

# 4-Round Luby-Rackoff Construction is a qPRP

Akinori Hosoyamada<sup>1,2</sup> and Tetsu Iwata<sup>2</sup>

<sup>1</sup> NTT Secure Platform Laboratories, Tokyo, Japan,  
hosoyamada.akinori@lab.ntt.co.jp

<sup>2</sup> 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, a recent work by 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, it has been a problem of much interest how many rounds are sufficient to achieve the provable security against quantum query attacks. This paper shows the answer to 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  $O(2^{n/12})$  quantum queries. We also give a query upper bound for the problem of distinguishing the 4-round Luby-Rackoff construction from a random permutation by showing a distinguishing qCPA with  $O(2^{n/6})$  quantum queries. Our result is the first one that shows 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 active research areas in cryptography research community since Shor developed the polynomial-time integer factoring quantum algorithm [30]. NIST is working on a standardization process for post-quantum public-key schemes such as public-key encryption, key-establishment, and digital signature schemes [27].

On the other hand, for symmetric key cryptography, it has been 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 of them are also broken in polynomial time by using Simon’s algorithm [31] if quantum adversaries have access to quantum circuits that implement keyed primitives [18,20,9,7,21,29,14,13,12,17], though they are proven or assumed to be secure in the classical setting. Now it is also important to study post-quantum security of symmetric-key schemes.

While many quantum query attacks on symmetric-key schemes have been proposed, the development on post-quantum provable security of symmetric-key schemes is limited. There are two possible post-quantum security notions for symmetric-key schemes: *standard security* and *quantum security* [33]. The standard security is the one that assumes adversaries have quantum computers, but have access to keyed oracles in a classical manner. On the other hand, the quantum security is the one that 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 popular ones such as DES [25] and Camellia [4] were designed based on this construction.

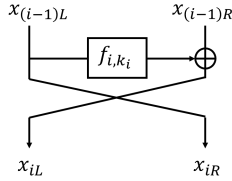
For families of functions  $f_i := \{f_{i,k} : \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2}\}_{k \in \mathcal{K}}$  that are parameterized by  $k$  in a key space  $\mathcal{K}$  ( $1 \leq i \leq r$ ), the  $r$ -round Luby-Rackoff construction  $\text{LR}_r(f_1, \dots, f_r)$  is defined as follows: First, keys  $k_1, \dots, k_r$  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

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

for  $i = 1, \dots, r$  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  $(\mathcal{K})^r$ .

In the classical setting, if each  $f_i$  is a secure PRF,  $\text{LR}_r$  becomes a secure PRP against chosen-plaintext attacks (CPAs) for  $r \geq 3$  and a secure PRP against chosen-ciphertext attacks (CCAs) for  $r \geq 4$  [23], i.e.,  $\text{LR}_r$  becomes a strong PRP. However, in the quantum setting, Kuwakado and Morii showed that  $\text{LR}_3$  can be distinguished in polynomial time from a truly random permutation by a quantum superposed chosen-plaintext attack [20] (qCPA).<sup>3</sup> Moreover, the

<sup>3</sup> Strictly speaking, the attack by Kuwakado and Morii works only for the case that all round functions are keyed permutations. Kaplan et al. [18] showed that the attack works for more general cases.



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

recent work by Ito et al. showed that  $\text{LR}_4$  can be distinguished in polynomial time by a quantum superposed chosen-ciphertext attack (qCCA) [17]. On the other hand, for any  $r$ , no post-quantum security proof of  $\text{LR}_r$  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  $r$  so that we can prove the post-quantum security of  $\text{LR}_r$ .

### 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  $\text{LR}_4$  is secure against qCPAs. In particular, we give a security bound of  $\text{LR}_4$  against qCPAs in the case that all round functions are truly random functions. We also give a query upper bound for the problem of distinguishing  $\text{LR}_4$  from a random permutation by showing a distinguishing attack. Concretely, we show the following theorems (see Table 1 for comparison of security proofs and attacks for  $\text{LR}_4$ ).

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

1.  $\text{LR}_4$  cannot be distinguished from a truly random permutation by qCPAs up to  $O(2^{n/12})$  quantum queries.
2. There exists a quantum algorithm that distinguishes  $\text{LR}_4$  from a truly random permutation with a constant probability by making  $O(2^{n/6})$  quantum chosen-plaintext queries.

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

**Technical details.** To give a quantum security proof for  $\text{LR}_4$  in the case that all round functions are truly random, we use the *compressed oracle technique* developed by Zhandry [37]. To be precise, we give an alternative formalization of the technique and use it.

Attack setting	Classical CPA	Classical CCA	Quantum CPA	Quantum CCA
Security proof	Secure up to $O(2^{n/4})$ queries [23]	Secure up to $O(2^{n/4})$ queries [23]	Secure up to $O(2^{n/12})$ queries [Ours] (Section 4)	No proofs (Insecure)
Distinguishing attack	$O(2^{n/4})$ queries [28]	$O(2^{n/4})$ queries [28]	$O(2^{n/6})$ queries [Ours] (Section 5)	$O(n)$ queries [17]

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

One of the challenging obstacles to give security proofs against quantum superposed query adversaries is that we cannot record *transcripts* of quantum queries and answers. While it is trivial that we can 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.

Zhandry’s compressed oracle technique enables us to overcome the obstacle in the case when oracles are truly random functions. The technique is so powerful that it can be used to show quantum indistinguishability of the Merkle-Damgård domain extender and quantum security for the Fujisaki-Okamoto transformation [37], in addition to the (tight) lower bounds for the multicollision-finding problems [22]. 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, while we see that the formalization of the technique is (necessarily) somewhat complex. It would be better that we have a simpler alternative formalization 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 of recording transcripts and compressing recorded data. The compression is necessary for efficient simulation of random functions, but we do not need it 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 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 *errors*. 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 errors. We believe that our alternative formalization and analyses for our oracle’s behavior help us understand Zhandry’s technique better, which would lead to even wider applications of the technique. See Section 3 for details on our alternative formalizaion.

By making heavy use of our recording standard oracle with errors, we complete the security proof of  $\text{LR}_4$  against quantum superposed query attacks, taking advantage of classical proof intuitions to some extent. First, we consider  $\text{LR}_3$ , the 3-round Luby-Rackoff construction, which is easy to be distinguished from a truly random permutation, and a slightly modified version of it, where the last-round state update of  $\text{LR}_3$  is modified. Our observation is that it seems hard even for quantum (chosen-plaintext) query adversaries to notice the modification, and we are actually able to show that this is indeed the case. Intuitively, the proof is possible since it is infeasible even for quantum query adversaries to produce collisions on the input of the third round. Second, we prove that a family of random permutations (i.e., a function  $P : \{0, 1\}^{n/2} \times \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  such that  $P(x, \cdot)$  is a truly random permutation over  $\{0, 1\}^{n/2}$  for each  $x$ ) is hard to distinguish from a truly random function. To show the first hardness result, we use our recording standard oracle with errors. On the other hand, for the second hardness result, we can show it by just combining some previous results. Once we prove these two hardness results, the rest of the proof can be done easily without any argument that is 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  $\text{LR}_4$ .

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

With respect to security proofs against quantum query adversaries for symmetric key schemes other than the ones we introduced above, there is a proof for standard modes of operations by Targhi et al. [3], one for the Carter-Wegman MACs by Boneh and Zhandry [6], one for NMAC by Song and Yun [32], and one for Davies-Meyer and Merkle-Damgård constructions by Hosoyamada and Yasuda [16]. Zhandry showed the PRP-PRF switching lemma in the quantum setting [35], and that quantum-secure PRPs can be constructed from quantum-secure PRFs by using a technique of format preserving encryption [36]. Czakowski 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].<sup>4</sup> Alagic and Russell proved that polynomial time attacks against symmetric-key schemes that make use of Simon’s algorithm can be prevented by replacing XOR operations with modular additions based on an algebraic hardness assumption [1], however,

<sup>4</sup> Note that the condition that the round function of the sponge construction is one-way is unusual in the context of classical symmetric-key provable security.

Bonnetain and Naya-Plasecia showed that the countermeasure is not practical [8]. Regarding standard security proofs (against quantum adversaries that make only classical queries) for symmetric-schemes, Mennink and Szepieniec proved security for XOR of PRPs [24]. Recently Czaikowski et al. [11] showed that the compressing technique can be extended to quantum oracles with non-uniform distributions such as a random permutation, and showed quantum indistinguishability of the sponge construction.

## 2 Preliminaries

This section describes notations and definitions. In this paper, any algorithm (or adversary) is supposed to be a quantum algorithm, and makes quantum superposed queries to oracles. For any finite sets  $X$  and  $Y$ , let  $\text{Func}(X, Y)$  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  $\{0, 1, \dots, 2^m - 1\}$ .

### 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 [26,19] for an introduction). We use the computational model of quantum circuits. We measure complexity of quantum algorithms by the number of queries, and the number of basic gates in addition to oracle gates. In this paper, by *basic gates* we denote the gates in the standard basis of quantum circuits  $\mathcal{Q}$  [19]. Let  $\|\cdot\|$  and  $\|\cdot\|_{\text{tr}}$  denote the norm of vectors and the trace norm of operators, respectively. In addition, let  $\text{td}(\cdot, \cdot)$  denote the trace distance. For Hermitian operators  $\rho, \sigma$  on a Hilbert space  $\mathcal{H}$ ,  $\text{td}(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_{\text{tr}}$  holds. For a mixed state  $\rho$  of a joint quantum system  $\mathcal{H}_A \otimes \mathcal{H}_B$ , let  $\text{tr}_B(\rho)$  (resp.,  $\text{tr}_A(\rho)$ ) denote the partial trace of  $\rho$  over  $\mathcal{H}_B$  (resp.,  $\mathcal{H}_A$ ). Moreover, for a pure state  $|\psi\rangle$  of the joint quantum system  $\mathcal{H}_A \otimes \mathcal{H}_B$ , we write  $\text{tr}_B(|\psi\rangle)$  (resp.,  $\text{tr}_A(|\psi\rangle)$ ) instead of  $\text{tr}_B(|\psi\rangle\langle\psi|)$  (resp.,  $\text{tr}_A(|\psi\rangle\langle\psi|)$ ), for simplicity. Similarly, for a pure state  $|\psi\rangle$  and a mixed state  $\rho$  of a quantum system  $\mathcal{H}$ , we write  $\text{td}(|\psi\rangle, \rho)$  and  $\text{td}(\rho, |\psi\rangle)$  instead of  $\text{td}(|\psi\rangle\langle\psi|, \rho)$  and  $\text{td}(\rho, |\psi\rangle\langle\psi|)$ , respectively. For an integer  $n \geq 1$ , by  $I_n$  and  $H^{\otimes n}$  we 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 short. 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  $\ell$ -qubit quantum system, for some integer  $\ell$ . 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 we 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 in a sequential order on the initial state  $|0^\ell\rangle$ . (We consider that  $O_f$  acts on the first  $(m+n)$ -qubits of  $\mathcal{A}$ 's quantum register.) Finally,  $\mathcal{A}$  measures the resulting quantum state  $U_q O_f U_{q-1} \cdots O_f U_0 |0^\ell\rangle$ , and returns the measurement result as the output.  $f$  may be chosen according to a distribution at the beginning of each game. Let us denote the event that  $\mathcal{A}$  runs relative to the oracle  $O_f$  and returns an output  $\alpha$  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 that quantum oracles are stateful, i.e., oracles have  $\ell'$ -qubit quantum states for an integer  $\ell' \geq 0$ .<sup>5</sup> In these cases, an oracle  $\mathcal{O}$  is modeled as a sequence of unitary operators  $(\mathcal{O}_1, \dots, \mathcal{O}_q)$  that acts on the first  $(m+n)$ -qubits of  $\mathcal{A}$ 's quantum register in addition to  $\mathcal{O}$ 's quantum register. When we run  $\mathcal{A}$  relative to the oracle  $\mathcal{O}$ , the unitary operators  $U_0 \otimes I_{\ell'}, \mathcal{O}_1, \dots, (U_{q-1} \otimes I_{\ell'}), \mathcal{O}_q, (U_q \otimes I_{\ell'})$  act in a sequential order on the initial state  $|0^\ell\rangle \otimes |\text{init}_{\mathcal{O}}\rangle$ , where  $|\text{init}_{\mathcal{O}}\rangle$  is the initial state of  $\mathcal{O}$ . Finally,  $\mathcal{A}$  measures the resulting quantum state  $(U_q \otimes I_{\ell'}) \mathcal{O}_q (U_{q-1} \otimes I_{\ell'}) \cdots \mathcal{O}_1 (U_0 \otimes I_{\ell'}) |0^\ell\rangle \otimes |\text{init}_{\mathcal{O}}\rangle$ , and returns the measurement result as the output. If  $\mathcal{O}$  has no state and  $\mathcal{O}_i = O_f$  holds for each  $i$ , the behavior of  $\mathcal{A}$  relative to  $\mathcal{O}$  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.  $\mathcal{O}$  may be chosen according to a distribution at the beginning of each game. We denote the event that  $\mathcal{A}$  runs relative to the oracle  $\mathcal{O}$  and returns an output  $\alpha$  by  $\alpha \leftarrow \mathcal{A}^{\mathcal{O}}()$  or by  $\mathcal{A}^{\mathcal{O}}() \rightarrow \alpha$ .

**Quantum distinguishing advantages.** Let  $\mathcal{A}$  be a quantum algorithm that makes at most  $q$  queries, outputs 0 or 1 as the final output, and let  $\mathcal{O}_1$  and  $\mathcal{O}_2$  be some oracles. We consider the situation that  $\mathcal{O}_1$  and  $\mathcal{O}_2$  are chosen randomly according to some distributions. We define the *quantum distinguishing advantage* of  $\mathcal{A}$  by

$$\mathbf{Adv}_{\mathcal{O}_1, \mathcal{O}_2}^{\text{dist}}(\mathcal{A}) := \left| \Pr_{\mathcal{O}_1}[\mathcal{A}^{\mathcal{O}_1}() \rightarrow 1] - \Pr_{\mathcal{O}_2}[\mathcal{A}^{\mathcal{O}_2}() \rightarrow 1] \right|. \quad (2)$$

<sup>5</sup> 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.

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

$$\mathbf{Adv}_{\mathcal{O}_1, \mathcal{O}_2}^{\text{dist}}(q) := \max_{\mathcal{A}} \left\{ \mathbf{Adv}_{\mathcal{O}_1, \mathcal{O}_2}^{\text{dist}}(\mathcal{A}) \right\}, \quad (3)$$

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

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

Let  $\mathcal{F} = \{F_k : \{0, 1\}^m \rightarrow \{0, 1\}^n\}_{k \in \mathcal{K}}$  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 an oracle access to  $O_{F_k}$  is given to adversaries. In addition, let  $\mathcal{A}$  be an oracle query algorithm that outputs 0 or 1. Then we define the quantum pseudorandom-function (qPRF) advantage by  $\mathbf{Adv}_{\mathcal{F}}^{\text{qPRF}}(\mathcal{A}) := \mathbf{Adv}_{\mathcal{F}, \text{RF}}^{\text{dist}}(\mathcal{A})$ . Similarly, we define  $\mathbf{Adv}_{\mathcal{F}}^{\text{qPRF}}(q)$  by  $\mathbf{Adv}_{\mathcal{F}}^{\text{qPRF}}(q) := \max_{\mathcal{A}} \left\{ \mathbf{Adv}_{\mathcal{F}}^{\text{qPRF}}(\mathcal{A}) \right\}$ , 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  $P \in \text{Perm}(\{0, 1\}^n)$  is chosen uniformly at random, and an oracle access to  $O_P$  is given to adversaries.

Let  $\mathcal{P} = \{P_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \mathcal{K}}$  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 an oracle access to  $O_{P_k}$  is given to adversaries. Let  $\mathcal{A}$  be an oracle query algorithm that outputs 0 or 1, and we define the quantum pseudorandom-permutation (qPRP) advantage by  $\mathbf{Adv}_{\mathcal{P}}^{\text{qPRP}}(\mathcal{A}) := \mathbf{Adv}_{\mathcal{P}, \text{RP}}^{\text{dist}}(\mathcal{A})$ . Similarly, we define  $\mathbf{Adv}_{\mathcal{P}}^{\text{qPRP}}(q)$  by  $\mathbf{Adv}_{\mathcal{P}}^{\text{qPRP}}(q) := \max_{\mathcal{A}} \left\{ \mathbf{Adv}_{\mathcal{P}}^{\text{qPRP}}(\mathcal{A}) \right\}$ , where the maximum is taken over all quantum algorithms  $\mathcal{A}$  that make at most  $q$  quantum queries.

**Security against efficient adversaries.** An algorithm  $\mathcal{A}$  is called *efficient* if it can be realized as a quantum circuit of which the number of basic gates and oracle gates is polynomial 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 of which the number of basic gates is polynomial in  $n$ .
2.  $\mathbf{Adv}_{\mathcal{F}}^{\text{qPRF}}(\mathcal{A})$  (resp.,  $\mathbf{Adv}_{\mathcal{P}}^{\text{qPRP}}(\mathcal{A})$ ) 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 [23] 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  $f_i := \{f_{i,k} : \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2}\}_{k \in \mathcal{K}}$  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  $\text{LR}_r(f_1, \dots, f_r) := \{\text{LR}_r(f_{1,k_1}, \dots, f_{r,k_r})\}_{k_1, \dots, k_r \in \mathcal{K}}$  with the key space  $(\mathcal{K})^r$ . For each fixed key  $(k_1, \dots, k_r)$ ,  $\text{LR}_r(f_{1,k_1}, \dots, f_{r,k_r})$  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

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

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

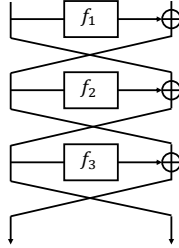


Fig. 2. The 3-round Luby-Rackoff construction.

The resulting function  $\text{LR}_r(f_{1,k_1}, \dots, f_{r,k_r}) : x_0 \mapsto x_r$  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 an oracle access to  $\text{LR}_r(f_1, \dots, f_r)$ , we consider the situation that keys  $k_1, \dots, k_r$  are first chosen independently and uniformly at random, and then the adversary runs relative to the stateless oracle  $O_{\text{LR}_r(f_{1,k_1}, \dots, f_{r,k_r})} : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus \text{LR}_r(f_{1,k_1}, \dots, f_{r,k_r})(x)\rangle$ . When each round function is chosen from  $\text{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$  uniformly at random (i.e., each  $f_i$  is the set of all functions  $\text{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$  for all  $i$ ), we use the notation  $\text{LR}_r$  for short.

## 3 An Alternative Formalization for the Compressed Oracle Technique

In many security proofs in the *classical* random oracle model (ROM), they 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” [37] 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 to the case that 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 for the cases that all round functions are truly random.

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

In provable security, especially for symmetric-key mode of operations, we often focus on security against information theoretic adversaries. When we are interested in such security, we do not care about efficient simulation of a random oracle, and thus we 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 in an intuitive manner by introducing the notion of errors. Since our oracle records transcripts of queries and its behavior is described with errors, we call our oracle *recording standard oracle with errors* and denote it by RstOE.

We believe that our alternative formalization and analyses for its behavior help us understand Zhandry’s technique better, which would lead to even wider applications of the technique.

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  $\text{stO}$  that is independent of  $f$ . In this subsection, we consider that each function  $f : \{0, 1\}^m \rightarrow \{0, 1\}^n$  is encoded into the  $(n2^m)$ -qubit state  $|f\rangle = |f(0)\|f(1)\|\dots\|f(2^m - 1)\rangle$ . The operator  $\text{stO}$  is the unitary operator that acts on  $(n + m + n2^m)$ -qubit states defined as

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

where  $\alpha_x \in \{0, 1\}^n$  for each  $0 \leq x \leq 2^m - 1$ . We can easily confirm that  $\text{stO} |x\rangle |y\rangle |f\rangle = |x\rangle |y \oplus f(x)\rangle |f\rangle$  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  $\text{stO}$  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

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

with probability  $1/2^{n2^m}$ . Here, we assume that  $\mathcal{A}$  has  $\ell$ -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 measure 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

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

Next, we change the basis of the  $y$  register and  $\alpha_i$  registers in (5) from the standard computational basis  $\{|u\rangle\}_{u \in \{0,1\}^n}$  to the one  $\{H^{\otimes n} |u\rangle\}_{u \in \{0,1\}^n}$ , which is called *Fourier basis*<sup>6</sup> by Zhandry [37]. In what follows, we use the symbol “ $\widehat{\phantom{x}}$ ” 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

$$\text{stO} |x\rangle |\widehat{y}\rangle \otimes |\widehat{\alpha_0}\rangle \cdots |\widehat{\alpha_{2^m-1}}\rangle = |x\rangle |\widehat{y}\rangle \otimes |\widehat{\alpha_0}\rangle \cdots |\widehat{\alpha_x \oplus y}\rangle \cdots |\widehat{\alpha_{2^m-1}}\rangle \quad (8)$$

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

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

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

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

(in superpositions) when an adversary makes a query. Thus

$$|\phi_{i+1}\rangle = \sum_{xyz\hat{D}} a'_{xyz\hat{D}} |xyz\rangle \otimes |\hat{D}\rangle \quad (10)$$

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

Zhandry's key observation is that, since  $\text{stO}$  adds at most one data to the  $\hat{D}$ -register in each query,  $\widehat{\alpha}_x \neq 0^n$  holds for at most  $i$  many  $x$ , and thus  $\hat{D}$  can be regarded as a database with at most  $i$  many non-zero entries. (Note that  $\hat{D}$  may contain less than  $i$  non-zero entries. For example, if a state  $|x\rangle|\hat{y}\rangle$  is successively queried to  $\text{stO}$  twice, then the database will remain unchanged since  $\text{stO} \cdot \text{stO} = I$ .) We use the same notation  $\hat{D}$  to denote database, and call it *Fourier database* since now we are using the Fourier basis for  $\hat{D}$ . Each entry of the database  $\hat{D}$  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  $\hat{D}$  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  $\hat{D}$  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 make it clear, let the Hadamard operator  $H^{\otimes n}$  act on each  $\widehat{\alpha}_x$  in  $\hat{D}$  and obtain another (superposition of) database  $D$ . Then, intuitively,  $D$  satisfies the condition “ $(x, \alpha_x) \in D$  corresponds to the condition that  $\mathcal{A}$  has queried  $x$  to the oracle and gotten the value  $\alpha_x$  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  $\text{CstO}$ . The whole quantum state of an adversary  $\mathcal{A}$  and the oracle just before the  $(i+1)$ -st query is

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

where each  $D$  is a standard database which contains at most  $i$  entries. Initially, the database  $D$  is empty. Intuitively, when  $\mathcal{A}$  makes a query  $|x, y\rangle$  to the oracle,  $\text{CstO}$  does the following three procedures.<sup>7</sup>

### The three procedures of $\text{CstO}$ .

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  $(x, \alpha_x)$  to  $D$ . Then respond with  $|x, y \oplus \alpha_x\rangle$ .

<sup>7</sup> We remark that these three-step procedures are a verbatim quotation from the original paper [37] of version 20180814:183812, except that the symbol  $y'$  and 0 are used instead of  $\alpha_x$  and  $0^n$ , respectively, in the original one.

3. Finally, regardless of whether the tuple was found or added, there is now a tuple  $(x, \alpha_x)$  in  $D$ , which may have to be removed. To do so, test whether the registers containing  $\alpha_x$  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 procedures: When an adversary makes a query  $x$  to the oracle, look for a tuple  $(x, \alpha_x)$  in the database. If one is found, respond with  $\alpha_x$  (this part corresponds to the first procedure of CstO). If no tuple is found, *choose  $\alpha_x$  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 procedure of CstO), respond with  $\alpha_x$ , and add  $(x, \alpha_x)$  to the database.

The third “test and forget” step is crucial and specific to the quantum setting. Intuitively, the third step forgets data which 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.** Based on the 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  $(i + 1)$ -th 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  $(i + 1)$ -th 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  $O(i(m+n))$ -qubit state by compressing databases. On the other hand, in our alternative 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  $f : \{0, 1\}^m \rightarrow \{0, 1\}^n$  as  $(n + 1)2^m$ -bit strings  $(0\|f(0)\|0\|f(1)\|\dots\|0\|f(2^m-1))$ . Remember that the whole quantum state before  $\mathcal{A}$  makes the  $(i + 1)$ -st query is described as

$$|\phi_{i+1}\rangle = (U_i \otimes I) \text{stO}(U_{i-1} \otimes I) \text{stO} \cdots \text{stO}(U_0 \otimes I) \left( |0^\ell\rangle \otimes \sum_f \frac{1}{\sqrt{2^{n2^m}}} |f\rangle \right). \quad (12)$$

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, secondly 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  $|\phi_{i+1}\rangle$ .

1. Let the Hadamard operator  $H^{\otimes n}$  act on the  $f(x)$  register for all  $x$ . Now the state becomes

$$\sum_{xyz\tilde{D}} a'_{xyz\tilde{D}} |xyz\rangle \otimes |\tilde{D}\rangle \quad (13)$$

for some complex numbers  $a'_{xyz\tilde{D}}$ , where each  $\tilde{D} = (0\|\hat{\alpha}_0)\|\cdots\|(0\|\hat{\alpha}_{2^m-1})$  is a concatenation of  $2^m$  many  $(n+1)$ -bit strings, and  $\hat{\alpha}_x \neq 0^n$  at most  $i$ -many  $x$ .

2. For each  $x$ , if  $\hat{\alpha}_x \neq 0^n$ , flip the bit just before  $\hat{\alpha}_x$ . Now each  $\tilde{D}$  changes to the bit strings  $(b_0\|\hat{\alpha}_0)\|\cdots\|(b_{2^m-1}\|\hat{\alpha}_{2^m-1})$ , where  $b_x \in \{0,1\}$ , and  $b_x = 1$  if and only if  $\hat{\alpha}_x \neq 0^n$ .
3. For each  $x \in \{0,1\}^n$ , let the  $n$ -bit Hadamard transformation  $H^{\otimes n}$  act on  $|\hat{\alpha}_x\rangle$  if and only if  $b_x = 1$ . Then the quantum state becomes

$$|\psi_{i+1}\rangle := \sum_{xyzD} a_{xyzD} |xyz\rangle \otimes |D\rangle \quad (14)$$

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  $\text{IH} := (I_1 \otimes H^{\otimes n})^{\otimes 2^m}$ . 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  $\text{CH} := (CH^{\otimes n})^{\otimes 2^m}$ , where  $CH := |0\rangle\langle 0| \otimes I_n + |1\rangle\langle 1| \otimes H^{\otimes n}$ .

We call the action of unitary operator  $U_{\text{enc}} := \text{CH} \cdot U_{\text{toggle}} \cdot \text{IH}$  and its conjugate  $U_{\text{enc}}^*$  *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  $\text{RstOE}$  defined by  $\text{RstOE} := (I \otimes U_{\text{enc}}) \cdot \text{stO} \cdot (I \otimes U_{\text{enc}}^*)$ .*

Note that  $|\psi_{i+1}\rangle = (U_i \otimes I)\text{RstOE}(U_{i-1} \otimes I)\text{RstOE} \cdots \text{RstOE}(U_0 \otimes I)(|0^\ell\rangle \otimes |0^{(n+1)2^m}\rangle)$  and  $|\phi_{i+1}\rangle = (I \otimes U_{\text{enc}}^*)|\psi_{i+1}\rangle$  hold for each  $i$ .

Next, we introduce some notations related to our recording standard oracle with errors, which are required to describe properties of  $\text{RstOE}$ .

**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  $b_x \neq 0$ . 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 value on  $x \in \{0,1\}^m$  is defined to be  $y$  if and only if  $b_x \neq 0$  and  $\alpha_x = y$ . We use the same notation  $D$  for this function. Moreover, we identify  $D$  with the set  $\{(x, D(x))\}_{x \in \text{dom}(D)} \subset \{0,1\}^m \times \{0,1\}^n$ . We say that *an entry of  $x$  is in  $D$*  if  $(x, y) \in D$  for some  $y$ . Unless otherwise noted, we always assume that  $D$  is valid.

We say that a valid database  $D$  is compatible with a function  $f : \{0,1\}^m \rightarrow \{0,1\}^n$  if  $D(x) = f(x)$  holds for each  $x$  in the domain of  $D$ . For each valid database  $D$ , let  $\text{comp}(D)$  denote the set of functions that are compatible with  $D$ .

If  $\|\psi\rangle - |\psi'\rangle$  is in  $O(\epsilon)$  for two vectors  $|\psi\rangle, |\psi'\rangle$ , and some parameter  $\epsilon$  (which will be a function of  $n$  in later applications), then we say that  $|\psi\rangle$  is equal to  $|\psi'\rangle$  with an error in  $O(\epsilon)$ , or just write  $|\psi\rangle = |\psi'\rangle$  with an error in  $O(\epsilon)$ .

The following proposition describes the core properties of RstOE.

**Proposition 1 (Core Properties).** *Let  $D$  be a valid database. Then, the following properties hold.*

1. Suppose that  $|D| \leq i$  holds. Then

$$U_{\text{enc}}^* |D\rangle = \sum_{f \in \text{comp}(D)} \sqrt{\frac{1}{|\text{comp}(D)|}} |f\rangle \quad (15)$$

holds with an error in  $O(\sqrt{i^2/2^n})$ .

2. Suppose that there is no entry of  $x$  in  $D$ . Then, for any  $y$ ,

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

with an error in  $O(1/\sqrt{2^n})$ . More precisely,

$$\begin{aligned} & \text{RstOE} |x, y\rangle \otimes |D \cup (x, \alpha)\rangle \\ &= |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle \\ &+ \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \left( |D\rangle - \left( \sum_{\gamma \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) \right) \\ &- \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes (|D \cup (x, \gamma)\rangle - |D_{\gamma}^{\text{invalid}}\rangle) \\ &+ \frac{1}{2^n} |x\rangle |\widehat{0^n}\rangle \otimes \left( 2 \sum_{\delta \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right) \end{aligned} \quad (16)$$

holds, where  $|D_\gamma^{\text{invalid}}\rangle$  is a superposition of invalid databases for each  $\gamma$ , and  $|\widehat{0^n}\rangle = H^{\otimes n} |0^n\rangle$ .

3. Suppose that there is no entry of  $x$  in  $D$ . Then, for any  $y$ ,

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

with an error in  $O(1/\sqrt{2^n})$ . To be more precise,

$$\begin{aligned} \text{RstOE } |x\rangle |y\rangle \otimes |D\rangle &= \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle \\ &+ \frac{1}{\sqrt{2^n}} |x\rangle |\widehat{0^n}\rangle \otimes \left( |D\rangle - \sum_{\gamma \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) \end{aligned} \tag{17}$$

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

Proposition 1 can be shown by straightforward calculations. For completeness, a proof of Proposition 1 is given in Section A in the appendix.

**An intuitive interpretation of Proposition 1.** The first property is a subsidiary one, which would be useful in later applications. When we ignore error terms, the second and third properties correspond to the first and second procedures of CstO, respectively: When an adversary makes a query  $x$  to the oracle, RstOE looks for a tuple  $(x, \alpha)$  in the database. If one is found, respond with  $\alpha$  (the second 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  $\alpha_x$ , and add  $(x, \alpha_x)$  to the database (the third property in the above proposition).

Note that we do not need any “test and forget” procedure to describe the second and third properties in Proposition 1. Thus we can intuitively capture time evolutions of databases with only the (classical) lazy-sampling-like arguments.

To get rid of the “test and forget” procedure, we have to introduce some errors. The error increases as the number of adversaries’ queries  $q$  increases, but it remains negligible as long as  $q \ll 2^{n/2}$ . Thus the error will not be problematic when we focus on the situation  $q \ll 2^{n/2}$ , which is the case for showing the security bound of the 4-round Luby-Rackoff construction.

In later applications, similarly to classical proofs, we introduce *good* and *bad* transcripts. The explicit formulas of the second and third properties will be used to show that, intuitively, adversaries cannot distinguish two oracles if transcripts are “good”. Moreover, the first property and the descriptions with errors of the second and third properties will be used to show that the probability that transcripts become “bad” is negligible.



## 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  $\text{LR}_4$  from random permutations  $\text{RP}$ , in the case that 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,*

$$\text{Adv}_{\text{LR}_4}^{\text{qPRP}}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^6}{2^{n/2}}}\right) \quad (18)$$

*holds.*

Since we can efficiently simulate truly random functions against efficient quantum algorithms [34], 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  $\text{LR}_4(f_1, f_2, f_3, f_4)$  is a quantumly secure PRP.*

To the end 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  $\text{LR}_3$  is proven to be secure against classical CPAs, how the quantum attack on  $\text{LR}_3$  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 things, and then explain where to start.

**An overview of a classical security proof for  $\text{LR}_3$ .** Here we give an overview of a *classical* proof for the security of  $\text{LR}_3$  against chosen plaintext attacks in the classical setting. For simplicity, we consider a proof for PRF security of  $\text{LR}_3$ .

Let  $\text{bad}_2$  be the event that an adversary makes two distinct plaintext queries  $(x_{0L}, x_{0R}) \neq (x'_{0L}, x'_{0R})$  to the real oracle  $\text{LR}_3$  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  $\text{bad}_3$  be the event that inputs to  $f_3$  collide, and define  $\text{bad} := \text{bad}_2 \vee \text{bad}_3$ .

If  $\text{bad}_2$  (resp.,  $\text{bad}_3$ ) does not occur, then the right-half (resp., left-half)  $n/2$  bits of  $\text{LR}_3$ 's outputs cannot be distinguished from truly random  $n/2$ -bit strings. Thus, unless the event  $\text{bad}$  occurs, adversaries cannot distinguish  $\text{LR}_3$  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  $\text{bad}$  occurs when  $\mathcal{A}$  runs relative to the oracle  $\text{LR}_3$  is in  $O(q^2/2^{n/2})$ . Thus we can deduce that  $\text{LR}_3$  is indistinguishable from a random function up to  $O(2^{n/4})$  queries.

**Quantum chosen plaintext attack on  $\text{LR}_3$ .** Next, we give an overview of the quantum chosen plaintext attack on  $\text{LR}_3$  by Kuwakado and Morii [20]. Note that we consider the setting that adversaries can make quantum superposition queries. The attack distinguishes  $\text{LR}_3$  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  $g_i : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  by  $g_i(x) = (\text{LR}_3(\alpha_i, x))_R \oplus \alpha_i$ , where  $(\text{LR}_3(\alpha_i, x))_R$  denote the right half  $n/2$ -bits of  $\text{LR}_3(\alpha_i, x)$ . In addition, define  $G : \{0, 1\} \times \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  by  $G(b, x) = g_b(x)$ . Then, it can be easily confirmed that  $g_0(x) = g_1(x \oplus s)$  holds 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 [31], making  $O(n)$  queries to  $G$ . In fact  $G$  can be implemented on an oracle-querying quantum circuit  $\mathcal{C}^{\text{LR}_3}$  by making  $O(1)$  queries to  $\text{LR}_3$ .<sup>8</sup>

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  $\text{RP}$ , the circuit  $\mathcal{C}^{\text{RP}}$  will implement an almost random function, which does not have any period with a high probability. Thus, if we run Simon’s algorithm on  $\mathcal{C}^{\text{RP}}$ , with a high probability, it does not output any period. Therefore, we can distinguish  $\text{LR}_3$  from  $\text{RP}$  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 the reason why quantum adversaries can distinguish  $\text{LR}_3$  from random permutations even though  $\text{LR}_3$  is proven to be indistinguishable from a random permutation in the classical setting.

We observe that quantum adversaries can make the event  $\text{bad}_2$  occur: Once we find the period  $1 \| s = 1 \| f_1(\alpha_0) \oplus f_2(\alpha_1)$  given the real oracle  $\text{LR}_3$ , 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  $\text{LR}_4$ : The idea.** As we explained above, the essence of the quantum attack on  $\text{LR}_3$  is finding collisions for inputs to the second round function  $f_2$ . On the other hand, it seems difficult to make collisions for inputs to the third round function  $f_3$  even for quantum (chosen-plaintext) query adversaries.

<sup>8</sup> Here we have to implement truncation of outputs of  $\mathcal{O}$  without destroying quantum states, which is pointed out to be non-trivial in the quantum setting [18]. However, it has been shown that this “truncation” issue can be overcome by using a technique observed in [15].

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

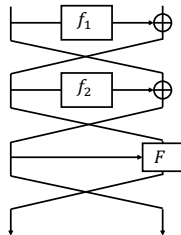


Fig. 3.  $\text{LR}'_3$

We will show it by combining the classical proof idea and our recording standard oracle with errors. Roughly speaking, we define “bad” databases to be the ones that contain “collisions at 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  $\text{LR}'_3$  from  $\text{LR}_3$  when databases are not bad.

Next, let  $\text{FamP}(\{0, 1\}^{n/2})$  be the set of functions  $F : \{0, 1\}^{n/2} \times \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  such that  $F(x, \cdot)$  is a permutation for each  $x$ . If  $P$  is chosen uniformly at random from  $\text{FamP}(\{0, 1\}^{n/2})$ , we say that  $P$  is a *family of random permutations*, or shortly FRP. Then, we intuitively see that it is hard to distinguish FRP from a random function RF from  $\{0, 1\}^n$  to  $\{0, 1\}^{n/2}$ .

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

1.  $\text{LR}'_3$  is hard to distinguish from  $\text{LR}_3$ , and
2. FRP is hard to distinguish from RF,

we can prove Theorem 3 with simple and easy arguments. In other words, showing those two properties are technically the most difficult parts in our proof for Theorem 3. To show the first property, we use our recording standard oracle with errors. On the other hand, for the second property, we can show it by just combining some previous results.

**Organization of the rest of Section 4.** Section 4.1 shows that  $\text{LR}'_3$  is hard to distinguish from  $\text{LR}_3$ . Section 4.2 shows that FRP 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 $\text{LR}'_3$ from $\text{LR}_3$

Here we show the following proposition.

**Proposition 2.** Let  $q$  be a positive integer. Let  $\mathcal{A}$  be an adversary that makes at most  $q$  quantum queries. Then,

$$\text{Adv}_{\text{LR}_3, \text{LR}'_3}^{\text{dist}}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^3}{2^{n/2}}}\right) \quad (19)$$

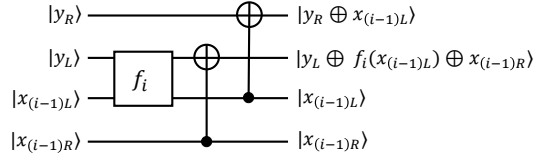
holds.

First, let us discuss the behavior of the quantum oracles of  $\text{LR}_3$  and  $\text{LR}'_3$ .

**Quantum oracle of  $\text{LR}_3$ .** Let  $O_{f_i}$  denote the quantum oracle of each round function  $f_i$ . In addition, let us define the unitary operator  $O_{\text{UP},i}$  that computes the state update of the  $i$ -th round by

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

$O_{\text{UP},i}$  can be implemented by making one query to  $f_i$  (see Fig. 4).



**Fig. 4.** Implementation of  $O_{\text{UP},i}$ .  $f_i$  will be implemented by using the recording standard oracle with errors.

Now  $O_{\text{LR}_3}$  can be implemented as follows by using  $\{O_{\text{UP},i}\}_{1 \leq i \leq 3}$ :

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  $O_{\text{UP},1}$ , and obtain

$$|x_{0L}, x_{0R}\rangle |y_L, y_R\rangle \otimes |x_{1L}, x_{1R}\rangle. \quad (20)$$

3. Compute the state  $(x_{2L}, x_{2R})$  by querying  $|x_{1L}, x_{1R}\rangle |0^n\rangle$  to  $O_{\text{UP},2}$ , and obtain

$$|x_{0L}, x_{0R}\rangle |y_L, y_R\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle. \quad (21)$$

4. Query  $|x_{2L}, x_{2R}\rangle |y_L, y_R\rangle$  to  $O_{\text{UP},3}$ , and obtain

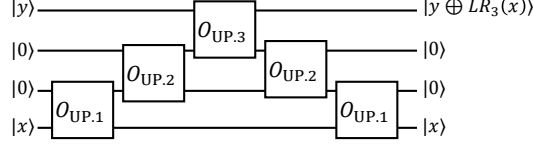
$$|x\rangle |y \oplus \text{LR}_3(x)\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle. \quad (22)$$

5. Uncompute Steps 2 and 3 to obtain

$$|x\rangle |y \oplus \text{LR}_3(x)\rangle. \quad (23)$$

6. Return  $|x\rangle |y \oplus \text{LR}_3(x)\rangle$ .

The above implementation is illustrated in Fig. 5.

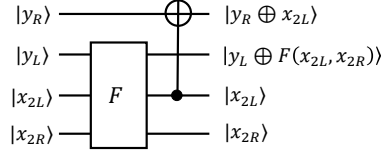


**Fig. 5.** Implementation of  $\text{LR}_3$ .

**Quantum oracle of  $\text{LR}'_3$ .** The quantum oracle of  $\text{LR}'_3$  is implemented in the same way as  $\text{LR}_3$ , except that the third round state update oracle  $O_{\text{UP}.3}$  is replaced with another oracle  $O'_{\text{UP}.3}$  defined as

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

$O'_{\text{UP}.3}$  is implemented by making one query to  $O_F$ , i.e., the quantum oracle of  $F$  (see Fig. 6).



**Fig. 6.** Implementation of  $O'_{\text{UP}.3}$ .  $F$  will be implemented by using the recording standard oracle with errors.

Below, we show the claim of the proposition by using the recording standard oracle with errors for  $f_1, f_2, f_3$ , and  $F$ . We consider that the oracles of these functions 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  $\text{LR}_3$ , the joint quantum states of the adversary and functions can be described as

$$\sum_{xyzD_1D_2D_3} a_{xyzD_1D_2D_3} |xyz\rangle \otimes |D_1\rangle |D_2\rangle |D_3\rangle \quad (24)$$

for some complex numbers  $a_{xyzD_1D_2D_3}$  such that  $\sum_{xyzD_1D_2D_3} |a_{xyzD_1D_2D_3}|^2 = 1$ . Here,  $x, y$ , and  $z$  correspond to the adversary's query, answer, and output registers, respectively. (If the oracle is  $\text{LR}'_3$ , then the registers  $|D_3\rangle$ , which corresponds to  $f_3$ , are replaced with  $|D_F\rangle$ , which corresponds to  $F$ .)

Next, we define good and bad databases for  $\text{LR}_3$  and  $\text{LR}'_3$ . Intuitively, we say that a tuple  $(D_1, D_2, D_3)$  (resp.,  $(D_1, D_2, D_F)$ ) for  $\text{LR}_3$  (resp.,  $\text{LR}'_3$ ) 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 there exists a one-to-one correspondence between good databases for  $\text{LR}_3$  and those for  $\text{LR}'_3$ , so that adversaries will not be able to distinguish  $\text{LR}'_3$  from  $\text{LR}_3$  as long as databases are good.

**Good and bad databases for  $\text{LR}_3$ .** Here we introduce the notion of *good* and *bad* for each tuple  $(D_1, D_2, D_3)$  of valid database for  $\text{LR}_3$ . 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  $\text{LR}'_3$ .** Next we introduce the notion of *good* and *bad* for each tuple  $(D_1, D_2, D_F)$  of valid database for  $\text{LR}'_3$ . We say that a valid database  $D_F$  is *without overlap* if each pair of distinct entries  $(x_{2L}, x_{2R}, \gamma)$  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  $x_{2R}$  and  $(x_{2L}, x_{2R}, x_{2R} \oplus \gamma) \in D_F$ .

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

*Remark 1.* For each good database  $(D_1, D_2, D_3)$  for  $\text{LR}_3$ , there exists a unique  $D_F$  without overlap such that  $[D_F]_3 = D_3$  and  $(D_1, D_2, D_F)$  is a good database for  $\text{LR}'_3$ , by definition of good databases. Similarly, for each good database  $(D_1, D_2, D_F)$  for  $\text{LR}'_3$ ,  $(D_1, D_2, [D_F]_3)$  becomes a good database for  $\text{LR}_3$ .

Next we define regular and irregular quantum states for the oracles  $O_{\text{LR}_3}$  and  $O_{\text{LR}'_3}$ . Roughly speaking, we will treat irregular states as some small error terms, and focus on regular states.

**Regular and irregular states of oracles.** Recall that, in addition to database registers, the quantum oracle  $O_{\text{LR}_3}$  uses ancillary  $2n$ -qubit registers to compute intermediate state after the first and second rounds (see (21) and (22)). We say that a state vector  $|D_1\rangle |D_2\rangle |D_3\rangle \otimes |x_1\rangle \otimes |x_2\rangle$  for  $O_{\text{LR}_3}$ , where  $|x_1\rangle \otimes |x_2\rangle$  is the ancillary  $2n$  qubits, is *irregular* if  $x_1 \neq 0^n \vee x_2 \neq 0^n$  holds, or at least one of the

three databases,  $D_1$ ,  $D_2$ , or  $D_3$ , is invalid. We say that the state vector is *regular* if it is not irregular. We define regular and irregular states for  $O_{LR'_3}$  similarly.

Next we define some modified versions of  $LR_3$  and  $LR'_3$ , which we denote by  $LR_3\text{-det}$  and  $LR'_3\text{-det}$ , respectively (“det” is an abbreviation of “detection of bad database”).

**The oracles  $LR_3\text{-det}$  and  $LR'_3\text{-det}$ .** The oracle  $LR_3\text{-det}$  is defined in the same way as  $LR_3$ , except that the oracle checks whether the database is bad (or the state of the oracle is irregular) after each query, and writes the result to an additional qubit. Note that we define regular and irregular states for  $LR_3\text{-det}$  in the same way as for  $LR_3$ . Additional qubits are prepared before an adversary  $\mathcal{A}$  runs ( $q$  additional qubits are sufficient if  $\mathcal{A}$  is a  $q$  query adversary). If  $i \neq j$ , the results of “detection of bad database” for the  $i$ -th and  $j$ -th queries are written in distinct qubits.

Intuitively,  $LR_3\text{-det}$  behaves as follows when  $\mathcal{A}$  makes the  $i$ -th query:

1. Check if the  $j$ -th additional qubit is 1 for  $1 \leq j \leq i - 1$  (i.e., check if the database has been bad before the  $i$ -th query). If so, do nothing. If not, go to the next step.
2. Make a query to  $O_{LR_3}$ .
3. Check if the database is bad, or the quantum state of  $O_{LR_3}$  is irregular. If so, flip the  $i$ -th additional qubit.

Next, we formally explain how the above procedures can be realized as a unitary operator. Let  $\Pi_{\text{bad}}$  be the projection to the space spanned by the vectors of *bad* databases, and irregular state vectors. In addition, let  $\Pi_{\text{flipped}}^{[i-1]}$  be the projection onto the space spanned by the vectors such that the  $j$ -th additional qubit is 1 for some  $1 \leq j \leq i - 1$ , and irregular state vectors.

Formally, for the  $i$ -th query, the behavior of the quantum oracle of  $LR_3\text{-det}$  is described by the unitary operator

$$\begin{aligned}
O_{LR_3\text{-det}} := & (\Pi_{\text{bad}} \otimes I_{i-1} \otimes X + (I - \Pi_{\text{bad}}) \otimes I_{i-1} \otimes I_1) \\
& \cdot (O_{LR_3} \otimes I_{i-1} \otimes I_1) \cdot ((I - \Pi_{\text{flipped}}^{[i-1]}) \otimes I_1) \\
& + \Pi_{\text{flipped}}^{[i-1]} \otimes I_1,
\end{aligned} \tag{25}$$

where  $I_{i-1}$  is the identity operator which acts on the first  $(i-1)$  additional qubits, in addition that  $I_1$  and  $X$  are the identity operator and the operator such that  $X|0\rangle = |1\rangle$  and  $X|1\rangle = |0\rangle$ , respectively, which act on the  $i$ -th additional qubit.

$LR'_3\text{-det}$  is constructed from  $LR'_3$  in the same way as  $LR_3\text{-det}$  is constructed from  $LR_3\text{-det}$  as above. The behaviors of the oracles of  $LR'_3\text{-det}$  and  $LR_3\text{-det}$  depend on  $i$ , though for simplicity, we always use the notations  $O_{LR'_3\text{-det}}$  and  $O_{LR_3\text{-det}}$  without  $i$ .

Below we first show that  $LR_3\text{-det}$  is hard to distinguish from  $LR'_3\text{-det}$ , and second show that  $LR_3\text{-det}$  (resp.,  $LR'_3\text{-det}$ ) is hard to distinguish from  $LR_3$  (resp.,  $LR'_3$ ).

**Hardness of distinguishing  $\text{LR}_3\text{-det}$  from  $\text{LR}'_3\text{-det}$ .** Let  $|\psi_i\rangle$  and  $|\psi'_i\rangle$  be the state just before the  $i$ -th query to  $\text{LR}_3\text{-det}$  and  $\text{LR}'_3\text{-det}$ , respectively. By abuse of notation, we let  $|\psi_{(q+1)}\rangle, |\psi'_{(q+1)}\rangle$  denote the quantum states  $(U_q \otimes I)O_{\text{LR}_3\text{-det}}|\psi_q\rangle$  and  $(U_q \otimes I)O_{\text{LR}'_3\text{-det}}|\psi'_q\rangle$ , respectively.

We need the following lemma. Intuitively, the lemma claims that any adversary cannot distinguish  $\text{LR}_3\text{-det}$  from  $\text{LR}'_3\text{-det}$  if databases are “good”.

**Lemma 1.** *For each  $j$ , let  $|\psi_j^{\text{good}}\rangle$  and  $|\psi'_j{}^{\text{good}}\rangle$  denote  $(I - \Pi_{\text{flipped}}^{[i-1]})|\psi_j\rangle$  and  $(I - \Pi_{\text{flipped}}^{[i-1]})|\psi'_j\rangle$ , respectively. Let  $\text{tr}_{\mathcal{D}_{123}}$  and  $\text{tr}_{\mathcal{D}_{12F}}$  denote the partial trace over databases and additional qubits for  $\text{LR}_3\text{-det}$  and  $\text{LR}'_3\text{-det}$ , respectively. Then,  $\text{tr}_{\mathcal{D}_{123}}(|\psi_i^{\text{good}}\rangle) = \text{tr}_{\mathcal{D}_{12F}}(|\psi'_i{}^{\text{good}}\rangle)$  holds for  $1 \leq i \leq q + 1$ .*

*Proof intuition.* Lemma 1 can be shown by straightforward algebraic calculations using the strict formulas of the second and third properties in Proposition 1. The equality holds owing to the one-to-one correspondences between good databases for  $\text{LR}_3$  and those for  $\text{LR}'_3$  (see Remark 1). A complete proof of Lemma 1 is given in Section B in the appendix.

We also need the following lemma, which intuitively claims that “good” states change to “bad” states only with a negligible probability.

**Lemma 2.** *For for each  $j$ ,  $\|I_{\text{bad}} \cdot O_{\text{LR}_3} |\psi_j^{\text{good}}\rangle\|$  and  $\|I_{\text{bad}} \cdot O_{\text{LR}'_3} |\psi'_j{}^{\text{good}}\rangle\|$  are in  $O(\sqrt{j/2^{n/2}})$ .*

*Proof intuition.* Here we give a proof intuition for  $\text{LR}_3$ . Owing to the second and third properties of Proposition 1 with errors, we can use classical lazy-sampling intuition (see explanations below Proposition 1). Roughly speaking, good databases change to bad if and only if a fresh query is made to  $f_1$  or  $f_2$ , and the corresponding input to  $f_3$  collides with some existing record in the database for  $f_3$ .

Since each database of  $|\psi_j^{\text{good}}\rangle$  has at most  $(j - 1)$  entries and outputs of  $f_1$  and  $f_2$  are  $(n/2)$ -bits, the input to  $f_3$  that corresponds to a fresh input to  $f_1$  or  $f_2$  collides with one of the existing records in  $D_3$  with a probability at most  $O(j/2^{n/2})$ . This corresponds to the claim that  $\|I_{\text{bad}} \cdot O_{\text{LR}_3} |\psi_j^{\text{good}}\rangle\|^2 \leq O(j/2^{n/2})$  holds. This argument actually ignores some errors, but the errors will be in  $O(\sqrt{1/2^{n/2}})$  due to Proposition 1. The claim for  $\text{LR}'_3$  can be shown in a similar way. A complete proof of Lemma 2 is given in Section C in the appendix.

The following proposition guarantees that it is hard to distinguish  $\text{LR}_3\text{-det}$  from  $\text{LR}'_3\text{-det}$ .

**Proposition 3.**  $\text{Adv}_{\text{LR}_3\text{-det}, \text{LR}'_3\text{-det}}^{\text{dist}}(\mathcal{A})$  is in  $O(\sqrt{q^3/2^{n/2}})$ .

*Proof intuition.* Due to Lemma 1,  $\mathcal{A}$  cannot distinguish  $\text{LR}_3\text{-det}$  from  $\text{LR}'_3\text{-det}$  as long as databases are good. Thus, intuitively, the distinguishing advantage is upper bounded by the square root of the probability that databases become



bad while  $\mathcal{A}$  makes  $q$  queries, which is further upper bounded by  $\sum_{1 \leq j \leq q} \|I_{\text{bad}} \cdot O_{\text{LR}_3\text{-det}} |\psi_j^{\text{good}}\rangle\| + \sum_{1 \leq j \leq q} \|I_{\text{bad}} \cdot O_{\text{LR}'_3\text{-det}} |\psi_j^{\text{good}}\rangle\|$ . From Lemma 2, this can be upper bounded by  $\sum_{1 \leq j \leq q} O(\sqrt{j/2^{n/2}}) + \sum_{1 \leq j \leq q} O(\sqrt{j/2^{n/2}}) = O(\sqrt{q^3/2^{n/2}})$ . A complete proof of Proposition 3 is given in Section D in the appendix.

**Hardness of distinguishing  $\text{LR}_3\text{-det}$  and  $\text{LR}'_3\text{-det}$  from  $\text{LR}_3$  and  $\text{LR}'_3$ .**  
The following proposition guarantees that it is hard to distinguish  $\text{LR}_3\text{-det}$  and  $\text{LR}'_3\text{-det}$  from  $\text{LR}_3$  and  $\text{LR}'_3$ , respectively.

**Proposition 4.**  $\text{Adv}_{\text{LR}_3, \text{LR}_3\text{-det}}^{\text{dist}}(\mathcal{A})$  and  $\text{Adv}_{\text{LR}'_3, \text{LR}'_3\text{-det}}^{\text{dist}}(\mathcal{A})$  are in  $O\left(\sqrt{q^3/2^{n/2}}\right)$ .

*Proof intuition.* We give a proof intuition for  $\text{LR}_3\text{-det}$  and  $\text{LR}_3$ . Since the databases of round functions for  $\text{LR}_3\text{-det}$  are the same as those for  $\text{LR}_3$ ,  $\mathcal{A}$  cannot distinguish  $\text{LR}_3\text{-det}$  from  $\text{LR}'_3\text{-det}$  as long as databases are good. Thus, roughly speaking, the distinguishing advantage is upper bounded by the square root of the probability that databases become bad while  $\mathcal{A}$  makes  $q$  queries. Owing to Lemma 2, we can show the claim in the same way as the proof intuition for Proposition 3. The claim for  $\text{LR}'_3\text{-det}$  and  $\text{LR}'_3$  can be shown in a similar way. A proof of Proposition 4 is given in Section E in the appendix.

**Proof of Proposition 2.** Finally, we show Proposition 2.

*Proof (of Proposition 2).*  $\text{Adv}_{\text{LR}_3, \text{LR}'_3}^{\text{dist}}(\mathcal{A})$  is upper bounded by  $\text{Adv}_{\text{LR}_3, \text{LR}_3\text{-det}}^{\text{dist}}(\mathcal{A}) + \text{Adv}_{\text{LR}_3\text{-det}, \text{LR}'_3\text{-det}}^{\text{dist}}(\mathcal{A}) + \text{Adv}_{\text{LR}'_3\text{-det}, \text{LR}'_3}^{\text{dist}}(\mathcal{A})$ . Thus, the claim of Proposition 2 follows from Proposition 3 and Proposition 4.  $\square$

## 4.2 Hardness of Distinguishing FRP from RF

Recall that  $\text{FamP}(\{0, 1\}^{n/2})$  is the set of functions  $F : \{0, 1\}^{n/2} \times \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  such that  $F(x, \cdot)$  is a permutation for each  $x$ , and if  $P$  is chosen uniformly at random from  $\text{FamP}(\{0, 1\}^{n/2})$ , we say that  $P$  is a *family of random permutations*, or shortly FRP. The following proposition claims that it is hard to distinguish FRP from RF.

**Proposition 5.** For any quantum adversary  $\mathcal{A}$  that makes at most  $q$  quantum queries,  $\text{Adv}_{\text{FRP}, \text{RF}}^{\text{dist}}(\mathcal{A}) \leq O\left(\sqrt{q^6/2^{n/2}}\right)$  holds.

*Proof intuition.* This proposition can be proven by just combining the two previous results: The first one is the indistinguishability of a random function and a random permutation shown by Zhandry [35], and the second one is the equivalence of oracle-indistinguishability and indistinguishability, which is first shown by Zhandry [33] and later generalized by Song and Yun [32]. If a function  $F : \{0, 1\}^{n/2} \times \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  is a random function RF (resp., a family of random permutations FRP),  $F(x, \cdot)$  is a random function (resp., a

random permutation) for each  $x \in \{0, 1\}^{n/2}$ . Roughly speaking,  $F$  can be regarded as an “oracle” that returns a random function (resp., random permutation) for each  $x$ . Then, from the equivalence of indistinguishability and oracle-indistinguishability, indistinguishability of RF and FRP (which is, intuitively, “oracle”-indistinguishability of a random function and a random permutation) follows from the indistinguishability of a random function and a random permutation from  $\{0, 1\}^{n/2}$  to  $\{0, 1\}^{n/2}$ , which is already shown as the first result above. See Section F in the appendix for a formal proof.

### 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  $\text{LR}_4$  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  $F, F' : \{0, 1\}^{n/2} \times \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  are random functions. Let us denote the modified function by  $\text{LR}_4''$ . In addition, by  $\text{LR}_2''(F, F')$  we denote the function defined by  $(x_L, x_R) \mapsto (F'(F(x_L, x_R), x_L), F(x_L, x_R))$  (see Fig. 7).

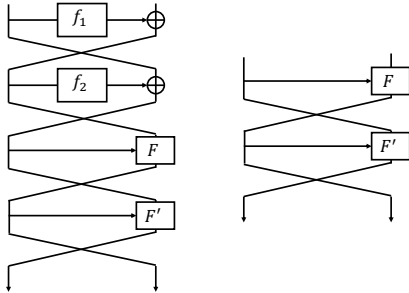


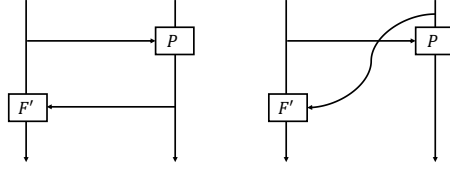
Fig. 7.  $\text{LR}_4''$  and  $\text{LR}_2''(F, F')$ .

Then, by applying Proposition 2 twice we can show that

$$\mathbf{Adv}_{\text{LR}_4, \text{LR}_4''}^{\text{dist}}(q) \leq O\left(\sqrt{\frac{q^3}{2^{n/2}}}\right) \quad (26)$$

holds.

Let us modify  $\text{LR}_2''(F, F')$  in such a way that  $F$  is replaced with a family of random permutations  $P$ , and denote the resulting function by  $\text{LR}_2''(P, F')$ . Then, from Proposition 5 it follows that  $\mathbf{Adv}_{\text{LR}_2''(F, F'), \text{LR}_2''(P, F')}^{\text{dist}}(q) \leq O(\sqrt{q^6/2^{n/2}})$  holds. Next, let us define a function  $G$  by  $G(x_L, x_R) = F'(x_L, x_R) \| P(x_L, x_R)$ , where  $F'$  is a random function and  $P$  is a family of random permutations (see



**Fig. 8.**  $\text{LR}'_2(P, F')$  and  $G$ .

Fig. 8). Then, the function distribution of  $\text{LR}'_2(P, F')$  is the same as that of  $G$ . (Note that  $P(x_L, x_R) \neq P(x_L, x'_R)$  always holds if  $x_R \neq x'_R$ . Thus, if  $(x_L, x_R) \neq (x'_L, x'_R)$ , the corresponding inputs to  $F'$  will be distinct.) Therefore we have that  $\text{Adv}_{\text{LR}'_2(P, F'), G}^{\text{dist}}(q) = 0$  holds. Moreover, from Proposition 5  $\text{Adv}_{\text{RF}, G}^{\text{dist}}(q) \leq O\left(\sqrt{q^6/2^{n/2}}\right)$  holds. Therefore  $\text{Adv}_{\text{LR}'_2(P, F'), \text{RF}}^{\text{dist}}(q) \leq O\left(\sqrt{q^6/2^{n/2}}\right)$  follows, which implies that

$$\text{Adv}_{\text{LR}'_4, \text{RF}}^{\text{dist}}(q) \leq O\left(\sqrt{\frac{q^6}{2^{n/2}}}\right) \quad (27)$$

holds.

Hence, from (26) and (27), it follows that  $\text{Adv}_{\text{LR}_4, \text{RF}}^{\text{dist}}(\mathcal{A}) \leq O\left(\sqrt{q^6/2^{n/2}}\right)$  holds for any quantum adversary  $\mathcal{A}$  that makes at most  $q$  quantum queries. In addition,  $\text{Adv}_{\text{RP}, \text{RF}}^{\text{dist}}(\mathcal{A}) \leq O(q^6/2^n)$  follows from Proposition 7. Therefore

$$\text{Adv}_{\text{LR}_4, \text{RP}}^{\text{dist}}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^6}{2^{n/2}}}\right) \quad (28)$$

follows, for any quantum adversary  $\mathcal{A}$  that makes at most  $q$  quantum queries, which completes the proof of the theorem.  $\square$

*Remark 2.* In the above proof, we went back and forth between random functions and (families of) random permutations, which may seem unnatural. Our proof strategy was motivated to avoid complex arguments that are specific to the quantum setting as much as possible.

## 5 A Query Upper Bound

Here we give a query upper bound for the problem of distinguishing  $\text{LR}_4$  from a random permutation by showing a distinguishing attack. Again, we consider the case that all round functions of  $\text{LR}_4$  are truly random functions, and show the following theorem.

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

*Proof intuition.* Intuitively, our distinguishing attack is just a quantum version of a classical collision-finding-based distinguishing attack [28]. Classical attack distinguishes  $\text{LR}_4$  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 make a  $O(2^{n/6})$ -query quantum distinguisher. (Note that, in general, we can 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 [35].) A complete proof is given in Section G in the appendix.

## 6 Concluding Remarks

This paper showed that  $\Omega(2^{n/12})$  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. To give security proofs, we gave an alternative formalization of the compressed oracle technique by Zhandry and applied it.

To give the tight bound for the problem of distinguishing the 4-round Luby-Rackoff construction from a random permutation is an important future work. It would be interesting 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 5 in a previous version of this paper (version 20190228:191424).

## References

1. Alagic, G., Russell, A.: Quantum-secure symmetric-key cryptography based on hidden shifts. In: Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings, Part III. pp. 65–93 (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: Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Proceedings. pp. 44–63 (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: Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Proceedings. pp. 39–56 (2000)
5. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings. Lecture Notes in Computer Science, vol. 7073, pp. 41–69. Springer (2011)
6. Boneh, D., Zhandry, M.: Quantum-secure message authentication codes. In: Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings. pp. 592–608 (2013)
7. Bonnetain, X.: Quantum key-recovery on full AEZ. In: Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Revised Selected Papers. pp. 394–406 (2017)
8. Bonnetain, X., Naya-Plasencia, M.: Hidden shift quantum cryptanalysis and implications. In: Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part I. pp. 560–592 (2018)
9. Bonnetain, X., Naya-Plasencia, M., Schrottenloher, A.: On quantum slide attacks. IACR Cryptology ePrint Archive **2018**, 1067 (2018)
10. Czajkowski, J., Bruinderink, L.G., Hülsing, A., Schaffner, C., Unruh, D.: Post-quantum security of the sponge construction. In: Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Proceedings. pp. 185–204 (2018)
11. Czajkowski, J., Majenz, C., Schaffner, C., Zur, S.: Quantum lazy sampling and game-playing proofs for quantum indistinguishability. 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. IACR Cryptology ePrint Archive **2017**, 1249 (2017)
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., Sasaki, Y.: Quantum demirci-selçuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions. In: Security and Cryptography for Networks - 11th International Conference, SCN 2018, Proceedings. pp. 386–403 (2018)
16. Hosoyamada, A., Yasuda, K.: Building quantum-one-way functions from block ciphers: Davies-meyer and Merkle-Damgård constructions. In: Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part I. pp. 275–304 (2018)
17. Ito, G., Hosoyamada, A., Matsumoto, R., Sasaki, Y., Iwata, T.: Quantum chosen-ciphertext attacks against Feistel ciphers. To appear at CT-RSA 2019

18. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Proceedings, Part II*. pp. 207–237 (2016)
19. Kitaev, A.Y., Shen, A.H., Vyalii, M.N.: *Classical and Quantum Computation*. American Mathematical Society, Boston, MA, USA (2002)
20. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: *IEEE International Symposium on Information Theory, ISIT 2010, Proceedings*. pp. 2682–2685 (2010)
21. Kuwakado, H., Morii, M.: Security on the quantum-type Even-Mansour cipher. In: *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012*. pp. 312–316 (2012)
22. Liu, Q., Zhandry, M.: On finding quantum multi-collisions. *IACR Cryptology ePrint Archive* **2018**, 1096 (2018), (To appear at Eurocrypt 2019)
23. Luby, M., Rackoff, C.: How to construct pseudo-random permutations from pseudo-random functions (abstract). In: *Advances in Cryptology - CRYPTO '85, Proceedings*. p. 447 (1985)
24. Mennink, B., Szepieniec, A.: XOR of PRPs in a quantum world. In: *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Proceedings*. pp. 367–383 (2017)
25. National Bureau of Standards: Data encryption standard. FIPS 46 (January 1977)
26. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information: 10th Anniversary Edition* (2010)
27. NIST: Announcing request for nominations for public-key post-quantum cryptographic algorithms. National Institute of Standards and Technology (2016)
28. Patarin, J.: New results on pseudorandom permutation generators based on the DES scheme. In: *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Proceedings*. pp. 301–312 (1991)
29. Santoli, T., Schaffner, C.: Using Simon’s algorithm to attack symmetric-key cryptographic primitives. *Quantum Information & Computation* **17**(1&2), 65–78 (2017)
30. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: *35th Annual Symposium on Foundations of Computer Science, Proceedings*. pp. 124–134 (1994)
31. Simon, D.R.: On the power of quantum computation. *SIAM J. Comput.* **26**(5), 1474–1483 (1997)
32. Song, F., Yun, A.: Quantum security of NMAC and related constructions - PRF domain extension against quantum attacks. In: *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Proceedings, Part II*. pp. 283–309 (2017)
33. Zhandry, M.: How to construct quantum random functions. In: *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, Proceedings*. pp. 679–687 (2012)
34. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Proceedings*. pp. 758–775 (2012)
35. Zhandry, M.: A note on the quantum collision and set equality problems. *Quantum Information & Computation* **15**(7&8), 557–567 (2015)
36. Zhandry, M.: A note on quantum-secure prps. *IACR Cryptology ePrint Archive* **2016**, 1076 (2016)
37. Zhandry, M.: How to record quantum queries, and applications to quantum indistinguishability. *IACR Cryptology ePrint Archive* **2018**, 276 (2018)

## A Proof of Proposition 1

This section gives a proof of Proposition 1.

*Proof (of Proposition 1).* Recall that RstOE is decomposed as

$$\text{RstOE} = (I \otimes \text{CH}) \cdot (I \otimes U_{\text{toggle}}) \cdot (I \otimes \text{IH}) \text{stO}(I \otimes \text{IH}^*) \cdot (I \otimes U_{\text{toggle}}^*) \cdot (I \otimes \text{CH}^*), \quad (29)$$

and that each  $D$  is described as a bit string  $(b_0 \| \alpha_0) \| \dots \| (b_{2^m-1} \| \alpha_{2^m-1})$ , 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. Let  $\alpha$  be an  $n$ -bit string, and  $U_{\text{toggle1}} := (I_1 \otimes |0^n\rangle \langle 0^n| + X \otimes (I_n - |0^n\rangle \langle 0^n|))$ . Then

$$\begin{aligned} & (I_1 \otimes H^{\otimes n}) \cdot U_{\text{toggle1}} \cdot \text{CH} |1\rangle |\alpha\rangle \\ &= (I_1 \otimes H^{\otimes n}) \cdot U_{\text{toggle1}} \left( \sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} |1\rangle |u\rangle \right) \\ &= (I_1 \otimes H^{\otimes n}) \left( \sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} |0\rangle |u\rangle \right) \\ &\quad + (I_1 \otimes H^{\otimes n}) \left( \frac{1}{\sqrt{2^n}} (|1\rangle |0^n\rangle - |0\rangle |0^n\rangle) \right) \\ &= |0\rangle |\alpha\rangle + |\epsilon\rangle \end{aligned} \quad (30)$$

holds, where  $|\epsilon\rangle := (I_1 \otimes H^{\otimes n}) \left( \frac{1}{\sqrt{2^n}} (|1\rangle |0^n\rangle - |0\rangle |0^n\rangle) \right)$ , and

$$(I_1 \otimes H^{\otimes n}) \cdot U_{\text{toggle1}} \cdot \text{CH} |0\rangle |0^n\rangle = \sum_{y \in \{0,1\}^n} \sqrt{\frac{1}{2^n}} |0\rangle |y\rangle \quad (31)$$

holds. Since  $U_{\text{enc}}^* = ((I_1 \otimes H^{\otimes n}) \cdot U_{\text{toggle1}} \cdot \text{CH})^{\otimes 2^m}$  holds by definition of  $U_{\text{enc}}^*$ , we have that

$$U_{\text{enc}}^* |D\rangle = \bigotimes_{j=0}^{2^m-1} |\eta_j\rangle \quad (32)$$

holds, where

$$|\eta_j\rangle = \begin{cases} |0\rangle |\alpha_j\rangle + |\epsilon\rangle & \text{if } b_j = 1, \\ \sum_{y \in \{0,1\}^n} \sqrt{\frac{1}{2^n}} |0\rangle |y\rangle & \text{if } b_j = 0. \end{cases}$$

Without loss of generality, we assume that  $b_j = 1$  for  $0 \leq j \leq i-1$  and  $b_j = 0$  for  $j \geq i$ . Let us define  $|\eta\rangle := \bigotimes_{j=i}^{2^m-1} \left( \sum_{y \in \{0,1\}^n} \sqrt{1/2^n} |0\rangle |y\rangle \right)$ . Then we have

$$U_{\text{enc}}^* |D\rangle = \bigotimes_{j=0}^{i-1} (|0\rangle |\alpha_j\rangle + |\epsilon\rangle) \otimes |\eta\rangle$$

$$\begin{aligned}
&= \bigotimes_{j=0}^{i-1} |0\|\alpha_j\rangle \otimes |\eta\rangle \\
&\quad + \sum_{0 \leq k \leq i-1} \left( \bigotimes_{j=0}^k |0\|\alpha_j\rangle \right) \otimes |\epsilon\rangle \otimes \left( \bigotimes_{j=k+2}^{i-1} (|0\|\alpha_j\rangle + |\epsilon\rangle) \right) \otimes |\eta\rangle \\
&= \sum_{f \in \text{comp}(D)} \sqrt{\frac{1}{|\text{comp}(D)|}} |f\rangle + |\epsilon'\rangle, \tag{33}
\end{aligned}$$

where  $|\epsilon'\rangle = \sum_{0 \leq k \leq i-1} (\bigotimes_{j=0}^k |0\|\alpha_j\rangle) \otimes |\epsilon\rangle \otimes (\bigotimes_{j=k+2}^{i-1} (|0\|\alpha_j\rangle + |\epsilon\rangle)) \otimes |\eta\rangle$ . Because  $\|\epsilon\rangle\| = \sqrt{1/2^{n-1}}$ ,  $\|\epsilon'\rangle\|$  is in  $O(i\sqrt{1/2^n}) = O(\sqrt{i^2/2^n})$ . Thus the first property holds.

Next, we show the second property. Since now the operator  $\text{RstOE}$  does not affect the registers of entry of  $x'$  in  $D$  for  $x' \neq x$ , it suffices to show that the claim holds for the case that  $D$  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  $(1\|\alpha)\|(0\|0^n)\|\dots\|(0\|0^n)$ . We have that  $U_{\text{enc}}^* = \text{IH}^* U_{\text{toggle}}^* \text{CH}^* = \text{IH} U_{\text{toggle}} \text{CH}$  and

$$\begin{aligned}
U_{\text{enc}}^* |D \cup (x, \alpha)\rangle &= \text{IH} U_{\text{toggle}} \left( \sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} |1\|u\rangle \right) \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\|0^n\rangle \right) \\
&= \text{IH} \left( \sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} |0\|u\rangle \right) \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\|0^n\rangle \right) \\
&\quad + \text{IH} \left( \frac{1}{\sqrt{2^n}} (|1\|0^n\rangle - |0\|0^n\rangle) \right) \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\|0^n\rangle \right) \\
&= |0\|\alpha\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right) + |\epsilon_1\rangle, \tag{34}
\end{aligned}$$

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

$$\begin{aligned}
&\text{stO}(I \otimes U_{\text{enc}}^* |x, y\rangle \otimes |D \cup (x, \alpha)\rangle) \\
&= |x, y \oplus \alpha\rangle \otimes |0\|\alpha\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right) + \text{stO}(|x, y\rangle \otimes |\epsilon_1\rangle). \tag{35}
\end{aligned}$$

Note that, from (34) it follows that

$$U_{\text{enc}} \left( |0\|\alpha\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right) + |\epsilon_1\rangle \right) = |D \cup (x, \alpha)\rangle. \tag{36}$$



Therefore

$$\begin{aligned}
& (I \otimes U_{\text{enc}}) \text{stO} (I \otimes U_{\text{enc}}^* |x, y\rangle \otimes |D \cup (x, \alpha)\rangle) \\
&= (I \otimes U_{\text{enc}}) \left( |x, y \oplus \alpha\rangle \otimes |0\rangle |\alpha\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0}^n\rangle \right) + \text{stO}(|x, y\rangle \otimes |\epsilon_1\rangle) \right) \\
&= (I \otimes U_{\text{enc}}) \left( |x, y \oplus \alpha\rangle \otimes |0\rangle |\alpha\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0}^n\rangle \right) + |x, y \oplus \alpha\rangle \otimes |\epsilon_1\rangle \right) \\
&\quad - (I \otimes U_{\text{enc}}) (|x, y \oplus \alpha\rangle \otimes |\epsilon_1\rangle) + (I \otimes U_{\text{enc}}) \text{stO}(|x, y\rangle \otimes |\epsilon_1\rangle) \\
&= |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle + |\epsilon_2\rangle \tag{37}
\end{aligned}$$

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

$$\begin{aligned}
& (I \otimes U_{\text{enc}}) \text{stO}(|x, y\rangle \otimes |\epsilon_1\rangle) \\
&= (I \otimes \text{CH} \cdot U_{\text{toggle}} \cdot \text{IH}) \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes (|1\rangle - |0\rangle) \\
&\quad \otimes |\gamma\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0}^n\rangle \right) \\
&= (I \otimes \text{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) \\
&\quad \otimes |\delta\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |0^n\rangle \right) \\
&= (I \otimes \text{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 \text{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 (|0\rangle \otimes (H^{\otimes n} |\gamma\rangle) - |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 (|1\rangle \otimes (H^{\otimes n} |0^n\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 |0\rangle \otimes (H^{\otimes n} |\gamma\rangle) \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)
\end{aligned}$$

$$\begin{aligned}
& + \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) \\
& - \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) \\
& + \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) \\
& + \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) \\
& - \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) \\
& + \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 |D_{\gamma}^{\text{invalid}}\rangle \\
& + \frac{1}{2^n} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |D\rangle \\
& - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |D \cup (x, \gamma)\rangle \\
& + \frac{2}{2^n} |x\rangle |\widehat{0}^n\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 (|D \cup (x, \gamma)\rangle - |D_{\gamma}^{\text{invalid}}\rangle) \\
& + \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), \tag{38}
\end{aligned}$$

where  $|D_{\gamma}^{\text{invalid}}\rangle$  is a superposition of invalid databases for each  $\gamma$ .

In addition, we have that

$$U_{\text{enc}} |\epsilon_1\rangle = (\text{CHU}_{\text{toggle}} \text{IH}) \frac{1}{\sqrt{2^n}} (|1\rangle - |0\rangle) |\widehat{0}^n\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0}^n\rangle \right)$$

$$\begin{aligned}
&= \text{CH} \frac{1}{\sqrt{2^n}} (|1\rangle - |0\rangle) |0^n\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |0^n\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} (|1\rangle |\widehat{0^n}\rangle - |0\rangle |0^n\rangle) \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |0^n\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle - \frac{1}{\sqrt{2^n}} |D\rangle \tag{39}
\end{aligned}$$

holds. Thus

$$(I \otimes U_{\text{enc}}) |x, y \oplus \alpha\rangle \otimes |\epsilon_1\rangle = \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \left( \left( \sum_{\gamma} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) - |D\rangle \right) \tag{40}$$

holds. Therefore

$$\begin{aligned}
&\text{RstOE} |x, y\rangle \otimes |D \cup (x, \alpha)\rangle \\
&= |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle \\
&\quad + \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \left( |D\rangle - \left( \sum_{\gamma} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) \right) \\
&\quad - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes (|D \cup (x, \gamma)\rangle - |D_{\gamma}^{\text{invalid}}\rangle) \\
&\quad + \frac{1}{2^n} |x\rangle |\widehat{0^n}\rangle \otimes \left( 2 \sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right) \tag{41}
\end{aligned}$$

holds, and this proves the second property.

Finally, we show the third 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 for the case that  $D$  has no entry. In addition, we can without loss of generality assume that  $x = 0^m$ . Now  $D$  corresponds to the bit string  $(0\|0^n)\|(0\|0^n)\|\dots\|(0\|0^n)$ , and we have that

$$\begin{aligned}
U_{\text{enc}}^* |D\rangle &= \text{IH}U_{\text{toggle}}\text{CH} |D\rangle \\
&= \left( \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |0\rangle |\alpha\rangle \right) \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right). \tag{42}
\end{aligned}$$

Hence it holds that

$$\text{stO}(I \otimes U_{\text{enc}}^*) |x, y\rangle \otimes |D\rangle = \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \otimes |0\rangle |\alpha\rangle \otimes \left( \bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right). \tag{43}$$

In addition, we have that

$$\begin{aligned}
& (I \otimes U_{\text{enc}}) \text{stO}(I \otimes U_{\text{enc}}^*) |x, y\rangle \otimes |D\rangle \\
&= (I \otimes (\text{CH}U_{\text{toggle}}\text{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) \\
&= (I \otimes (\text{CH}U_{\text{toggle}})) \left( \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \right. \\
&\quad \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) \\
&= (I \otimes \text{CH}) \left( \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \right. \\
&\quad \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 \text{CH}) \left( \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \right. \\
&\quad \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) \tag{44}
\end{aligned}$$

holds. Therefore the third property also holds.  $\square$

## B Proof of Lemma 1

This section proves Lemma 1. First we show the following lemma, which shows that the behavior of  $O'_{\text{UP},3}$  for  $D_F$  without overlap is the same as that of  $O_{\text{UP},3}$  for  $[D_F]_3$ . In this section we omit writing the additional  $q$  qubits that are introduced

to write detection results for  $\text{LR}_3\text{-det}$  and  $\text{LR}'_3\text{-det}$ , and the  $2n$  ancillary qubits that are used to compute the intermediate states after the first and second rounds (see (21) and (22)), as long as they are  $|0^a\rangle$  and  $|0^{2n}\rangle$ , respectively, for short.

**Lemma 3.** *It holds that*

$$\begin{aligned} & \langle x'_{2L}, x'_{2R}, y'_L, y'_R | \otimes \langle D'_F | O'_{\text{UP}.3} | x_{2L}, x_{2R}, y_L, y_R \rangle \otimes |D_F\rangle \\ &= \langle x'_{2L}, x'_{2R}, y'_L, y'_R | \otimes \langle [D'_F]_3 | O_{\text{UP}.3} | x_{2L}, x_{2R}, y_L, y_R \rangle \otimes |[D_F]_3 \rangle \end{aligned} \quad (45)$$

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  $O'_{\text{UP}.3}$  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  $(x_{2L}, x_{2R}, \alpha)$ , or (2)  $D_F$  has no entry.

First we show the claim for the first case that  $D_F = \{(x_{2L}, x_{2R}, \alpha)\}$ . In this case, by Proposition 1 we have that

$$\begin{aligned} & O'_{\text{UP}.3} |x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |D_F\rangle \\ &= |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, x_{2R}, \alpha)\rangle \\ &+ \frac{1}{\sqrt{2^n}} |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left( |\emptyset\rangle - \left( \sum_{\gamma} \frac{1}{\sqrt{2^n}} |(x_{2L}, x_{2R}, \gamma)\rangle \right) \right) \\ &- \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x_{2L}, x_{2R}, y_L \oplus \gamma, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, x_{2R}, \gamma)\rangle \\ &+ \frac{1}{2^n} |x_{2L}, x_{2R}\rangle |\widehat{0^n}\rangle |y_R \oplus x_{2L}\rangle \otimes \left( 2 \sum_{\delta} \frac{1}{\sqrt{2^n}} |(x_{2L}, x_{2R}, \delta)\rangle - |\emptyset\rangle \right) \\ &+ |\text{invalid}\rangle \end{aligned} \quad (46)$$

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

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

$$\begin{aligned}
&= |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \alpha)]_3\rangle \\
&\quad + \frac{1}{\sqrt{2^n}} |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left( |\emptyset\rangle - \left( \sum_{\gamma} \frac{1}{\sqrt{2^n}} |[(x_{2L}, x_{2R}, \gamma \oplus x_{2R})]_3\rangle \right) \right) \\
&\quad - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x_{2L}, x_{2R}, y_L \oplus \gamma \oplus x_{2R}, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \gamma \oplus x_{2R})]_3\rangle \\
&\quad + \frac{1}{2^n} |x_{2L}, x_{2R}\rangle |\widehat{0^n}\rangle |y_R \oplus x_{2L}\rangle \otimes \left( 2 \sum_{\delta} \frac{1}{\sqrt{2^n}} |[(x_{2L}, x_{2R}, \delta \oplus x_{2R})]_3\rangle - |\emptyset\rangle \right) \\
&\quad + |\text{invalid}'\rangle \\
&= |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \alpha)]_3\rangle \\
&\quad + \frac{1}{\sqrt{2^n}} |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left( |\emptyset\rangle - \left( \sum_{\gamma} \frac{1}{\sqrt{2^n}} |[(x_{2L}, x_{2R}, \gamma)]_3\rangle \right) \right) \\
&\quad - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x_{2L}, x_{2R}, y_L \oplus \gamma, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \gamma)]_3\rangle \\
&\quad + \frac{1}{2^n} |x_{2L}, x_{2R}\rangle |\widehat{0^n}\rangle |y_R \oplus x_{2L}\rangle \otimes \left( 2 \sum_{\delta} \frac{1}{\sqrt{2^n}} |[(x_{2L}, x_{2R}, \delta)]_3\rangle - |\emptyset\rangle \right) \\
&\quad + |\text{invalid}'\rangle, \tag{47}
\end{aligned}$$

where  $|\text{invalid}'\rangle$  is a vector containing invalid databases. From (46) and (47), 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 that  $D_F$  is empty by straightforward calculations using the third property of Proposition 1.  $\square$

Next we show the following lemma, which shows that the behavior of  $\text{LR}'_3$  for good databases is the same as that of  $\text{LR}_3$ .

**Lemma 4.** *It holds that*

$$\begin{aligned}
&\langle x'_{0L}, x'_{0R}, y'_L, y'_R | \otimes \langle D'_1, D'_2, D'_F | O_{\text{LR}'_3} | x_{0L}, x_{0R}, y_L, y_R \rangle \otimes |D_1, D_2, D_F\rangle \\
&= \langle x'_{0L}, x'_{0R}, y'_L, y'_R | \otimes \langle D'_1, D'_2, [D'_F]_3 | O_{\text{LR}_3} | x_{0L}, x_{0R}, y_L, y_R \rangle \otimes |D_1, D_2, [D_F]_3\rangle \tag{48}
\end{aligned}$$

for any  $x_{0L}, x_{0R}, y_L, y_R, x'_{0L}, x'_{0R}, y'_L, y'_R \in \{0, 1\}^{n/2}$  and any valid and good databases  $(D_1, D_2, D_F)$  and  $(D'_1, D'_2, D'_F)$  for  $\text{LR}'_3$ .

*Proof.* Note that  $O_{\text{UP}.i} = O_{\text{UP}.i}^*$  for  $i = 1, 2$ , and recall that

$$O_{\text{LR}_3} = (O_{\text{UP}.2} O_{\text{UP}.1})^* O_{\text{UP}.3} (O_{\text{UP}.2} O_{\text{UP}.1})$$

and

$$O_{\text{LR}'_3} = (O_{\text{UP}.2} O_{\text{UP}.1})^* O'_{\text{UP}.3} (O_{\text{UP}.2} O_{\text{UP}.1})$$

hold (see Fig. 6). Since  $O_{\text{UP}.1}$  and  $O_{\text{UP}.2}$  do not affect the  $D_3$  and  $D_F$  registers, the claim follows from Lemma 3.  $\square$

Next we show Lemma 1. Actually we prove a stronger claim below.

**Lemma 5.** *For each  $i$ , there exists a complex number  $a_{xyzD_1D_2D_F}^{(i)}$  for each tuple  $(x, y, z)$  (here  $x$  and  $y$  correspond to the query and answer registers of  $\mathcal{A}$ , and  $z$  corresponds to the remaining register of  $\mathcal{A}$ ), such that*

$$\sum_{\substack{x,y,z \\ (D_1,D_2,D_F):\text{good}}} |a_{xyzD_1D_2D_F}^{(i)}|^2 \leq 1$$

holds, in addition that

$$|\psi_i^{\text{good}}\rangle = \sum_{\substack{xyz \\ (D_1,D_2,D_F):\text{good}}} a_{xyzD_1D_2D_F}^{(i)} |x, y, z\rangle \otimes |D_1\rangle |D_2\rangle |D_F\rangle \quad (49)$$

and

$$|\psi_i^{\text{good}}\rangle = \sum_{\substack{xyz \\ (D_1,D_2,D_F):\text{good}}} a_{xyzD_1D_2D_F}^{(i)} |x, y, z\rangle \otimes |D_1\rangle |D_2\rangle |[D_F]_3\rangle \quad (50)$$

hold. In particular,

$$\text{tr}_{\mathcal{D}_{123}} \left( |\psi_i^{\text{good}}\rangle \langle \psi_i^{\text{good}}| \right) = \text{tr}_{\mathcal{D}_{12F}} \left( |\psi_i^{\text{good}}\rangle \langle \psi_i^{\text{good}}| \right) \quad (51)$$

holds for  $1 \leq i \leq q + 1$ .

*Proof.* We show the claim by induction. Since all databases are empty before the first query, the claim holds for  $i = 2$  (i.e., the claim holds for  $|\psi_1^{\text{good}}\rangle$  and  $|\psi_1^{\text{good}}\rangle$ ). Assume that the claim holds for  $i$ . We show the claim also holds for  $(i + 1)$ .

Recall that for each good database  $(D_1, D_2, D_3)$  for  $\text{LR}_3$ , there exists a unique  $D_F$  without overlap such that  $[D_F]_3 = D_3$  and  $(D_1, D_2, D_F)$  is a good database for  $\text{LR}'_3$ , by definition of good databases. Similarly, for each good database  $(D_1, D_2, D_F)$  for  $\text{LR}'_3$ ,  $(D_1, D_2, [D_F]_3)$  becomes a good database for  $\text{LR}_3$ . Thus, there exists  $a_{xyzD_1D_2D_F}^{(i+1)}$  and  $b_{xyzD_1D_2D_F}^{(i+1)}$  for each tuple  $(x, y, z)$  and good  $(D_1, D_2, D_F)$  such that

$$\sum_{\substack{x,y,z \\ (D_1,D_2,D_F):\text{good}}} |a_{xyzD_1D_2D_F}^{(i+1)}|^2, \quad \sum_{\substack{x,y,z \\ (D_1,D_2,D_F):\text{good}}} |b_{xyzD_1D_2D_F}^{(i+1)}|^2 \leq 1.$$

holds, in addition that

$$|\psi_{i+1}^{\text{good}}\rangle = \sum_{\substack{xyz \\ (D_1,D_2,D_F):\text{good}}} a_{xyzD_1D_2D_F}^{(i+1)} |x, y, z\rangle \otimes |D_1\rangle |D_2\rangle |D_F\rangle \quad (52)$$

and

$$|\psi_{i+1}^{\text{good}}\rangle = \sum_{\substack{xyz \\ (D_1,D_2,D_F):\text{good}}} b_{xyzD_1D_2D_F}^{(i+1)} |x, y, z\rangle \otimes |D_1\rangle |D_2\rangle |[D_F]_3\rangle \quad (53)$$

hold.

Since  $|\psi'_{i+1}{}^{\text{good}}\rangle = (I - \Pi_{\text{bad}}) \cdot O_{\text{LR}'_3} |\psi'_i{}^{\text{good}}\rangle$  holds, we have that

$$\begin{aligned}
& a_{xyzD_1D_2D_F}^{(i+1)} \\
&= \langle x, y, z | \langle D_1, D_2, D_F | (I - \Pi_{\text{bad}}) \cdot O_{\text{LR}'_3} |\psi'_i{}^{\text{good}}\rangle \\
&= \sum_{\substack{x'y'z' \\ (D'_1, D'_2, D'_F): \text{good}}} a_{x'y'z'D'_1D'_2D'_F}^{(i)} \langle x, y, z | \langle D_1, D_2, D_F | O_{\text{LR}'_3} |x', y', z'\rangle |D'_1, D'_2, D'_F\rangle
\end{aligned} \tag{54}$$

holds for good  $(D_1, D_2, D_F)$ . In addition, since  $|\psi_{i+1}{}^{\text{good}}\rangle = (I - \Pi_{\text{bad}}) \cdot O_{\text{LR}_3} |\psi_i{}^{\text{good}}\rangle$  holds, we have that

$$\begin{aligned}
& b_{xyzD_1D_2D_F}^{(i+1)} \\
&= \langle x, y, z | \langle D_1, D_2, [D_F]_3 | (I - \Pi_{\text{bad}}) \cdot O_{\text{LR}_3} |\psi_{i-1}{}^{\text{good}}\rangle \\
&= \sum_{\substack{x'y'z' \\ (D'_1, D'_2, D'_F): \text{good}}} a_{x'y'z'D'_1D'_2D'_F}^{(i)} \langle x, y, z | \langle D_1, D_2, [D_F]_3 | O_{\text{LR}'_3} |x', y', z'\rangle |D'_1, D'_2, [D'_F]_3\rangle
\end{aligned} \tag{55}$$

holds for good  $(D_1, D_2, D_F)$ .

From Lemma 4, the right hand side of (54) is equal to that of (55). Thus  $b_{xyzD_1D_2D_F}^{(i+1)} = a_{xyzD_1D_2D_F}^{(i+1)}$  holds for each  $x, y, z$  and each good  $(D_1, D_2, D_F)$ . Therefore the claim also holds for  $(i + 1)$ , which completes the proof.  $\square$

## C Proof of Lemma 2

*Proof (of Lemma 2).* We show that the claim holds for  $\text{LR}_3$  and  $|\psi_j{}^{\text{good}}\rangle$ . The claim for  $\text{LR}'_3$  and  $|\psi'_j{}^{\text{good}}\rangle$  can be shown in a similar way. In this proof we omit writing the additional  $q$  qubits that are introduced to write detection results for  $\text{LR}_3\text{-det}$  and  $\text{LR}'_3\text{-det}$ , and the  $2n$  ancillary qubits that are used to compute the intermediate states after the first and second rounds (see (21) and (22)), as long as they are  $|0^q\rangle$  and  $|0^{2n}\rangle$ , respectively, for short. Remember that the oracle of  $\text{LR}_3$  is decomposed as  $O_{\text{LR}_3} = O_{\text{UP}.1} \cdot O_{\text{UP}.2} \cdot O_{\text{UP}.3} \cdot O_{\text{UP}.2} \cdot O_{\text{UP}.1}$ . Since the computational basis is the orthonormal basis, it suffices to show that the claim holds for the case  $|\psi_j{}^{\text{good}}\rangle = |x_0, y, z\rangle \otimes |D_1\rangle |D_2\rangle |D_3\rangle$  for each  $x = x_{0L} \| x_{0R}, y = y_L \| y_R, z$  ( $x$  and  $y$  correspond to  $\mathcal{A}$ 's first and second  $n$ -qubit register, respectively, and  $z$  correspond to  $\mathcal{A}$ 's remaining register), and each good database  $(D_1, D_2, D_3)$ . Note that  $|D_1|, |D_2| \leq 2(j-1)$  and  $|D_3| \leq j-1$  hold, since each query to the recording standard oracle with errors  $\text{RstOE}$  affects only the qubits that correspond to a single entry of each database. Since  $O_{\text{LR}_3}$  does not affect the  $|z\rangle$  register, for simplicity, we omit writing it in this proof.

We consider three separate cases I, II, and III, and study how the quantum state will change when  $O_{\text{UP}.1}, O_{\text{UP}.2}, O_{\text{UP}.3}, O_{\text{UP}.2}, O_{\text{UP}.1}$ , and  $\Pi_{\text{bad}}$  act on



$|\psi_j^{\text{good}}\rangle$ , in a sequential order. Case I is the one that  $(x_{0L}, \alpha) \in D_1$  and  $(x_{0R} \oplus \alpha, \beta) \in D_2$  for some  $\alpha$  and  $\beta$ . Case II is the one that  $(x_{0L}, \alpha) \in D_1$  for some  $\alpha$  and there is no entry of  $x_{0R} \oplus \alpha$  in  $D_2$ . Case III is the one that there is no entry of  $x_{0L}$  in  $D_1$ .

*Remark 3.* Intuitively, Case I is the case that the queries to  $f_1$  and  $f_2$  are not fresh. Case II is the one that the query to  $f_1$  is not fresh but the query to  $f_2$  is fresh. Case III is the one that the query to  $f_1$  is fresh.

**Case I:**  $(x_{0L}, \alpha) \in D_1$  and  $(x_{0R} \oplus \alpha, \beta) \in D_2$  for some  $\alpha$  and  $\beta$ .

In this case, after the first query to  $O_{\text{UP},2}$ , by Proposition 1 the whole quantum state becomes

$$|x_{0L}, x_{0R}, y_L, y_R\rangle \otimes |D_1\rangle |D_2\rangle |D_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle, \quad (56)$$

with an error in  $O(\sqrt{1/2^{n/2}})$ . Here  $x_{1L} = x_{0R} \oplus \alpha$ ,  $x_{1R} = x_{0L}$ ,  $x_{2L} = x_{1R} \oplus \beta$ , and  $x_{2R} = x_{1L}$ . We further separate Case I into two sub-cases Case I-i and Case I-ii.

**Case I-i:**  $(x_{2L}, \gamma) \in D_3$  for some  $\gamma$ .

Let  $x_{3L} := x_{2R} \oplus \gamma$  and  $x_{3R} := x_{2L}$ . Then, after the final query to  $O_{\text{UP},1}$ , by Proposition 1 the whole quantum state becomes

$$|x_{0L}, x_{0R}, y_L \oplus x_{3L}, y_R \oplus x_{3L}\rangle \otimes |D_1\rangle |D_2\rangle |D_3\rangle \quad (57)$$

with errors in  $O(\sqrt{1/2^{n/2}})$ . In particular, the database remains good with an error in  $O(\sqrt{1/2^{n/2}})$ . Therefore  $\Pi_{\text{bad}} \cdot O_{\text{LR}_3} |\psi_j^{\text{good}}\rangle = 0$  with an error in  $O(\sqrt{1/2^{n/2}})$ , which implies that the claim holds for this Case I-i.

**Case I-ii: There is no entry of  $x_{2L}$  in  $D_3$ .**

In this case, after the query to  $O_{\text{UP},3}$ , by Proposition 1 the whole quantum state becomes

$$\sum_{\gamma} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L \oplus (x_{2R} \oplus \gamma), y_R \oplus x_{2L}\rangle \otimes |D_1\rangle |D_2\rangle |D_3 \cup (x_{2L}, \gamma)\rangle \otimes |x_{1L}, x_{1R}\rangle |x_{2L}, x_{2R}\rangle \quad (58)$$

with an error in  $O(\sqrt{1/2^{n/2}})$ . Thus, after the final query to  $O_{\text{UP},1}$ , each normalized summand of (58) becomes

$$|x_{0L}, x_{0R}, y_L \oplus (x_{2R} \oplus \gamma), y_R \oplus x_{2L}\rangle \otimes |D_1\rangle |D_2\rangle |D_3 \cup (x_{2L}, \gamma)\rangle \quad (59)$$

with an error in  $O(\sqrt{1/2^{n/2}})$ . In particular, the database of (59) remains good. Therefore (59) becomes 0 with an error in  $O(\sqrt{1/2^{n/2}})$  after the operation of  $\Pi_{\text{bad}}$ , with an error in  $O(\sqrt{1/2^{n/2}})$ . Since the summands of (58) are orthogonal to each other,  $\Pi_{\text{bad}} \cdot O_{\text{LR}_3} |\psi_j^{\text{good}}\rangle = 0$  with an error in  $O(\sqrt{1/2^{n/2}})$ , which implies that the claim holds for this Case I-ii.

**Case II:**  $(x_{0L}, \alpha) \in D_1$  for some  $\alpha$  and there is no entry of  $x_{0R} \oplus \alpha$  in  $D_2$ . Again, let  $x_{1L} := x_{0R} \oplus \alpha$  and  $x_{1R} := x_{0L}$ . In this case, after the first query to  $O_{UP.2}$ , by Proposition 1 the whole quantum state becomes

$$\begin{aligned}
& \sum_{\beta} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \\
& \quad \otimes |D_1\rangle |D_2 \cup (x_{1L}, \beta)\rangle |D_3\rangle \otimes |x_{1L}, x_{1R}\rangle |\beta \oplus x_{1R}, x_{2R}\rangle \\
= & \sum_{\substack{\beta: \exists \text{ an entry of} \\ \beta \oplus x_{1R} \text{ in } D_3}} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \\
& \quad \otimes |D_1\rangle |D_2 \cup (x_{1L}, \beta)\rangle |D_3\rangle \otimes |x_{1L}, x_{1R}\rangle |\beta \oplus x_{1R}, x_{2R}\rangle \quad (60) \\
+ & \sum_{\substack{\beta: \nexists \text{ an entry of} \\ \beta \oplus x_{1R} \text{ in } D_3}} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \\
& \quad \otimes |D_1\rangle |D_2 \cup (x_{1L}, \beta)\rangle |D_3\rangle \otimes |x_{1L}, x_{1R}\rangle |\beta \oplus x_{1R}, x_{2R}\rangle, \quad (61)
\end{aligned}$$

where  $x_{2R} = x_{1L}$ , with an error in  $O(\sqrt{1/2^{n/2}})$ . Below we further separate Case II into sub-cases Case II-i and Case II-ii. Case II-i is the case that there exists an entry of  $\beta \oplus x_{1R}$  in  $D_3$ , which corresponds to the term (60). Case II-ii is the case that there exists no entry of  $\beta \oplus x_{1R}$  in  $D_3$ , which corresponds to the term (61).

**Case II-i:**  $(\beta \oplus x_{1R}, \gamma) \in D_3$  for some  $\gamma$ .

Let us denote the term (60) by |II-i>. Then, since  $|D_3| \leq j - 1$  holds,

$$|\{\beta \mid \exists \text{ an entry of } \beta \oplus x_{1R} \text{ in } D_3\}| \leq j - 1$$

follows. In addition, since the summands of (60) are orthogonal to each other,  $\|\text{II-i}\|^2 \leq O(j/2^{n/2})$  holds. Therefore  $\|\text{II-i}\| \leq O(\sqrt{j/2^{n/2}})$  follows.

**Case II-ii:** There is no entry of  $\beta \oplus x_{1R}$  in  $D_3$ .

After the operation of  $O_{UP.3}$ , by Proposition 1 each normalized summand of the term (61) becomes

$$\begin{aligned}
& \sum_{\gamma} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L \oplus (x_{2R} \oplus \gamma), y_R \oplus x_{2L}\rangle \\
& \quad \otimes |D_1\rangle |D_2 \cup (x_{1L}, \beta)\rangle |D_3 \cup (x_{2L}, \gamma)\rangle \\
& \quad \otimes |x_{1L}, x_{1R}\rangle |x_{2L}, x_{2R}\rangle \quad (62)
\end{aligned}$$

with an error in  $O(\sqrt{1/2^{n/2}})$ , where  $x_{2L} = \beta \oplus x_{1R}$ . Thus, after the last operations of  $O_{UP.2}$  and  $O_{UP.1}$ , each normalized summand of the term (62) becomes

$$|x_{0L}, x_{0R}, y_L \oplus (x_{2R} \oplus \gamma), y_R \oplus x_{2L}\rangle \otimes |D_1\rangle |D_2 \cup (x_{1L}, \beta)\rangle |D_3 \cup (x_{2L}, \gamma)\rangle \quad (63)$$

with an error in  $O(\sqrt{1/2^{n/2}})$ . In particular, the database of the term (63) is good with an error in  $O(\sqrt{1/2^{n/2}})$ , which implies that the term (63) becomes 0 with

an error in  $O(\sqrt{1/2^{n/2}})$  after the operation of  $\Pi_{\text{bad}}$ . Hence, due to orthogonality of each summands, the term (62) will be 0 after the operations of  $O_{\text{UP},2}$ ,  $O_{\text{UP},1}$ , and  $\Pi_{\text{bad}}$ , with an error in  $O(\sqrt{1/2^{n/2}})$ . Therefore, due to orthogonality of each summands, the term (61) will be 0 after the operations of  $O_{\text{UP},3}$ ,  $O_{\text{UP},2}$ ,  $O_{\text{UP},1}$ , and  $\Pi_{\text{bad}}$ , with an error in  $O(\sqrt{1/2^{n/2}})$ .

Combining analyses of Cases II-i and II-ii,

$$\left\| \Pi_{\text{bad}} \cdot O_{\text{LR}_3} |\psi_j^{\text{good}}\rangle \right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \quad (64)$$

follows in Case II.

**Case III: there is no entry of  $x_{0L}$  in  $D_1$ .**

In this case, after the first query to  $O_{\text{UP},1}$ , by Proposition 1 the whole quantum state becomes

$$\begin{aligned} & \sum_{\alpha} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \otimes |D_1 \cup (x_{0L}, \alpha)\rangle |D_2\rangle |D_3\rangle \otimes |x_{0R} \oplus \alpha, x_{0L}\rangle \\ &= \sum_{\alpha: \exists (\alpha \oplus x_{0R})\text{-entry in } D_2} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \\ & \quad \otimes |D_1 \cup (x_{0L}, \alpha)\rangle |D_2\rangle |D_3\rangle \otimes |x_{0R} \oplus \alpha, x_{0L}\rangle \quad (65) \end{aligned}$$

$$\begin{aligned} &+ \sum_{\alpha: \nexists (\alpha \oplus x_{0R})\text{-entry in } D_2} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \\ & \quad \otimes |D_1 \cup (x_{0L}, \alpha)\rangle |D_2\rangle |D_3\rangle \otimes |x_{0R} \oplus \alpha, x_{0L}\rangle \quad (66) \end{aligned}$$

with an error in  $O(\sqrt{1/2^{n/2}})$ .

Below we further separate Case III into sub-cases Case III-i and Case III-ii. Case III-i is the case that there exists an entry of  $\alpha \oplus x_{0R}$  in  $D_2$ , which corresponds to the term (65). Case III-ii is the case that there exists no entry of  $\alpha \oplus x_{0R}$  in  $D_2$ , which corresponds to the term (66).

**Case III-i:  $(\alpha \oplus x_{0R}, \beta) \in D_2$  for some  $\beta$ .**

Since  $|D_2| \leq 2(j-1)$ , we have that

$$\begin{aligned} & \left\| \sum_{\alpha: \exists (\alpha \oplus x_{0R})\text{-entry in } D_2} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \right. \\ & \quad \left. \otimes |D_1 \cup (x_{0L}, \alpha)\rangle |D_2\rangle |D_3\rangle \otimes |x_{0R} \oplus \alpha, x_{0L}\rangle \right\|^2 \\ &= \frac{1}{2^{n/2}} \cdot |\{\alpha | \exists \beta \text{ s.t. } (\alpha \oplus x_{0R}, \beta) \in D_2\}| \leq O\left(\frac{j}{2^{n/2}}\right) \quad (67) \end{aligned}$$

holds. Hence the norm of (65) is upper bounded by  $O(\sqrt{j/2^{n/2}})$ .

**Case III-ii: There is no entry of  $(\alpha \oplus x_{0R})$  in  $D_2$ .**

Let  $x_{1L} := x_{0R} \oplus \alpha$  and  $x_{1R} := x_{0L}$ . After the operation of the  $O_{UP,2}$ , each normalized summand of (66) changes to

$$\begin{aligned} & \sum_{\beta} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \\ & \quad \otimes |D_1 \cup (x_{0L}, \alpha)\rangle |D_2 \cup (x_{1L}, \beta)\rangle |D_3\rangle \otimes |x_{1L}, x_{1R}\rangle |x_{1R} \oplus \beta, x_{1L}\rangle \\ = & \sum_{\beta: \exists (\beta \oplus x_{1R})\text{-entry in } D_3} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \\ & \quad \otimes |D_1 \cup (x_{0L}, \alpha)\rangle |D_2 \cup (x_{1L}, \beta)\rangle |D_3\rangle \otimes |x_{1L}, x_{1R}\rangle |x_{1R} \oplus \beta, x_{1L}\rangle \end{aligned} \quad (68)$$

$$\begin{aligned} + & \sum_{\beta: \exists (\beta \oplus x_{1R})\text{-entry in } D_3} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L, y_R\rangle \\ & \quad \otimes |D_1 \cup (x_{0L}, \alpha)\rangle |D_2 \cup (x_{1L}, \beta)\rangle |D_3\rangle \otimes |x_{1L}, x_{1R}\rangle |x_{1R} \oplus \beta, x_{1L}\rangle. \end{aligned} \quad (69)$$

Since  $|D_3| \leq j - 1$ , we can show that the norm of (68) is in  $O(\sqrt{j/2^{n/2}})$ , in the same way as we showed the norm of (65) is in  $O(\sqrt{j/2^{n/2}})$ .

Next we focus on the term (69). After the operation of  $O_{UP,3}$ , each normalized summand of (69) becomes

$$\begin{aligned} & \sum_{\gamma} \sqrt{\frac{1}{2^{n/2}}} |x_{0L}, x_{0R}, y_L \oplus (\gamma \oplus x_{2R}), y_R \oplus x_{2L}\rangle \\ & \quad \otimes |D_1 \cup (x_{0L}, \alpha)\rangle |D_2 \cup (x_{1L}, \beta)\rangle |D_3 \cup (x_{2L}, \gamma)\rangle \otimes |x_{1L}, x_{1R}\rangle |x_{2L}, x_{2R}\rangle, \end{aligned} \quad (70)$$

where  $x_{2L} = x_{1R} \oplus \beta$  and  $x_{2R} = x_{1L}$ . Note that the database of each summand of (70) is good. Thus, after the operations of  $O_{UP,2}$ ,  $O_{UP,1}$ , and  $\Pi_{\text{bad}}$ , each summand of (70) becomes 0 with an error in  $O(\sqrt{1/2^{n/2}})$ , by Proposition 1. Therefore, since the summands of (70) are orthogonal to each other, (70) becomes 0 with an error in  $O(\sqrt{1/2^{n/2}})$  after the operations of  $O_{UP,2}$ ,  $O_{UP,1}$ , and  $\Pi_{\text{bad}}$ . Hence it follows that (69) becomes 0 with an error in  $O(\sqrt{1/2^{n/2}})$  after the operations of  $O_{UP,3}$ ,  $O_{UP,2}$ ,  $O_{UP,1}$ , and  $\Pi_{\text{bad}}$ , since the summands of (69) are orthogonal to each other.

From analyses of Cases III-i and III-ii, it follows that

$$\left\| \Pi_{\text{bad}} \cdot O_{LR_3} |\psi_j^{\text{good}}\rangle \right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \quad (71)$$

also holds in Case III. □

## D Proof of Proposition 3

*Proof (of Proposition 3).* Recall that  $|\psi_i\rangle$  and  $|\psi'_i\rangle$  are the states just before the  $i$ -th query to LR<sub>3</sub>-det and LR'<sub>3</sub>-det, respectively. By abuse of notation, we let  $|\psi_{(q+1)}\rangle, |\psi'_{(q+1)}\rangle$  denote the quantum states  $(U_q \otimes I)O_{\text{LR}_3\text{-det}}|\psi_q\rangle$  and  $(U_q \otimes I)O_{\text{LR}'_3\text{-det}}|\psi'_q\rangle$ , respectively. Moreover, let  $|\phi_{(q+1)}\rangle, |\phi'_{(q+1)}\rangle$  be the states just before the final measurements for the cases that the adversary  $\mathcal{A}$  runs relative to LR<sub>3</sub>-det and LR'<sub>3</sub>-det, respectively. Since now we are considering that the random functions  $f_1, f_2, f_3, F$  are implemented by the recording standard oracle with errors, there are unitary operators  $U_{\text{FinDec}}^{123}$  and  $U_{\text{FinDec}}^{12F}$  that acts on database registers such that  $|\phi_{q+1}\rangle = (I \otimes U_{\text{FinDec}}^{123})|\psi_{q+1}\rangle$  and  $|\phi'_{q+1}\rangle = (I \otimes U_{\text{FinDec}}^{12F})|\psi'_{q+1}\rangle$ . First, we have that

$$\begin{aligned} \text{Adv}_{\text{LR}_3\text{-det}, \text{LR}'_3\text{-det}}^{\text{dist}}(\mathcal{A}) &\leq \text{td} \left( \text{tr}_{\mathcal{D}_{123}} (|\phi_{(q+1)}\rangle), \text{tr}_{\mathcal{D}_{12F}} (|\phi'_{(q+1)}\rangle) \right) \\ &= \text{td} \left( \text{tr}_{\mathcal{D}_{123}} (|\psi_{(q+1)}\rangle), \text{tr}_{\mathcal{D}_{12F}} (|\psi'_{(q+1)}\rangle) \right) \end{aligned} \quad (72)$$

holds.

Now we show the following claim.

*Claim.* Let  $\rho$  be a mixed state of a joint quantum system  $\mathcal{H}_A \otimes \mathcal{H}_B$ . Let  $\Pi : \mathcal{H}_B \rightarrow \mathcal{H}_B$  be an orthogonal projector and  $U_{A1}, U_{A2} : \mathcal{H}_A \rightarrow \mathcal{H}_A$  be unitary operators. Define a unitary operator  $U : \mathcal{H}_A \otimes \mathcal{H}_B \rightarrow \mathcal{H}_A \otimes \mathcal{H}_B$  by  $U := U_{A1} \otimes \Pi + U_{A2} \otimes (I - \Pi)$ . Then

$$\begin{aligned} \text{tr}_B(U\rho U^*) &= \text{tr}_B((U_{A1} \otimes \Pi)\rho(U_{A1} \otimes \Pi)^*) \\ &\quad + \text{tr}_B((U_{A2} \otimes (I - \Pi))\rho(U_{A2} \otimes (I - \Pi))^*) \end{aligned} \quad (73)$$

holds, where  $\text{tr}_B$  is the partial trace over  $\mathcal{H}_B$ . In particular,

$$\text{tr}_B(U|\psi\rangle) = \text{tr}_B((U_{A1} \otimes \Pi)|\psi\rangle) + \text{tr}_B((U_{A2} \otimes (I - \Pi))|\psi\rangle) \quad (74)$$

holds for any pure state  $|\psi\rangle$  of  $\mathcal{H}_A \otimes \mathcal{H}_B$ .

*Proof.* First, we have that

$$\begin{aligned} \text{tr}_B(U\rho U^*) &= \text{tr}_B((U_{A1} \otimes \Pi)\rho(U_{A1} \otimes \Pi)^*) \\ &\quad + \text{tr}_B((U_{A2} \otimes (I - \Pi))\rho(U_{A2} \otimes (I - \Pi))^*) \\ &\quad + \text{tr}_B((U_{A1} \otimes \Pi)\rho(U_{A2} \otimes (I - \Pi))^*) \\ &\quad + \text{tr}_B((U_{A2} \otimes (I - \Pi))\rho(U_{A1} \otimes \Pi)^*) \end{aligned} \quad (75)$$

holds. Moreover, since  $(U_{A1} \otimes \Pi)\rho(U_{A2} \otimes (I - \Pi))^* = (U_{A1} \otimes I)(I \otimes \Pi)\rho(I \otimes (I - \Pi))^*(U_{A2} \otimes I)^*$  holds, it follows that

$$\begin{aligned} \text{tr}_B((U_{A1} \otimes \Pi)\rho(U_{A2} \otimes (I - \Pi))^*) &= U_{A1}\text{tr}_B((I \otimes \Pi)\rho(I \otimes (I - \Pi))^*)U_{A2}^* \\ &= U_{A1}\text{tr}_B((I \otimes \Pi)(I \otimes (I - \Pi))^*\rho)U_{A2}^* \end{aligned}$$

$$\begin{aligned}
&= U_{A1} \text{tr}_B (I \otimes (\Pi \cdot (I - \Pi))) \rho U_{A2}^* \\
&= 0,
\end{aligned} \tag{76}$$

and similarly we have that

$$\text{tr}_B ((U_{A2} \otimes (I - \Pi)) \rho (U_{A1} \otimes \Pi)^*) = 0. \tag{77}$$

The claim follows from (75), (76), and (77).  $\square$

Recall that  $(I - \Pi_{\text{flipped}}^{[i-1]}) |\psi_i\rangle$  and  $(I - \Pi_{\text{flipped}}^{[i-1]}) |\psi'_i\rangle$  are denoted by  $|\psi_i^{\text{good}}\rangle$  and  $|\psi'_i{}^{\text{good}}\rangle$ , respectively. In addition, let us denote  $\Pi_{\text{flipped}}^{[i-1]} |\psi_i\rangle$  and  $\Pi_{\text{flipped}}^{[i-1]} |\psi'_i\rangle$  by  $|\psi_i^{\text{bad}}\rangle$  and  $|\psi'_i{}^{\text{bad}}\rangle$ , respectively. Since  $|\psi_i\rangle = U_{i-1} \cdot O_{\text{LR}_3\text{-det}} |\psi_{i-1}\rangle$  and

$$\begin{aligned}
O_{\text{LR}_3\text{-det}} &= (\Pi_{\text{bad}} \otimes I_{i-1} \otimes X + (I - \Pi_{\text{bad}}) \otimes I_{i-1} \otimes I_1) \\
&\quad \cdot (O_{\text{LR}_3} \otimes I_{i-1} \otimes I_1) \cdot ((I - \Pi_{\text{flipped}}^{[i-1]}) \otimes I_1) \\
&\quad + \Pi_{\text{flipped}}^{[i-1]} \otimes I_1
\end{aligned} \tag{78}$$

holds, from the above claim it follows that

$$\begin{aligned}
\text{tr}_{\mathcal{D}_{123}} (|\psi_i\rangle) &= \text{tr}_{\mathcal{D}_{123}} \left( U_{i-1} \cdot (\Pi_{\text{bad}} \otimes X + (I - \Pi_{\text{bad}}) \otimes I_1) \cdot O_{\text{LR}_3} \cdot |\psi_{i-1}^{\text{good}}\rangle \right) \\
&\quad + \text{tr}_{\mathcal{D}_{123}} (U_{i-1} \cdot |\psi_{i-1}^{\text{bad}}\rangle) \\
&= \text{tr}_{\mathcal{D}_{123}} \left( U_{i-1} \cdot (\Pi_{\text{bad}} \otimes X) \cdot O_{\text{LR}_3} \cdot |\psi_{i-1}^{\text{good}}\rangle \right) \\
&\quad + \text{tr}_{\mathcal{D}_{123}} \left( U_{i-1} \cdot ((I - \Pi_{\text{bad}}) \otimes I_1) \cdot O_{\text{LR}_3} \cdot |\psi_{i-1}^{\text{good}}\rangle \right) \\
&\quad + \text{tr}_{\mathcal{D}_{123}} (U_{i-1} \cdot |\psi_{i-1}^{\text{bad}}\rangle) + \rho + \rho^*,
\end{aligned} \tag{79}$$

where

$$\begin{aligned}
\rho &= \text{tr}_{\mathcal{D}_{123}} \left( U_{i-1} \cdot (\Pi_{\text{bad}} \otimes X) \cdot O_{\text{LR}_3} \cdot |\psi_{i-1}^{\text{good}}\rangle \langle \psi_{i-1}^{\text{good}}| \right. \\
&\quad \left. \cdot O_{\text{LR}_3}^* \cdot ((I - \Pi_{\text{bad}}) \otimes I_1)^* \cdot U_{i-1}^* \right).
\end{aligned} \tag{80}$$

Note that, for any Hilbert space  $L_1$  and  $L_2$ , and any Hermite operator  $A$  on  $L_1 \otimes L_2$ ,  $\|\text{tr}_{L_2}(\rho)\|_{\text{tr}} = \|\rho\|_{\text{tr}}$  holds. In addition,  $\| |\psi\rangle \langle \phi| \|_{\text{tr}} \leq \| |\psi\rangle \| \cdot \| |\phi\rangle \|$  holds for any vectors  $|\psi\rangle$  and  $|\phi\rangle$ . Thus we have that

$$\begin{aligned}
&\|\rho\|_{\text{tr}} \\
&= \left\| U_{i-1} \cdot (\Pi_{\text{bad}} \otimes X) \cdot O_{\text{LR}_3} \cdot |\psi_{i-1}^{\text{good}}\rangle \langle \psi_{i-1}^{\text{good}}| \cdot O_{\text{LR}_3}^* \cdot ((I - \Pi_{\text{bad}}) \otimes I_1)^* \cdot U_{i-1}^* \right\|_{\text{tr}} \\
&\leq \left\| (\Pi_{\text{bad}} \otimes X) \cdot O_{\text{LR}_3} \cdot |\psi_{i-1}^{\text{good}}\rangle \right\| \cdot \left\| ((I - \Pi_{\text{bad}}) \otimes I_1) \cdot O_{\text{LR}_3} \cdot |\psi_{i-1}^{\text{good}}\rangle \right\| \\
&\leq \left\| (\Pi_{\text{bad}} \otimes X) \cdot O_{\text{LR}_3} \cdot |\psi_{i-1}^{\text{good}}\rangle \right\| \leq O \left( \sqrt{\frac{i}{2^{n/2}}} \right),
\end{aligned} \tag{81}$$

where we used the claim of Lemma 2 for the last inequality.

Similarly, for  $|\psi'_i\rangle$  we have that

$$\begin{aligned}\mathrm{tr}_{\mathcal{D}_{123}}(|\psi'_i\rangle) &= \mathrm{tr}_{\mathcal{D}_{123}}\left(U_{i-1} \cdot (\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}_3} \cdot |\psi'_{i-1}{}^{\mathrm{good}}\rangle\right) \\ &\quad \mathrm{tr}_{\mathcal{D}_{123}}\left(U_{i-1} \cdot ((I - \Pi_{\mathrm{bad}}) \otimes I_1) \cdot O_{\mathrm{LR}_3} \cdot |\psi'_{i-1}{}^{\mathrm{good}}\rangle\right) \\ &\quad + \mathrm{tr}_{\mathcal{D}_{123}}\left(U_{i-1} \cdot |\psi'_{i-1}{}^{\mathrm{bad}}\rangle\right) + \rho' + \rho'^*,\end{aligned}\tag{82}$$

where

$$\begin{aligned}\rho' &= \mathrm{tr}_{\mathcal{D}_{123}}\left(U_{i-1} \cdot (\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}_3} \cdot |\psi'_{i-1}{}^{\mathrm{good}}\rangle \langle \psi'_{i-1}{}^{\mathrm{good}}| \right. \\ &\quad \left. \cdot O_{\mathrm{LR}_3}^* \cdot ((I - \Pi_{\mathrm{bad}}) \otimes I_1)^* \cdot U_{i-1}^*\right),\end{aligned}\tag{83}$$

and

$$\|\rho'\|_{\mathrm{tr}} \leq O\left(\sqrt{\frac{i}{2^{n/2}}}\right)\tag{84}$$

holds.

Now we have that

$$\begin{aligned}\mathrm{td}(\mathrm{tr}_{\mathcal{D}_{123}}(|\psi_i\rangle), \mathrm{tr}_{\mathcal{D}_{12F}}(|\psi'_i\rangle)) &\leq \mathrm{td}\left(\mathrm{tr}_{\mathcal{D}_{123}}\left(U_{i-1} \cdot ((I - \Pi_{\mathrm{bad}}) \otimes I_1) \cdot O_{\mathrm{LR}_3} |\psi_{i-1}{}^{\mathrm{good}}\rangle\right), \right. \\ &\quad \left. \mathrm{tr}_{\mathcal{D}_{12F}}\left(U_{i-1} \cdot ((I - \Pi_{\mathrm{bad}}) \otimes I_1) \cdot O_{\mathrm{LR}'_3} |\psi'_{i-1}{}^{\mathrm{good}}\rangle\right)\right) \\ &\quad + \mathrm{td}\left(\mathrm{tr}_{\mathcal{D}_{123}}\left(U_{i-1} \cdot (\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}_3} |\psi_{i-1}{}^{\mathrm{good}}\rangle\right), \right. \\ &\quad \left. \mathrm{tr}_{\mathcal{D}_{12F}}\left(U_{i-1} \cdot (\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}'_3} |\psi'_{i-1}{}^{\mathrm{good}}\rangle\right)\right) \\ &\quad + \mathrm{td}\left(\mathrm{tr}_{\mathcal{D}_{123}}\left(U_{i-1} |\psi_{i-1}{}^{\mathrm{bad}}\rangle\right), \mathrm{tr}_{\mathcal{D}_{12F}}\left(U_{i-1} |\psi'_{i-1}{}^{\mathrm{bad}}\rangle\right)\right) \\ &\quad + \|\rho\|_{\mathrm{tr}} + \|\rho^*\|_{\mathrm{tr}} + \|\rho'\|_{\mathrm{tr}} + \|\rho'^*\|_{\mathrm{tr}}.\end{aligned}\tag{85}$$

In addition, since  $U_{i-1}$  affects only  $\mathcal{A}$ 's register, and  $\mathrm{td}$  is invariant under unitary transformations, we have that

$$\begin{aligned}\mathrm{td}(\mathrm{tr}_{\mathcal{D}_{123}}(|\psi_i\rangle), \mathrm{tr}_{\mathcal{D}_{12F}}(|\psi'_i\rangle)) &\leq \mathrm{td}\left(\mathrm{tr}_{\mathcal{D}_{123}}\left(((I - \Pi_{\mathrm{bad}}) \otimes I_1) \cdot O_{\mathrm{LR}_3} |\psi_{i-1}{}^{\mathrm{good}}\rangle\right), \right. \\ &\quad \left. \mathrm{tr}_{\mathcal{D}_{12F}}\left(((I - \Pi_{\mathrm{bad}}) \otimes I_1) \cdot O_{\mathrm{LR}'_3} |\psi'_{i-1}{}^{\mathrm{good}}\rangle\right)\right) \\ &\quad + \mathrm{td}\left(\mathrm{tr}_{\mathcal{D}_{123}}\left((\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}_3} |\psi_{i-1}{}^{\mathrm{good}}\rangle\right), \right. \\ &\quad \left. \mathrm{tr}_{\mathcal{D}_{12F}}\left((\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}'_3} |\psi'_{i-1}{}^{\mathrm{good}}\rangle\right)\right) \\ &\quad + \mathrm{td}\left(\mathrm{tr}_{\mathcal{D}_{123}}(|\psi_{i-1}{}^{\mathrm{bad}}\rangle), \mathrm{tr}_{\mathcal{D}_{12F}}(|\psi'_{i-1}{}^{\mathrm{bad}}\rangle)\right) + O\left(\sqrt{\frac{i}{2^{n/2}}}\right)\end{aligned}\tag{86}$$

holds.

From Lemma 1, it follows that

$$\mathrm{tr}_{\mathcal{D}_{123}} \left( |\psi_i^{\mathrm{good}}\rangle \right) = \mathrm{tr}_{\mathcal{D}_{12F}} \left( |\psi_i^{\prime\mathrm{good}}\rangle \right) \quad (87)$$

holds for any  $1 \leq i \leq q+1$ . Moreover,  $((I - \Pi_{\mathrm{bad}}) \otimes I_1) \cdot O_{\mathrm{LR}_3} |\psi_{i-1}^{\mathrm{good}}\rangle = |\psi_i^{\mathrm{good}}\rangle$  and  $((I - \Pi_{\mathrm{bad}}) \otimes I_1) \cdot O_{\mathrm{LR}_3} |\psi_{i-1}^{\prime\mathrm{good}}\rangle = |\psi_i^{\prime\mathrm{good}}\rangle$  hold. Thus

$$\begin{aligned} & \mathrm{td} \left( \mathrm{tr}_{\mathcal{D}_{123}} \left( ((I - \Pi_{\mathrm{bad}}) \otimes I_1) \cdot O_{\mathrm{LR}_3} |\psi_{i-1}^{\mathrm{good}}\rangle \right), \right. \\ & \quad \left. \mathrm{tr}_{\mathcal{D}_{12F}} \left( ((I - \Pi_{\mathrm{bad}}) \otimes I_1) \cdot O_{\mathrm{LR}'_3} |\psi_{i-1}^{\prime\mathrm{good}}\rangle \right) \right) = 0 \end{aligned} \quad (88)$$

holds. In addition, from the claim in p. 45 it follows that

$$\mathrm{tr}_{\mathcal{D}_{123}} (|\psi_{i-1}\rangle) = \mathrm{tr}_{\mathcal{D}_{123}} (|\psi_{i-1}^{\mathrm{good}}\rangle) + \mathrm{tr}_{\mathcal{D}_{123}} (|\psi_{i-1}^{\mathrm{bad}}\rangle)$$

and

$$\mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_{i-1}'\rangle) = \mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_{i-1}^{\prime\mathrm{good}}\rangle) + \mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_{i-1}^{\prime\mathrm{bad}}\rangle)$$

hold, which implies that

$$\mathrm{td} \left( \mathrm{tr}_{\mathcal{D}_{123}} (|\psi_{i-1}\rangle), \mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_{i-1}'\rangle) \right) = \mathrm{td} \left( \mathrm{tr}_{\mathcal{D}_{123}} (|\psi_{i-1}^{\mathrm{bad}}\rangle), \mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_{i-1}^{\prime\mathrm{bad}}\rangle) \right) \quad (89)$$

holds.

From (86), (88), and (89), we can show that

$$\begin{aligned} & \mathrm{td} \left( \mathrm{tr}_{\mathcal{D}_{123}} (|\psi_i\rangle), \mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_i'\rangle) \right) \\ & \leq \mathrm{td} \left( \mathrm{tr}_{\mathcal{D}_{123}} \left( (\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}_3} |\psi_{i-1}^{\mathrm{good}}\rangle \right), \right. \\ & \quad \left. \mathrm{tr}_{\mathcal{D}_{12F}} \left( (\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}'_3} |\psi_{i-1}^{\prime\mathrm{good}}\rangle \right) \right) \\ & \quad + \mathrm{td} \left( \mathrm{tr}_{\mathcal{D}_{123}} (|\psi_{i-1}\rangle), \mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_{i-1}'\rangle) \right) + O \left( \sqrt{\frac{i}{2^{n/2}}} \right) \\ & \leq \left\| \mathrm{tr}_{\mathcal{D}_{123}} \left( (\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}_3} |\psi_{i-1}^{\mathrm{good}}\rangle \right) \right\|_{\mathrm{tr}} \\ & \quad + \left\| \mathrm{tr}_{\mathcal{D}_{12F}} \left( (\Pi_{\mathrm{bad}} \otimes X) \cdot O_{\mathrm{LR}'_3} |\psi_{i-1}^{\prime\mathrm{good}}\rangle \right) \right\|_{\mathrm{tr}} \\ & \quad + \mathrm{td} \left( \mathrm{tr}_{\mathcal{D}_{123}} (|\psi_{i-1}\rangle), \mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_{i-1}'\rangle) \right) + O \left( \sqrt{\frac{i}{2^{n/2}}} \right) \\ & \leq \mathrm{td} \left( \mathrm{tr}_{\mathcal{D}_{123}} (|\psi_{i-1}\rangle), \mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_{i-1}'\rangle) \right) + O \left( \sqrt{\frac{i}{2^{n/2}}} \right) \end{aligned} \quad (90)$$

holds, where we used the claim of Lemma 2 again for the last inequality. Therefore, by induction it follows that

$$\mathrm{td} \left( \mathrm{tr}_{\mathcal{D}_{123}} (|\psi_i\rangle), \mathrm{tr}_{\mathcal{D}_{12F}} (|\psi_i'\rangle) \right) \leq \sum_{1 \leq j \leq i-1} O \left( \sqrt{\frac{j}{2^{n/2}}} \right) \leq O \left( \sqrt{\frac{i^3}{2^{n/2}}} \right) \quad (91)$$



for each  $1 \leq i \leq q + 1$ . The claim of the proposition follows from (72) and (91).  $\square$

## E Proof of Proposition 4

*Proof (of Proposition 4).* We give a proof for  $\text{LR}_3$  and  $\text{LR}_3\text{-det}$ . The claim for  $\text{LR}'_3$  and  $\text{LR}'_3\text{-det}$  can be proven in the same way. Let  $|\eta_i\rangle$  and  $|\psi_i\rangle$  be the states just before  $\mathcal{A}$  makes the  $i$ -th query, when  $\mathcal{A}$  runs relative to  $\text{LR}_3$  and  $\text{LR}_3\text{-det}$ , respectively. By abuse of notation, we let  $|\eta_{(q+1)}\rangle, |\psi_{(q+1)}\rangle$  denote the quantum states  $(U_q \otimes I)O_{\text{LR}_3}|\eta_q\rangle$  and  $(U_q \otimes I)O_{\text{LR}_3\text{-det}}|\psi_q\rangle$ , respectively. Then we have that  $|\eta_1\rangle = |\psi_1\rangle$ . Moreover, let  $|\xi_{(q+1)}\rangle, |\phi_{(q+1)}\rangle$  be the states just before the final measurements for the cases that the adversary  $\mathcal{A}$  runs relative to  $\text{LR}_3$  and  $\text{LR}_3\text{-det}$ , respectively. Since now we are considering that the random functions  $f_1, f_2$ , and  $f_3$  are implemented by the recording standard oracle with errors, there is a unitary operator  $U_{\text{FinDec}}^{123}$  that acts on database registers such that  $|\xi_{q+1}\rangle = (I \otimes U_{\text{FinDec}}^{123})|\eta_{q+1}\rangle$  and  $|\phi_{q+1}\rangle = (I \otimes U_{\text{FinDec}}^{123})|\psi_{q+1}\rangle$ .

In addition, let us define an operator  $\hat{O}_{\text{LR}_3}$  by

$$\begin{aligned} \hat{O}_{\text{LR}_3} &= (O_{\text{LR}_3} \otimes I_{i-1} \otimes I_1) \cdot ((I - \Pi_{\text{flipped}}^{[i-1]}) \otimes I_1) \\ &\quad + \Pi_{\text{flipped}}^{[i-1]} \otimes I_1, \end{aligned} \quad (92)$$

where  $I_{i-1}$  is the identity operator on the first  $(i-1)$  additional qubits, and  $I_1$  is one on the  $i$ -th additional qubit. The definition of this operator depends on  $i$ , but we use the same notation  $\hat{O}_{\text{LR}_3}$  for all  $i$ , for simplicity. (Intuitively,  $\hat{O}_{\text{LR}_3}$  is an intermediate operator between  $O_{\text{LR}_3}$  and  $O_{\text{LR}_3\text{-det}}$ : Similarly to  $O_{\text{LR}_3\text{-det}}$ , the new operator  $\hat{O}_{\text{LR}_3}$  does nothing if one of the first  $(i-1)$  additional qubits is 1. However, unlike  $O_{\text{LR}_3\text{-det}}$ ,  $\hat{O}_{\text{LR}_3}$  does not flip the  $i$ -th additional qubit even if the database becomes bad, after each query.)

Assume that  $\mathcal{A}$  has  $\ell$ -qubit states, and the database register has  $d$ -qubits in total. Then, since the additional  $q$  qubits are set to 0 at the beginning, it holds that

$$|\eta_i\rangle = (U_i \otimes I)\hat{O}_{\text{LR}_3} \cdots \hat{O}_{\text{LR}_3}(U_0 \otimes I)(|0^\ell\rangle \otimes |0^d\rangle \otimes |0^q\rangle) \quad (93)$$

and

$$|\psi_i\rangle = (U_i \otimes I)O_{\text{LR}_3\text{-det}} \cdots O_{\text{LR}_3\text{-det}}(U_0 \otimes I)(|0^\ell\rangle \otimes |0^d\rangle \otimes |0^q\rangle), \quad (94)$$

for each  $i$  (we omit writing the  $2n$  ancillary qubits that are used to compute the intermediate states after the first and second rounds).

Now we have that

$$\begin{aligned} &\text{Adv}_{\text{LR}_3, \text{LR}_3\text{-det}}^{\text{dist}}(\mathcal{A}) \\ &\leq \left\| |\xi_{(q+1)}\rangle - |\phi_{(q+1)}\rangle \right\| \\ &= \left\| |\eta_{(q+1)}\rangle - |\psi_{(q+1)}\rangle \right\| \\ &= \left\| (U_q \otimes I)\hat{O}_{\text{LR}_3} \cdots \hat{O}_{\text{LR}_3}(U_0 \otimes I)(|0^\ell\rangle \otimes |0^d\rangle \otimes |0^q\rangle) \right\| \end{aligned}$$

$$\begin{aligned}
& - (U_q \otimes I) O_{\text{LR}_3\text{-det}} \cdots O_{\text{LR}_3\text{-det}}(U_0 \otimes I)(|0^\ell\rangle \otimes |0^d\rangle \otimes |0^g\rangle) \Big\| \\
\leq & \sum_{1 \leq i \leq q} \left\| (U_q \otimes I) \hat{O}_{\text{LR}_3} \cdots (U_i \otimes I) \hat{O}_{\text{LR}_3} (U_{i-1} \otimes I) O_{\text{LR}_3\text{-det}} \right. \\
& \quad \left. \cdots O_{\text{LR}_3\text{-det}}(U_0 \otimes I)(|0^\ell\rangle \otimes |0^d\rangle \otimes |0^g\rangle) \right. \\
& \quad \left. - (U_q \otimes I) \hat{O}_{\text{LR}_3} \cdots (U_{i+1} \otimes I) \hat{O}_{\text{LR}_3} (U_i \otimes I) O_{\text{LR}_3\text{-det}} \right. \\
& \quad \left. \cdots O_{\text{LR}_3\text{-det}}(U_0 \otimes I)(|0^\ell\rangle \otimes |0^d\rangle \otimes |0^g\rangle) \right\| \tag{95}
\end{aligned}$$

$$\begin{aligned}
& = \sum_{1 \leq i \leq q} \left\| (U_q \otimes I) \hat{O}_{\text{LR}_3} \cdots (U_i \otimes I) \left( \hat{O}_{\text{LR}_3} |\psi_i\rangle - O_{\text{LR}_3\text{-det}} |\psi_i\rangle \right) \right\| \\
& = \sum_{1 \leq i \leq q} \left\| \hat{O}_{\text{LR}_3} |\psi_i\rangle - O_{\text{LR}_3\text{-det}} |\psi_i\rangle \right\| \tag{96}
\end{aligned}$$

holds.

Let us again denote  $\Pi_{\text{flipped}}^{[i-1]} |\psi_i\rangle$  by  $|\psi_i^{\text{good}}\rangle$ . Since

$$\begin{aligned}
O_{\text{LR}_3\text{-det}} & = (\Pi_{\text{bad}} \otimes I_{i-1} \otimes X + (I - \Pi_{\text{bad}}) \otimes I_{i-1} \otimes I_1) \\
& \quad \cdot (O_{\text{LR}_3} \otimes I_{i-1} \otimes I_1) \cdot ((I - \Pi_{\text{flipped}}^{[i-1]}) \otimes I_1) \\
& \quad + \Pi_{\text{flipped}}^{[i-1]} \otimes I_1 \tag{97}
\end{aligned}$$

holds by definition of  $O_{\text{LR}_3\text{-det}}$ , and

$$\begin{aligned}
\hat{O}_{\text{LR}_3} & = (\Pi_{\text{bad}} \otimes I_{i-1} \otimes I_1 + (I - \Pi_{\text{bad}}) \otimes I_{i-1} \otimes I_1) \\
& \quad \cdot (O_{\text{LR}_3} \otimes I_{i-1} \otimes I_1) \cdot ((I - \Pi_{\text{flipped}}^{[i-1]}) \otimes I_1) \\
& \quad + \Pi_{\text{flipped}}^{[i-1]} \otimes I_1 \tag{98}
\end{aligned}$$

holds, we have that

$$\begin{aligned}
& \left\| \hat{O}_{\text{LR}_3} |\psi_i\rangle - O_{\text{LR}_3\text{-det}} |\psi_i\rangle \right\| \\
& = \left\| (\Pi_{\text{bad}} \otimes X) O_{\text{LR}_3} |\psi_i^{\text{good}}\rangle - (\Pi_{\text{bad}} \otimes I_1) O_{\text{LR}_3} |\psi_i^{\text{good}}\rangle \right\| \\
& \leq 2 \left\| (\Pi_{\text{bad}} \otimes I_1) O_{\text{LR}_3} |\psi_i\rangle \right\|. \tag{99}
\end{aligned}$$

From (96), (99), and Lemma 2, it follows that

$$\text{Adv}_{\text{LR}_3, \text{LR}_3\text{-det}}^{\text{dist}}(\mathcal{A}) \leq \sum_{1 \leq j \leq q} O\left(\sqrt{\frac{j}{2^{n/2}}}\right) = O\left(\sqrt{\frac{q^3}{2^{n/2}}}\right) \tag{100}$$

holds, which completes the proof.  $\square$

## F Proof of Proposition 5

Here we give a proof of Proposition 5.

Let  $\mathcal{O}_1$  and  $\mathcal{O}_2$  be (stateless) oracles of functions  $f_1, f_2 : X \rightarrow Y$  which are chosen according to distributions  $D_1$  and  $D_2$  on  $\text{Func}(X, Y)$ , respectively. In addition, let  $D_1^Z$  be the distribution on  $\text{Func}(Z \times X, Y)$  such that, if we sample a function  $F$  according to  $D_1^Z$ ,  $F(z, \cdot) \in \text{Func}(X, Y)$  is sampled according to  $D_1$  independently for each  $z \in Z$ . Let  $D_2^Z$  be the distribution which is defined from  $D_2$  in the same way. Define  $\mathcal{O}_1^Z$  and  $\mathcal{O}_2^Z$  to be the (stateless) oracles of functions  $F_1, F_2 : Z \times X \rightarrow Y$  which are chosen according to distributions  $D_1^Z$  and  $D_2^Z$ , respectively. Then the following proposition holds, which is first essentially shown by Zhandry [33], and later generalized by Song and Yun [32]. Note that, in the following proposition, we consider (quantum) information theoretic adversaries, and do not care about whether they are efficient quantum algorithms.

**Proposition 6 (Theorem 1.1 in [33], Theorem 3.3 in [32]).** *For any quantum query adversary  $\mathcal{A}$  that makes at most  $q$  quantum queries, there exists an adversary  $\mathcal{B}$  that makes  $2q$  quantum queries and satisfies*

$$\text{Adv}_{\mathcal{O}_1^Z, \mathcal{O}_2^Z}^{\text{dist}}(\mathcal{A}) \leq 12\sqrt{q^3 \cdot \text{Adv}_{\mathcal{O}_1, \mathcal{O}_2}^{\text{dist}}(\mathcal{B})}. \quad (101)$$

In addition to Proposition 6, we use the following proposition shown by Zhandry [35].

**Proposition 7 (Theorem 2 in of [35]).** *For any quantum query adversary  $\mathcal{A}$  that makes at most  $q$  quantum queries,  $\text{Adv}_{\text{RP}}^{\text{qPRF}}(\mathcal{A}) \leq O(q^3/2^{n/2})$  holds. (Here we consider a random permutation over  $\{0, 1\}^{n/2}$ .)*

Combining Propositions 6 and 7, we can prove Proposition 5 as follows.

*Proof (of Proposition 5).* Let  $X, Y$ , and  $Z$  be  $\{0, 1\}^{n/2}$ . In addition, let  $\mathcal{O}_1, \mathcal{O}_2$  denote the oracle of a random function and a random permutation (from  $\{0, 1\}^{n/2}$  to  $\{0, 1\}^{n/2}$ ), respectively. Then  $\mathcal{O}_1^Z$  and  $\mathcal{O}_2^Z$  become the oracles of FRP and RF, respectively (here, RF denotes a random function from  $n$ -bit to  $n/2$ -bit). Then, from Propositions 6 and 7, it follows that there exists a quantum adversary  $\mathcal{B}$  that makes at most  $2q$  quantum queries and satisfies

$$\begin{aligned} \text{Adv}_{\mathcal{O}_1^Z, \mathcal{O}_2^Z}^{\text{dist}}(\mathcal{A}) &\leq 12\sqrt{q^3 \cdot \text{Adv}_{\mathcal{O}_1, \mathcal{O}_2}^{\text{dist}}(\mathcal{B})} = 12\sqrt{q^3 \cdot \text{Adv}_{\text{RP}}^{\text{qPRF}}(\mathcal{B})} \\ &\leq O\left(\sqrt{q^6/2^{n/2}}\right), \end{aligned} \quad (102)$$

which completes the proof.  $\square$

## G Proof of Theorem 4

First, we describe an overview of a classical attack [28]. Let us denote the composition of two independent random functions from  $\{0, 1\}^{n/2}$  to  $\{0, 1\}^{n/2}$  by  $\text{RF} \circ \text{RF}$ .

**An overview of a classical attack.** Suppose that we are given an oracle access to  $\mathcal{O}$ , which is either the 4-round Luby-Rackoff construction  $\text{LR}_4$  or a random permutation from  $\{0, 1\}^n$  to  $\{0, 1\}^n$ . Let us define a function  $G^{\mathcal{O}} : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  that depends on  $\mathcal{O}$  by

$$G^{\mathcal{O}}(x) := \left( \mathcal{O}(0^{n/2}, x) \right)_R \oplus x, \quad (103)$$

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

When  $\mathcal{O}$  is the 4-round Luby-Rackoff construction  $\text{LR}_4$ , we have that  $G^{\mathcal{O}}(x) = f_3(f_2(x \oplus f_1(0^{n/2}))) \oplus f_1(0^{n/2})$  holds. Thus, if all round functions of  $\text{LR}_4$  are truly random functions, the function distribution of  $G^{\mathcal{O}}$  will be the same as that of the composition of two independent random functions  $\text{RF} \circ \text{RF}$ . On the other hand, when  $\mathcal{O}$  is a random permutation from  $\{0, 1\}^n$  to  $\{0, 1\}^n$ , the function distribution of  $G^{\mathcal{O}}$  will be almost the same as that of the truly random function  $\text{RF}$  from  $\{0, 1\}^{n/2}$  to  $\{0, 1\}^{n/2}$ .

Since  $\text{RF} \circ \text{RF}$  has twice as many collisions as  $\text{RF}$  has, we can distinguish  $\text{LR}_4$  from a truly random permutation by making  $O((2^{n/2})^{1/2}) = O(2^{n/4})$  queries to  $G^{\mathcal{O}}$ .

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

**Lemma 6.** *Let us denote the composition of two independent random functions from  $\{0, 1\}^{n/2}$  to  $\{0, 1\}^{n/2}$  by  $\text{RF} \circ \text{RF}$ . Then, there exists a quantum algorithm  $\mathcal{B}$  that makes  $O(2^{n/6})$  quantum queries and satisfies  $\text{Adv}_{\text{RF} \circ \text{RF}}^{\text{qPRF}}(\mathcal{B}) = \Omega(1)$ . That is, there exists an algorithm that distinguishes  $\text{RF} \circ \text{RF}$  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  $F : X \rightarrow Y$  be a function. Then there is a quantum algorithm that judges if there exist distinct elements  $x_1, x_2 \in X$  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  $1 \leq N \leq 2^{n/2}$  there exists a quantum algorithm  $\mathcal{D}_N$  such that, given oracle access to a function  $F : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$ , it outputs 1 if there exist distinct elements  $x_1, x_2 \in [N]$  such that  $F(x_1) = F(x_2)$ , and 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  $F|_{[N]} : [N] \rightarrow \{0, 1\}^{n/2}$ , which is the restriction of  $F$  to  $[N]$ .)

Here we give an analysis of the qPRF advantage of  $\mathcal{D}_N$  on  $\text{RF} \circ \text{RF}$ , for each  $N$ . For a function  $F : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  and a subset  $Z \in \{0, 1\}^{n/2}$ , let  $\text{coll}_Z^F$  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

$$\begin{aligned} \Pr_F \left[ \neg \text{coll}_{[N]}^F \right] &= \left( 1 - \frac{1}{2^{n/2}} \right) \cdot \left( 1 - \frac{2}{2^{n/2}} \right) \cdots \left( 1 - \frac{N-1}{2^{n/2}} \right) \\ &= \prod_{j=1}^{N-1} \left( 1 - \frac{j}{2^{n/2}} \right) \end{aligned} \quad (104)$$

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

$$\begin{aligned} \Pr_{F_1, F_2} \left[ \neg \text{coll}_{[N]}^{F_2 \circ F_1} \right] &= \Pr_{F_2} \left[ \neg \text{coll}_{F_1([N])}^{F_2} \mid \neg \text{coll}_{[N]}^{F_1} \right] \cdot \Pr_{F_1} \left[ \neg \text{coll}_{[N]}^{F_1} \right] \\ &= \left( \Pr_F \left[ \neg \text{coll}_{[N]}^F \right] \right)^2. \end{aligned} \quad (105)$$

Now we have that

$$\begin{aligned} \text{Adv}_{\text{RF} \circ \text{RF}}^{\text{qPRF}}(\mathcal{D}_N) &= \text{Adv}_{\text{RF}, \text{RF} \circ \text{RF}}^{\text{dist}}(\mathcal{D}_N) \\ &= \left| \Pr_F \left[ \mathcal{D}_N^F() \rightarrow 1 \right] - \Pr_{F_1, F_2} \left[ \mathcal{D}_N^{F_2 \circ F_1}() \rightarrow 1 \right] \right| \\ &\geq \left| \Pr_F \left[ \text{coll}_{[N]}^F \right] - \Pr_{F_1, F_2} \left[ \text{coll}_{[N]}^{F_2 \circ F_1} \right] \right| - \frac{2}{30}, \end{aligned} \quad (106)$$

where we used the property that the error of  $\mathcal{D}_N$  is smaller than  $1/30$ . In addition, from (105) it follows that

$$\begin{aligned} &\left| \Pr_F \left[ \text{coll}_{[N]}^F \right] - \Pr_{F_1, F_2} \left[ \text{coll}_{[N]}^{F_2 \circ F_1} \right] \right| \\ &= \Pr_{F_1, F_2} \left[ \text{coll}_{[N]}^{F_2 \circ F_1} \right] - \Pr_F \left[ \text{coll}_{[N]}^F \right] \\ &= \left( 1 - \left( \Pr_F \left[ \neg \text{coll}_{[N]}^F \right] \right)^2 \right) - \left( 1 - \Pr_F \left[ \neg \text{coll}_{[N]}^F \right] \right) \\ &= \Pr_F \left[ \neg \text{coll}_{[N]}^F \right] \left( 1 - \Pr_F \left[ \neg \text{coll}_{[N]}^F \right] \right) \end{aligned} \quad (107)$$

holds. Therefore we have that

$$\text{Adv}_{\text{RF} \circ \text{RF}}^{\text{qPRF}}(\mathcal{D}_N) \geq \Pr_F \left[ \neg \text{coll}_{[N]}^F \right] \left( 1 - \Pr_F \left[ \neg \text{coll}_{[N]}^F \right] \right) - \frac{2}{30} \quad (108)$$

holds. Now we show the following claim.

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

$$\frac{3}{5} \geq \prod_{j=1}^{N_0-1} \left(1 - \frac{j}{2^{n/2}}\right) \geq \frac{1}{5} \quad (109)$$

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

$$\begin{aligned} \prod_{j=1}^{N-1} \left(1 - \frac{j}{2^{n/2}}\right) &\geq \left(1 - \frac{N}{2^{n/2}}\right)^N \\ &= \left(\left(1 - \frac{N}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N}}\right)^{-\frac{N^2}{2^{n/2}}} \end{aligned} \quad (110)$$

holds, in addition that

$$\prod_{j=1}^{N-1} \left(1 - \frac{j}{2^{n/2}}\right) \leq \prod_{j=1}^{N-1} \left(e^{-\frac{j}{2^{n/2}}}\right) = e^{-\frac{N(N-1)}{2 \cdot 2^{n/2}}} \quad (111)$$

holds. Thus

$$e^{-\frac{N(N-1)}{2 \cdot 2^{n/2}}} \geq p_N \geq \left(\left(1 - \frac{N}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N}}\right)^{-\frac{N^2}{2^{n/2}}} \quad (112)$$

holds.

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

$$\begin{aligned} e^{-\frac{N_0(N_0-1)}{2 \cdot 2^{n/2}}} &= e^{-\frac{N_0 \cdot N_0}{2 \cdot 2^{n/2}}} + \left(e^{-\frac{N_0(N_0-1)}{2 \cdot 2^{n/2}}} - e^{-\frac{N_0 \cdot N_0}{2 \cdot 2^{n/2}}}\right) \\ &= \frac{1}{2} + \left(\left(\frac{1}{2}\right)^{\frac{N_0-1}{N_0}} - \frac{1}{2}\right) \end{aligned} \quad (113)$$

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  $\lim_{x \rightarrow +0} f(x) = e$  holds, we have that

$$\left(1 - \frac{N_0}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N_0}} \leq e + \frac{1}{10} \quad (114)$$

holds for sufficiently large  $n$ . Thus

$$\left(\left(1 - \frac{N_0}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N_0}}\right)^{-\frac{N_0^2}{2^{n/2}}} \geq \left(e + \frac{1}{10}\right)^{-\frac{N_0^2}{2^{n/2}}} = \left(e + \frac{1}{10}\right)^{-2 \log 2} \geq \frac{1}{5} \quad (115)$$

holds for sufficiently large  $n$ .

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

$$\frac{3}{5} \geq p_{N_0} \geq \frac{1}{5} \quad (116)$$

holds for sufficiently large  $n$ . Hence the claim follows.  $\square$

From the above claim and (104), there exists a parameter  $N_0$  which is in  $O(2^{n/4})$ , and

$$\frac{3}{5} \geq \Pr_F \left[ -\text{coll}_{[N_0]}^F \right] \geq \frac{1}{5} \quad (117)$$

holds for sufficiently large  $n$ . Hence, from (106) we have that

$$\text{Adv}_{\text{RF} \circ \text{RF}}^{\text{qPRF}}(\mathcal{D}_{N_0}) \geq \frac{1}{5} \left( 1 - \frac{3}{5} \right) - \frac{2}{30} = \frac{1}{75} \geq \Omega(1). \quad (118)$$

Therefore, if we put  $\mathcal{B} := \mathcal{D}_{N_0}$ , this  $\mathcal{B}$  satisfies the claim of the lemma, since (118) 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.  $\square$

Next we show the following proposition.

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

*Proof.* Suppose that we are given an oracle access to  $\mathcal{O}$ , which is either the 4-round Luby-Rackoff construction  $\text{LR}_4$  or a random function from  $\{0, 1\}^n$  to  $\{0, 1\}^n$ . Recall that the function  $G^\mathcal{O} : \{0, 1\}^{n/2} \rightarrow \{0, 1\}^{n/2}$  is defined by

$$G^\mathcal{O}(x) := \left( \mathcal{O}(0^{n/2}, x) \right)_R \oplus x, \quad (119)$$

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

Now we define a quantum algorithm  $\mathcal{A}$  as the following procedures.

1. Let  $\mathcal{B}$  be the same algorithm in Lemma 6.
2. Run  $\mathcal{B}$  relative to  $G^\mathcal{O}$ .
3. If  $\mathcal{B}$  returns 1, output 1. If  $\mathcal{B}$  returns 0, output 0.

Here we give an analysis of  $\mathcal{A}$ . When  $\mathcal{O}$  is the 4-round Luby-Rackoff construction  $\text{LR}_4$ , we have that  $G^\mathcal{O}(x) = f_3(f_2(x \oplus f_1(0^{n/2}))) \oplus f_1(0^{n/2})$  holds. Since we are considering the case that all round functions of  $\text{LR}_4$  are truly random functions, the function distribution of  $G^\mathcal{O}$  will be the same as that of  $\text{RF} \circ \text{RF}$ . On the other hand, when  $\mathcal{O}$  is a random function from  $\{0, 1\}^n$  to  $\{0, 1\}^n$ , the function

<sup>9</sup> Here we have to implement truncation of  $\mathcal{O}$ 's outputs by using a technique observed in [15].

distribution of  $G^{\mathcal{O}}$  will be the same as that of the truly random function from  $\{0, 1\}^{n/2}$  to  $\{0, 1\}^{n/2}$ . Thus, from Lemma 6 we have that

$$\mathbf{Adv}_{\text{LR}_4}^{\text{qPRF}}(\mathcal{A}) = \mathbf{Adv}_{\text{RF} \circ \text{RF}}^{\text{qPRF}}(\mathcal{B}) = \Omega(1) \quad (120)$$

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

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

$$\begin{aligned} \mathbf{Adv}_{\text{LR}_4}^{\text{qPRP}}(\mathcal{A}) &\geq \mathbf{Adv}_{\text{LR}_4}^{\text{qPRF}}(\mathcal{A}) - \mathbf{Adv}_{\text{RP,RF}}^{\text{dist}}(\mathcal{A}) \\ &\geq \Omega(1) - O(1/2^{n/2}) = \Omega(1), \end{aligned} \quad (121)$$

where we used the fact that, for any quantum adversary  $\mathcal{A}'$  that makes at most  $q$  queries, the distinguishing advantage  $\mathbf{Adv}_{\text{RP,RF}}^{\text{dist}}(\mathcal{A}')$  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 7). Thus the claim of the theorem holds.  $\square$