resp., the left halves of inputs to D_F collide). Roughly speaking, “good” and “bad” vectors correspond to the states with good and bad databases, respectively.

If we were in the classical setting, databases would correspond to transcripts, and we would define the “good” and “bad” vectors to be the (classical) states with good and bad transcripts, respectively. As long as transcripts are good, the behaviors of the oracles LR_3 and LR_3' are the same and they are indistinguishable. Basically we can also use a similar intuition in the quantum setting for “good” states, and thus there exists complex number $a^{(j)}_{x,y,z,D_1,D_2,D_F}$ that satisfies (40) and (41).

For the inequalities (42) on “bad” states, when a classical adversary $\mathcal{A}$ makes the j-th query to LR_3 (resp., LR_3'), a good classical state (good transcript) changes to a bad state (bad transcript) only if a new query is made to f_1 or f_2, and the input to f_3 (resp., the left half of the input to F) collides with a previous input to f_3 (resp., the left half of a previous input to F). Such a “bad” event happens with a probability p in $O(j/2^n)$. In the quantum setting, roughly speaking, the difference between the norms of the j-th bad vector $|\psi_j^{\mathsf{bad}}\rangle$ (resp., $|\psi_j'^{\mathsf{bad}}\rangle$) and the $(j-1)$-th bad vector $|\psi_{j-1}^{\mathsf{bad}}\rangle$ (resp., $|\psi_{j-1}'^{\mathsf{bad}}\rangle$) corresponds to $\sqrt{p}$, which is in $O(\sqrt{j/2^n})$. Thus we obtain (42).

A very rough proof intuitions is as stated. However, to be more precise, an existing record (x,α) in a database will later be deleted or overwritten with a different record in the quantum setting, and the effect of such deletion and overwriting is too large to be ignored. Therefore we have to perform more careful and quantum-specific analysis by using Proposition 2 and Proposition 3.

Proof (of Proposition 5). We show the proposition by induction on j. Remember that the oracles of LR_3 and LR_3' are decomposed as $O_{\mathsf{LR}_3} = O_{\mathrm{UP}.1} \cdot O_{\mathrm{UP}.2} \cdot O_{\mathrm{UP}.3} \cdot O_{\mathrm{UP}.2} \cdot O_{\mathrm{UP}.1}$ and $O_{\mathsf{LR}_3'} = O_{\mathrm{UP}.1} \cdot O_{\mathrm{UP}.2} \cdot O'_{\mathrm{UP}.3} \cdot O_{\mathrm{UP}.2} \cdot O_{\mathrm{UP}.1}$. We check how the quantum states change when $O_{\mathrm{UP}.1}$, $O_{\mathrm{UP}.2}$, $O_{\mathrm{UP}.3}$ (resp., $O'_{\mathrm{UP}.3}$), $O_{\mathrm{UP}.2}$, and $O_{\mathrm{UP}.1}$ act on $|\psi_j\rangle$ (resp., $|\psi_j'\rangle$) in a sequential order. The claim obviously holds for $j=1$ by setting $|\psi_1^{\mathsf{good}}\rangle := |\psi_1\rangle$ and $|\psi_1'^{\mathsf{good}}\rangle := |\psi_1'\rangle$. Below we show the claim on $|\psi_{j+1}\rangle$ and $|\psi_{j+1}'\rangle$ holds if the claim on $|\psi_k\rangle$ and $|\psi_k'\rangle$ holds for $k = 1,\ldots,j$.

Recall that, in addition to database registers, the quantum oracle O_{LR_3} uses ancillary $2n$-qubit registers to compute the intermediate state after the first and second rounds (see (33) and (34)). We say that a state vector $|D_1\rangle\,|D_2\rangle\,|D_3\rangle \otimes |x_1\rangle \otimes |x_2\rangle$ for O_{LR_3}, where $|x_1\rangle \otimes |x_2\rangle$ is the ancillary $2n$ qubits, is *regular* if $x_1 = 0^n$, $x_2 = 0^n$ and the database is valid. We define regular states for $O_{\mathsf{LR}'_3}$ similarly. Since the encoding operator U_{enc} of RstOE for f_i $(1 \le i \le 3)$ and F does not act on the ancillary $2n$-qubit registers, we always obtain regular vectors when we measure $|\psi_j\rangle$ and $|\psi'_j\rangle$. Similarly, we say that a state vector $|D_1\rangle\,|D_2\rangle\,|D_3\rangle \otimes |x_1\rangle \otimes |x_2\rangle$ for O_{LR_3} is *preregular* if $x_2 = 0^n$ and the database is valid, and define preregular states for $O_{\mathsf{LR}'_3}$ similarly. When we measure the states just before the first action of $O_{\mathrm{UP}.2}$ or just after the second action of $O_{\mathrm{UP}.2}$, we always measure preregular vectors. In this proof, for the sake of brevity, we do not write (a part of) the ancillary qubits that are used to compute the intermediate states, as long as they are $|0^m\rangle$ for some m.

Let Π_{good} and Π_{bad} denote the projections onto the vector space spanned by the vectors that correspond to good databases and bad databases, respectively. Let Π_{reg} and Π_{prereg} be the projections onto the spaces spanned by the vectors that correspond to regular and preregular states, respectively.

Action of the first $O_{\mathrm{UP}.1}$.

Here we show the following claim.

Claim (Action of the first $O_{\mathrm{UP}.1}$*).* There exist vectors $|\psi_j^{\mathsf{good},1}\rangle$, $|\psi_j^{\mathsf{bad},1}\rangle$, $|\psi_j^{'\mathsf{good},1}\rangle$, $|\psi_j^{'\mathsf{bad},1}\rangle$ that satisfy the following properties.

1. $O_{\mathrm{UP}.1}\,|\psi_j\rangle = |\psi_j^{\mathsf{good},1}\rangle + |\psi_j^{\mathsf{bad},1}\rangle$ and $O_{\mathrm{UP}.1}\,|\psi'_j\rangle = |\psi_j^{'\mathsf{good},1}\rangle + |\psi_j^{'\mathsf{bad},1}\rangle$.
2. There exists complex number $a^{(j),1}_{x,y,z,D_1,D_2,D_F}$ such that

$$|\psi_j^{\mathsf{good},1}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F\\ (D_1,D_2,D_F)\,:\,\text{good}\\ D_1(x_L)\neq\perp}} a^{(j),1}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle,$$

$$|\psi_j^{'\mathsf{good},1}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F\\ (D_1,D_2,D_F)\,:\,\text{good}\\ D_1(x_L)\neq\perp}} a^{(j),1}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1L}, x_{1R}\rangle\,.$$

3. The vector $|D_1, D_2, D_F\rangle$ in $|\psi_j^{'\mathsf{good},1}\rangle$ (resp., $|D_1, D_2, [D_F]_3\rangle$ in $|\psi_j^{\mathsf{good},1}\rangle$) has non-zero quantum amplitude only if $|D_1| \le 2(j-1)+1$, $|D_2| \le 2(j-1)$, and $|D_F| \le j-1$.
4. $\|\,|\psi_j^{\mathsf{bad},1}\rangle\,\|$ and $\|\,|\psi_j^{'\mathsf{bad},1}\rangle\,\|$ are upper bounded as

$$\|\,|\psi_j^{\mathsf{bad},1}\rangle\,\| \le \|\,|\psi_j^{\mathsf{bad}}\rangle\,\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \quad \|\,|\psi_j^{'\mathsf{bad},1}\rangle\,\| \le \|\,|\psi_j^{'\mathsf{bad}}\rangle\,\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right).$$

Here, $x_{1L} = D_1(x_L) \oplus x_R$ and $x_{1R} = x_L$ for each summand of $|\psi_j^{\mathsf{good},1}\rangle$ and $|\psi_j^{'\mathsf{good},1}\rangle$.

Proof. Since the response of the first $O_{\mathrm{UP}.1}$ is written into an auxiliary register that is initially set to be $|0^{n/2}, 0^{n/2}\rangle$, by applying Proposition 3 to RstOE of f_1 there exist vectors $|\epsilon\rangle$, $|\epsilon'\rangle$ such that $\| \, |\epsilon\rangle \, \|, \| \, |\epsilon'\rangle \, \| \leq O(\sqrt{1/2^{n/2}})$, and

$$\begin{aligned}
&\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1} \, |\psi_j^{\mathsf{good}}\rangle \\
&\quad = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\,\mathrm{good} \\ D_1(x_L)\neq\perp}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x, y, z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \\
&\qquad\qquad\qquad \otimes |x_R \oplus D_1(x_L), x_L\rangle \\
&\quad - \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F \\ (D_1,D_2,D_F):\,\mathrm{good} \\ D_1(x_L)\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x, y, z\rangle \\
&\qquad\qquad\qquad \otimes |D_1 \setminus (x_L, D_1(x_L)) \cup (x_L, \gamma), D_2, [D_F]_3\rangle \\
&\qquad\qquad\qquad \otimes |x_R \oplus \gamma, x_L\rangle \\
&\quad + \sum_{\substack{x,y,z,D_1,D_2,D_F,\alpha \\ (D_1,D_2,D_F):\,\mathrm{good} \\ D_1(x_L)=\perp}} \sqrt{\frac{1}{2^{n/2}}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x, y, z\rangle \otimes |D_1 \cup (x_L, \alpha), D_2, [D_F]_3\rangle \\
&\qquad\qquad\qquad \otimes |x_R \oplus \alpha, x_L\rangle \\
&\quad + |\epsilon\rangle
\end{aligned} \tag{43}$$

and

$$\begin{aligned}
&\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1} \, |\psi_j^{'\mathsf{good}}\rangle \\
&\quad = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\,\mathrm{good} \\ D_1(x_L)\neq\perp}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x, y, z\rangle \otimes |D_1, D_2, D_F\rangle \\
&\qquad\qquad\qquad \otimes |x_R \oplus D(x_L), x_L\rangle \\
&\quad - \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F \\ (D_1,D_2,D_F):\,\mathrm{good} \\ D_1(x_L)\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x, y, z\rangle \\
&\qquad\qquad\qquad \otimes |D_1 \setminus (x_L, D_1(x_L)) \cup (x_L, \gamma), D_2, D_F\rangle \\
&\qquad\qquad\qquad \otimes |x_R \oplus \gamma, x_L\rangle \\
&\quad + \sum_{\substack{x,y,z,D_1,D_2,D_F,\alpha \\ (D_1,D_2,D_F):\,\mathrm{good} \\ D_1(x_L)=\perp}} \sqrt{\frac{1}{2^{n/2}}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x, y, z\rangle \otimes |D_1 \cup (x_L, \alpha), D_2, D_F\rangle \\
&\qquad\qquad\qquad \otimes |x_R \oplus \alpha, x_L\rangle \\
&\quad + |\epsilon'\rangle
\end{aligned} \tag{44}$$

hold.

Now, put

$$\begin{aligned}
|\psi_j^{\mathsf{good},1}\rangle &:= \Pi_{\mathsf{good}}\left(\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\,|\psi_j^{\mathsf{good}}\rangle - |\epsilon\rangle\right), \quad |\psi_j^{\mathsf{bad},1}\rangle := O_{\mathrm{UP}.1}\,|\psi_j\rangle - |\psi_j^{\mathsf{good},1}\rangle,\\
|\psi_j'^{\mathsf{good},1}\rangle &:= \Pi_{\mathsf{good}}\left(\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\,|\psi_j'^{\mathsf{good}}\rangle - |\epsilon'\rangle\right), \quad |\psi_j'^{\mathsf{bad},1}\rangle := O_{\mathrm{UP}.1}\,|\psi_j'\rangle - |\psi_j'^{\mathsf{good},1}\rangle.
\end{aligned}$$

Then the first property of the claim holds by definition, and the second and third properties immediately follow from (43) and (44) and the assumption on $|\psi_j\rangle$ and $|\psi_j'\rangle$.

Next, on the first term of the right hand side of (44) we have

$$\begin{aligned}
&\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,D_1,D_2,D_F\\(D_1,D_2,D_F)\,:\,\mathrm{good}\\D_1(x_L)\neq\bot}} a^{(j)}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\otimes|D_1,D_2,D_F\rangle\\
&\qquad\qquad\otimes|x_R\oplus D_1(x_L),x_L\rangle\\
&= 0. \qquad (45)
\end{aligned}$$

On the second term of the right hand side of (44) we have

$$\begin{aligned}
&\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F\\(D_1,D_2,D_F)\,:\,\mathrm{good}\\D_1(x_L)\neq\bot}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\\
&\qquad\otimes|D_1\setminus(x_L,D_1(x_L))\cup(x_L,\gamma),D_2,D_F\rangle\otimes|x_R\oplus\gamma,x_L\rangle\\
&= \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F\\(D_1\cup(x_L,\alpha),D_2,D_F)\,:\,\mathrm{good}\\D_1(x_L)=\bot\\(D_1\cup(x_L,\gamma),D_2,D_F)\,:\,\mathrm{bad}}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x_L,\alpha),D_2,D_F}\,|x,y,z\rangle\\
&\qquad\otimes|D_1\cup(x_L,\gamma),D_2,D_F\rangle\otimes|x_R\oplus\gamma,x_L\rangle\\
&= \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F\\(D_1\cup(x_L,\alpha),D_2,D_F)\,:\,\mathrm{good}\\D_1(x_L)=\bot\\(D_1\cup(x_L,\gamma),D_2,D_F)\,:\,\mathrm{bad}\\D_2(x_{1L})\neq\bot\wedge[D_F]_3(x_{2L})\neq\bot}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x_L,\alpha),D_2,D_F}\,|x,y,z\rangle\\
&\qquad\otimes|D_1\cup(x_L,\gamma),D_2,D_F\rangle\otimes|x_R\oplus\gamma,x_L\rangle \qquad (46)\\
&+ \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F\\(D_1\cup(x_L,\alpha),D_2,D_F)\,:\,\mathrm{good}\\D_1(x_L)=\bot\\(D_1\cup(x_L,\gamma),D_2,D_F)\,:\,\mathrm{bad}\\D_2(x_{1L})=\bot\vee(D_2(x_{1L})\neq\bot\wedge[D_F]_3(x_{2L})=\bot)}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x_L,\alpha),D_2,D_F}\,|x,y,z\rangle
\end{aligned}$$

$$\otimes |D_1 \cup (x_L, \gamma), D_2, D_F\rangle \otimes |x_R \oplus \gamma, x_L\rangle, \tag{47}$$

where $x_{1L} := \alpha \oplus x_R$, and $x_{2L} := D_2(x_{1L}) \oplus x_L$ when $D_2(x_{1L}) \neq \bot$.

Here we give an upper bound of the norm of the term(46). Note that, if a tuple $(x, (D_1 \cup (x_L, \gamma), D_2, D_F))$ satisfies the conditions

1. $D_1(x_L) = \bot$,
2. $(D_1 \cup (x_L, \gamma), D_2, D_F)$ is bad,

then the number of α such that

1. $(D_1 \cup (x_L, \alpha), D_2, D_F)$ becomes good,
2. $D_2(x_{1L}) \neq \bot$ (here, $x_{1L} := \alpha \oplus x_R$), and
3. $[D_F]_3(x_{2L}) \neq \bot$ (here, $x_{2L} := D_2(x_{1L}) \oplus x_L$),

is at most $|D_2| \leq 2(j-1)$. Hence

$$\left\| \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1\cup(x_L,\alpha),D_2,D_F)\text{ : good} \\ D_1(x_L)=\bot \\ (D_1\cup(x_L,\gamma),D_2,D_F)\text{ : bad} \\ D_2(x_{1L})\neq\bot\wedge[D_F]_3(x_{2L})\neq\bot}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x_L,\alpha),D_2,D_F} |x,y,z\rangle \right.$$

$$\left. \otimes |D_1 \cup (x_L, \gamma), D_2, D_F\rangle \otimes |x_R \oplus \gamma, x_L\rangle \right\|^2$$

$$= \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F \\ D_1(x_L)=\bot \\ (D_1\cup(x_L,\gamma),D_2,D_F)\text{ : bad}}} \frac{1}{2^n} \left| \sum_{\substack{\alpha:(D_1\cup(x_L,\alpha),D_2,D_F)\text{ is good} \\ D_2(x_{1L})\neq\bot\wedge[D_F]_3(x_{2L})\neq\bot}} a^{(j)}_{x,y,z,D_1\cup(x_L,\alpha),D_2,D_F} \right|^2$$

$$\leq \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F \\ D_1(x_L)=\bot \\ (D_1\cup(x_L,\gamma),D_2,D_F)\text{ : bad}}} \frac{1}{2^n} \cdot 2(j-1) \cdot \sum_{\substack{\alpha:(D_1\cup(x_L,\alpha),D_2,D_F)\text{ is good} \\ D_2(x_{1L})\neq\bot\wedge[D_F]_3(x_{2L})\neq\bot}} \left| a^{(j)}_{x,y,z,D_1\cup(x_L,\alpha),D_2,D_F} \right|^2$$

$$= \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1\cup(x_L,\alpha),D_2,D_F)\text{ : good} \\ D_1(x_L)=\bot \\ (D_1\cup(x_L,\gamma),D_2,D_F)\text{ : bad} \\ D_2(x_{1L})\neq\bot\wedge[D_F]_3(x_{2L})\neq\bot}} \frac{2(j-1)}{2^n}$$

$$\leq \sum_{\gamma} \frac{2(j-1)}{2^n} = \frac{2(j-1)}{2^{n/2}} \tag{48}$$

holds, where we used the convexity of the function $X \mapsto X^2$ for the first inequality.

Next, we give an upper bound of the norm of the term(47). Note that, for each tuple $(x, \alpha, (D_1, D_2, D_F))$ that satisfies

1. $D_1(x_L) = \perp$,
2. $(D_1 \cup (x_L, \alpha), D_2, D_F)$ is good, and
3. $D_2(x_{1L}) = \perp$ or $D_2(x_{1L}) \neq \perp \wedge [D_F]_3(x_{2L}) = \perp$ (here, $x_{1L} := \alpha \oplus x_R$ and $x_{2L} := D_2(x_{1L}) \oplus x_L$),

the number of γ such that $(D_1 \cup (x_L, \gamma), D_2, D_F)$ becomes bad is at most $|D_F| \leq j - 1$. Thus we have

$$\left\| \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1 \cup (x_L,\alpha),D_2,D_F)\,:\,\text{good} \\ D_1(x_L)=\perp \\ (D_1 \cup (x_L,\gamma),D_2,D_F)\,:\,\text{bad} \\ D_2(x_{1L})=\perp \vee (D_2(x_{1L})\neq\perp \wedge [D_F]_3(x_{2L})=\perp)}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1 \cup (x_L,\alpha),D_2,D_F} |x, y, z\rangle \right.$$
$$\left. \otimes |D_1 \cup (x_L, \gamma), D_2, D_F\rangle \otimes |x_R \oplus \gamma, x_L\rangle \right\|^2 .$$

$$= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x_L)=\perp}} \sum_{\substack{\gamma \\ (D_1 \cup (x_L,\gamma),D_2,D_F)\,:\,\text{bad}}} \left| \sum_{\substack{\alpha \\ (D_1 \cup (x_L,\alpha),D_2,D_F)\,:\,\text{good} \\ D_2(x_{1L})=\perp \vee (D_2(x_{1L})\neq\perp \wedge [D_F]_3(x_{2L})=\perp)}} \frac{a^{(j)}_{x,y,z,D_1 \cup (x_L,\alpha),D_2,D_F}}{2^{n/2}} \right|^2$$

$$\leq \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x_L)=\perp}} \sum_{\substack{\gamma \\ (D_1 \cup (x_L,\gamma),D_2,D_F)\,:\,\text{bad}}} \sum_{\substack{\alpha \\ (D_1 \cup (x_L,\alpha),D_2,D_F)\,:\,\text{good} \\ D_2(x_{1L})=\perp \vee (D_2(x_{1L})\neq\perp \wedge [D_F]_3(x_{2L})=\perp)}} \frac{\left| a^{(j)}_{x,y,z,D_1 \cup (x_L,\alpha),D_2,D_F} \right|^2}{2^{n/2}}$$

$$= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x_L)=\perp}} \sum_{\substack{\alpha \\ (D_1 \cup (x_L,\alpha),D_2,D_F)\,:\,\text{good} \\ D_2(x_{1L})=\perp \vee (D_2(x_{1L})\neq\perp \wedge [D_F]_3(x_{2L})=\perp)}} \left| a^{(j)}_{x,y,z,D_1 \cup (x_L,\alpha),D_2,D_F} \right|^2 \sum_{\substack{\gamma \\ (D_1 \cup (x_L,\gamma),D_2,D_F)\,:\,\text{bad}}} \frac{1}{2^{n/2}}$$

$$\leq \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x_L)=\perp}} \sum_{\substack{\alpha \\ (D_1 \cup (x_L,\alpha),D_2,D_F)\,:\,\text{good} \\ D_2(x_{1L})=\perp \vee (D_2(x_{1L})\neq\perp \wedge [D_F]_3(x_{2L})=\perp)}} \left| a^{(j)}_{x,y,z,D_1 \cup (x_L,\alpha),D_2,D_F} \right|^2 \cdot \frac{j-1}{2^{n/2}}$$

$$\leq \frac{j-1}{2^{n/2}}, \tag{49}$$

where we used the convexity of the function $X \mapsto X^2$ for the first inequality.

From (46) - (49),

$$\begin{aligned}
&\Bigg\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F\\ (D_1,D_2,D_F)\,:\,\text{good}\\ D_1(x_L)\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \left|x,y,z\right\rangle \\
&\qquad\qquad \otimes \left|D_1 \setminus (x_L, D_1(x_L)) \cup (x_L,\gamma), D_2, D_F\right\rangle \otimes \left|x_R \oplus \gamma, x_L\right\rangle \Bigg\| \\
&\le O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \qquad (50)
\end{aligned}$$

follows.

In addition, on the third term of the right hand side of (44) we have

$$\begin{aligned}
&\Bigg\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,D_1,D_2,D_F,\alpha\\ (D_1,D_2,D_F)\,:\,\text{good}\\ D_1(x_L)=\perp}} \sqrt{\frac{1}{2^{n/2}}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \left|x,y,z\right\rangle \otimes \left|D_1 \cup (x_L,\alpha), D_2, D_F\right\rangle \\
&\qquad \otimes \left|x_R \oplus \alpha, x_L\right\rangle \Bigg\|^2 \\
&= \sum_{\substack{x,y,z,D_1,D_2,D_F\\ (D_1,D_2,D_F)\,:\,\text{good}\\ D_1(x_L)=\perp}} |a^{(j)}_{x,y,z,D_1,D_2,D_F}|^2 \sum_{\alpha:(D_1\cup(x_L,\alpha),D_2,D_F)\text{ is bad}} \frac{1}{2^{n/2}} \\
&\le \sum_{\substack{x,y,z,D_1,D_2,D_F\\ (D_1,D_2,D_F)\,:\,\text{good}\\ D_1(x_L)=\perp}} |a^{(j)}_{x,y,z,D_1,D_2,D_F}|^2 \cdot O\left(\frac{j}{2^{n/2}}\right) \\
&\le O\left(\frac{j}{2^{n/2}}\right). \qquad (51)
\end{aligned}$$

From (45), (50), and (51),

$$\left\|\Pi_{\mathsf{bad}}\left(\Pi_{\mathsf{valid}} O_{\mathrm{UP.1}} \left|\psi'^{\mathsf{good}}_j\right\rangle - \left|\epsilon'\right\rangle\right)\right\| \le O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \qquad (52)$$

follows. Since $\Pi_{\mathsf{valid}} O_{\mathrm{UP.1}} |\psi'_j\rangle = O_{\mathrm{UP.1}} |\psi'_j\rangle$, we have

$$\begin{aligned}
\left\| |\psi_j'^{\mathsf{bad},1}\rangle \right\| &= \left\| O_{\mathrm{UP.1}} |\psi'_j\rangle - |\psi_1'^{\mathsf{good},1}\rangle \right\| \\
&= \left\| \Pi_{\mathsf{valid}} O_{\mathrm{UP.1}} \left(|\psi_j'^{\mathsf{good}}\rangle + |\psi_j'^{\mathsf{bad}}\rangle \right) - |\psi_1'^{\mathsf{good},1}\rangle \right\| \\
&\leq \left\| \Pi_{\mathsf{valid}} O_{\mathrm{UP.1}} |\psi_j'^{\mathsf{good}}\rangle - |\psi_1'^{\mathsf{good},1}\rangle \right\| + \left\| \Pi_{\mathsf{valid}} O_{\mathrm{UP.1}} |\psi_j'^{\mathsf{bad}}\rangle \right\| \\
&= \left\| \Pi_{\mathsf{valid}} O_{\mathrm{UP.1}} |\psi_j'^{\mathsf{good}}\rangle - \Pi_{\mathsf{good}} \left(\Pi_{\mathsf{valid}} O_{\mathrm{UP.1}} |\psi_j'^{\mathsf{good}}\rangle - |\epsilon'\rangle \right) \right\| + \left\| |\psi_j'^{\mathsf{bad}}\rangle \right\| \\
&= \left\| \Pi_{\mathsf{bad}} \left(\Pi_{\mathsf{valid}} O_{\mathrm{UP.1}} |\psi_j'^{\mathsf{good}}\rangle - |\epsilon'\rangle \right) \right\| + \left\| |\psi_j'^{\mathsf{bad}}\rangle \right\| \\
&\leq O\left(\sqrt{\frac{j}{2^{n/2}}} \right) + \left\| |\psi_j'^{\mathsf{bad}}\rangle \right\| .
\end{aligned}$$

Similarly we can also show $\left\| |\psi_j^{\mathsf{bad},1}\rangle \right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}} \right) + \left\| |\psi_j^{\mathsf{bad}}\rangle \right\|$. Therefore the fourth property of the claim also holds. □

Action of the first $O_{\mathrm{UP.2}}$.

The following claim can be shown by applying Proposition 3 on f_2 in the same way as we showed the claim for the action of the first $O_{\mathrm{UP.1}}$ by applying Proposition 3 on f_1.

Claim (Action of the first $O_{\mathrm{UP.2}}$). There exist vectors $|\psi_j^{\mathsf{good},2}\rangle$, $|\psi_j^{\mathsf{bad},2}\rangle$, $|\psi_j'^{\mathsf{good},2}\rangle$, $|\psi_j'^{\mathsf{bad},2}\rangle$ that satisfy the following properties.

1. $O_{\mathrm{UP.2}} O_{\mathrm{UP.1}} |\psi_j\rangle = |\psi_j^{\mathsf{good},2}\rangle + |\psi_j^{\mathsf{bad},2}\rangle$ and $O_{\mathrm{UP.2}} O_{\mathrm{UP.1}} |\psi'_j\rangle = |\psi_j'^{\mathsf{good},2}\rangle + |\psi_j'^{\mathsf{bad},2}\rangle$.
2. There exists complex number $a^{(j),2}_{x,y,z,D_1,D_2,D_F}$ such that

$$|\psi_j^{\mathsf{good},2}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,\text{good} \\ D_1(x_L)\neq\bot, D_2(x_{1L})\neq\bot}} a^{(j),2}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle ,$$

$$|\psi_j'^{\mathsf{good},2}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,\text{good} \\ D_1(x_L)\neq\bot, D_2(x_{1L})\neq\bot}} a^{(j),2}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle .$$

3. The vector $|D_1, D_2, D_F\rangle$ in $|\psi_j'^{\mathsf{good},2}\rangle$ (resp., $|D_1, D_2, [D_F]_3\rangle$ in $|\psi_j^{\mathsf{good},2}\rangle$) has non-zero quantum amplitude only if $|D_1| \leq 2(j-1)+1$, $|D_2| \leq 2(j-1)+1$, and $|D_F| \leq j-1$.
4. $\|\,|\psi_j^{\mathsf{bad},2}\rangle\,\|$ and $\|\,|\psi_j'^{\mathsf{bad},2}\rangle\,\|$ are upper bounded as

$$\|\,|\psi_j^{\mathsf{bad},2}\rangle\,\| \leq \|\,|\psi_j^{\mathsf{bad}}\rangle\,\| + O\left(\sqrt{\frac{j}{2^{n/2}}} \right), \quad \|\,|\psi_j'^{\mathsf{bad},2}\rangle\,\| \leq \|\,|\psi_j'^{\mathsf{bad}}\rangle\,\| + O\left(\sqrt{\frac{j}{2^{n/2}}} \right).$$

Here, $x_{1L} = D_1(x_L) \oplus x_R$, $x_{1R} = x_L$, $x_{2L} = D_2(x_{1L}) \oplus x_{1R}$, and $x_{2R} = x_{1L}$ for each summand of $|\psi_j^{\mathsf{good},2}\rangle$ and $|\psi_j^{\prime\mathsf{good},2}\rangle$.

Action of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$.

Here we show the following claim.

Claim (Action of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$). Let $|\psi_j^{\mathsf{good},3}\rangle := \Pi_{\mathsf{valid}} O_{\mathrm{UP}.3} |\psi_j^{\mathsf{good},2}\rangle$, $|\psi_j^{\mathsf{bad},3}\rangle := O_{\mathrm{UP}.3} O_{\mathrm{UP}.2} O_{\mathrm{UP}.1} |\psi_j\rangle - |\psi_j^{\mathsf{good},3}\rangle$, $|\psi_j^{\prime\mathsf{good},3}\rangle := \Pi_{\mathsf{valid}} O_{\mathrm{UP}.3} |\psi_j^{\prime\mathsf{good},2}\rangle$, and $|\psi_j^{\prime\mathsf{bad},3}\rangle := O_{\mathrm{UP}.3} O_{\mathrm{UP}.2} O_{\mathrm{UP}.1} |\psi'_j\rangle - |\psi_j^{\prime\mathsf{good},3}\rangle$. Then the following properties hold.

1. There exists complex number $a^{(j),3}_{x,y,z,D_1,D_2,D_F}$ such that

$$|\psi_j^{\mathsf{good},3}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\text{good} \\ D_1(x_L)\neq\perp, D_2(x_{1L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle,$$

$$|\psi_j^{\prime\mathsf{good},3}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\text{good} \\ D_1(x_L)\neq\perp, D_2(x_{1L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle.$$

2. The vector $|D_1, D_2, D_F\rangle$ in $|\psi_j^{\prime\mathsf{good},3}\rangle$ (resp., $|D_1, D_2, [D_F]_3\rangle$ in $|\psi_j^{\mathsf{good},3}\rangle$) has non-zero quantum amplitude only if $|D_1| \le 2(j-1)+1$, $|D_2| \le 2(j-1)+1$, and $|D_F| \le j$.
3. $\| |\psi_j^{\mathsf{bad},3}\rangle \|$ and $\| |\psi_j^{\prime\mathsf{bad},3}\rangle \|$ are upper bounded as

$$\| |\psi_j^{\mathsf{bad},3}\rangle \| \le \| |\psi_j^{\mathsf{bad}}\rangle \| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \quad \| |\psi_j^{\prime\mathsf{bad},3}\rangle \| \le \| |\psi_j^{\prime\mathsf{bad}}\rangle \| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right).$$

Here, $x_{1L} = D_1(x_L) \oplus x_R$, $x_{1R} = x_L$, $x_{2L} = D_2(x_{1L}) \oplus x_{1R}$, and $x_{2R} = x_{1L}$ for each summand of $|\psi_j^{\mathsf{good},3}\rangle$ and $|\psi_j^{\prime\mathsf{good},3}\rangle$.

Proof. First, for each summand $|x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle$ of $|\psi_j^{\prime\mathsf{good},2}\rangle$, we have that

$$\Pi_{\mathsf{bad}} \Pi_{\mathsf{valid}} O'_{\mathrm{UP}.3} |x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle = 0$$

by definition of good databases. Therefore, we have

$$\Pi_{\mathsf{bad}} |\psi_j^{\prime\mathsf{good},3}\rangle = \Pi_{\mathsf{bad}} \Pi_{\mathsf{valid}} O'_{\mathrm{UP}.3} |\psi_j^{\prime\mathsf{good},2}\rangle = 0,$$

which implies

$$|\psi_j^{\prime\mathsf{good},3}\rangle = \Pi_{\mathsf{good}} |\psi_j^{\prime\mathsf{good},3}\rangle.$$

Similarly,

$$|\psi_j^{\mathsf{good},3}\rangle = \Pi_{\mathsf{good}} |\psi_j^{\mathsf{good},3}\rangle$$

holds. Now the first property of the claim follows from the second property in the claim for the first action of $O_{\mathrm{UP}.2}$ and Lemma 1. The second property of the claim follows from the third property in the claim for the first action of $O_{\mathrm{UP}.2}$.

Moreover, we have

$$\begin{aligned}\left\| |\psi_j^{\mathsf{bad},3}\rangle \right\| &= \left\| O_{\mathrm{UP}.3} O_{\mathrm{UP}.2} O_{\mathrm{UP}.1} |\psi_j\rangle - |\psi_j^{\mathsf{good},3}\rangle \right\| \\ &= \left\| \Pi_{\mathsf{valid}} O_{\mathrm{UP}.3} O_{\mathrm{UP}.2} O_{\mathrm{UP}.1} |\psi_j\rangle - \Pi_{\mathsf{valid}} O_{\mathrm{UP}.3} |\psi_j^{\mathsf{good},2}\rangle \right\| \\ &= \left\| \Pi_{\mathsf{valid}} O_{\mathrm{UP}.3} |\psi_j^{\mathsf{bad},2}\rangle \right\| \\ &\leq \left\| |\psi_j^{\mathsf{bad},2}\rangle \right\| \\ &\leq \| |\psi_j^{\mathsf{bad}}\rangle \| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \end{aligned} \tag{53}$$

where we used the fourth property in the claim for the first action of $O_{\mathrm{UP}.2}$ in the last inequality. Similarly, $\left\| |\psi_j^{\prime\mathsf{bad},3}\rangle \right\| \leq \| |\psi_j^{\prime\mathsf{bad}}\rangle \| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right)$ follows. Therefore the third property of the claim holds. □

Action of the second $O_{\mathrm{UP}.2}$.

We show that the following claim holds.

Claim (Action of the second $O_{\mathrm{UP}.2}$*).* Let $|\psi_j^{\mathsf{good},4}\rangle := \Pi_{\mathsf{good}} \Pi_{\mathsf{prereg}} O_{\mathrm{UP}.2} |\psi_j^{\mathsf{good},3}\rangle$, $|\psi_j^{\mathsf{bad},4}\rangle := O_{\mathrm{UP}.2} O_{\mathrm{UP}.3} O_{\mathrm{UP}.2} O_{\mathrm{UP}.1} |\psi_j\rangle - |\psi_j^{\mathsf{good},4}\rangle$, $|\psi_j^{\prime\mathsf{good},4}\rangle := \Pi_{\mathsf{good}} \Pi_{\mathsf{prereg}} O_{\mathrm{UP}.2} |\psi_j^{\prime\mathsf{good},3}\rangle$, and $|\psi_j^{\prime\mathsf{bad},4}\rangle := O_{\mathrm{UP}.2} O_{\mathrm{UP}.3} O_{\mathrm{UP}.2} O_{\mathrm{UP}.1} |\psi_j'\rangle - |\psi_j^{\prime\mathsf{good},4}\rangle$. Then the following properties hold.

1. There exists complex number $a^{(j),4}_{x,y,z,D_1,D_2,D_F}$ such that

$$|\psi_j^{\mathsf{good},4}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\text{good} \\ D_1(x_L)\neq\perp}} a^{(j),4}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle,$$

$$|\psi_j^{\prime\mathsf{good},4}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\text{good} \\ D_1(x_L)\neq\perp}} a^{(j),4}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1L}, x_{1R}\rangle.$$

2. The vector $|D_1, D_2, D_F\rangle$ in $|\psi_j^{\prime\mathsf{good},4}\rangle$ (resp., $|D_1, D_2, [D_F]_3\rangle$ in $|\psi_j^{\mathsf{good},4}\rangle$) has non-zero quantum amplitude only if $|D_1| \leq 2(j-1)+1$, $|D_2| \leq 2j$, and $|D_F| \leq j$.
3. $\| |\psi_j^{\mathsf{bad},4}\rangle \|$ and $\| |\psi_j^{\prime\mathsf{bad},4}\rangle \|$ are upper bounded as

$$\| |\psi_j^{\mathsf{bad},4}\rangle \| \leq \| |\psi_j^{\mathsf{bad}}\rangle \| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \quad \| |\psi_j^{\prime\mathsf{bad},4}\rangle \| \leq \| |\psi_j^{\prime\mathsf{bad}}\rangle \| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right).$$

Here, $x_{1L} = D_1(x_L) \oplus x_R$ and $x_{1R} = x_L$ for each summand of $|\psi_j^{\mathsf{good},4}\rangle$ and $|\psi_j^{\prime\mathsf{good},4}\rangle$.

Proof. The first property follows from the first property of Proposition 2 and the first property in the claim on the actions of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$. In addition, the second property follows from the second property in the claim on the actions of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$. Below, we show the third property.

Let $\Pi_{D_3:\not\perp}$ and $\Pi_{D_3:\perp}$ be the projections onto the spaces spanned by the vectors $|x,y,z\rangle \otimes |D_1,D_2,D_3\rangle \otimes |x_{1L},x_{1R}\rangle \otimes |x_{2L},x_{2R}\rangle$ such that $D_3(x_{2L}) \neq \perp$ and $D_3(x_{2L}) = \perp$, respectively.

Then we have

$$\begin{aligned}
&\Pi_{D_3:\not\perp} |\psi_j^{\mathsf{good},3}\rangle \\
&\quad= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)\neq\perp, D_2(x_{1L})\neq\perp \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1,D_2,[D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{1L},x_{1R}\rangle \otimes |x_{2L},x_{2R}\rangle \\
&\quad= \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \otimes |D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{1L},x_{1R}\rangle \otimes |x_{2L},x_{2R}\rangle,
\end{aligned}$$

where $x_{1L} := D_1(x_L) \oplus x_R$, $x_{1R} := x_L$, $x_{2L} := \alpha \oplus x_{1R}$, and $x_{2R} := x_{1L}$ for each summand in the right hand side. By applying the first property of Proposition 2 to f_2 we have

$$\begin{aligned}
&\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathrm{UP}.2} \Pi_{D_3:\not\perp} |\psi_j^{\mathsf{good},3}\rangle \\
&\quad= \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathrm{UP}.2} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \otimes |D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{1L},x_{1R}\rangle \otimes |x_{2L},x_{2R}\rangle \\
&\quad= \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \otimes |D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{1L},x_{1R}\rangle \otimes |0^{n/2},0^{n/2}\rangle \\
&\qquad + \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \\
&\qquad\qquad \otimes |D_1\rangle \left(|D_2\rangle - \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |D_2\cup(x_{1L},\gamma)\rangle \right) |[D_F]_3\rangle
\end{aligned}$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle$$

$$- \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x_L)\neq\bot, D_2(x_{1L})=\bot \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good} \\ [D_F]_3(x_{2L})\neq\bot}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1\right\rangle \left(\left|D_2 \cup (x_{1L}, \gamma)\right\rangle - \left|D^{\mathsf{invalid}}_{\gamma}\right\rangle\right) \left|[D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|\alpha \oplus \gamma, 0^{n/2}\right\rangle$$

$$+ \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\bot, D_2(x_{1L})=\bot \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good} \\ [D_F]_3(x_{2L})\neq\bot}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1\right\rangle \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}} \left|D_2 \cup (x_{1L}, \delta)\right\rangle - \left|D_2\right\rangle\right) \left|[D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|\widehat{0^{n/2}}, 0^{n/2}\right\rangle$$

$$= \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\bot, D_2(x_{1L})=\bot \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good} \\ [D_F]_3(x_{2L})\neq\bot}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1, D_2 \cup (x_{1L}, \alpha), [D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle \tag{54}$$

$$+ \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\bot, D_2(x_{1L})=\bot \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good} \\ [D_F]_3(x_{2L})\neq\bot}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1, D_2, [D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle \tag{55}$$

$$- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x_L)\neq\bot, D_2(x_{1L})=\bot \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good} \\ [D_F]_3(x_{2L})\neq\bot}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1, D_2 \cup (x_{1L}, \gamma), [D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle \tag{56}$$

$$- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\bot, D_2(x_{1L})=\bot \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good} \\ [D_F]_3(x_{2L})\neq\bot}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1, D_2 \cup (x_{1L}, \alpha), [D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle \tag{57}$$

$$+ \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F) : \text{good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{3n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle$$
$$\otimes |D_1\rangle \left(2\sum_{\delta} \frac{1}{\sqrt{2^{n/2}}} |D_2 \cup (x_{1L},\delta)\rangle - |D_2\rangle\right) |[D_F]_3\rangle$$
$$\otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle \,. \tag{58}$$

On the term (54), we have

$$\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F) : \text{good} \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle$$
$$\otimes |D_1, D_2 \cup (x_{1L},\alpha), [D_F]_3\rangle$$
$$\otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle$$
$$= 0 \tag{59}$$

since all databases are good.

On the term (55), we have

$$\Bigg\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F) : \text{good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle$$
$$\otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle \Bigg\|^2$$
$$= \Bigg\| \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp}} \sum_{\substack{\alpha \\ (D_1,D_2\cup(x_{1L},\alpha),D_F) : \text{good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle$$
$$\otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle \Bigg\|^2$$

$$= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp}} \frac{1}{2^{n/2}} \left| \sum_{\substack{\alpha \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{ good} \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \right|^2 .$$

Now, for each (x, y, z, D_1, D_2, D_F) such that $D_1(x_L) \neq \perp$ and $D_2(x_{1L}) = \perp$ (recall that $x_{1L} := x_R \oplus D_1(x_L)$), the number of α such that $[D_F]_3(x_{2L}) \neq \perp$ (recall that $x_{2L} := x_L \oplus \alpha$) and $(D_1, D_2 \cup (x_{1L}, \alpha), D_F)$ becomes good is at most $|D_F| \leq j$. Hence, from the convexity of the function $X \mapsto X^2$,

$$\begin{aligned}
&\left| \sum_{\substack{\alpha \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{ good} \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \right|^2 \\
&\leq \left| \sum_{\substack{\alpha \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{ good} \\ [D_F]_3(x_{2L})\neq\perp}} \left| a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \right| \right|^2 \\
&\leq j \cdot \sum_{\substack{\alpha \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{ good} \\ [D_F]_3(x_{2L})\neq\perp}} \left| a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \right|^2
\end{aligned}$$

holds, which implies that

$$\begin{aligned}
&\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{ good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x, y, z\rangle \right. \\
&\qquad\qquad \left. \otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle \right\|^2 \\
&\leq \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp}} \frac{j}{2^{n/2}} \sum_{\substack{\alpha \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{ good} \\ [D_F]_3(x_{2L})\neq\perp}} \left| a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \right|^2 \\
&\leq O\left(\frac{j}{2^{n/2}}\right) \qquad (60)
\end{aligned}$$

holds.

Here we give an upper bound of the norm of the term (56). Note that, if a tuple $(x, (D_1, D_2 \cup (x_L, \gamma), D_F))$ satisfies the conditions

1. $D_1(x_L) \neq \perp$,
2. $(D_1, D_2 \cup (x_{1L}, \gamma), D_F)$ is bad,

then the number of α such that

1. $(D_1, D_2 \cup (x_{1L}, \alpha), D_F)$ becomes good,
2. $D_2(x_{1L}) = \perp$ (here, $x_{1L} := D_1(x_L) \oplus x_R$), and
3. $[D_F]_3(x_{2L}) \neq \perp$ (here, $x_{2L} := \alpha \oplus x_L$),

is at most $|D_F| \leq j$. Therefore we can show

$$\begin{aligned}
&\Bigg\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\text{ : good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x, y, z\rangle \\
&\qquad\qquad \otimes |D_1, D_2 \cup (x_{1L}, \gamma), [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle \Bigg\|^2 \\
&= \Bigg\| \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\text{ : good} \\ [D_F]_3(x_{2L})\neq\perp \\ (D_1,D_2\cup(x_{1L},\gamma),D_F)\text{:bad}}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x, y, z\rangle \\
&\qquad\qquad \otimes |D_1, D_2 \cup (x_{1L}, \gamma), [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle \Bigg\|^2 \\
&\leq \frac{j}{2^{n/2}} \qquad (61)
\end{aligned}$$

in the same way as we showed (48).

On the term (57), we have

$$\begin{aligned}&\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good}\\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \\ &\qquad\qquad\qquad\otimes |D_1, D_2\cup(x_{1L},\alpha),[D_F]_3\rangle \otimes |x_{1L},x_{1R}\rangle \otimes |0^{n/2},0^{n/2}\rangle \\ &\quad = 0, \end{aligned} \tag{62}$$

since all databases are good.

On the term (58),

$$\begin{aligned}&\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good}\\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{3n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \right.\\ &\qquad\qquad \otimes |D_1\rangle \left(2\sum_{\delta}\frac{1}{\sqrt{2^{n/2}}}|D_2\cup(x_{1L},\delta)\rangle - |D_2\rangle\right)|[D_F]_3\rangle \\ &\qquad\qquad \left. \otimes |x_{1L},x_{1R}\rangle \otimes |0^{n/2},0^{n/2}\rangle \right\| \\ &\quad \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \end{aligned} \tag{63}$$

follows from (60) and (61).

From (54)–(63),

$$\left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_F:\not\perp}|\psi_j^{\mathsf{good},3}\rangle\right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{64}$$

follows.

In the same way as we obtained (54)–(58), by applying the first property of Proposition 2 to f_2, we have

$$\begin{aligned}&\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_3:\perp}|\psi_j^{\mathsf{good},3}\rangle \\ &\quad = \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good}\\ [D_F]_3(x_{2L})=\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \end{aligned}$$

$$\otimes \left|D_1, D_2 \cup (x_{1L}, \alpha), [D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle \tag{65}$$

$$+ \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\text{ : good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1, D_2, [D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle \tag{66}$$

$$- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\text{ : good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1, D_2 \cup (x_{1L}, \gamma), [D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle \tag{67}$$

$$- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\text{ : good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1, D_2 \cup (x_{1L}, \alpha), [D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle \tag{68}$$

$$+ \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\text{ : good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{2^{3n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1\right\rangle \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}} \left|D_2 \cup (x_{1L}, \delta)\right\rangle - \left|D_2\right\rangle \right) \left|[D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle . \tag{69}$$

On the term (65), we have

$$\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\text{ : good} \\ [D_F]_3(x_{2L})=\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x, y, z\right\rangle$$

$$\otimes \left|D_1, D_2 \cup (x_{1L}, \alpha), [D_F]_3\right\rangle$$

$$\otimes \left|x_{1L}, x_{1R}\right\rangle \otimes \left|0^{n/2}, 0^{n/2}\right\rangle$$

$$= 0 \tag{70}$$

since all databases are good.

On the term (66), we have

$$
\begin{aligned}
&\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})=\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x,y,z\right\rangle \\
&\qquad\qquad\qquad \otimes \left|D_1,D_2,[D_F]_3\right\rangle \otimes \left|x_{1L},x_{1R}\right\rangle \otimes \left|0^{n/2},0^{n/2}\right\rangle \\
&= 0 \qquad (71)
\end{aligned}
$$

since all databases are good.

Next, we give an upper bound of the norm of the term (67). Note that, for each tuple $(x,\alpha,(D_1,D_2,D_F))$ that satisfies

1. $D_1(x_L)\neq\perp$,
2. $(D_1,D_2\cup(x_{1L},\alpha),D_F)$ is good, and
3. $[D_F]_3(x_{2L})=\perp$ (here, $x_{1L}:=D_1(x_L)\oplus x_R$ and $x_{2L}:=\alpha\oplus x_L$),

the number of γ such that $(D_1\cup(x_L,\gamma),D_2,D_F)$ becomes bad is at most $|D_F|\leq j$. Hence we have that

$$
\begin{aligned}
&\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F\\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})=\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} \left|x,y,z\right\rangle \right. \\
&\qquad\qquad \left. \otimes \left|D_1,D_2\cup(x_{1L},\gamma),[D_F]_3\right\rangle \otimes \left|x_{1L},x_{1R}\right\rangle \otimes \left|0^{n/2},0^{n/2}\right\rangle \right\|^2 \\
&= \sum_{\substack{x,y,z,D_1,D_2,D_F\\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp}} \sum_{\substack{\gamma\\ (D_1,D_2\cup(x_{1L},\gamma),D_F)\,:\,\text{bad}}} \\
&\qquad\qquad \cdot \left| \sum_{\substack{\alpha\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})=\perp}} \frac{a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}}{2^{n/2}} \right|^2 \\
&\leq \sum_{\substack{x,y,z,D_1,D_2,D_F\\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp}} \sum_{\substack{\gamma\\ (D_1,D_2\cup(x_{1L},\gamma),D_F)\,:\,\text{bad}}}
\end{aligned}
$$

$$\cdot\left(\frac{1}{2^{n/2}}\cdot\sum_{\substack{\alpha\\(D_1,D_2\cup(x_{1L},\alpha),D_F):\text{good}\\ [D_F]_3(x_{2L})=\perp}}\left|a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\right|^2\right)$$

$$\leq O\left(\frac{j}{2^{n/2}}\right), \tag{72}$$

holds, where we used the convexity of the function $X\mapsto X^2$ for the inequality.

On the term (68), we have

$$\Pi_{\mathsf{bad}}\sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp\\(D_1,D_2\cup(x_{1L},\alpha),D_F):\text{good}\\ [D_F]_3(x_{2L})=\perp}}\frac{1}{2^{n/2}}a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle$$

$$\otimes|D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle\otimes|x_{1L},x_{1R}\rangle\otimes|0^{n/2},0^{n/2}\rangle$$

$$=0, \tag{73}$$

since all databases are good.

On the term (69),

$$\left\|\Pi_{\mathsf{bad}}\sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp,D_2(x_{1L})=\perp\\(D_1,D_2\cup(x_{1L},\alpha),D_F):\text{good}\\ [D_F]_3(x_{2L})=\perp}}\frac{1}{2^{3n/2}}a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle\right.$$

$$\otimes|D_1\rangle\left(2\sum_{\delta}\frac{1}{\sqrt{2^{n/2}}}|D_2\cup(x_{1L},\delta)\rangle-|D_2\rangle\right)|[D_F]_3\rangle$$

$$\left.\otimes|x_{1L},x_{1R}\rangle\otimes|0^{n/2},0^{n/2}\rangle\right\|$$

$$\leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{74}$$

follows from (71) and (72).

From (65)–(74),

$$\left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_F:\perp}\,|\psi_j^{\mathsf{good},3}\rangle\right\|\leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{75}$$

follows.

Therefore,

$$\begin{aligned}
&\left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&\leq \left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_F:\not\perp}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| + \left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_F:\perp}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&\leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \qquad (76)
\end{aligned}$$

follows from (64) and (75).

Since $O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\left|\psi_j\right\rangle = \Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\left|\psi_j\right\rangle$,

$$\begin{aligned}
&\left\|\left|\psi_j^{\mathsf{bad},4}\right\rangle\right\| \\
&= \left\|O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\left|\psi_j\right\rangle - \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&= \left\|\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\left|\psi_j\right\rangle - \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&= \left\|\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left(\left|\psi_j^{\mathsf{good},3}\right\rangle + \left|\psi_j^{\mathsf{bad},3}\right\rangle\right) - \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&\leq \left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| + \left\|\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{bad},3}\right\rangle\right\| \\
&\leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) + \left\|\left|\psi_j^{\mathsf{bad},3}\right\rangle\right\| \\
&\leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) + \left\|\left|\psi_j^{\mathsf{bad}}\right\rangle\right\|
\end{aligned}$$

follows from the claim on the action of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$. We can show

$$\left\|\left|\psi_j^{\prime\mathsf{bad},4}\right\rangle\right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) + \left\|\left|\psi_j^{\prime\mathsf{bad}}\right\rangle\right\| \qquad (77)$$

in the same way, and the third property of the claim also holds. □

Action of the second $O_{\mathrm{UP}.1}$.

Let $\left|\psi_{j+1}^{\mathsf{good}}\right\rangle := \Pi_{\mathsf{good}}\Pi_{\mathsf{reg}}O_{\mathrm{UP}.1}\left|\psi_j^{\mathsf{good},4}\right\rangle$, $\left|\psi_{j+1}^{\mathsf{bad}}\right\rangle := \left|\psi_{j+1}\right\rangle - \left|\psi_{j+1}^{\mathsf{good}}\right\rangle$, $\left|\psi_{j+1}^{\prime\mathsf{good}}\right\rangle := \Pi_{\mathsf{good}}\Pi_{\mathsf{reg}}O_{\mathrm{UP}.1}\left|\psi_j^{\prime\mathsf{good},4}\right\rangle$, and $\left|\psi_{j+1}^{\prime\mathsf{bad}}\right\rangle := \left|\psi'_{j+1}\right\rangle - \left|\psi_{j+1}^{\prime\mathsf{good}}\right\rangle$. Then we can show these $\left|\psi_{j+1}^{\mathsf{good}}\right\rangle$, $\left|\psi_{j+1}^{\mathsf{bad}}\right\rangle$, $\left|\psi_{j+1}^{\prime\mathsf{good}}\right\rangle$, and $\left|\psi_{j+1}^{\prime\mathsf{bad}}\right\rangle$ satisfy the desired properties in Proposition 5, in the same way as we showed the claim on the action of the second $O_{\mathrm{UP}.2}$. □

Finishing the proof of Proposition 4.

Proof (of Proposition 4). Let $\left|\psi_j^{\mathsf{good}}\right\rangle$, $\left|\psi_j^{\mathsf{bad}}\right\rangle$, $\left|\psi_j^{\prime\mathsf{good}}\right\rangle$, and $\left|\psi_j^{\prime\mathsf{bad}}\right\rangle$ be the vectors as in Proposition 5. Then

$$\left\|\left|\psi_{q+1}^{\mathsf{bad}}\right\rangle\right\| \leq \sum_{1\leq j\leq q} O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \leq O\left(\sqrt{\frac{j^3}{2^{n/2}}}\right) \qquad (78)$$

follows. Similarly,

$$\left\| |\psi'^{\mathsf{bad}}_{q+1}\rangle \right\| \leq O\left(\sqrt{\frac{j^3}{2^{n/2}}}\right) \tag{79}$$

holds.

Let $\mathsf{tr}_{\mathcal{D}_{123}}$ and $\mathsf{tr}_{\mathcal{D}_{123}}$ denote the partial trace operations over the databases for LR_3 and LR'_3, respectively. Then

$$\mathsf{td}\left(\mathsf{tr}_{\mathcal{D}_{123}}\left(|\psi^{\mathsf{good}}_{q+1}\rangle\langle\psi^{\mathsf{good}}_{q+1}|\right), \mathsf{tr}_{\mathcal{D}_{123}}\left(|\psi'^{\mathsf{good}}_{q+1}\rangle\langle\psi'^{\mathsf{good}}_{q+1}|\right)\right) = 0 \tag{80}$$

follows from (40) and (41).

Therefore

$$\begin{aligned}
\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_3,\mathsf{LR}'_3}(\mathcal{A}) &\leq \mathsf{td}\left(\mathsf{tr}_{\mathcal{D}_{123}}\left(|\psi_{q+1}\rangle\langle\psi_{q+1}|\right), \mathsf{tr}_{\mathcal{D}_{123}}\left(|\psi'_{q+1}\rangle\langle\psi'_{q+1}|\right)\right) \\
&\leq \mathsf{td}\left(\mathsf{tr}_{\mathcal{D}_{123}}\left(|\psi^{\mathsf{good}}_{q+1}\rangle\langle\psi^{\mathsf{good}}_{q+1}|\right), \mathsf{tr}_{\mathcal{D}_{123}}\left(|\psi'^{\mathsf{good}}_{q+1}\rangle\langle\psi'^{\mathsf{good}}_{q+1}|\right)\right) \\
&\quad + 2\left\| |\psi^{\mathsf{bad}}_{q+1}\rangle \right\| + 2\left\| |\psi'^{\mathsf{bad}}_{q+1}\rangle \right\| \\
&\leq O\left(\sqrt{\frac{j^3}{2^{n/2}}}\right)
\end{aligned} \tag{81}$$

holds, which completes the proof. □

4.2 Hardness of Distinguishing LR''_2 from RF

The goal of this subsection is to show the following proposition.

Proposition 6. *For any quantum adversary $\mathcal{A}$ that makes at most q quantum queries, $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}''_2,\mathsf{RF}}(\mathcal{A}) \leq O\left(\sqrt{q^3/2^{n/2}}\right)$ holds.*

Let $F_1 : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ and $F'_2 : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ be independent random functions. Let $\mathsf{RF}' : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2} \times \{0,1\}^{n/2}$ be the function defined by

$$\mathsf{RF}'(x_L, x_R) := (F'_2(x_{1L}, x_{1R}, x_R), x_{1L}),$$

where $(x_{1L}, x_{1R}) := (F_1(x_L, x_R), x_L)$ (see Fig. 8). Note that RF' is in fact a random function since F_1 and F'_2 are random functions. In what follows, we show

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}''_2,\mathsf{RF}'}(\mathcal{A}) \leq O\left(\sqrt{q^3/2^{n/2}}\right)$$

instead of showing $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}''_2,\mathsf{RF}}(\mathcal{A}) \leq O\left(\sqrt{q^3/2^{n/2}}\right)$.

We use the same proof strategy as in Section 4.1. That is, we define good and bad databases for LR''_2 and RF' in such a way that

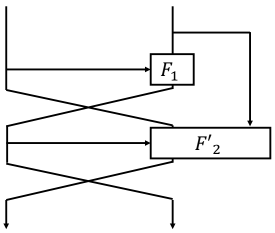

Fig. 8. RF'

1. There exists a one-to-one correspondence between good databases for LR''_2 and those for RF'.
2. The behavior of the oracle LR''_2 on a good database is almost the same as that of the oracle RF' on the corresponding good database.
3. "Good" states change to "bad" states with a small probability.

Intuitively, we define "bad" databases as those with collisions on the leftmost $(n/2)$ bits of the input to F_2 or F'_2, and "good" databases as those without such collisions.

Quantum oracle of LR''_2. Let O_{F_i} denote the quantum oracle of each round function F_i. In addition, let us define the unitary operator $O_{\mathrm{UP}.i}$ that computes the state update of the first round by

$$\begin{aligned} O_{\mathrm{UP}.i} &: |x_{(i-1)L}, x_{(i-1)R}\rangle\, |y_L, y_R\rangle \\ &\mapsto |x_{(i-1)L}, x_{(i-1)R}\rangle\, |(y_L, y_R) \oplus (F_i(x_{(i-1)L}, x_{(i-1)R}), x_{(i-1)L})\rangle\,. \end{aligned}$$

$O_{\mathrm{UP}.i}$ can be implemented by making one query to F_i. Then $O_{\mathsf{LR}''_2}$ can be implemented as follows by using $O_{\mathrm{UP}.1}$ and $O_{\mathrm{UP}.2}$:

1. Take $|x\rangle\,|y\rangle = |x_{0L}, x_{0R}\rangle\,|y_L, y_R\rangle$ as an input.
2. Compute the state (x_{1L}, x_{1R}) by querying $|x_{0L}, x_{0R}\rangle\,|0^n\rangle$ to $O_{\mathrm{Up}.1}$, and obtain
$$|x_{0L}, x_{0R}\rangle\,|y_L, y_R\rangle \otimes |x_{1L}, x_{1R}\rangle\,.$$
3. Query $|x_{1L}, x_{1R}\rangle\,|y_L, y_R\rangle$ to $O_{\mathrm{UP}.2}$, and obtain
$$|x\rangle\,|y \oplus \mathsf{LR}''_2(x)\rangle \otimes |x_{1L}, x_{1R}\rangle\,.$$
4. Uncompute Step 2 to obtain
$$|x\rangle\,|y \oplus \mathsf{LR}''_2(x)\rangle\,.$$
5. Return $|x\rangle\,|y \oplus \mathsf{LR}''_2(x)\rangle$.

Quantum oracle of RF'. The quantum oracle of RF' is implemented in the same way as LR_2'', except that the second round state update oracle $O_{\mathrm{UP}.2}$ is replaced with another oracle $O'_{\mathrm{UP}.2}$ defined as

$$\begin{aligned} O'_{\mathrm{UP}.2} : &|x_{0R}, x_{1L}, x_{1R}\rangle |y_L, y_R\rangle \\ &\mapsto |x_{0R}, x_{1L}, x_{1R}\rangle |(y_L, y_R) \oplus (F'_2(x_{1L}, x_{1R}, x_{0R}), x_{1L})\rangle . \end{aligned}$$

In what follows, we consider that the oracles of F_1, F_2, and F'_2 are implemented with the recording standard oracle with errors, and we use D_1, D_2, and D'_2 to denote (valid) databases for F_1, F_2, and F'_2, respectively.

Good and bad databases for LR_2''. Here we introduce the notion of *good* and *bad* for each tuple (D_1, D_2) of valid database for LR_2''. We say that a valid database D_2 is *without overlap* if each pair of distinct entries (x_{1L}, x_{1R}, β) and $(x'_{1L}, x'_{1R}, \beta')$ in D_2 satisfies $x_{1L} \neq x'_{1L}$. We say that (D_1, D_2) is good if D_2 is without overlap, and for each entry $(x_{1L}, x_{1R}, \beta) \in D_2$, there exists exactly one entry $(x_{0L}, x_{0R}, \alpha) \in D_1$ such that $\alpha = x_{1L}$ and $x_{1R} = x_{0L}$. We say that (D_1, D_2) is bad if it is not good.

Good and bad databases for RF'. Next, we introduce the notion of *good* and *bad* for each tuple (D_1, D'_2) of valid database for RF'. In addition, we say that a valid database D'_2 is *without overlap* if each pair of distinct entries $(x_{1L}, x_{1R}, x_{0R}, \beta)$ and $(x'_{1L}, x'_{1R}, x'_{0R}, \beta')$ in D'_2 satisfies $x_{1L} \neq x'_{1L}$. We say that (D_1, D'_2) is good if D'_2 is without overlap, and for each entry $(x_{1L}, x_{1R}, x_{0R}, \beta) \in D'_2$, there exists exactly one entry $(x_{0L}, x_{0R}, \alpha) \in D_1$ such that $\alpha = x_{1L}$ and $x_{1R} = x_{0L}$. We say that (D_1, D'_2) is bad if it is not good.

In addition, we say that a valid database D'_2 for F'_2 is *normal* if $D'_2(x_{1L}, x_{1R}, x_{0R}) \neq \bot$, then $D'_2(x'_{1L}, x_{1R}, x_{0R}) = \bot$ for all $x'_{1L} \neq x_{1L}$. Note that, for each good database (D_1, D'_2) for RF', D'_2 becomes normal by definition.

Compatibility of D'_2 with D_2. Let D'_2 be a valid and normal database for F'_2 without overlap and D_2 be a valid database for F_2 without overlap. We say that D'_2 is compatible with D_2 if the following conditions are satisfied:

1. If $(x_{1L}, x_{1R}, x_{0R}, \beta) \in D'_2$, then $(x_{1L}, x_{1R}, \beta) \in D_2$.
2. If $(x_{1L}, x_{1R}, \beta) \in D_2$, there is a unique x_{0R} such that $(x_{1L}, x_{1R}, x_{0R}, \beta) \in D'_2$.

For each valid and normal D'_2 for F'_2 without overlap, a unique valid database for F_2 without overlap exists, which we denote by $[D'_2]_2$.

Remark 2. For each good database (D_1, D_2) for LR_2'', a unique D'_2 without overlap exists such that $[D'_2]_2 = D_2$ and (D_1, D'_2) is a good database for RF', by the definition of good databases. Similarly, for each good database (D_1, D'_2) for RF', $(D_1, [D'_2]_2)$ becomes a good database for LR_2''. That is, there exists a one-to-one correspondence between good databases for LR_2'' and those for RF'.

The following lemma shows that the behavior of $O'_{\mathrm{UP}.2}$ on a valid and normal databases D'_2 for F'_2 without overlap is the same as that of $O_{\mathrm{UP}.2}$ on the corresponding database $[D'_2]_2$ for F_2.

Lemma 2. *It holds that*

$$\begin{aligned}&\langle \tilde{x}_{0R}, \tilde{x}_{1L}, \tilde{x}_{1R}, \tilde{y}_L, \tilde{y}_R| \otimes \langle \tilde{D}'_2|\, O'_{\mathrm{UP}.2}\, |x_{0R}, x_{1L}, x_{1R}, y_L, y_R\rangle \otimes |D'_2\rangle \\ &= \langle \tilde{x}_{0R}, \tilde{x}_{1L}, \tilde{x}_{1R}, \tilde{y}_L, \tilde{y}_R| \otimes \langle [\tilde{D}'_2]_2|\, O_{\mathrm{UP}.2}\, |x_{0R}, x_{1L}, x_{1R}, y_L, y_R\rangle \otimes |[D'_2]_2\rangle\end{aligned}$$

for any $x_{0R}, x_{1L}, x_{1R}, y_L, y_R, \tilde{x}_{0R}, \tilde{x}_{1L}, \tilde{x}_{1R}, \tilde{y}_L, \tilde{y}_R \in \{0,1\}^{n/2}$ and any valid and normal databases D'_2 and $\tilde{D}'_2$ for F'_2 without overlap.

We omit to write the proof because the lemma can be shown in the same way as we showed Lemma 1.

Let $|\psi_j\rangle$ and $|\psi'_j\rangle$ be the joint quantum states of the adversary $\mathcal{A}$ and the oracle just before making the j-th query when $\mathcal{A}$ runs relative to LR''_2 and RF', respectively. In addition, by $|\psi_{q+1}\rangle$ and $|\psi'_{q+1}\rangle$ we similarly denote the states just before the final measurement, by abuse of notation. Then the following proposition holds.

Proposition 7. *For each $j = 1, \ldots, q+1$, there exist vectors $|\psi_j^{\mathsf{good}}\rangle$, $|\psi_j^{\mathsf{bad}}\rangle$, $|\psi_j^{'\mathsf{good}}\rangle$, $|\psi_j^{'\mathsf{bad}}\rangle$, and complex number $a^{(j)}_{x,y,z,D_1,D'_2}$ such that*

$$\begin{aligned}|\psi_j\rangle = |\psi_j^{\mathsf{good}}\rangle + |\psi_j^{\mathsf{bad}}\rangle, &\quad |\psi'_j\rangle = |\psi_j^{'\mathsf{good}}\rangle + |\psi_j^{'\mathsf{bad}}\rangle,\\ |\psi_j^{\mathsf{good}}\rangle = &\sum_{\substack{x,y,z,D_1,D'_2\\ (D_1,D'_2)\,:\,good}} a^{(j)}_{x,y,z,D_1,D'_2}\, |x,y,z\rangle \otimes |D_1, [D'_2]_2\rangle,\\ |\psi_j^{'\mathsf{good}}\rangle = &\sum_{\substack{x,y,z,D_1,D'_2\\ (D_1,D'_2)\,:\,good}} a^{(j)}_{x,y,z,D_1,D'_2}\, |x,y,z\rangle\, |x,y,z\rangle \otimes |D_1, D'_2\rangle,\end{aligned}$$

the vector $|D_1, D'_2\rangle$ in $|\psi_j^{'\mathsf{good}}\rangle$ (resp., $|D_1, [D'_2]_2\rangle$ in $|\psi_j^{\mathsf{good}}\rangle$) has non-zero quantum amplitude only if $|D_1| \leq 2(j-1)$ and $|D'_2| \leq j-1$, and

$$\|\,|\psi_j^{\mathsf{bad}}\rangle\,\| \leq \left\||\psi_{j-1}^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \quad \|\,|\psi_j^{'\mathsf{bad}}\rangle\,\| \leq \left\||\psi_{j-1}^{'\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right),$$

hold (we set $|\psi_0^{\mathsf{bad}}\rangle = 0$ and $|\psi_0^{'\mathsf{bad}}\rangle = 0$).

The proposition can be shown in a similar way as we showed Proposition 5, and thus we omit to write the entire proof. Since here only two random functions are involved in each oracle while three random functions are involved in each oracle in Proposition 5, the proof becomes simpler: When we prove Proposition 7, we can skip to show the claims that correspond to those for the actions of $O_{\mathrm{UP}.2}$ in the proof of Proposition 5.

Now we can show that $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}''_2,\mathsf{RF}'}(\mathcal{A}) \leq O\left(\sqrt{q^3/2^{n/2}}\right)$ follows from Proposition 7 in the same way as we showed that Proposition 4 follows from Proposition 5. Therefore Proposition 6 holds.

4.3 Proof of Theorem 3

This subsection finishes our proof of Theorem 3, by using the results given in Sections 4.1 and 4.2.

Proof (of Theorem 3). First, let us modify LR_4 in such a way that the state updates of the third and fourth rounds are replaced with $(x_{2L}, x_{2R}) \mapsto (x_{3L}, x_{3R}) := (F(x_{2L}, x_{2R}), x_{2L})$ and $(x_{3L}, x_{3R}) \mapsto (x_{4L}, x_{4R}) := (F'(x_{3L}, x_{3R}), x_{3L})$, respectively, where $F, F' : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ are random functions. Let us denote the modified function by LR_4''. In addition, let LR_4''' be the composition of LR_2 with a random function $\mathsf{RF} : \{0,1\}^n \to \{0,1\}^n$ (see Fig. 9).

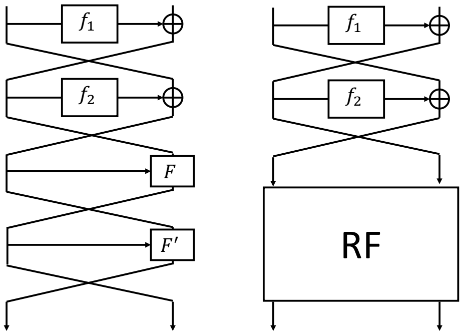

Fig. 9. LR_4'' and LR_4'''.

Then, by applying Proposition 4 twice, we can show that

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4,\mathsf{LR}_4''}(q) \leq O\left(\sqrt{\frac{q^3}{2^{n/2}}}\right) \tag{82}$$

holds. In addition,

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4'',\mathsf{LR}_4'''}(q) \leq O\left(\sqrt{\frac{q^3}{2^{n/2}}}\right) \tag{83}$$

follows from Proposition 6, and

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4''',\mathsf{RF}}(q) = 0 \tag{84}$$

holds since LR_2 is a permutation.

From Proposition 1, (82), (83), (84) we have

$$\begin{aligned}
&\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4,\mathsf{RP}}(q) \\
&\quad \leq \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4,\mathsf{LR}_4''}(q) + \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4'',\mathsf{LR}_4'''}(q) + \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4''',\mathsf{RF}}(q) + \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{RF},\mathsf{RP}}(q) \\
&\quad \leq O\left(\sqrt{\frac{q^3}{2^{n/2}}}\right),
\end{aligned}$$

which completes the proof of the theorem. □

5 Matching Upper Bound

Here we show that the query lower bound derived from Theorem 3 is tight by showing the matching upper bound. Again, we consider the case that all round functions of LR_4 are truly random functions, and show the following theorem.

Theorem 4. *A quantum algorithm $\mathcal{A}$ exists that makes $O(2^{n/6})$ quantum queries and satisfies $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathsf{LR}_4}(\mathcal{A}) = \Omega(1)$.*

Proof intuition. Intuitively, our distinguishing attack is just a quantum version of a classical collision-finding-based distinguishing attack [29]. A classical attack distinguishes LR_4 from a random permutation by finding a collision of a function that takes values in $\{0,1\}^{n/2}$, which requires $O(\sqrt{2^{n/2}}) = O(2^{n/4})$ queries in the quantum setting. However, finding a collision of the function requires only $O(\sqrt[3]{2^{n/2}}) = O(2^{n/6})$ queries in the quantum setting, which enables us to build a $O(2^{n/6})$-query quantum distinguisher. (Note that we can generally find a collision of random functions from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$ with $O(\sqrt[3]{2^{n/2}}) = O(2^{n/6})$ quantum queries [36].)

5.1 Proof of Theorem 4

First, we describe an overview of a classical attack [29]. Let us denote the composition of two independent random functions from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$ by $\mathsf{RF} \circ \mathsf{RF}$.

An overview of a classical attack. Suppose that we are given an oracle access to O, which is either the 4-round Luby-Rackoff construction LR_4 or a random permutation from $\{0,1\}^n$ to $\{0,1\}^n$. Let us define a function $G^O : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ that depends on O by

$$G^O(x) := \left(O(0^{n/2}, x)\right)_R \oplus x, \tag{85}$$

where $\left(O(0^{n/2}, x)\right)_R$ is the right half $n/2$ bits of $O(0^{n/2}, x)$. We can implement G^O by making $O(1)$ queries.

When O is the 4-round Luby-Rackoff construction LR_4, we have that $G^O(x) = f_3(f_2(x \oplus f_1(0^{n/2}))) \oplus f_1(0^{n/2})$ holds. Thus, if all round functions of LR_4 are truly random functions, the function distribution of G^O will be the same as that of the composition of two independent random functions $\mathsf{RF} \circ \mathsf{RF}$. On the other hand, when O is a random permutation from $\{0,1\}^n$ to $\{0,1\}^n$, the function distribution of G^O will be almost the same as that of the truly random function RF from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$.

Since $\mathsf{RF} \circ \mathsf{RF}$ has twice as many collisions as RF, we can distinguish LR_4 from a truly random permutation by making $O((2^{n/2})^{1/2}) = O(2^{n/4})$ queries to G^O.

Conversion of the classical attack to a quantum attack. Next, we explain how to convert the classical attack above into a quantum attack that makes $O(2^{n/6})$ quantum queries and prove Theorem 4. The following lemma is crucial. It shows that we can distinguish $\mathsf{RF} \circ \mathsf{RF}$ from RF by making $O((2^{n/2})^{1/3}) = O(2^{n/6})$ quantum queries.

Lemma 3. *Let us denote the composition of two independent random functions from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$ by $\mathsf{RF} \circ \mathsf{RF}$. Then, a quantum algorithm $\mathcal{B}$ exists that makes $O(2^{n/6})$ quantum queries and satisfies $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{B}) = \Omega(1)$. That is, an algorithm exists that distinguishes $\mathsf{RF} \circ \mathsf{RF}$ from a random function with a constant probability, by making $O(2^{n/6})$ quantum queries.*

Proof. We use the following fact that is shown by Ambainis [2].

Fact 1 (Theorem 3 in [2]). *Let X and Y be finite sets, and $F : X \to Y$ be a function. Then there is a quantum algorithm that judges if distinct elements $x_1, x_2 \in X$ exist such that $F(x_1) = F(x_2)$ with bounded error by making $O(|X|^{2/3})$ quantum queries to F.*

Let $[N] \subset \{0,1\}^{n/2}$ denote the subset $\{0,1,\dots,N-1\}$ for each integer $1 \leq N \leq 2^{n/2}$. By using the above fact, we can deduce that for $1 \leq N \leq 2^{n/2}$ a quantum algorithm $\mathcal{D}_N$ exists such that, given oracle access to a function $F : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$, it outputs 1 if distinct elements $x_1, x_2 \in [N]$ exist such that $F(x_1) = F(x_2)$, and it outputs 0 otherwise, with an error that is smaller than $1/30$, by making $O(|N|^{2/3})$ quantum queries. (We can make such $\mathcal{D}_N$ by iteratively running Ambainis' algorithm $O(1)$ times for $F|_{[N]} : [N] \to \{0,1\}^{n/2}$, which is the restriction of F to $[N]$.)

Here we give an analysis of the qPRF advantage of $\mathcal{D}_N$ on $\mathsf{RF} \circ \mathsf{RF}$, for each N. For a function $F : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ and a subset $Z \in \{0,1\}^{n/2}$, let coll^F_Z denote the event that F has a collision in Z, i.e., there are distinct $x_1, x_2 \in Z$ such that $F(x_1) = F(x_2)$. Then, we have that

$$\begin{aligned}\Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right] &= \left(1 - \frac{1}{2^{n/2}}\right)\cdot\left(1 - \frac{2}{2^{n/2}}\right)\cdots\left(1 - \frac{N-1}{2^{n/2}}\right)\\ &= \prod_{j=1}^{N-1}\left(1 - \frac{j}{2^{n/2}}\right) \qquad (86)\end{aligned}$$

holds, where F is chosen from $\mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$ uniformly at random. In addition, when F_1 and F_2 are chosen from $\mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$ uniformly at random, we have that

$$\begin{aligned}\Pr_{F_1,F_2}\left[\neg\mathsf{coll}^{F_2\circ F_1}_{[N]}\right] &= \Pr_{F_2}\left[\neg\mathsf{coll}^{F_2}_{F_1([N])}\middle|\neg\mathsf{coll}^{F_1}_{[N]}\right]\cdot\Pr_{F_1}\left[\neg\mathsf{coll}^{F_1}_{[N]}\right]\\ &= \left(\Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right)^2. \qquad (87)\end{aligned}$$

Now we have that

$$\begin{aligned}\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{D}_N) &= \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{RF},\mathsf{RF}\circ\mathsf{RF}}(\mathcal{D}_N)\\ &= \left|\Pr_F\left[\mathcal{D}^F_N() \to 1\right] - \Pr_{F_1,F_2}\left[\mathcal{D}^{F_2\circ F_1}_N() \to 1\right]\right|\\ &\geq \left|\Pr_F\left[\mathsf{coll}^F_{[N]}\right] - \Pr_{F_1,F_2}\left[\mathsf{coll}^{F_2\circ F_1}_{[N]}\right]\right| - \frac{2}{30}, \qquad (88)\end{aligned}$$

where we used the property that the error of $\mathcal{D}_N$ is smaller than $1/30$. In addition, from (87), it follows that

$$\begin{aligned}
&\left|\Pr_F\left[\mathsf{coll}^F_{[N]}\right] - \Pr_{F_1,F_2}\left[\mathsf{coll}^{F_2\circ F_1}_{[N]}\right]\right| \\
&\quad = \Pr_{F_1,F_2}\left[\mathsf{coll}^{F_2\circ F_1}_{[N]}\right] - \Pr_F\left[\mathsf{coll}^F_{[N]}\right] \\
&\quad = \left(1 - \left(\Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right)^2\right) - \left(1 - \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right) \\
&\quad = \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\left(1 - \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right) \qquad (89)
\end{aligned}$$

holds. Therefore, we have that

$$\mathbf{Adv}^{\mathsf{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{D}_N) \geq \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\left(1 - \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right) - \frac{2}{30} \qquad (90)$$

holds. Now we show the following claim.

Claim. There exists a parameter N_0 that is in $O(2^{n/4})$, and

$$\frac{3}{5} \geq \prod_{j=1}^{N_0-1}\left(1 - \frac{j}{2^{n/2}}\right) \geq \frac{1}{5} \qquad (91)$$

holds for sufficiently large n.

Proof. First, let us denote $p_N := \prod_{j=1}^{N-1}\left(1 - \frac{j}{2^{n/2}}\right)$. For each $1 \leq N \leq 2^{n/2}$, we have that

$$\begin{aligned}
\prod_{j=1}^{N-1}\left(1 - \frac{j}{2^{n/2}}\right) &\geq \left(1 - \frac{N}{2^{n/2}}\right)^N \\
&= \left(\left(1 - \frac{N}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N}}\right)^{-\frac{N^2}{2^{n/2}}} \qquad (92)
\end{aligned}$$

holds. In addition,

$$\prod_{j=1}^{N-1}\left(1 - \frac{j}{2^{n/2}}\right) \leq \prod_{j=1}^{N-1}\left(e^{-\frac{j}{2^{n/2}}}\right) = e^{-\frac{N(N-1)}{2\cdot 2^{n/2}}} \qquad (93)$$

holds. Thus

$$e^{-\frac{N(N-1)}{2\cdot 2^{n/2}}} \geq p_N \geq \left(\left(1 - \frac{N}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N}}\right)^{-\frac{N^2}{2^{n/2}}} \qquad (94)$$

holds.

Next, let us put $N_0 := 2^{n/4} \cdot \sqrt{2\log 2}$. Then

$$e^{-\frac{N_0(N_0-1)}{2\cdot 2^{n/2}}} = e^{-\frac{N_0\cdot N_0}{2\cdot 2^{n/2}}} + \left(e^{-\frac{N_0(N_0-1)}{2\cdot 2^{n/2}}} - e^{-\frac{N_0\cdot N_0}{2\cdot 2^{n/2}}}\right)$$
$$= \frac{1}{2} + \left(\left(\frac{1}{2}\right)^{\frac{N_0-1}{N_0}} - \frac{1}{2}\right) \tag{95}$$

holds, and thus $e^{-\frac{N_0(N_0-1)}{2\cdot 2^{n/2}}} \leq 3/5$ holds for sufficiently large n. In addition, since the function $f(x) = (1-x)^{-1/x}$ increases as x increases for $0 < x < 1$ and $\lim_{x\to+0} f(x) = e$ holds, we have that

$$\left(1 - \frac{N_0}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N_0}} \leq e + \frac{1}{10} \tag{96}$$

holds for sufficiently large n. Thus

$$\left(\left(1 - \frac{N_0}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N_0}}\right)^{-\frac{N_0^2}{2^{n/2}}} \geq \left(e + \frac{1}{10}\right)^{-\frac{N_0^2}{2^{n/2}}} = \left(e + \frac{1}{10}\right)^{-2\log 2} \geq \frac{1}{5} \tag{97}$$

holds for sufficiently large n.

Therefore, if we put $N_0 := 2^{n/4} \cdot \sqrt{2\log 2}$,

$$\frac{3}{5} \geq p_{N_0} \geq \frac{1}{5} \tag{98}$$

holds for sufficiently large n. Hence the claim follows. □

From the above claim and (86), a parameter N_0 exists that is in $O(2^{n/4})$, and

$$\frac{3}{5} \geq \Pr_F\left[\neg\mathsf{coll}^F_{[N_0]}\right] \geq \frac{1}{5} \tag{99}$$

holds for sufficiently large n. Hence, from (88) we have that

$$\mathbf{Adv}^{\mathsf{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{D}_{N_0}) \geq \frac{1}{5}\left(1 - \frac{3}{5}\right) - \frac{2}{30} = \frac{1}{75} \geq \Omega(1). \tag{100}$$

Therefore, if we put $\mathcal{B} := \mathcal{D}_{N_0}$, this $\mathcal{B}$ satisfies the claim of the lemma, since (100) holds and $\mathcal{D}_{N_0}$ makes at most $O((N_0)^{2/3}) = O((2^{n/4})^{2/3}) = O(2^{n/6})$ quantum queries. □

Next we show the following proposition.

Proposition 8. *A quantum algorithm $\mathcal{A}$ exists that makes $O(2^{n/6})$ quantum queries and satisfies $\mathbf{Adv}^{\mathsf{qPRF}}_{\mathsf{LR}_4}(\mathcal{A}) = \Omega(1)$.*

Proof. Suppose that we are given an oracle access to O, which is either the 4-round Luby-Rackoff construction LR_4 or a random function from $\{0,1\}^n$ to $\{0,1\}^n$. Recall that the function $G^O : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ is defined by

$$G^O(x) := \left(O(0^{n/2}, x)\right)_R \oplus x, \tag{101}$$

where $\left(O(0^{n/2}, x)\right)_R$ is the right half $n/2$ bits of $O(0^{n/2}, x)$. We can implement a quantum circuit that computes G^O by making $O(1)$ queries.[9]

Now we define a quantum algorithm $\mathcal{A}$ as the following three-step procedure.

1. Let $\mathcal{B}$ be the same algorithm as in Lemma 3.
2. Run $\mathcal{B}$ relative to G^O.
3. If $\mathcal{B}$ returns 1, output 1. If $\mathcal{B}$ returns 0, output 0.

Here we analyze $\mathcal{A}$. When O is the 4-round Luby-Rackoff construction LR_4, we have that $G^O(x) = f_3(f_2(x \oplus f_1(0^{n/2}))) \oplus f_1(0^{n/2})$ holds. Since we are considering the case that all round functions of LR_4 are truly random functions, the function distribution of G^O will be the same as that of $\mathsf{RF} \circ \mathsf{RF}$. On the other hand, when O is a random function from $\{0,1\}^n$ to $\{0,1\}^n$, the function distribution of G^O will be the same as that of the truly random function from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$. Thus, from Lemma 3 we have that

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{LR}_4}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{B}) = \Omega(1) \tag{102}$$

holds. In addition, since $\mathcal{B}$ makes at most $O(2^{n/6})$ quantum queries and G makes only $O(1)$ queries to O, $\mathcal{A}$ makes at most $O(2^{n/6})$ quantum queries. Therefore the claim of the proposition holds. □

Finally we prove Theorem 4.

Proof (of Theorem 4). Let $\mathcal{A}$ be the same algorithm as in Proposition 8. Then, from Proposition 8 it follows that

$$\begin{aligned}\mathbf{Adv}^{\mathrm{qPRP}}_{\mathsf{LR}_4}(\mathcal{A}) &\geq \mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{LR}_4}(\mathcal{A}) - \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{RP},\mathsf{RF}}(\mathcal{A}) \\ &\geq \Omega(1) - O(1/2^{n/2}) = \Omega(1),\end{aligned} \tag{103}$$

where we used the fact that, for any quantum adversary $\mathcal{A}'$ that makes at most q queries, the distinguishing advantage $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{RP},\mathsf{RF}}(\mathcal{A}')$ is upper bounded by $O(q^3/2^n)$ for a random function and a random permutation from $\{0,1\}^n$ to $\{0,1\}^n$ (see Proposition 1). Thus the claim of the theorem holds. □

6 Concluding Remarks

In this paper, we showed that $\Omega(2^{n/6})$ quantum queries are required to distinguish the (n-bit block) 4-round Luby-Rackoff construction from a random permutation by qCPAs. In particular, the 4-round Luby-Rackoff construction becomes a quantumly secure PRP against qCPAs if round functions are quantumly secure PRFs. We also gave a qCPA that distinguishes the 4-round Luby-Rackoff construction from a random permutation with $O(2^{n/6})$ quantum queries and showed that $\Theta(2^{n/6})$ is the tight bound. To give security proofs, we gave an alternative formalization of the compressed oracle technique by Zhandry and applied it. We believe that our alternative formalization and analyses

[9] Here we have to truncate O's outputs by using a technique observed in [17].

for its behavior help us understanding Zhandry's technique better, which will lead to the technique begin applied even more widely.

An important future work is to see if the provable security bound improves when we increase the number of rounds. Also, analyzing the security of the Luby-Rackoff constructions against *qCCAs* is left as an interesting open question. It would be a challenging problem since we have to treat inverse (decryption) queries to quantum oracles. Oracles that allow inverse quantum queries are usually much harder to deal with than the ones that allow only forward quantum queries, and some other new techniques would be required for the analysis.

Acknowledgments

The authors thank Qipeng Liu and anonymous reviewers for pointing out an issue of Proposition 6 in a previous version of this paper. The second author was supported in part by JSPS KAKENHI Grant Number JP20K11675.

References

1. Alagic, G., Russell, A.: Quantum-secure symmetric-key cryptography based on hidden shifts. In: EUROCRYPT 2017, Proceedings, Part III. LNCS, vol. 11693, pp. 65–93. Springer (2017)
2. Ambainis, A.: Quantum walk algorithm for element distinctness. SIAM J. Comput. **37**(1), 210–239 (2007)
3. Anand, M.V., Targhi, E.E., Tabia, G.N., Unruh, D.: Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In: PQCrypto 2016, Proceedings. LNCS, vol. 11505, pp. 44–63. Springer (2016)
4. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: Camellia: A 128-bit block cipher suitable for multiple platforms - design and analysis. In: SAC 2000, Proceedings. LNCS, vol. 2012, pp. 39–56. Springer (2000)
5. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: ASIACRYPT 2011, Proceedings. LNCS, vol. 7073, pp. 41–69. Springer (2011)
6. Boneh, D., Zhandry, M.: Quantum-secure message authentication codes. In: EUROCRYPT 2013, Proceedings. LNCS, vol. 7881, pp. 592–608. Springer (2013)
7. Bonnetain, X.: Quantum key-recovery on full AEZ. In: SAC 2017, Proceedings. LNCS, vol. 10719, pp. 394–406. Springer (2017)
8. Bonnetain, X., Naya-Plasencia, M.: Hidden shift quantum cryptanalysis and implications. In: ASIACRYPT 2018, Proceedings, Part I. LNCS, vol. 11272, pp. 560–592. Springer (2018)
9. Bonnetain, X., Naya-Plasencia, M., Schrottenloher, A.: On quantum slide attacks, Appeared at SAC 2019
10. Czajkowski, J., Bruinderink, L.G., Hülsing, A., Schaffner, C., Unruh, D.: Post-quantum security of the sponge construction. In: PQCrypto 2018, Proceedings. LNCS, vol. 11505, pp. 185–204. Springer (2018)
11. Czajkowski, J., Majenz, C., Schaffner, C., Zur, S.: Quantum lazy sampling and game-playing proofs for quantum indifferentiability. IACR Cryptology ePrint Archive **2019**, 428 (2019)
12. Dong, X., Dong, B., Wang, X.: Quantum attacks on some Feistel block ciphers. IACR Cryptology ePrint Archive **2018**, 504 (2018)

13. Dong, X., Li, Z., Wang, X.: Quantum cryptanalysis on some generalized feistel schemes. SCIENCE CHINA Information Sciences **62**(2), 22501:1–22501:12 (2019)
14. Dong, X., Wang, X.: Quantum key-recovery attack on Feistel structures. SCIENCE CHINA Information Sciences **61**(10), 102501:1–102501:7 (2018)
15. Hosoyamada, A., Iwata, T.: 4-round Luby-Rackoff construction is a qPRP. In: ASIACRYPT 2019, Proceedings, Part I. LNCS, vol. 11921, pp. 145–174. Springer (2019)
16. Hosoyamada, A., Iwata, T.: 4-round Luby-Rackoff construction is a qPRP. Cryptology ePrint Archive, Report 2019/243 (2019), version 20190913:015401
17. Hosoyamada, A., Sasaki, Y.: Quantum Demiric-Selçuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions. In: SCN 2018, Proceedings. LNCS, vol. 11035, pp. 386–403. Springer (2018)
18. Hosoyamada, A., Yasuda, K.: Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In: ASIACRYPT 2018, Proceedings, Part I. LNCS, vol. 11272, pp. 275–304. Springer (2018)
19. Ito, G., Hosoyamada, A., Matsumoto, R., Sasaki, Y., Iwata, T.: Quantum chosen-ciphertext attacks against feistel ciphers. In: CT-RSA 2019, Proceedings. LNCS, vol. 11405, pp. 391–411. Springer (2019)
20. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: CRYPTO 2016, Proceedings, Part II. LNCS, vol. 11693, pp. 207–237. Springer (2016)
21. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: ISIT 2010, Proceedings. pp. 2682–2685. IEEE (2010)
22. Kuwakado, H., Morii, M.: Security on the quantum-type Even-Mansour cipher. In: ISITA 2012, Proceedings. pp. 312–316. IEEE (2012)
23. Liu, Q., Zhandry, M.: On finding quantum multi-collisions. In: EUROCRYPT 2019, Proceedings, Part III. LNCS, vol. 11478, pp. 189–218. Springer (2019)
24. Luby, M., Rackoff, C.: How to construct pseudo-random permutations from pseudo-random functions (abstract). In: CRYPTO '85, Proceedings. LNCS, vol. 218, p. 447. Springer (1985)
25. Mennink, B., Szepieniec, A.: XOR of PRPs in a quantum world. In: PQCrypto 2017, Proceedings. LNCS, vol. 10346, pp. 367–383. Springer (2017)
26. National Bureau of Standards: Data encryption standard. FIPS 46 (January 1977)
27. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition (2010)
28. NIST: Announcing request for nominations for public-key post-quantum cryptographic algorithms. National Institute of Standards and Technology (2016)
29. Patarin, J.: New results on pseudorandom permutation generators based on the DES scheme. In: CRYPTO '91, Proceedings. LNCS, vol. 576, pp. 301–312. Springer (1991)
30. Santoli, T., Schaffner, C.: Using Simon's algorithm to attack symmetric-key cryptographic primitives. Quantum Information & Computation **17**(1&2), 65–78 (2017)
31. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: FOCS 1994, Proceedings. pp. 124–134. IEEE (1994)
32. Simon, D.R.: On the power of quantum computation. SIAM J. Comput. **26**(5), 1474–1483 (1997)
33. Song, F., Yun, A.: Quantum security of NMAC and related constructions - PRF domain extension against quantum attacks. In: CRYPTO 2017, Proceedings, Part II. LNCS, vol. 10402, pp. 283–309. Springer (2017)
34. Zhandry, M.: How to construct quantum random functions. In: FOCS 2012, Proceedings. pp. 679–687. IEEE (2012)
35. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: CRYPTO 2012, Proceedings. LNCS, vol. 7417, pp. 758–775. Springer (2012)

36. Zhandry, M.: A note on the quantum collision and set equality problems. Quantum Information & Computation **15**(7&8), 557–567 (2015)
37. Zhandry, M.: A note on quantum-secure PRPs. IACR Cryptology ePrint Archive **2016**, 1076 (2016)
38. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. Cryptology ePrint Archive, Report 2018/276 (2018), version 20180814:183812
39. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. In: CRYPTO 2019, Proceedings, Part II. LNCS, vol. 11693, pp. 239–268. Springer (2019)

A On the Technical Error in the Preliminary Version

The previous version [15,16] contained an error in the proof to upper bound the norms of bad vectors (which corresponds to the proof for (42) of Proposition 5 in this version).

Roughly speaking, the previous version set $|\psi_j^{\mathsf{good}}\rangle := \Pi_{\mathsf{good}}\Pi_{\mathsf{reg}} O_{\mathsf{LR}_3} |\psi_{j-1}^{\mathsf{good}}\rangle$ for each j and claimed that $\|\Pi_{\mathsf{irreg}\vee\mathsf{bad}} O_{\mathsf{LR}_3} |\psi_{j-1}^{\mathsf{good}}\rangle\| \leq O(\sqrt{j/2^{n/2}})$ holds (instead of claiming (42) in the current version), where $\Pi_{\mathsf{irreg}\vee\mathsf{bad}}$ is the projection onto the space spanned by the vectors that contain *irregular states or* bad databases, i.e., $\Pi_{\mathsf{irreg}\vee\mathsf{bad}} = I - \Pi_{\mathsf{good}}\Pi_{\mathsf{reg}}$. Here, a vector is called irregular if it is not regular.[10] To prove the upper bound $\|\Pi_{\mathsf{irreg}\vee\mathsf{bad}} O_{\mathsf{LR}_3} |\psi_j^{\mathsf{good}}\rangle\| \leq O(\sqrt{j/2^{n/2}})$, the previous version first decomposed the vector $|\psi_j^{\mathsf{good}}\rangle$ on an orthonormal system S and proved $\|\Pi_{\mathsf{irreg}\vee\mathsf{bad}} O_{\mathsf{LR}_3} |\phi\rangle\| \leq O(\sqrt{j/2^{n/2}})$ for all $|\phi\rangle \in S$ such that $\langle\phi|\psi_j^{\mathsf{good}}\rangle \neq 0$. However, this does not immediately imply $\|\Pi_{\mathsf{irreg}\vee\mathsf{bad}} O_{\mathsf{LR}_3} |\psi_j^{\mathsf{good}}\rangle\| \leq O(\sqrt{j/2^{n/2}})$.

It turns out that the norm of the irregular component of $O_{\mathsf{LR}_3} |\psi_j^{\mathsf{good}}\rangle$ (which we denote $\Pi_{\mathsf{irreg}} O_{\mathsf{LR}_3} |\psi_j^{\mathsf{good}}\rangle$) may be much larger than $\sqrt{j/2^{n/2}}$, and in fact we do not have to care about the norm of the irregular component of $\Pi_{\mathsf{irreg}} O_{\mathsf{LR}_3} |\psi_j^{\mathsf{good}}\rangle$ to prove the indistinguishability of O_{LR_3} and $O_{\mathsf{LR}'_3}$.

Hence we changed the proof strategy in Section 4.1. In particular, this version does not use additional oracles $O_{\mathsf{LR}_3\text{-det}}$ and $O_{\mathsf{LR}'_3\text{-det}}$ that are used in the previous version. By removing $O_{\mathsf{LR}_3\text{-det}}$ and $O_{\mathsf{LR}'_3\text{-det}}$ the proof strategy has become simpler.

[10] To be more precise, the previous version used the notation Π_{bad} instead of $\Pi_{\mathsf{bad}\vee\mathsf{irreg}}$.