Quantum Security of FOX Construction based on Lai-Massey Scheme

Amit Kumar Chauhan and Somitra Kumar Sanadhya

Indian Institute of Technology Jodhpur, India
{amitchauhan,somitra}@iitj.ac.in

Abstract. The Lai-Massey scheme is an important cryptographic approach to design block ciphers from secure pseudorandom functions. It has been used in the designs of IDEA and IDEA-NXT. At ASIACRYPT' 99, Vaudenay showed that the 3-round and 4-round Lai-Massey scheme are secure against chosen-plaintext attacks (CPAs) and chosen-ciphertext attacks (CCAs), respectively, in the classical setting. At SAC'04, Junod and Vaudenay proposed a new family of block ciphers based on the Lai-Massey scheme, namely FOX. In this work, we analyze the security of the FOX cipher in the quantum setting, where the attacker can make quantum superposed queries to the oracle. Our results are as follows:

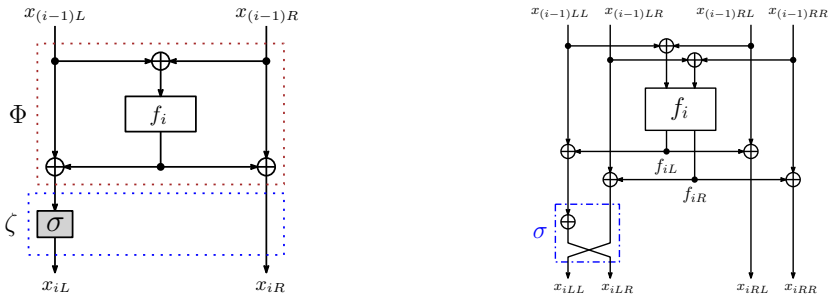
- The 3-round FOX construction is not a pseudorandom permutation against quantum chosen-plaintext attacks (qCPAs), and the 4-round FOX construction is not a strong pseudorandom permutation against quantum chosen-ciphertext attacks (qCCAs). Essentially, we build quantum distinguishers against the 3-round and 4-round FOX constructions, using Simon's algorithm.
- The 4-round FOX construction is a pseudorandom permutation against qCPAs. Concretely, we prove that the 4-round FOX construction is secure up to $O(2^{n/12})$ quantum queries. Our security proofs use the compressed oracle technique introduced by Zhandry. More precisely, we use an alternative formalization of the compressed oracle technique introduced by Hosoyamada and Iwata.

Keywords: Symmetric-key cryptography · Lai-Massey scheme · FOX cipher · Simon's algorithm · Quantum chosen-plaintext attacks · quantum chosen-ciphertext attacks · Compressed oracle technique.

1 Introduction

A block cipher is an important cryptographic primitive that is widely used for data encryption, data authentication, and to build one-way functions. A block cipher is a pseudo-random permutation (PRP), i.e., for a distinct key it provides distinct permutations that cannot be distinguished from a random permutation in polynomial time. Some of the popular designing approaches are based on the Feistel network, the Lai-Massey scheme, and the substitution-permutation network. Luby and Rackoff [LR88] showed that the 3-round and 4-round Feistel constructions are secure PRPs against chosen-plaintext attacks (CPAs) and chosen-ciphertext attacks (CCAs), respectively. Similar to the Feistel network, Vaudenay [Vau99] showed that the 3-round and 4-round Lai-Massey constructions [LM90] are secure PRPs against CPAs and CCAs, respectively. Following the Lai-Massey scheme, Junod and Vaudenay [JV04] proposed a family of block ciphers, namely FOX. Later, FOX was also announced under IDEA-NXT by MediaCrypt AG [AG07], as a successor of IDEA.

FOX Cipher. The high level structure of FOX cipher adopts the Lai-Massey scheme [LM90], operating on an arbitrary group G. It consists of two layers: a non-linear layer Φ which applies the round function f, and a linear layer ζ which applies the function σ as an orthomorphism such that σ and $x \mapsto \sigma(x) - x$ are both permutations (see Figure 1a). In the FOX design, the group $(G, +)$ is chosen to be $(\{0,1\}^{n/2}, \oplus)$, and the orthomorphism σ is defined as $\sigma(y_1, y_2) = (y_2, y_1 \oplus y_2)$, where $y_1, y_2 \in (\{0,1\}^{n/2}, \oplus)$. The detailed description of the design can be found in [JV04].



(a) 1-round of LM. (b) 1-round of FOX.

Figure 1: Round transformation of the Lai-Massey (LM) scheme and FOX cipher.

Let $f_i := \{f_{i,k} : \{0,1\}^{n/2} \to \{0,1\}^{n/2}\}$ be a family of functions that is parameterized by k from a key space $\mathcal{K}$ $(1 \le i \le r)$. The r-round FOX construction $\mathsf{FOX}_r(f_1, \ldots, f_r)$ is defined as follows: first, keys $k_1, \ldots, k_r$ are chosen independently and uniformly at random from $\mathcal{K}$. For each input $x_0 = x_{0LL}||x_{0LR}||x_{0RL}||x_{0RR}$, where $x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR} \in \{0,1\}^{n/4}$, the i-th state is updated as $x_{(i-1)LL}||x_{(i-1)LR}||x_{(i-1)RL}||x_{(i-1)RR} \mapsto x_{iLL}||x_{iLR}||x_{iRL}||x_{iRR}$, where $x_{iLL}, x_{iLR}, x_{iRL}, x_{iRR}$ are given by

$$
\begin{aligned}
x_{iLL} &:= x_{(i-1)LR} \oplus f_{iR}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR}) \\
x_{iLR} &:= x_{(i-1)LL} \oplus x_{(i-1)LR} \oplus f_{iL}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR}) \\
&\qquad \oplus f_{iR}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR}) \\
x_{iRL} &:= x_{(i-1)RL} \oplus f_{iL}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR}) \\
x_{iRR} &:= x_{(i-1)RR} \oplus f_{iR}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR})
\end{aligned}
$$

for $i = 1, \ldots, r$ in a sequential order (see Figure 1b). Here, f_{iL} and f_{iR} denote the left and right halves of f_i, respectively. In the classical setting, if each f_i is a secure PRF then FOX_r is a PRP against CPAs for $r \ge 3$ and a strong PRP against CCAs for $r \ge 4$ [WLLZ09].

Analyzing the quantum security of various cryptographic primitives has become an important question in the last decade. In public-key cryptography, Shor's seminal work [Sho94] showed that factoring large integers and computing discrete logarithms with quantum computers is possible in polynomial time. This result completely breaks public-key schemes such as RSA, ECDSA, and ECDH in the quantum setting. On the other hand, in the case of symmetric-key cryptography, it was believed that the security of symmetric-key schemes would not be much affected by quantum computers. The only caveat was Grover's search algorithm [Gro96] that provides square-root improvement in exhaustive key search attacks. However, a series of recent results has shown that some symmetric-key schemes can be broken in polynomial time by using Simon's algorithm if quantum adversaries have access to quantum circuits that implement keyed primitives such as block ciphers, message authentication codes [KM10, KLLN16a, Bon17, LM17, SS17, BNS19, IHM+19, DDW20]. Further improvements based on Grover's algorithm and its derivatives have been presented on block ciphers [KLLN16b, BNS19, BGLP21] and hash functions [HS20, DSS+20, CKS21, NDJY21].

In particular, Kuwakado and Morii [KM10] showed that the 3-round Feistel construction is not a PRP against quantum chosen-plaintext attacks (qCPAs). Recently, Ito et al. [IHM+19] showed that the 4-round Feistel construction is not a strong PRP against quantum chosen-ciphertext attacks (qCCAs). These attacks primarily rely on Simon's algorithm [Sim97] that can find a hidden period in polynomial-time. Hosoyamada and Iwata [HI19] asked a fundamental question about the quantum security of the Feistel construction, namely "how many rounds are sufficient to achieve provable security against quantum query attacks". They answered this question by using Zhandry's compressed oracle technique [Zha19] and showed that 4-rounds of the Feistel structure are sufficient to provide security against qCPAs. Motivated by these results on the Feistel construction, we focus on analyzing the security of FOX cipher against an attacker having access to quantum superposed queries to the cryptographic oracle.

1.1 Our Contributions

The main technical contributions of this work are as follows:

- We present a quantum CPA distinguisher against the 3-round FOX construction FOX_3. We do this by carefully choosing the inputs to FOX_3 such that the inputs to the second round function f_2 collide, and then we define an appropriate function G which is periodic (see Lemma 1). By running Simon's algorithm on the oracle G, we can recover its hidden secret-period in polynomial time.
- We develop a more challenging quantum CCA distinguisher against the 4-round FOX construction FOX_4 by connecting the FOX and inverse FOX ciphers. To connect the 4-round FOX and the inverse 4-round FOX ciphers, we add appropriate constants in between so that we are able to define a suitable periodic function G (see Lemma 2), whose period can be recovered in polynomial time with Simon's algorithm. In contrast, in the classical setting, only 2-round CPA and 3-round CCA distinguishers are known against the FOX construction.
- Thereafter, we show that the 4-round FOX construction FOX_4 is a PRP against qCPAs. In particular, we give a security bound of FOX_4 against qCPAs when all the round functions are truly random. The concrete bound is stated in Theorem 1.

A summary of distinguishing attacks for FOX construction, the Lai-Massey scheme and the Feistel network is given in Table 1.

Table 1: Comparison of the number of attacked rounds in various settings.

Construction	Classical CPA Distinguisher	Classical CCA Distinguisher	Quantum CPA Distinguisher	Quantum CCA Distinguisher
Feistel	2 [LR88]	3 [LR88]	3 [KM10]	4 [IHM+19]
Lai-Massey	2 [Vau99]	3 [Vau99]	–	–
FOX	2 [WLLZ09]	3 [WLLZ09]	3 [Ours, § 4]	4 [Ours, § 5]

1.2 Organization of the Paper

This paper is organized as follows. Section 2 describes preliminaries, definitions, and Simon's algorithm. Section 3 gives an overview of the RstOE technique. Section 4 presents our quantum CPA distinguisher against the 3-round FOX construction FOX_3 that shows that the 3-round FOX construction FOX_3 is not a PRP. Section 5 presents our quantum CCA distinguisher against the 4-round FOX construction FOX_4 that shows that the 4-round FOX construction FOX_4 is not a strong PRP. Section 6 provides the quantum security proof of FOX_4 to be a PRP against qCPAs. Finally, Section 7 concludes our work.

2 Preliminaries

Throughout this work, we assume that all algorithms (or adversaries) are quantum algorithms and are allowed to make quantum superposed queries to various oracles. We assume that readers are familiar with basics of quantum computation and finite dimensional linear algebra (see textbooks such as [NC11] for an introduction).

2.1 Basic Notations

For strings $x, y \in \{0,1\}^n$, we denote their concatenation as $x||y$. The length of the string x is denoted by $|x|$. For any n-bit string x, we denote the left-half $n/4$-bits of the left-half $n/2$-bits of x by x_{LL}. In the same way, the right-half $n/4$-bits of the left-half $n/2$-bits of x is denoted by x_{LR}. We similarly define x_{RL} and x_{RR} as well. For any finite sets X and Y, let $\mathsf{Func}(X,Y)$ denote the set of all functions from X to Y. Let $\mathsf{Perm}(X)$ denote the set of all permutations from X onto itself. For a function $F \in \mathsf{Func}(X,Y)$, we denote the left and right halves of F by F_L and F_R, respectively. For a finite set $\mathcal{X}$, we write $X \xleftarrow{\$} \mathcal{X}$ for sampling an element uniformly from $\mathcal{X}$ and assigning the result to X. We denote a database by D that consists of input-output pairs for some function f. For an input x and output $\alpha := \alpha_1||\alpha_2$ for D, we denote $D_L(x) := \alpha_1$ and $D_R(x) := \alpha_2$ as the left and right halves of D's output, respectively.

2.2 Quantum Computation

We use the standard quantum circuit model of quantum computation. Complexity of quantum algorithms is measured by the number of queries they make and the number of gates required to implement the algorithms. We assume that quantum circuits are composed of quantum gates that are chosen from a fixed universal gate set (i.e., Clifford+T gates). We denote Hadamard operator by H, and identity operator by I_n. In addition, for a vector ϕ and a positive integer m, we sometimes use the same notation $|\phi\rangle$ to denote the $|\phi\rangle \otimes |0^m\rangle$ or $|0^m\rangle \otimes |\phi\rangle$ for simplicity, when it will cause no confusion. Let $\|\cdot\|$ and $\|\cdot\|_{\mathsf{tr}}$ denote the norm of vector and trace norm of matrix, respectively. $\mathsf{td}(\cdot,\cdot)$ denotes the trace distance. For Hermitian operators ρ, σ on a Hilbert space $\mathcal{H}$, the trace distance $\mathsf{td}(\rho,\sigma) := \frac{1}{2}\|\rho - \sigma\|_{\mathsf{tr}}$ holds. For a mixed state ρ of a joint quantum system $\mathcal{H}_A \otimes \mathcal{H}_B$, let $\mathsf{tr}_B(\rho)$ (resp. $\mathsf{tr}_A(\rho)$) denote the partial trace of ρ over $\mathcal{H}_B$ (resp. $\mathcal{H}_A$).

2.3 Quantum Algorithms and Quantum Oracles

Following previous works (e.g., see [BDF+11]), we model an (oracle-aided) quantum algorithm $\mathcal{A}$ that makes at most q quantum queries to a single oracle as a sequence of unitary operators $(U_0, U_1, \ldots, U_q)$, where U_i corresponds to $\mathcal{A}$'s offline computation after the i-th oracle query for $i \geq 1$, and U_0 corresponds to $\mathcal{A}$'s initial computation. In addition, the quantum state space of $\mathcal{A}$ is a tensor product $\mathcal{H}_{\mathsf{query}} \otimes \mathcal{H}_{\mathsf{answer}} \otimes \mathcal{H}_{\mathsf{work}}$, where $\mathcal{H}_{\mathsf{query}}$, $\mathcal{H}_{\mathsf{answer}}$, and $\mathcal{H}_{\mathsf{work}}$ correspond to the register to make queries to the oracle, the register to receive answers from the oracle, and the register for $\mathcal{A}$'s offline computations, respectively. After the application of the final unitary operator U_q, $\mathcal{A}$'s entire state is measured, and the measurement result (a classical bit string) is returned as the output. When $\mathcal{A}$ does not take any initial input, we assume that $\mathcal{A}$'s initial state is set to be $|0^s\rangle$ for some positive integer s. When $\mathcal{A}$ takes a classical input $x \in \{0,1\}^m$, we assume that $\mathcal{A}$'s initial state is set to be $|x\rangle$ by convention.

A quantum oracle $\mathcal{O}$ is modeled as a sequence of unitary operator $(O_1, \ldots, O_q)$. $\mathcal{O}$ may have some randomness, and each O_i may be chosen randomly according to a distribution at the beginning of each game. $\mathcal{O}$ can maintain its own state. If $\mathcal{O}$ has s'-qubit quantum states, then joint quantum states of $\mathcal{A}$ and $\mathcal{O}$ are $(s+s')$-qubit quantum states. We

denote $\mathcal{O}$'s private state space as $\mathcal{H}_{\mathsf{state}}$. When $\mathcal{A}$ makes the i-th query, the unitary operator O_i acts on $\mathcal{H}_{\mathsf{query}} \otimes \mathcal{H}_{\mathsf{answer}} \otimes \mathcal{H}_{\mathsf{state}}$. We assume that the initial state of $\mathcal{A}$ is set to $|x\rangle$ when $\mathcal{A}$ runs relative to the quantum oracle $\mathcal{O}$ on input x, and $|\mathsf{init}\rangle$ be the initial state of the oracle's private space $\mathcal{H}_{\mathsf{state}}$. Then the initial whole quantum state is expressed as $|x\rangle \otimes |\mathsf{init}\rangle$. The whole quantum state just before the i-th query is $U_{i-1}O_{i-1}U_{i-2}O_{i-2}\cdots O_1U_0|x\rangle \otimes |\mathsf{init}\rangle$, and the whole quantum state just before the final measurement $U_qO_qU_{q-1}O_{q-1}\cdots O_1U_0|x\rangle \otimes |\mathsf{init}\rangle$. We denote the event that $\mathcal{A}$ runs relative to the oracle $\mathcal{O}$ and returns an output z by $z \leftarrow \mathcal{A}^{\mathcal{O}}(x)$.

Example of an oracle. Let F be a family of functions from $\{0,1\}^m$ to $\{0,1\}^n$. Suppose that a quantum algorithm $\mathcal{A}$ runs relative to a quantum oracle $\mathcal{O}_F$ that first chooses f randomly from F (according to a distribution on F) and gives $\mathcal{A}$ a quantum oracle access to f. Then $\mathcal{H}_{\mathsf{query}}$ and $\mathcal{H}_{\mathsf{answer}}$ are defined as m-qubit space and n-qubit space, respectively. $\mathcal{O}_F$ has no quantum states, and each O_i is the unitary operator defined by $O_i : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$. When f is chosen uniformly at random, then it is the quantum oracle of a random function.

2.4 Security Definitions

Quantum distinguishing advantages. Let $\mathcal{A}$ be a quantum algorithm that makes at most q queries and outputs 0 or 1, and let $\mathcal{O}_1$ and $\mathcal{O}_2$ be some oracles. We define the quantum distinguishing advantage of $\mathcal{A}$ by

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

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

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

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

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

Let $\mathcal{F}$ denote the quantum oracle for keyed functions, i.e. the oracle such that a function $F_k \in \{\{0,1\}^m \to \{0,1\}^n\}$ is chosen for a random $k \in \mathcal{K}$ and adversaries are given oracle access to it. In addition, let $\mathcal{A}$ be an algorithm with query access to the oracles RF or $\mathcal{F}$. Then we define the quantum pseudorandom function (qPRF) advantage against the keyed function family F_k by

$$\mathbf{Adv}^{\mathsf{qPRF}}_{\mathcal{F}}(\mathcal{A}) := \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{F},\mathsf{RF}}(\mathcal{A}).$$

Similarly, we define $\mathbf{Adv}^{\mathsf{qPRF}}_{\mathcal{F}}(q)$ by

$$\mathbf{Adv}^{\mathsf{qPRF}}_{\mathcal{F}}(q) := \max_{\mathcal{A}} \left\{ \mathbf{Adv}^{\mathsf{qPRF}}_{\mathcal{F}}(\mathcal{A}) \right\},$$

where the maximum is taken over all quantum algorithms $\mathcal{A}$ that makes at most q queries.

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

Let $\mathcal{P}$ denote the quantum oracle for keyed permutations, i.e. the oracle such that a permutation $P_k \in \mathsf{Perm}(\{0,1\}^n)$ is chosen for a random $k \in \mathcal{K}$ and adversaries are given oracle access to it. In addition, let $\mathcal{A}$ be an algorithm with query access to the oracles RP or $\mathcal{P}$. Then we define the quantum pseudorandom permutation (qPRP) advantage against the keyed permutation family P_k by

$$\mathbf{Adv}^{\mathsf{qPRP}}_{\mathcal{P}}(\mathcal{A}) := \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{P},\mathsf{RP}}(\mathcal{A}).$$

Similarly, we define $\mathbf{Adv}^{\mathsf{qPRP}}_{\mathcal{P}}(q)$ by

$$\mathbf{Adv}^{\mathsf{qPRP}}_{\mathcal{P}}(q) := \max_{\mathcal{A}} \left\{ \mathbf{Adv}^{\mathsf{qPRP}}_{\mathcal{P}}(\mathcal{A}) \right\},$$

where the maximum is taken over all quantum algorithms $\mathcal{A}$ that make at most q queries.

Security against efficient adversaries. An algorithm $\mathcal{A}$ is called efficient if it can be realized as a quantum circuit that has a polynomial number of quantum gates in the security parameter 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 and evaluation of a randomly chosen function from $\mathcal{F}$ (resp., permutation from $\mathcal{P}$) can be performed by an efficient algorithm.
2. $\mathbf{Adv}^{\mathsf{qPRF}}_{\mathcal{F}}(\mathcal{A})$ (resp., $\mathbf{Adv}^{\mathsf{qPRP}}_{\mathcal{P}}(\mathcal{A})$) is negligible for any efficient algorithm $\mathcal{A}$.

2.5 Simon's Algorithm

The period-finding problem is hard classically, but quantum mechanically, it can be solved in polynomial time.

Problem 1 (Simon's problem)**.** *Let $s \in \{0,1\}^n \backslash \{0\}^n$ and $h : \{0,1\}^n \to \{0,1\}^n$ be a function that satisfies the following two conditions: (1) $h(x) = h(x \oplus s)\ \forall\ x \in \{0,1\}^n$, and (2) if $h(x) = h(x')$, then either $x' = x$ or $x' = x \oplus s$. Given an oracle access to f, find s.*

The first condition is equivalent to function h being periodic, with period $s \neq 0^n$. Therefore, we call the above problem (black-box) period finding problem. Solving this problem is hard classically, but in quantum domain, Simon's algorithm [Sim97] can solve the above 1 with $O(n)$ queries, using $O(n)$ qubits.

Next, we explain how Simon's algorithm works. We assume that we have access to the quantum oracle U_h, which is defined as $U_h |x\rangle |z\rangle = |x\rangle |z \oplus h(x)\rangle$. For an n-qubit state $|x\rangle$, Hadamard transformation $H^{\otimes n}$ is defined as $H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x.y} |y\rangle$. Simon proposed a circuit $\mathcal{S}_h$ that computes a vector that is orthogonal to s for a periodic function h, which is defined as $\mathcal{S}_h = (H^{\otimes n} \otimes \mathbb{I}_n) \cdot U_h \cdot (H^{\otimes n} \otimes \mathbb{I}_n)$ and works as follows.

$$\begin{aligned}
\mathcal{S}_h |0^n\rangle |0^n\rangle &= (H^{\otimes n} \otimes \mathbb{I}_n) \cdot U_h \cdot (H^{\otimes n} \otimes \mathbb{I}_n) |0^n\rangle |0^n\rangle \\
&= (H^{\otimes n} \otimes \mathbb{I}_n) \cdot U_h \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |0^n\rangle \\
&= (H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |h(x)\rangle \\
&= \frac{1}{2^n} \sum_{x,y} (-1)^{x.y} |y\rangle |y \oplus h(x)\rangle \qquad (1)
\end{aligned}$$

If h satisfies $h(x) = h(x') \iff x' = x \oplus s$, then equation (Equation 1) can be rearranged as follows.

$$\frac{1}{2^n} \sum_{x \in V, y} ((-1)^{x.y} + (-1)^{(x \oplus s).y}) \left|y\right\rangle \left|y \oplus h(x)\right\rangle,$$

where V is a linear subspace on $\{0,1\}^n$ of dimension $(n-1)$ that partitions $\{0,1\}^n$ into cosets V and $V + s$. The vector y such that $y.s \equiv 1 \pmod 2$ satisfies $((-1)^{x.y} + (-1)^{(x \oplus s).y}) = 0$. Therefore, the vector y that we obtain by measuring $\mathcal{S}_h \left|0^n\right\rangle \left|0^n\right\rangle$ satisfies $y.s \equiv 0 \pmod 2$. By repeating this measurement for $O(n)$ times, we obtain $(n-1)$ linearly independent vectors that are all orthogonal to s with a high probability. Then we can recover s by solving the system of linear equations with $O(n^3)$ classical steps.

One can note that the function h derived from a symmetric-key scheme usually does not satisfy the second condition in Problem 1. However, Kaplan et al. [KLLN16a] showed that Simon's algorithm still usually works even if the second condition is relaxed to the following variant: (2') $\Pr_{x \xleftarrow{\$} \{0,1\}^n}[h(x \oplus s') = h(x)] \leq 1/2$ holds for any $\tilde{s} \in \{0,1\}^n \backslash \{0^n, s\}$. Intuitively, this condition says that there does not exist any $\tilde{s} \neq 0^n$ (other than s) such that "h is almost periodic on $\tilde{s}$." □

2.6 Quantum Security Tools

We recall quantum version of PRP-PRF switching lemma, and how to compute a linear function quantumly.

Proposition 1 (Quantum PRP-PRF switching lemma, Theorem 2 in [Zha15])**.** *For any quantum adversary $\mathcal{A}$ that makes at most q quantum queries to a random permutation over $\{0,1\}^n$, $\mathbf{Adv}^{qPRF}_{RP}(\mathcal{A}) \leq O(q^3/2^n)$ holds.*

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

Proposition 2 (Proposition 5 in [HI19])**.** *For any quantum adversary $\mathcal{A}$ that makes at most q quantum queries, $\mathbf{Adv}^{dist}_{FRP,RF}(q) \leq O(\sqrt{q^6/2^{n/2}})$ holds.*

Given an input x and access to the oracle O_f for a linear function f, the output $f(x)$ can be computed using a single quantum query. However, Hosoyamada and Sasaki [HS18] have shown that it is possible to compute the truncation of $f(x)$ on some bits using only one quantum query to O_f. Bhaumik et al. [BBC+21] extend this result to compute any linear function, not just truncation, using only one quantum query.

Proposition 3 (Lemma 2 in [BBC+21])**.** *Let $f : \{0,1\}^n \to \{0,1\}^m$ be a function, and $O_f : \left|x\right\rangle \left|y\right\rangle \mapsto \left|x\right\rangle \left|y \oplus f(x)\right\rangle$. Let $g : \{0,1\}^m \to \{0,1\}^\ell$ be an $\mathbb{F}_2$-linear function. Then it is possible to construct the oracle $O_{g \circ f} : \left|x\right\rangle \left|y\right\rangle \mapsto \left|x\right\rangle \left|y \oplus (g \circ f)(x)\right\rangle$ using a single query to O_f.*

3 Overview of Recording Standard Oracle with Errors

Next, we provide an overview of the recording standard oracle with errors [HI19], which is an alternative formalization of Zhandry's compressed oracle technique [Zha19]. It enables us to record transcripts of queries made to random functions.

3.1 Standard Oracle.

A random function f is chosen uniformly at random from $\mathsf{Func}(\{0,1\}^m, \{0,1\}^n)$. Quantum oracle access to the function f can be realized by the unitary operator $O_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$. Below, we describe an equivalent model for quantum oracle of a random function, which we call the *standard oracle* (StO).

The function $f : \{0,1\}^m \to \{0,1\}^n$ can be represented as its truth table: a vector of size 2^m where each component is an n-bit string. That is, it can be encoded into an $n \cdot 2^m$-bit string as $f(0)||f(1)||\cdots||f(2^m-1)$. However, we suppose that $f : \{0,1\}^m \to \{0,1\}^n$ can be encoded into an $(n+1)\cdot 2^m$-bit string as $(0||f(0))||(0||f(1))||\cdots||(0||f(2^m-1))$, and f is identified with this bit string[1]. Let StO be the unitary operator that acts on $(n+m+(n+1)2^m)$-qubit states, and is defined as

$$\mathsf{StO} : |x\rangle|y\rangle \otimes |S\rangle \mapsto |x\rangle|y \oplus s_x\rangle \otimes |S\rangle, \tag{2}$$

where $x \in \{0,1\}^m$, $y \in \{0,1\}^n$, and $S = (b_0||s_0)||(b_1||s_1)||\cdots||(b_{2^m-1}||s_{2^m-1})$ with $b_i \in \{0,1\}$ and $s_i \in \{0,1\}^n$ for each $i \in \{0,1\}^m$. When the operator StO does not act on the register b_i for each i, we have $\mathsf{StO} : |x\rangle|y\rangle \otimes |f\rangle \mapsto |x\rangle|y \oplus f(x)\rangle \otimes |f\rangle$ for each function f.

Thus, the standard oracle is the quantum oracle such that the initial state of the oracle is $\sum_f \sqrt{1/2^{n\cdot 2^m}}|f\rangle$ and each quantum query is processed with StO. For any quantum algorithm $\mathcal{A}$ and any (classical) possible output z, it holds that

$$\mathsf{Pr}[z \leftarrow \mathcal{A}^{\mathsf{StO}}] = \mathsf{Pr}[z \leftarrow \mathcal{A}^{\mathsf{RF}}].$$

Notations related to RstOE. Let the database D can be encoded as an $(n+1)\cdot 2^m$-bit string $(b_0||d_0)||\cdots||(b_{2^m-1}||d_{2^m-1})$, where $b_i \in \{0,1\}$, and $d_i \in \{0,1\}^n$ for $0 \le i \le 2^m-1$. We call D a valid database if $d_x \neq 0^n$ holds only if $b_x = 1$. We call D an invalid database if it is not a valid database. Note that, in a valid database, b_x can be either 0 or 1 when $d_x = 0^n$. Hence, for a valid database D, we write

$$D(x) = \begin{cases} y & \text{when } b_x = 1 \text{ and } d_x = y, \\ \perp & \text{when } b_x = 0. \end{cases}$$

When two valid databases $D \neq D'$ which match on all but one input x, such that $D(x) = \perp$ but $D'(x) = \alpha$ $(\neq \perp)$, we write $D' = D \cup \{(x,\alpha)\}$ and $D = D' \backslash \{(x,\alpha)\}$.

On the other hand, when a database D' is invalid, it must have an entry (x,β) such that $b_x = 0$ while $\beta \neq 0^n$. We denote this invalid entry by $(x,\beta)^{\mathsf{invalid}}$. This allows us to construct an invalid database D' from a valid database D (with $D(x) = \perp$) differing in the entry (x,β) as $D' = D \cup (x,\beta)^{\mathsf{invalid}}$.

3.2 Recording Standard Oracle with Errors

Let IH, $\mathsf{U}_{\mathsf{toggle}}$, and CH be unitary operators that act on $(n+1)\cdot 2^m$-qubit states defined as follows:

$$\mathsf{IH} := (I \otimes H^{\otimes n})^{\otimes 2^m},$$
$$\mathsf{U}_{\mathsf{toggle}} := (I_1 \otimes |0^n\rangle\langle 0^n| + X \otimes (I_n - |0^n\rangle\langle 0^n|))^{\otimes 2^m} \text{ where } X|b\rangle = |b \oplus 1\rangle, \text{ and}$$
$$\mathsf{CH} := (CH_n)^{\otimes 2^m} \text{ where } CH_n := |0\rangle\langle 0| \otimes I_n + |1\rangle\langle 1| \otimes H^{\otimes n}.$$

Let $U_{\mathsf{enc}} := \mathsf{CH} \cdot U_{\mathsf{toggle}} \cdot \mathsf{IH}$ and $U_{\mathsf{dec}} := U_{\mathsf{enc}}^*$. We define the unitary operator RstOE that acts on $(n+m+(n+1)\cdot 2^m)$-qubit states by

$$\mathsf{RstOE} := (I_{m+n} \otimes U_{\mathsf{enc}}) \cdot \mathsf{StO} \cdot (I_{m+n} \otimes U_{\mathsf{dec}}). \tag{3}$$

[1] Prefixing $f(i)$ with bit "0" appears redundant at this stage. However, it is required so that the notation for StO is compatible with that for the "Recording Standard Oracle with Errors" introduced later.

Then the recording standard oracle with errors RstOE is defined as follows:

Definition 1 (Recording standard oracle with errors)**.** The recording standard oracle with errors is the quantum oracle such that its initial state is $|0^{(n+1)2^m}\rangle$ and each quantum query is processed with the unitary operator RstOE.

The following proposition shows the main properties of RstOE.

Proposition 4 (Proposition 1 in [HI19, HI20])**.** *Let $x \in \{0,1\}^m$ and D be a valid database such that $D(x) = \perp$. Then the following properties hold.*

1. *For any $y, \alpha \in \{0,1\}^n$, there exists a vector $|\epsilon_1\rangle$ such that*

$$\mathsf{RstOE}|x,y\rangle \otimes |D \cup (x,\alpha)\rangle = |x, y \oplus \alpha\rangle \otimes |D \cup (x,\alpha)\rangle + |\epsilon_1\rangle \tag{4}$$

and $|| \, |\epsilon_1\rangle \, || \leq O(\sqrt{1/2^n})$. More precisely,

$$|\epsilon_1\rangle = \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \left(|D\rangle - \left(\sum_{\beta \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |D \cup (x,\beta)\rangle \right) \right) \tag{5}$$

$$- \frac{1}{\sqrt{2^n}} \sum_{\beta \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \beta\rangle \left(|D \cup (x,\beta)\rangle - |D_\beta^{\mathsf{invalid}}\rangle \right) \tag{6}$$

$$+ \frac{1}{2^n} |x\rangle |\widehat{0^n}\rangle \left(2 \sum_{\beta \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |D \cup (x,\beta)\rangle - |D\rangle \right), \tag{7}$$

where $|D_\beta^{\mathsf{invalid}}\rangle$ is a superposition of invalid databases for each β defined by $|D_\beta^{\mathsf{invalid}}\rangle = \sum_{\gamma \neq 0^n} \frac{(-1)^{\beta \cdot \gamma}}{\sqrt{2^n}} |D \cup (x,\gamma)^{\mathsf{invalid}}\rangle$ and $|\widehat{0^n}\rangle := H^{\otimes 0^n} |0^n\rangle$.

2. *For any $y \in \{0,1\}^n$, there exists a vector $|\epsilon_2\rangle$ such that*

$$\mathsf{RstOE}|x,y\rangle \otimes |D\rangle = \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \otimes |D \cup (x,\alpha)\rangle + |\epsilon_2\rangle \tag{8}$$

and $|| \, |\epsilon_2\rangle \, || \leq O(\sqrt{1/2^n})$. More precisely,

$$|\epsilon_2\rangle = \frac{1}{\sqrt{2^n}} |x\rangle |\widehat{0^n}\rangle \left(|D\rangle - \sum_{\beta \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |D \cup (x,\beta)\rangle \right), \tag{9}$$

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

Remark 1. Roughly speaking, Proposition 4 states that RstOE behaves as a quantum version of the classical lazy sampling (up to a small error) when the state before a query is not superposed. The first property is analogous to the property of classical lazy sampling that respects prior queries. That is, if the query x has already been queried and was responded with α then the response to the current query is α as before, possibly with some errors. The second property is analogous to the classical one for the case when a query x has not been posed earlier. In this case, RstOE samples α uniformly at random and responds with it, possibly with some errors. When the initial state before a query is superposed, the effect of the error terms $|\epsilon_1\rangle$ and $|\epsilon_2\rangle$ becomes non-negligible, and quantum-specific properties (such that a record is deleted or overwritten from the database) emerge. Therefore, careful analysis of quantum security proofs with RstOE is required.

Next, we recall an important Proposition from [HI19, HI20] which shows that when an adversary's register to receive responses from the oracle (i.e., the $|y\rangle$ register) is not superposed, we can ignore the effect that an existing record (x, α) will be deleted from a database. Nevertheless, we cannot ignore the effect that an existing record (x, α) will be overwritten with another record (x, γ).

Proposition 5 (Proposition 3 in [HI19, HI20])**.** *Let y be a fixed n-bit string, and*

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

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

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

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

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

4 Quantum CPA Distinguisher against 3-Round FOX

We now describe a quantum CPA distinguisher against the 3-round FOX construction FOX_3. To construct the CPA-distinguisher, we first define a function h using FOX_3 and show that it is periodic. We then apply Simon's algorithm to h to recover its hidden period in polynomial time.

We write $f(k_i,\cdot)$ as f_i. We also express f_i as $f_{iL}||f_{iR}$, where f_{iL} and f_{iR} denote the left and right halves of f_i, respectively. Let FOX_3 denote the encryption algorithm of the 3-round FOX construction. Figure 2 illustrates FOX_3.

Let $f_1, f_2, f_3 \in \mathsf{Func}(\{0,1\}^{n/2},\{0,1\}^{n/2})$ be the round functions of the FOX construction. FOX_3 takes a plaintext X as input where $X = (x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) \in (\{0,1\}^{n/4})^4$ and outputs a ciphertext $Y = (x_{3LL}, x_{3LR}, x_{3RL}, x_{3RR}) \in (\{0,1\}^{n/4})^4$. These

are given by

$$\begin{aligned}
x_{3LL} &= x_{0LL} \oplus x_{0LR} \oplus g_{1L} \oplus g_{1R} \oplus g_{2R} \oplus g_{3L},\\
x_{3LR} &= x_{0LL} \oplus g_{1L} \oplus g_{2L} \oplus g_{2R} \oplus g_{3R},\\
x_{3RL} &= x_{0RL} \oplus g_{1L} \oplus g_{2L} \oplus g_{3L},\\
x_{3RR} &= x_{0RR} \oplus g_{1R} \oplus g_{2R} \oplus g_{3R},
\end{aligned}$$

where g_{iL} and g_{iR} denote the left and right halves of the output g_i of the function f_i (see Figure 2). For $i = 1, 2, 3$, the outputs g_i are defined as

$$\begin{aligned}
g_1 &= f_1\big((x_{0LL} \oplus x_{0RL}), (x_{0LR} \oplus x_{0RR})\big),\\
g_2 &= f_2\big((x_{0LR} \oplus x_{0RL} \oplus g_{1L} \oplus g_{1R}), (x_{0LL} \oplus x_{0LR} \oplus x_{0RR} \oplus g_{1L})\big),\\
g_3 &= f_3\big((x_{0LL} \oplus x_{0LR} \oplus x_{0RL} \oplus g_{1R} \oplus g_{2L} \oplus g_{2R}), (x_{0LL} \oplus x_{0RR} \oplus g_{1L} \oplus g_{1R} \oplus g_{2L})\big).
\end{aligned}$$

Let $\Pi \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^n)$ be a random permutation that takes a plaintext input $X = (x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) \in (\{0,1\}^{n/4})^4$ and outputs a ciphertext $Y = (x_{3LL}, x_{3LR}, x_{3RL}, x_{3RR}) \in (\{0,1\}^{n/4})^4$.

Problem 2. *Let $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$ be either FOX_3 or a random permutation $\Pi \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^n)$. Given access to the quantum oracle $\mathcal{O}$ with unitary operator $U_{\mathcal{O}} : |X\rangle |Y\rangle \mapsto |X\rangle |Y \oplus \mathcal{O}(X)\rangle$, where $X, Y \in \{0,1\}^n$, the goal is to distinguish the two cases.*

Let us first fix two arbitrary distinct constants $\alpha_0, \alpha_1 \in \{0,1\}^{n/4}$. For $b \in \{0,1\}$, and $X = (x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) \in (\{0,1\}^{n/4})^4$, we construct the function $G^{\mathcal{O}}$ which is defined as:

$$\begin{aligned}
G^{\mathcal{O}} : \{0,1\} \times \{0,1\}^n &\to \{0,1\}^{n/4}\\
(b, X) &\mapsto x_{3LR} \oplus x_{3RL} \oplus (x_{3RR} \oplus \alpha_b),
\end{aligned}$$

where $X = (x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) = (x \oplus \alpha_b, y, x, y \oplus \alpha_b)$ with $x, y \in \{0,1\}^{n/4}$, and $(x_{3LL}, x_{3LR}, x_{3RL}, x_{3RR}) = \mathcal{O}(x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR})$.

More precisely, the function $G^{\mathcal{O}}$ which is illustrated in Figure 2, can be described as

$$\begin{aligned}
G^{\mathcal{O}}(b, x \oplus \alpha_b, y, x, y \oplus \alpha_b) = x \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{2R}\Big(&\big(x \oplus y \oplus f_{1L}(\alpha_b, \alpha_b)\\
&\oplus f_{1R}(\alpha_b, \alpha_b)\big), \big(x \oplus f_{1L}(\alpha_b, \alpha_b)\big)\Big). \qquad (10)
\end{aligned}$$

We now define another function $h(b, x, y)$ using Equation (10), which is as follows:

$$h(b, x, y) := G^{\mathcal{O}}(b, x \oplus \alpha_b, y, x, y \oplus \alpha_b). \qquad (11)$$

Note that both $G^{\mathcal{O}}$ and h can be evaluated in quantum superpositions. We can realize the unitary operator $U_h : |X\rangle |Y\rangle \mapsto |X\rangle |Y \oplus h(X)\rangle$ which makes quantum queries to h. Hence we can apply Simon's algorithm [Sim97] to recover the period of the function h when it is periodic.

Lemma 1. *If $\mathcal{O} = \mathsf{FOX}_3$, the function h satisfies $h(b, x, y) = h(b', x', y')$ if $b' = b \oplus 1$, $x' = x \oplus f_{1L}(\alpha_0\alpha_0) \oplus f_{1L}(\alpha_1\alpha_1)$ and $y' = y \oplus f_{1R}(\alpha_0\alpha_0) \oplus f_{1R}(\alpha_1\alpha_1)$ for any $x, x', y, y' \in \{0,1\}^{n/4}$. That is, h has the period $(1, s) = \big(1, f_{1L}(\alpha_0\alpha_0) \oplus f_{1L}(\alpha_1\alpha_1), f_{1R}(\alpha_0\alpha_0) \oplus f_{1R}(\alpha_1\alpha_1)\big)$.*

Proof. Let us consider the intermediate state value after 1-round of FOX given by the following expression

$$(x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}) = \zeta(\Phi(X)) = \zeta\big(\Phi(x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR})\big). \qquad (12)$$

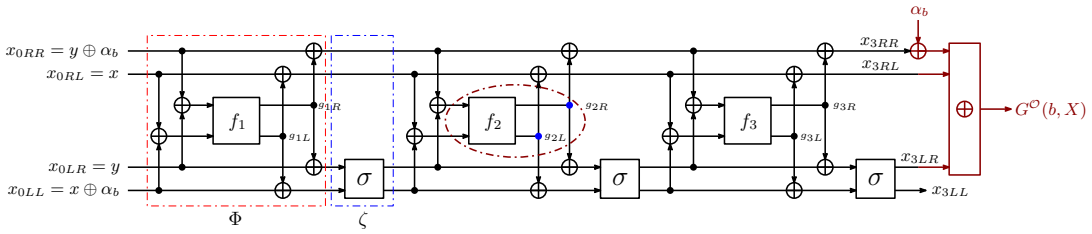


Figure 2: The function $G^{\mathcal{O}}$ with FOX_3, where $\mathcal{O} = \mathsf{FOX}_3$, and $f_i \in \mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$. A detailed view of $G^{\mathcal{O}}$ (with all intermediate calculations after each round) is also provided in Appendix A.

To build a qCPA distinguisher against FOX_3, our goal is to find two different inputs $X = (x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR})$ and $X' = (x'_{0LL}, x'_{0LR}, x'_{0RL}, x'_{0RR})$ such that the inputs $\big((x_{1LL} \oplus x_{1RL}), (x_{1LR} \oplus x_{1RR})\big)$ and $\big((x'_{1LL} \oplus x'_{1LR}), (x'_{1RL} \oplus x'_{1RR})\big)$ to the function f_2 collide. The inputs and outputs of f_2 are shown in red-colored oval in Figure 2.

Considering the input X as $X = (x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) = (x \oplus \alpha_b, y, x, y \oplus \alpha_b)$ with $b \in \{0,1\}$, Equation (12) becomes

$$\begin{aligned}(x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}) &= \zeta\big(\Phi(x \oplus \alpha_b, y, x, y \oplus \alpha_b)\big)\\ &= \zeta\big(x \oplus \alpha_b \oplus f_{1L}(\alpha_b, \alpha_b), y \oplus f_{1R}(\alpha_b, \alpha_b), x \oplus f_{1L}(\alpha_b, \alpha_b), y \oplus \alpha_b \oplus f_{1R}(\alpha_b, \alpha_b)\big)\\ &= \big(y \oplus f_{1R}(\alpha_b, \alpha_b), x \oplus y \oplus \alpha_b \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{1R}(\alpha_b, \alpha_b), x \oplus f_{1L}(\alpha_b, \alpha_b),\\ &\qquad y \oplus \alpha_b \oplus f_{1R}(\alpha_b, \alpha_b)\big). \quad (13)\end{aligned}$$

On the other hand, if we consider the input X' as $X' = (x'_{0LL}, x'_{0LR}, x'_{0RL}, x'_{0RR}) = \big(x \oplus \alpha_{b\oplus 1} \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), y \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1), x \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), y \oplus \alpha_{b\oplus 1} \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1)\big)$, then Equation (12) becomes

$$\begin{aligned}(x'_{1LL}, x'_{1LR}, x'_{1RL}, x'_{1RR}) &= \zeta\big(\Phi(X')\big)\\ &= \zeta\big(\Phi(x \oplus \alpha_{b\oplus 1} \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), y \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1),\\ &\qquad x \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), y \oplus \alpha_{b\oplus 1} \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1))\big)\\ &= \zeta\big((x \oplus \alpha_{b\oplus 1} \oplus f_{1L}(\alpha_b, \alpha_b), y \oplus f_{1R}(\alpha_b, \alpha_b), x \oplus f_{1L}(\alpha_b, \alpha_b),\\ &\qquad y \oplus \alpha_{b\oplus 1} \oplus f_{1R}(\alpha_b, \alpha_b))\big)\\ &= \big(y \oplus f_{1R}(\alpha_b, \alpha_b), x \oplus y \oplus \alpha_{b\oplus 1} \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{1R}(\alpha_b, \alpha_b), x \oplus f_{1L}(\alpha_b, \alpha_b),\\ &\qquad y \oplus \alpha_{b\oplus 1} \oplus f_{1R}(\alpha_b, \alpha_b)\big). \quad (14)\end{aligned}$$

From Equations (13) and (14), we can easily see that

$$\begin{aligned}&x_{1LL} \oplus x_{1RL} = x'_{1LL} \oplus x'_{1RL} = x \oplus y \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{1R}(\alpha_b, \alpha_b), \text{ and}\\ &x_{1LR} \oplus x_{1RR} = x'_{1LR} \oplus x'_{1RR} = x \oplus f_{1L}(\alpha_b, \alpha_b).\end{aligned}$$

This shows that the inputs to second round function f_2 collide.

On summing up x_{3LR}, x_{3RL} and x_{3RR} with α_b (see Figure 2), the function $G^{\mathcal{O}}$ can be described as given in Equation (10). Using $G^{\mathcal{O}}$, we can show that h, as defined in Equation (11), has the claimed period since it satisfies

$$\begin{aligned}h(b', x', y') &= G^{\mathcal{O}}\big(b \oplus 1, x \oplus \alpha_{b\oplus 1} \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1),\\ &\qquad x \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), y \oplus \alpha_{b\oplus 1} \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1)\big)\\ &= x \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{2R}\big((x \oplus y \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{1R}(\alpha_b, \alpha_b)), (x \oplus f_{1L}(\alpha_b, \alpha_b))\big)\end{aligned}$$

$$= G^{\mathcal{O}}(b, x \oplus \alpha_b, y, x, y \oplus \alpha_b)$$
$$= h(b, x, y).$$

This proves the lemma. □

Therefore, we can construct a distinguisher against FOX_3 by applying Simon's algorithm to h, whose period $(1, s)$ can be recovered in polynomial time. As a result, the 3-round FOX construction is not a PRP against qCPAs.

5 Quantum CCA Distinguisher against the 4-Round FOX

To develop a qCCA distinguisher against the 4-round FOX construction FOX_4, we use a strategy similar to the one described in Section 4. That is, we construct a function h using FOX_4 and show that it is periodic and then recover this period by applying Simon's algorithm to h. Recall that the orthomorphism σ for the FOX construction is defined as $\sigma(x_1, x_2) = (x_2, x_1 \oplus x_2) = (y_1, y_2)$, and thus its inverse σ' can be defined as $\sigma'(y_1, y_2) = (y_1 \oplus y_2, y_1) = (x_2 \oplus x_1 \oplus x_2, x_2) = (x_1, x_2)$.

We write $f(k_i, \cdot)$ as f_i as in the previous section. Let FOX_4 denote the encryption algorithm of the 4-round FOX construction, and FOX_4^{-1} denote its decryption algorithm. Let $f_1, f_2, f_3, f_4 \in \mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$ be the round functions of the FOX construction. The encryption $\mathsf{FOX}_4 : (x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) \mapsto (x_{4LL}, x_{4LR}, x_{4RL}, x_{4RR})$ is defined as

$$x_{4LL} = x_{0LL} \oplus g_{1L} \oplus g_{2L} \oplus g_{2R} \oplus g_{3R} \oplus g_{4L}, \tag{15}$$
$$x_{4LR} = x_{0LR} \oplus g_{1R} \oplus g_{2L} \oplus g_{3L} \oplus g_{3R} \oplus g_{4R}, \tag{16}$$
$$x_{4RL} = x_{0RL} \oplus g_{1L} \oplus g_{2L} \oplus g_{3L} \oplus g_{4L}, \tag{17}$$
$$x_{4RR} = x_{0LL} \oplus g_{1R} \oplus g_{2R} \oplus g_{3R} \oplus g_{4R}, \tag{18}$$

where g_{iL} and g_{iR} denote the left and right halves of output g_i of the function f_i as shown in Figure 3. For $i = 1, 2, 3, 4$, functions g_i are defined as follows:

$$g_1 = f_1\big((x_{0LL} \oplus x_{0RL}), (x_{0LR} \oplus x_{0RR})\big), \tag{19}$$
$$g_2 = f_2\big((x_{0LR} \oplus x_{0RL} \oplus g_{1L} \oplus g_{1R}), (x_{0LL} \oplus x_{0LR} \oplus x_{0RR} \oplus g_{1L})\big), \tag{20}$$
$$g_3 = f_3\big((x_{0LL} \oplus x_{0LR} \oplus x_{0RL} \oplus g_{1R} \oplus g_{2L} \oplus g_{2R}), (x_{0LL} \oplus x_{0RR} \oplus g_{1L} \oplus g_{1R} \oplus g_{2L})\big), \tag{21}$$
$$g_4 = f_4\big((x_{0LL} \oplus x_{0RL} \oplus g_{2R} \oplus g_{3L} \oplus g_{3R}), (x_{0LR} \oplus x_{0RR} \oplus g_{2L} \oplus g_{2R} \oplus g_{3L})\big). \tag{22}$$

The decryption $\mathsf{FOX}_4^{-1} : (x_{4LL}, x_{4LR}, x_{4RL}, x_{4RR}) \mapsto (x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR})$ is defined by

$$x_{0LL} = x_{4LL} \oplus g'_{4L} \oplus g'_{3R} \oplus g'_{2L} \oplus g'_{1L}, \tag{23}$$
$$x_{0LR} = x_{0LR} \oplus g'_{4R} \oplus g'_{3L} \oplus g'_{3R} \oplus g'_{2L} \oplus g'_{1R}, \tag{24}$$
$$x_{0RL} = x_{0RL} \oplus g'_{4L} \oplus g'_{3L} \oplus g'_{2L} \oplus g'_{1L}, \tag{25}$$
$$x_{0RR} = x_{0RR} \oplus g'_{4R} \oplus g'_{3R} \oplus g'_{2R} \oplus g'_{1R}, \tag{26}$$

where g'_{iL} and g'_{iR} denote the left and right halves of output g'_i of the function f_i during the decryption process. For $i = 4, 3, 2, 1$, functions g'_i are defined as follows:

$$g'_4 = f_4\big((x_{4LL} \oplus x_{4RL}), (x_{4LR} \oplus x_{4RR})\big), \tag{27}$$
$$g'_3 = f_3\big((x_{4LL} \oplus x_{4LR} \oplus x_{4RL} \oplus g'_{4R}), (x_{4LL} \oplus x_{4RR} \oplus g'_{4L} \oplus g'_{4R})\big), \tag{28}$$
$$g'_2 = f_2\big((x_{4LR} \oplus x_{4RL} \oplus g'_{4L} \oplus g'_{4R} \oplus g'_{3R}), (x_{4LL} \oplus x_{4LR} \oplus x_{4RR} \oplus g'_{4L})\big) \tag{29}$$

$$g'_1 = f_1\big((x_{4LL} \oplus x_{4RL} \oplus g'_{3L} \oplus g'_{3R} \oplus g'_{2R}), (x_{4LR} \oplus x_{4RR} \oplus g'_{3L} \oplus g'_{2L} \oplus g'_{2R})\big). \tag{30}$$

Let $\Pi \xleftarrow{\$} \mathsf{Perm}(\{0,1\}^n)$ be a random permutation that takes input as a plaintext $X = (x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) \in (\{0,1\}^{n/4})^4$ and outputs a ciphertext $Y = (x_{4LL}, x_{4LR}, x_{4RL}, x_{4RR}) \in (\{0,1\}^{n/4})^4$.

Problem 3. *Let $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$ be either FOX_4 or Π. Given access to the quantum oracle $\mathcal{O}$ and $\mathcal{O}^{-1}$, our goal is to distinguish these two cases.*

Suppose that $\alpha_0, \alpha_1 \in \{0,1\}^{n/4}$ be two arbitrary distinct constants. We construct the function $G^{\mathcal{O}}$ as follows:

$$\begin{aligned} G^{\mathcal{O}} : \{0,1\} \times \{0,1\}^n &\to \{0,1\}^{n/4} \\ (b, X) &\mapsto x'_{0LL} \oplus x'_{0LR} \oplus x'_{0RL} \oplus x'_{0RR}, \end{aligned}$$

where $(x_{4LL}, x_{4LR}, x_{4RL}, x_{4RR}) = \mathcal{O}(x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) = \mathcal{O}(x \oplus \alpha_b, y, x, y \oplus \alpha_b)$, and $(x'_{0LL}, x'_{0LR}, x'_{0RL}, x'_{0RR}) = \mathcal{O}^{-1}\big((x_{4LL} \oplus \alpha_0 \oplus \alpha_1), x_{4LR}, (x_{4RL} \oplus \alpha_0 \oplus \alpha_1), (x_{4RR} \oplus \alpha_0 \oplus \alpha_1)\big)$.

That is, $G^{\mathcal{O}}$ is designed by first encrypting $X = (x \oplus \alpha_b, y, x, y \oplus \alpha_b)$ to obtain the ciphertext $(x_{4LL}, x_{4LR}, x_{4RL}, x_{4RR})$, and then decrypting $\big((x_{4LL} \oplus \alpha_0 \oplus \alpha_1), x_{4LR}, (x_{4RL} \oplus \alpha_0 \oplus \alpha_1), (x_{4RR} \oplus \alpha_0 \oplus \alpha_1)\big)$ to obtain the plaintext $(x'_{0LL}, x'_{0LR}, x'_{0RL}, x'_{0RR})$.

If $\mathcal{O}$ is FOX_4, then by connecting FOX_4 and FOX_4^{-1}, the function $G^{\mathcal{O}}$ is illustrated in Figure 3. Formally, the function $G^{\mathcal{O}}$ can be described as

$$G^{\mathcal{O}}(b, X) = g_{2L}(b, X) \oplus g'_{2L}(b, X) \oplus g_{3L}(b, X) \oplus g'_{3L}(b, X) \oplus g_{3R}(b, X) \oplus g'_{3R}(b, X), \tag{31}$$

where $g_{2L}(b, X)$ and $g_{2R}(b, X)$ denote the left and right halves of $g_2(b, X)$, $g_{3L}(b, X)$, and likewise for g_3, g'_2, and g'_3.

$$g_2(b, X) = f_2\Big(\big(x \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{1R}(\alpha_b, \alpha_b)\big), \big(x \oplus f_{1L}(\alpha_b \alpha_b)\big)\Big) \tag{32}$$

$$\begin{aligned} g_3(\beta, X) = f_3\Big(&\big(\alpha_b \oplus f_{1R}(\alpha_b, \alpha_b) \oplus g_{2L} \oplus g_{2R}\big), \\ &\big(x \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{1R}(\alpha_b, \alpha_b) \oplus g_{2L}\big)\Big) \end{aligned} \tag{33}$$

$$\begin{aligned} g'_3(\beta, X) = f_3\Big(&\big(\alpha_{b\oplus 1} \oplus f_{1R}(\alpha_b, \alpha_b) \oplus g_{2L} \oplus g_{2R}\big), \\ &\big(x \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{1R}(\alpha_b, \alpha_b) \oplus g_{2L}\big)\Big) \end{aligned} \tag{34}$$

$$\begin{aligned} g'_2(b, X) = f_2\Big(&\big(x \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{1R}(\alpha_b, \alpha_b) \oplus g_{3R} \oplus g'_{3R}\big), \\ &\big(x \oplus \alpha_0 \oplus \alpha_1 \oplus f_{1L}(\alpha_b, \alpha_b) \oplus g_{3L} \oplus g'_{3L} \oplus g_{3R} \oplus g'_{3R}\big)\Big). \end{aligned} \tag{35}$$

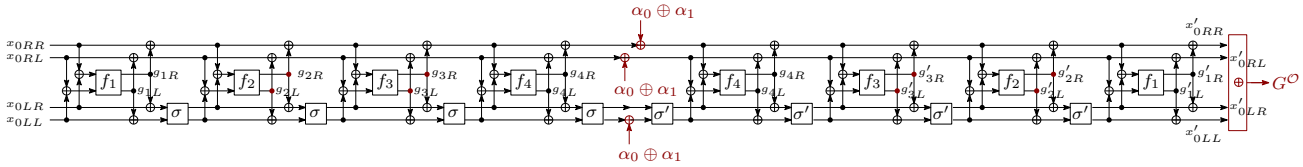


Figure 3: The function $G^{\mathcal{O}}$ with $\mathcal{O} = \mathsf{FOX}_4$, $\mathcal{O}^{-1} = \mathsf{Inverse\text{-}FOX}_4$, and $f_i \in \mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$. A detailed view of $G^{\mathcal{O}}$ with all intermediate calculations is also provided in Appendix B.

We now design a function h based on $G^{\mathcal{O}}$ defined by Equation (31) as follows:

$$h(b, x, y) := G^{\mathcal{O}}(b, X) = G^{\mathcal{O}}(b, x \oplus \alpha_b, y, x, y \oplus \alpha_b). \tag{36}$$

Lemma 2. *If $\mathcal{O} = \mathsf{FOX}_4$, the function h satisfies the following*

$$h(b, x, y) = h(b \oplus 1, x \oplus f_{1L}(\alpha_0\alpha_0) \oplus f_{1L}(\alpha_1\alpha_1), y \oplus f_{1R}(\alpha_0\alpha_0) \oplus f_{1R}(\alpha_1\alpha_1)).$$

That is, h has the period $(1, s) = \big(1, f_{1L}(\alpha_0\alpha_0) \oplus f_{1L}(\alpha_1\alpha_1), f_{1R}(\alpha_0\alpha_0) \oplus f_{1R}(\alpha_1\alpha_1)\big)$.

Proof. Assume that $X = (x \oplus \alpha_b, y, x, y \oplus \alpha_b)$. Now consider the function $g_2(b, X)$ as defined in (32):

$$g_2(b, X) = f_2\Big(\big(x \oplus f_{1L}(\alpha_b, \alpha_b) \oplus f_{1R}(\alpha_b, \alpha_b)\big), \big(x \oplus f_{1L}(\alpha_b, \alpha_b)\big)\Big).$$

It can be easily observed that the above expression is similar to the one given in Equation (10), and we have already shown in Lemma 1 that the following holds

$$g_2\big((b, X) \oplus (1, t)\big) = g_2(b, X) \tag{37}$$

for some value of t given by

$$\begin{aligned} t = \big(&\alpha_0 \oplus \alpha_1 \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1), \\ &f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), \alpha_0 \oplus \alpha_1 \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1)\big). \end{aligned} \tag{38}$$

Further, notice that $\{\alpha_b, \alpha_b \oplus \alpha_0 \oplus \alpha_1\} = \{\alpha_0, \alpha_1\}$. Based on this fact, our next claim is that the function $g_3 \oplus g_3'$ also satisfies $(g_3 \oplus g_3')\big((b, X) \oplus (1, t)\big) = (g_3 \oplus g_3')(b, X)$ for some t. From Equations (33), (34) and the fact that $g_2\big((b, X) \oplus (1, t)\big) = g_2(b, X)$, we can easily see that the following holds for the value of t given in Equation (38) :

$$g_3\big((b, X) \oplus (1, t)\big) \oplus g_3'\big((b, X) \oplus (1, t)\big) = g_3(b, X) \oplus g_3'(b, X). \tag{39}$$

We now claim that $g_2'(b, X)$ also satisfies the condition $g_2'\big((b, X) \oplus (1, t)\big) = g_2'(b, X)$. From Equation (35), we can observe that g_2' depends upon g_2, g_3 and g_3'. Thus, using Equations (37) and (39), it also holds that

$$g_2'\big((b, X) \oplus (1, t)\big) = g_2'(b, X). \tag{40}$$

Consequently, the function $G^{\mathcal{O}}$ defined in (31) also satisfies $G^{\mathcal{O}}\big((b, X) \oplus (1, t)\big) = G^{\mathcal{O}}(b, X)$ for the value of t given in Equation (38).

Therefore, we can conclude that the function h as defined in Equation (36), has the claimed period, since we have

$$\begin{aligned} &h\big(b \oplus 1, x \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), y \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1)\big) \\ &\quad = G^{\mathcal{O}}\big(b \oplus 1, x \oplus \alpha_{b\oplus 1} \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1), \\ &\qquad\qquad x \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), y \oplus \alpha_{b\oplus 1} \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1)\big) \\ &\quad = G^{\mathcal{O}}(b, x \oplus \alpha_b, y, x, y \oplus \alpha_b) \\ &\quad = h(b, x, y). \end{aligned}$$

This completes the proof of the lemma. □

6 Security Proof: 4-round FOX is a PRP against qCPAs

This section gives a quantum query lower bound for the problem of distinguishing 4-round FOX construction FOX_4 from a random permutation RP, under the assumption that all the round functions of FOX_4 are truly random functions. Specifically, we prove the following theorem.

Theorem 1. *Let q be a positive integer and $\mathcal{A}$ be an adversary that makes at most q quantum queries. Further, let $\mathbf{Adv}^{qPRP}_{\mathsf{FOX}_4}(\mathcal{A})$ denote the advantage of adversary $\mathcal{A}$ in distinguishing FOX_4 from a random permutation. Then, the following holds*

$$\mathbf{Adv}^{qPRP}_{\mathsf{FOX}_4}(\mathcal{A}) \in O(\sqrt{q^6/2^{n/2}}).$$

Next, we define a collision event at the output of round r of the FOX construction. If we can find two different values colliding at the input to f_{r+1} then this will allow an adversary to distinguish the Lai-Massey scheme from a random permutation.

Definition 2 (XOR-Collision)**.** Assume the output of two queries at round r is $(x_{(r)LL}, x_{(r)LR}, x_{(r)RL}, x_{(r)RR})$ and $(x'_{(r)LL}, x'_{(r)LR}, x'_{(r)RL}, x'_{(r)RR})$, $r \geq 0$, we say that two queries *collide* at round r if the following two conditions are satisfied:

1. $x_{(r)LL} \oplus x_{(r)RL} = x'_{(r)LL} \oplus x'_{(r)RL}$, and
2. $x_{(r)LR} \oplus x_{(r)RR} = x'_{(r)LR} \oplus x'_{(r)RR}$.

An Overview of Classical Security Proof for FOX_3 by Luo et al. [LLH15]. We briefly discuss a classical proof for the security of FOX_3 against chosen plaintext attacks. Let bad_2 be the event that an adversary makes two distinct plaintext queries $(x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) \neq (x'_{0LL}, x'_{0LR}, x'_{0RL}, x'_{0RR})$ to the real oracle FOX_3 such that the inputs $(x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR})$ and $(x'_{1LL} \oplus x'_{1RL}, x'_{1LR} \oplus x'_{1RR})$ to the second round function f_2 are equal, i.e., inputs to f_2 collide. In addition, let bad_3 be the event that inputs to f_3 collide. Define $\mathsf{bad} := \mathsf{bad}_2 \wedge \mathsf{bad}_3$. If bad_2 (resp. bad_3) does not occur then FOX_3's outputs cannot be distinguished from truly random strings. Thus, unless the event bad occurs, adversaries cannot distinguish FOX_3 from random functions.

If the number of queries made by an adversary $\mathcal{A}$ is at most q, we can show that the probability for the bad event to occur is $O(q^2/2^{n/2})$. Thus we can deduce that FOX_3 is indistinguishable from a random function up to $O(2^{n/4})$ queries.

Observation: Why does the classical proof technique not extend to the quantum setting? It is interesting to observe that quantum adversaries can distinguish FOX_3 from random permutations even though FOX_3 is proven to be indistinguishable from a random permutation in the classical setting.

As described in Section 4, we can efficiently find the period $(1, s) = \big(1, \big(\alpha_0 \oplus \alpha_1 \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1), f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), \alpha_0 \oplus \alpha_1 \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1)\big)\big)$ given quantum access to the oracle FOX_3 with $O(n)$ quantum queries. Once the period is known, it is easy to create a bad_2 event (collision on the input of f_2) in two queries as follows.

Take $x \in \{0,1\}^{n/4}$ arbitrarily and set $(x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}) = (x \oplus \alpha_0, 0, x, \alpha_0)$ and $(x'_{0LL}, x'_{0LR}, x'_{0RL}, x'_{0RR}) = \big(x \oplus \alpha_1 \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1), x \oplus f_{1L}(\alpha_0, \alpha_0) \oplus f_{1L}(\alpha_1, \alpha_1), \alpha_1 \oplus f_{1R}(\alpha_0, \alpha_0) \oplus f_{1R}(\alpha_1, \alpha_1)\big)$. Then the corresponding inputs to f_2 become $\big(x \oplus f_{1L}(\alpha_0\alpha_0) \oplus f_{1R}(\alpha_0\alpha_0)), (x \oplus f_{1L}(\alpha_0\alpha_0)\big)$ for both the plaintexts.

This shows that the classical proof idea for the security of FOX_3 does not work in the quantum setting.

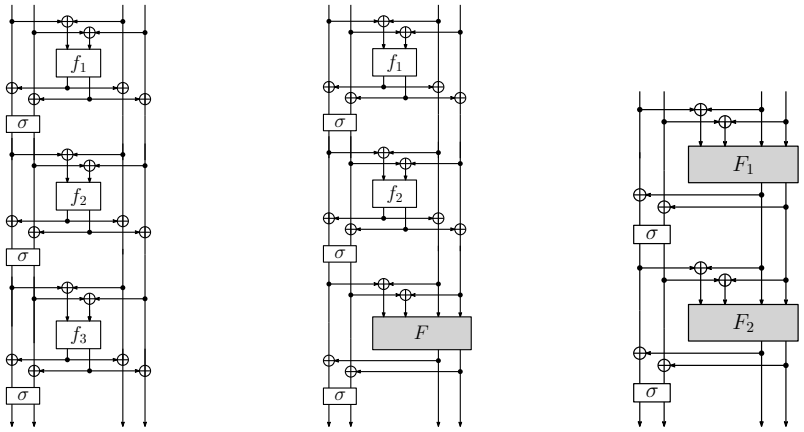
Quantum Security Proof for FOX_4: The idea. The essence of the quantum attack on FOX_3 is to find a collision on the inputs to the second round function f_2. On the other hand, finding collisions for inputs to the third round function f_3 seems difficult even for quantum (chosen-plaintext) query adversaries. We later prove that this is indeed the case.

With these observations, our starting point is to modify FOX_3 to a new function FOX'_3 such that even quantum adversaries can't distinguish between these two. The modified function FOX'_3 (see Figure 4b) uses the first two round functions f_1 and f_2 exactly the same as FOX_3. The third state update for FOX'_3 is modified as follows.

$$\begin{aligned}(x_{3LL}, x_{3LR}, x_{3RL}, x_{3RR}) := \big(&x_{2LR} \oplus F_R(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}),\\ &x_{2LL} \oplus x_{2LR} \oplus F_L(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR})\\ &\qquad \oplus F_R(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}),\\ &F_L(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}),\\ &F_R(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR})\big),\end{aligned}$$

where $F : \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \to \{0,1\}^{n/2}$ is a random function.

We show that it is hard to distinguish FOX'_3 from FOX_3. The idea behind the modification of FOX_3 to FOX'_3 is to avoid one of the two colliding conditions mentioned in Definition 2. We show this by using the "recording standard oracle with errors" proof technique. We define "bad" databases as the ones that contains "collisions at inputs to the third round function". Then we show that the probability that a bad database is measured is negligible. We also show that the adversary cannot distinguish FOX'_3 from FOX_3 when the database is not bad.



(a) FOX_3 (b) FOX'_3 (c) FOX'_2

Figure 4: The modified versions of FOX_3 and FOX_2.

Next, let FOX'_2 denotes a modified version of the 2-round FOX construction (see Figure 4c) such that the first state update is modified as follows

$$\begin{aligned}(x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}) := \big(&x_{0LR} \oplus F_{1R}(x_{0LL} \oplus x_{0RL}, x_{0LR} \oplus x_{0RR}, x_{0RL}, x_{0RR}),\\ &x_{0LL} \oplus x_{0LR} \oplus F_{1L}(x_{0LL} \oplus x_{0RL}, x_{0LR} \oplus x_{0RR}, x_{0RL}, x_{0RR})\\ &\qquad \oplus F_{1R}(x_{0LL} \oplus x_{0RL}, x_{0LR} \oplus x_{0RR}, x_{0RL}, x_{0RR}),\\ &F_{1L}(x_{0LL} \oplus x_{0RL}, x_{0LR} \oplus x_{0RR}, x_{0RL}, x_{0RR}),\\ &F_{1R}(x_{0LL} \oplus x_{0RL}, x_{0LR} \oplus x_{0RR}, x_{0RL}, x_{0RR})\big),\end{aligned}$$

where $F_1 : \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \to \{0,1\}^{n/2}$ is a random function.

Furthermore, the second state update is modified as

$$\begin{aligned}(x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}) := \big(&x_{1LR} \oplus F_{2R}(x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR}, x_{1RL}, x_{1RR}),\\ &x_{1LL} \oplus x_{1LR} \oplus F_{2L}(x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR}, x_{1RL}, x_{1RR})\\ &\qquad \oplus F_{2R}(x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR}, x_{1RL}, x_{1RR}),\\ &F_{2L}(x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR}, x_{1RL}, x_{1RR}),\\ &F_{2R}(x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR}, x_{1RL}, x_{1RR})\big),\end{aligned}$$

where $F_2 : \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \to \{0,1\}^{n/2}$ is a random function. Then, we intuitively see that FOX'_2 is hard to distinguish from a random function RF from $\{0,1\}^n$ to $\{0,1\}^{n/2}$.

Our next goal is to show the two properties mentioned above, i.e.,

1. FOX'_3 is hard to distinguish from FOX_3, and
2. FOX'_2 is hard to distinguish from RF.

Once these two properties are proven, the proof of Theorem 1 follows in a straightforward manner. To show the first property, we use the recording standard oracle with errors technique. For the second property, we can show it by using some previous results.

6.1 Hardness of Distinguishing FOX'_3 from FOX_3

Proposition 6. *Let $\mathcal{A}$ be an adversary that makes at most q quantum queries. Then,* $\mathbf{Adv}^{dist}_{\mathsf{FOX}'_3,\mathsf{FOX}_3}(\mathcal{A}) \leq O(\sqrt{q^3/2^{n/2}})$.

First, we discuss the behavior of the quantum oracles for FOX'_3 and FOX_3.

Quantum Oracle for FOX_3. Let O_{f_i} be the quantum oracle for each round function f_i. In addition, let us define the unitary operator $O_{\mathsf{UP}.i}$ that computes the state update of the i-th round by

$$\begin{aligned}O_{\mathsf{UP}.i} : &|x_{(i-1)LL}, x_{(i-1)LR}, x_{(i-1)RL}, x_{(i-1)RR}\rangle\,|y_{LL}\rangle\,|y_{LR}\rangle\,|y_{RL}\rangle\,|y_{RR}\rangle\\ \mapsto\ &|x_{(i-1)LL}, x_{(i-1)LR}, x_{(i-1)RL}, x_{(i-1)RR}\rangle\\ &|y_{LL} \oplus x_{(i-1)LR} \oplus f_{iR}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR})\rangle\\ &|y_{LR} \oplus x_{(i-1)LL} \oplus x_{(i-1)LR} \oplus f_{iR}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR})\\ &\qquad \oplus f_{iR}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR})\rangle\\ &|y_{RL} \oplus x_{(i-1)RL} \oplus f_{iL}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR})\rangle\\ &|y_{RR} \oplus x_{(i-1)RR} \oplus f_{iR}(x_{(i-1)LL} \oplus x_{(i-1)RL}, x_{(i-1)LR} \oplus x_{(i-1)RR})\rangle\,.\end{aligned}$$

Following Proposition 3, the oracle $O_{\mathsf{UP}.i}$ can be implemented by making a single query to f_i. The same is $O_{\mathsf{UP}.i}$ is also illustrated in Figure 5.

This allows us to implement quantum oracle for FOX_3 by making two queries to $O_{\mathsf{UP}.1}$ and $O_{\mathsf{UP}.2}$, and one query to $O_{\mathsf{UP}.3}$ (see Figure 6).

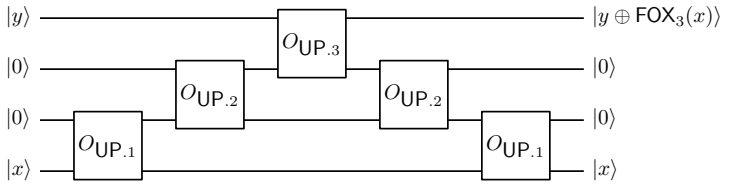


Figure 6: Implementation of FOX_3.

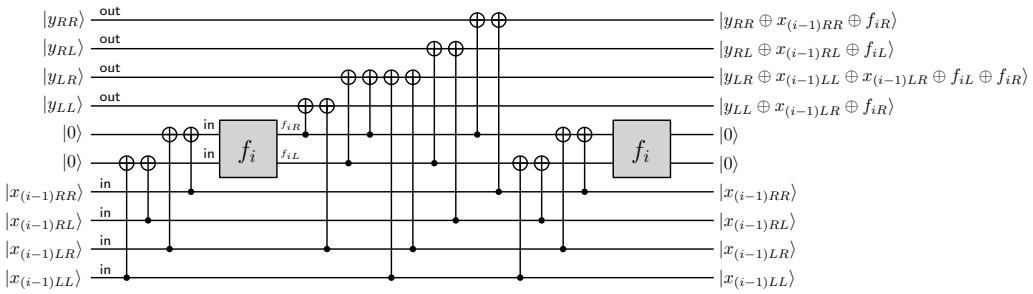


Figure 5: Implementation of $O_{\mathsf{UP}.i}$. The function f_i can be implemented using RstOE.

Quantum Oracle for FOX'_3. The quantum oracle for FOX'_3 is implemented in the same way as FOX_3, except that the third round state update oracle $O_{\mathsf{UP}.3}$ is replaced with another oracle $O'_{\mathsf{UP}.3}$ defined as

$$\begin{aligned}
O'_{\mathsf{UP}.3} : &|x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}\rangle\,|y_{LL}\rangle\,|y_{LR}\rangle\,|y_{RL}\rangle\,|y_{RR}\rangle \\
&\mapsto |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}\rangle \\
&\quad |y_{LL} \oplus x_{2LR} \oplus F_R(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2LR}, x_{2RR})\rangle \\
&\quad |y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus F_L(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2LR}, x_{2RR}) \\
&\qquad\qquad \oplus F_R(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2LR}, x_{2RR})\rangle \\
&\quad |y_{RL} \oplus F_L(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2LR}, x_{2RR})\rangle \\
&\quad |y_{RR} \oplus F_L(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2LR}, x_{2RR})\rangle\,.
\end{aligned}$$

Following Proposition 3, we can also implement $O'_{\mathsf{UP}.3}$ by making one query to O_F (the quantum oracle of F).

In what follows, we consider that the oracles for the functions f_i and F are implemented as the recording standard oracle with errors, and we use D_1, D_2, D_3, and D_F to denote (valid) databases for f_1, f_2, f_3, and F, respectively. In particular, after the i-th query of an adversary to FOX_3, the joint quantum states of the adversary and these functions can be described as $\sum_{x,y,z,D_1,D_2,D_3} a_{x,y,z,D_1,D_2,D_3}\,|x,y,z\rangle \otimes |D_1\rangle\,|D_2\rangle\,|D_3\rangle$ for some complex numbers a_{x,y,z,D_1,D_2,D_3} such that $\sum_{x,y,z,D_1,D_2,D_3} |a_{x,y,z,D_1,D_2,D_3}|^2 = 1$. Here, x, y, and z correspond to the adversary's register to send queries to the oracles, receive answers from oracles, and perform offline computations, respectively. (If the oracle is FOX'_3, then the register $|D_3\rangle$ corresponding to f_3 is replaced with $|D_F\rangle$ corresponding to F.)

Next, we define good and bad databases for FOX_3 and FOX'_3. Intuitively, we say that a tuple (D_1, D_2, D_3) (resp. (D_1, D_2, D_F)) for FOX_3 (resp. FOX'_3) is bad if and only if it contains the information that some inputs to f_3 (resp. 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 FOX_3 and those for FOX'_3.

Good and Bad databases for FOX_3. We say that a database (D_1, D_2, D_3) for FOX_3 is good if, for each entry $((x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}), \gamma) \in D_3$ (where $\gamma = (\gamma_1||\gamma_2)$), there exists exactly one pair $(((x_{0LL} \oplus x_{0RL}, x_{0LR} \oplus x_{0RR}), \alpha), ((x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR}), \beta)) \in D_1 \times D_2$ (where $\alpha = \alpha_1||\alpha_2$ and $\beta = \beta_1||\beta_2$) such that $x_{0LL} \oplus x_{0LR} \oplus x_{0RL} \oplus \alpha_2 \oplus \beta_1 \oplus \beta_2 = x_{2LL} \oplus x_{2RL}$ and $x_{0LL} \oplus x_{0RR} \oplus \alpha_1 \oplus \alpha_2 \oplus \beta_1 = x_{2LR} \oplus x_{2RR}$. We say that (D_1, D_2, D_3) is bad if it is not good.

Good and Bad Databases for FOX'_3. We say that a valid database D_F is *without overlap* if each pair of distinct entries $((x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \gamma)$ and $((x'_{2LL} \oplus x'_{2RL}, x'_{2LR} \oplus x'_{2RR}, x'_{2RL}, x'_{2RR}), \gamma')$ in D_F satisfies $x_{2RL} \neq x'_{2RL}$, $x_{2RR} \neq x_{2RR}$,

and $x_{2LL} \oplus x_{2RL} \neq x'_{2LL} \oplus x'_{2RL}$, $x_{2LR} \oplus x_{2RR} \neq x'_{2LR} \oplus x'_{2RR}$. Further, we say that (D_1, D_2, D_F) is good if D_F is without overlap, and for each entry $((x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \gamma) \in D_F$, there exists exactly one pair $(((x_{0LL} \oplus x_{0RL}, x_{0LR} \oplus x_{0RR}), \alpha), ((x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR}), \beta)) \in D_1 \times D_2$ (where $\alpha = \alpha_1 || \alpha_2$ and $\beta = \beta_1 || \beta_2$) such that $x_{0LL} \oplus x_{0LR} \oplus x_{0RL} \oplus \alpha_2 \oplus \beta_1 \oplus \beta_2 = x_{2LL} \oplus x_{2RL}$ and $x_{0LL} \oplus x_{0RR} \oplus \alpha_1 \oplus \alpha_2 \oplus \beta_1 = x_{2LR} \oplus x_{2RR}$. 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 $((x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \gamma) \in D_F$ with $\gamma = \gamma_1 || \gamma_2$, then $((x_{2LL} \oplus x_{2RL}, x_{2RL} \oplus x_{2RR}), (x_{2RL} \oplus \gamma_1, x_{2RR} \oplus \gamma_2)) \in D_3$.
2. If $((x_{2LL} \oplus x_{2RL}, x_{2RL} \oplus x_{2RR}), \gamma) \in D_3$ with $\gamma = \gamma_1 || \gamma_2$, then there exists a unique pair (x_{2RL}, x_{2RR}) such that $((x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), (x_{2RL} \oplus \gamma_1, x_{2RR} \oplus \gamma_2)) \in D_F$.

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

Next, we present the following lemma which shows that the behavior of $O'_{\mathsf{UP}.3}$ for D_F without overlap is the same as that of $O_{\mathsf{UP}.3}$ for $[D_F]_3$, i.e., there is a one-to-one correspondence between good databases for FOX_3 and FOX'_3.

Lemma 3. *Let D_F and D'_F be valid databases for f_3 and F without overlap. Then, for arbitrary x_{2LL}, $x_{2LR}, x_{2RL}, x_{2RR}, x'_{2LL}, x'_{2LR}, x'_{2RL}, x'_{2RR} \in \{0,1\}^{n/4}$, and $y_{LL}, y_{LR}, y_{RL}, y_{RR}, , y'_{LL}, y'_{LR}, y'_{RL}, y'_{RR} \in \{0,1\}^{n/4}$, the following holds:*

$$\begin{aligned}
&\langle x'_{2LL}, x'_{2LR}, x'_{2RL}, x'_{2RR}, x'_{2LL} \oplus x'_{2RL}, x'_{2LR} \oplus x'_{2RR}, y'_{LL}, y'_{LR}, y'_{RL}, y'_{RR}| \\
&\qquad \otimes \langle D'_F | O'_{UP.3} | x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, \\
&\qquad\qquad y_{LL}, y_{LR}, y_{RL}, y_{RR} \rangle \otimes |D_F\rangle \\
&= \langle x'_{2LL}, x'_{2LR}, x'_{2RL}, x'_{2RR}, x'_{2LL} \oplus x'_{2RL}, x'_{2LR} \oplus x'_{2RR}, y'_{LL}, y'_{LR}, y'_{RL}, y'_{RR}| \\
&\qquad \otimes \langle [D'_F]_3 | O_{UP.3} | x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, \\
&\qquad\qquad y_{LL}, y_{LR}, y_{RL}, y_{RR} \otimes |[D_F]_3\rangle \,. \qquad (41)
\end{aligned}$$

Proof. It suffices to consider the case that $x_{2LL} = x'_{2LL}$, $x_{2LR} = x'_{2LR}$, $x_{2RL} = x'_{2RL}$ and $x_{2RR} = x'_{2RR}$ since the oracle does not affect the input registers. Moreover, the database $O'_{\mathsf{UP}.3}$ affects only the entry of $(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR})$ in D_F when it acts on $|x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2LR}, x_{2RL} \oplus x_{2RR}, y_{LL}, y_{LR}, y_{RL}, y_{RR}\rangle \otimes |D_F\rangle$. Therefore, it is sufficient to show that the claim for the following two cases:

1. D_F has only a single entry of the form $((x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \gamma)$,
2. D_F has no entry (i.e., $D_F = \phi$).

In the case (ii), $[D_F]_3$ is also empty and Equation (41) follows from Equations (8) and (9) in Proposition 4. In the case (i), $[D_F]_3$ has only a single entry, and Equation (41) follows from Equations (4)-(7) in Proposition 4.

We show the claim for the first case where $D_F = \{(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \alpha\}$. Let $\alpha := \alpha_1 || \alpha_2$, $\gamma := \gamma_1 || \gamma_2$ and $\delta := \delta_1 || \delta_2$. By using the first property of Proposition 4, we have

$$\begin{aligned}
&O'_{\mathsf{UP}.3} \, |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, y_{LL}, y_{LR}, y_{RL}, y_{RR}\rangle \otimes |D_F\rangle \\
&\quad = |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, y_{LL} \oplus x_{2LR} \oplus \alpha_2,
\end{aligned}$$

$$
\begin{aligned}
&\qquad\qquad y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus \alpha_1 \oplus \alpha_2, y_{RL} \oplus \alpha_1, y_{RR} \oplus \alpha_2\rangle \\
&\quad \otimes |(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \alpha\rangle \\
&+ \frac{1}{\sqrt{2^{n/2}}} |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, y_{LL} \oplus x_{2LR} \\
&\qquad\qquad \oplus \alpha_2, y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus \alpha_1 \oplus \alpha_2, y_{RL} \oplus \alpha_1, y_{RR} \oplus \alpha_2\rangle \\
&\qquad \left(|\phi\rangle - \left(\sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \gamma\rangle \right) \right) \\
&- \frac{1}{\sqrt{2^{n/2}}} \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, \\
&\qquad y_{LL} \oplus x_{2LR} \oplus \gamma_2, y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus \gamma_1 \oplus \gamma_2, y_{RL} \oplus \gamma_1, y_{RR} \oplus \gamma_2\rangle \\
&\quad \otimes |(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \gamma\rangle \\
&+ \frac{1}{\sqrt{2^{n/2}}} |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}\rangle |\tilde{0^n}\rangle \\
&\qquad \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}} |(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \delta\rangle - |\phi\rangle \right) \\
&+ |\mathsf{invalid}\rangle ,
\end{aligned}
$$

where ϕ is empty database and $|\mathsf{invalid}\rangle$ is a vector containing invalid databases.

In addition, we have that $[D_F]_3 = \{(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}), (x_{2RL} \oplus \alpha_1)||(x_{2RR} \oplus \alpha_2)\}$, and hence it follows:

$$
\begin{aligned}
&O_{\mathsf{UP}.3} |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, y_{LL}, y_{LR}, y_{RL}, y_{RR}\rangle \otimes |[D_F]_3\rangle \\
&\quad = |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, y_{LL} \oplus x_{2LR} \oplus \alpha_2, \\
&\qquad\qquad y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus \alpha_1 \oplus \alpha_2, y_{RL} \oplus \alpha_1, y_{RR} \oplus \alpha_2\rangle \\
&\qquad\qquad \otimes |(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}), (\alpha_1 \oplus x_{2RL})||(\alpha_2 \oplus x_{2RR})\rangle \\
&\qquad + \frac{1}{\sqrt{2^{n/2}}} |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, y_{LL} \oplus x_{2LR} \\
&\qquad\qquad \oplus \alpha_2, y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus \alpha_1 \oplus \alpha_2, y_{RL} \oplus \alpha_1, y_{RR} \oplus \alpha_2\rangle \\
&\qquad\qquad \left(|\phi\rangle - \left(\sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}), \gamma\rangle \right) \right) \\
&\qquad - \frac{1}{\sqrt{2^{n/2}}} \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, \\
&\qquad\qquad y_{LL} \oplus x_{2LR} \oplus \gamma_2 \oplus x_{2RR}, y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus \gamma_1 \oplus x_{2RL} \oplus \gamma_2 \oplus x_{2RR}, \\
&\qquad\qquad\qquad y_{RL} \oplus \gamma_1 \oplus x_{2RL}, y_{RR} \oplus \gamma_2 \oplus x_{2RR}\rangle \\
&\qquad\qquad \otimes |(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}), \gamma\rangle \\
&\qquad + \frac{1}{\sqrt{2^{n/2}}} |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}\rangle |\tilde{0^n}\rangle \\
&\qquad\qquad \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}} |(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}), \delta\rangle - |\phi\rangle \right) \\
&\qquad + |\mathsf{invalid}'\rangle \\
&\quad = |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, y_{LL} \oplus x_{2LR} \oplus \alpha_2, \\
&\qquad\qquad y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus \alpha_1 \oplus \alpha_2, y_{RL} \oplus \alpha_1, y_{RR} \oplus \alpha_2\rangle \\
&\qquad \otimes |[(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), (x_{2RL} \oplus \alpha_1)||(x_{2RR} \oplus \alpha_2)]_3\rangle
\end{aligned}
$$

$$
\begin{aligned}
&+ \frac{1}{\sqrt{2^{n/2}}}|x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, y_{LL} \oplus x_{2LR} \\
&\qquad \oplus \alpha_2, y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus \alpha_1 \oplus \alpha_2, y_{RL} \oplus \alpha_1, y_{RR} \oplus \alpha_2\rangle \\
&\quad \left(|\phi\rangle - \left(\sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}}|[(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \gamma)]_3\rangle \right) \right) \\
&- \frac{1}{\sqrt{2^{n/2}}} \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}}|x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, \\
&\qquad y_{LL} \oplus x_{2LR} \oplus \gamma_2, y_{LR} \oplus x_{2LL} \oplus x_{2LR} \oplus \gamma_1 \oplus \gamma_2, y_{RL} \oplus \gamma_1, y_{RR} \oplus \gamma_2\rangle \\
&\qquad \otimes |[(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \gamma)]_3\rangle \\
&+ \frac{1}{\sqrt{2^{n/2}}} |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}, x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}\rangle |0^{\tilde{n}}\rangle \\
&\quad \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}}|[(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \delta)]_3\rangle - |\phi\rangle \right) \\
&+ |\mathsf{invalid}'\rangle \,,
\end{aligned}
$$

where $|\mathsf{invalid}'\rangle$ is a vector containing invalid databases. Thus, the claim holds for the first case when $D_F = \{(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}), \alpha\}$.

Similarly, we can show that the claim holds for the second case when D_F is empty by straightforward calculations using the second property of Proposition 4. □

Regular and Irregular States of Oracles. Recall that, in addition to database registers, the quantum oracle O_{FOX_3} uses ancillary $2n$-qubit registers to compute the intermediate state after the first and second rounds. 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_{FOX_3}, where $|x_1\rangle \otimes |x_2\rangle$ is the ancillary $2n$ qubits, is *irregular* if $x_1 \neq 0^n$, $x_2 \neq 0^n$ and at least one of the databases (D_1, D_2, or D_3) is invalid. We say that the state vector is *regular* if it is not irregular. Similarly, we define the regular and irregular states for $O_{\mathsf{FOX}'_3}$. In addition, 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_{FOX_3} is *preregular* if $x_2 = 0^n$ and the database is valid. We can define preregular states for $O_{\mathsf{FOX}'_3}$ similarly.

Technical Core to Prove the Indistinguishability of FOX_3 and FOX'_3. Let $|\psi_i\rangle$ and $|\psi'_i\rangle$ be the joint quantum states of the adversary $\mathcal{A}$ and the oracle just before making the i-th query when $\mathcal{A}$ runs relative to FOX_3 and FOX'_3, respectively. In addition, let $|\psi_{q+1}\rangle$ and $|\psi'_{q+1}\rangle$ denote the states just before the final measurement. Then, we have

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

for some complex numbers a_{x,y,z,D_1,D_2,D_3} such that

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

Here, $x = x_{0LL}||x_{0LR}||x_{0RL}||x_{0RR}$, $y = y_{LL}||y_{LR}||y_{RL}||y_{RR}$, and z correspond to the adversary's registers to send queries to the oracles, receive answers from oracles, and perform offline computations, respectively ($x_{0LL}, x_{0LR}, x_{0RL}, x_{0RR}, y_{LL}, y_{LR}, y_{RL}, y_{RR} \in \{0,1\}^{n/4}$). Note that $|D_1|, |D_2| \leq 2(j-1)$ and $|D_3| \leq (j-1)$, since each query to the RstOE affects only the qubits that correspond to a single entry to each database. Similarly, $|\psi'_j\rangle$ can be decomposed on the computational basis.

Showing the following proposition is the technical core to prove Proposition 6.

Proposition 7. *For each $1 \leq j \leq q+1$, there exist vectors $|\psi_j^{good}\rangle$, $|\psi_j^{bad}\rangle$, $|\psi_j^{'good}\rangle$, $|\psi_j^{'bad}\rangle$, and complex numbers $a^{(j)}_{x,y,z,D_1,D_2,D_F}$ such that*

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

$$|\psi_j^{good}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good}} a^{(j)}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle \otimes |D_1,D_2,[D_F]_3\rangle\,, \tag{42}$$

$$|\psi_j^{'good}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good}} a^{(j)}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle \otimes |D_1,D_2,D_F\rangle\,. \tag{43}$$

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

$$\| \, |\psi_j^{bad}\rangle \, \| \leq \| \, |\psi_{j-1}^{bad}\rangle \, \| + \epsilon_{bad}^{(j-1)}, \quad \| \, |\psi_j^{'bad}\rangle \, \| \leq \| \, |\psi_{j-1}^{'bad}\rangle \, \| + \epsilon_{bad}^{'(j-1)}, \tag{44}$$

where $\epsilon_{bad}^{(j-1)}, \epsilon_{bad}^{'(j-1)} \leq O\left(\sqrt{j/2^{n/2}}\right)$ (we set $|\psi_j^{bad}\rangle = 0$ and $|\psi_j^{'bad}\rangle = 0$).

Proof Intuition. We now explain some intuitions behind the proof strategy. When we define good and bad databases, we choose good databases so that the following conditions hold (in addition that there exists a one-to-one correspondence between good databases for FOX_3 and FOX'_3).

1. The behavior of FOX_3 on a good database (D_1,D_2,D_3) is the same as that of FOX'_3 on the corresponding database $(D_1,D_2,[D_F]_3)$. (see Lemma 3)
2. The "probability" (in a quantum sense) that a good database (D_1,D_2,D_3) for FOX_3 (resp. (D_1,D_2,D_F) for FOX'_3) changes to a bad database at each query of FOX_3 (resp. FOX'_3) is small.

The first condition ensures that the adversary cannot distinguish between FOX_3 and FOX'_3 as long as the databases are good, which leads to the existence of vectors $|\psi_j^{\mathsf{good}}\rangle$ and $|\psi_j^{'\mathsf{good}}\rangle$ that satisfies (42) and (43) for each j. We can show this using induction on j. Let Π_{good} and Π_{valid} denote the projections onto the space spanned by vectors that correspond to good and valid databases, respectively. After applying Proposition 4 to O_{FOX_3}, we can set $|\psi_{j+1}^{\mathsf{good}}\rangle := \Pi_{\mathsf{good}}\left(\Pi_{\mathsf{valid}}\mathsf{RstOE}\; O_{\mathsf{FOX}_3}\,|\psi_j^{\mathsf{good}}\rangle - |\epsilon_j^{\mathsf{bad}}\rangle\right)$ and $|\psi_{j+1}^{\mathsf{bad}}\rangle := |\psi_{j+1}\rangle - |\psi_{j+1}^{\mathsf{good}}\rangle$; and similarly we can set for $|\psi_{j+1}^{'\mathsf{good}}\rangle$. Therefore, if the error term $|\epsilon_j^{\mathsf{bad}}\rangle$ is negligible, then we can easily show the properties given in (42) and (43) hold for $j+1$.

The "probability" in the second condition corresponds to the terms $\left(\epsilon_{\mathsf{bad}}^{(j)}\right)^2$ and $\left(\epsilon_{\mathsf{bad}}^{'(j)}\right)^2$. If we can show that $\left(\epsilon_{\mathsf{bad}}^{(j)}\right)^2$ and $\left(\epsilon_{\mathsf{bad}}^{'(j)}\right)^2$ are negligible then we can show the indistinguishability of FOX_3 and FOX'_3 using Proposition 4 similar to classical lazy sampling. On the other hand, the good database changes 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 $|\psi_j^{\mathsf{good}}\rangle$ has at most $(j-1)$ entries and the outputs of f_1 and f_2 are $n/2$-bits, the input to f_3 collides with one of the existing records in D_3 with a probability p in $O(j/2^{n/2})$. In the quantum setting, roughly speaking, the difference between the norms of the j-th bad vector $|\psi_j^{\mathsf{bad}}\rangle$ (resp., $|\psi_j^{'\mathsf{bad}}\rangle$) and the $(j-1)$-th bad vector $|\psi_{j-1}^{\mathsf{bad}}\rangle$ (resp., $|\psi_{j-1}^{'\mathsf{bad}}\rangle$) is bounded by $\sqrt{p}$, which is $O(\sqrt{j/2^{n/2}})$. This corresponds to the claim that $\| \, |\psi_j^{\mathsf{bad}}\rangle \, \| \leq \| \, |\psi_{j-1}^{\mathsf{bad}}\rangle \, \| + O\left(\sqrt{j/2^{n/2}}\right)$. The claim for FOX'_3 can be shown in a similar way. □

Next, we provide the complete proof of Proposition 7. Note that an existing record (x, α) in the database D will later be deleted or overwritten with a different record in the quantum setting, and the effect of such deletion and overwriting is too large to be ignored. Therefore, we have to perform more careful and quantum-specific analysis by using Proposition 4 and Proposition 5.

Proof (of Proposition 7). We show the proposition by using mathematical induction on j. First, recall that the oracles of FOX_3 and FOX'_3 are decomposed as $O_{\mathsf{FOX}_3} = O_{\mathsf{UP}.1} \cdot O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.3} \cdot O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.1}$ and $O_{\mathsf{FOX}_3} = O_{\mathsf{UP}.1} \cdot O_{\mathsf{UP}.2} \cdot O'_{\mathsf{UP}.3} \cdot O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.1}$. We check how the quantum states change when $O_{\mathsf{UP}.1}$, $O_{\mathsf{UP}.2}$, $O_{\mathsf{UP}.3}$ (resp., $O'_{\mathsf{UP}.3}$), $O_{\mathsf{UP}.2}$, and $O_{\mathsf{UP}.1}$ act on $|\psi_j\rangle$ (resp. $|\psi'_j\rangle$) in a sequential order. The claim obviously holds for $j = 1$ by setting $|\psi_1^{\mathsf{good}}\rangle := |\psi_1\rangle$ and $|\psi_1^{'\mathsf{good}}\rangle := |\psi'_1\rangle$. By applying induction, we can show the claim on $|\psi_{j+1}\rangle$ and $|\psi'_{j+1}\rangle$ holds if the claim on $|\psi_k\rangle$ and $|\psi'_k\rangle$ holds for $k = 1, \ldots, j$.

Let Π_{good} and Π_{bad} denote the projections onto the vector space spanned by the vectors that correspond to good databases and bad databases, respectively. In addition, let Π_{reg} and Π_{prereg} be the projections onto the spaces spanned by the vectors that correspond to regular and preregular states, respectively. We emphasize that the recording standard oracle with errors is used to implement the function f for each oracle $O_{\mathsf{UP}.i}$, $1 \leq i \leq 3$.

Further, we use shorthand notations in the proofs of lemmas below, by defining $x' := (x_{LL} \oplus x_{RL}, x_{LR} \oplus x_{RR})$, $x'_1 := (x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR})$, $x'_2 := (x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR})$, $\alpha := \alpha_1 || \alpha_2$ and $\gamma := \gamma_1 || \gamma_2$. For a database D with entry $(x, \alpha = \alpha_1 || \alpha_2)$, $D_L(x) := \alpha_1$ and $D_R(x) := \alpha_2$ denote the left and right halves of D's output, respectively.

Next, we study how the states $|\psi_j\rangle$ and $|\psi'_j\rangle$ change when five unitary operators act in sequential order. First, we show the following lemma.

Lemma 4 (Action of the first $O_{\mathsf{UP}.1}$)**.** *Suppose that there exist j and vectors $|\psi_i^{\mathsf{good}}\rangle$, $|\psi_i^{\mathsf{bad}}\rangle$, $|\psi_i^{'\mathsf{good}}\rangle$ and $|\psi_i^{'\mathsf{bad}}\rangle$ that satisfy Proposition 7 for $i = 1, \ldots, j$. Then, there exists vectors $|\psi_j^{\mathsf{good},1}\rangle$, $|\psi_j^{\mathsf{bad},1}\rangle$, $|\psi_j^{'\mathsf{good},1}\rangle$ and $|\psi_j^{'\mathsf{bad},1}\rangle$ that satisfy the following properties:*

1. $O_{\mathsf{UP}.1} |\psi_j\rangle = |\psi_j^{\mathsf{good},1}\rangle + |\psi_j^{\mathsf{bad},1}\rangle$, *and* $O_{\mathsf{UP}.1} |\psi'_j\rangle = |\psi_j^{'\mathsf{good},1}\rangle + |\psi_j^{'\mathsf{bad},1}\rangle$.

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

$$|\psi_j^{\mathsf{good},1}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x') \neq \perp}} a^{(j),1}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle ,$$

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

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

4. $\| |\psi_j^{\mathsf{bad},1}\rangle \|$ *and* $\| |\psi_j^{'\mathsf{bad},1}\rangle \|$ *are upper bounded as*

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

where $x_{1LL} = x_{LR} \oplus D_{1R}(x')$, $x_{1LR} = x_{LL} \oplus x_{LR} \oplus D_{1L}(x') \oplus D_{1R}(x')$, $x_{1RL} = x_{RL} \oplus D_{1L}(x')$, *and* $x_{1RR} = x_{RR} \oplus D_{1R}(x')$ *for each summand of* $|\psi_j^{\mathsf{good},1}\rangle$ *and* $|\psi_j^{'\mathsf{good},1}\rangle$.

Proof. Let Π_{valid} denote the projection onto the space spanned by the vectors that correspond to valid databases. Further, the response of the first $O_{\mathsf{UP}.1}$ is written into an auxiliary register that is initially set to be $|0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle$.

By applying Proposition 5 to RstOE of f_1, the following hold:

$$
\begin{aligned}
&\Pi_{\mathsf{valid}} O_{\mathsf{UP}.1} |\psi_j^{\mathsf{good}}\rangle \\
&\quad = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\,\mathrm{good}, D_1(x')\neq\perp}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \\
&\qquad \otimes |x_{LR} \oplus D_{1R}(x'), x_{LL} \oplus x_{LR} \oplus D_{1L}(x') \oplus D_{1R}(x'), x_{RL} \oplus D_{1L}(x'), x_{RR} \oplus D_{1R}(x')\rangle \\
&\qquad - \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F \\ (D_1,D_2,D_F):\,\mathrm{good}, D_1(x')\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \\
&\qquad\qquad \otimes |D_1 \backslash (x', D_1(x')) \cup (x', \gamma), D_2, [D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{LR} \oplus \gamma_2, x_{LL} \oplus x_{LR} \oplus \gamma_1 \oplus \gamma_2, x_{RL} \oplus \gamma_1, x_{RR} \oplus \gamma_2)\rangle \\
&\qquad + \sum_{\substack{x,y,z,D_1,D_2,D_F,\alpha \\ (D_1,D_2,D_F):\,\mathrm{good}, D_1(x')=\perp}} \sqrt{\frac{1}{2^{n/2}}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1 \cup (x', \alpha), D_2, [D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{LR} \oplus \alpha_2, x_{LL} \oplus x_{LR} \oplus \alpha_1 \oplus \alpha_2, x_{RL} \oplus \alpha_1, x_{RR} \oplus \alpha_2\rangle \\
&\qquad + |\epsilon\rangle\,, \qquad (45)
\end{aligned}
$$

and

$$
\begin{aligned}
&\Pi_{\mathsf{valid}} O_{\mathsf{UP}.1} |\psi_j^{'\mathsf{good}}\rangle \\
&\quad = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\,\mathrm{good}, D_1(x')\neq\perp}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \\
&\qquad \otimes |x_{LR} \oplus D_{1R}(x'), x_{LL} \oplus x_{LR} \oplus D_{1L}(x') \oplus D_{1R}(x'), x_{RL} \oplus D_{1L}(x'), x_{RR} \oplus D_{1R}(x')\rangle \\
&\qquad - \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F \\ (D_1,D_2,D_F):\,\mathrm{good}, D_1(x')\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \\
&\qquad\qquad \otimes |D_1 \backslash (x', D_1(x')) \cup (x', \gamma), D_2, D_F\rangle \\
&\qquad\qquad \otimes |x_{LR} \oplus \gamma_2, x_{LL} \oplus x_{LR} \oplus \gamma_1 \oplus \gamma_2, x_{RL} \oplus \gamma_1, x_{RR} \oplus \gamma_2)\rangle \\
&\qquad + \sum_{\substack{x,y,z,D_1,D_2,D_F,\alpha \\ (D_1,D_2,D_F):\,\mathrm{good}, D_1(x')=\perp}} \sqrt{\frac{1}{2^{n/2}}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1 \cup (x', \alpha), D_2, D_F\rangle \\
&\qquad\qquad \otimes |x_{LR} \oplus \alpha_2, x_{LL} \oplus x_{LR} \oplus \alpha_1 \oplus \alpha_2, x_{RL} \oplus \alpha_1, x_{RR} \oplus \alpha_2\rangle \\
&\qquad + |\epsilon'\rangle\,. \qquad (46)
\end{aligned}
$$

Now, we can set

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

Then the first property of the claim holds by definition, and the second and third properties immediately follow from (45) and (46) and the assumption on $|\psi_j\rangle$ and $|\psi'_j\rangle$.

Next, on the first term of right-hand side of (46), we have

$$\begin{aligned}\Pi_{\mathsf{bad}} &\sum_{\substack{x,y,z,D_1,D_2,D_F\\(D_1,D_2,D_F)\text{: good},D_1(x')\neq\perp}} a^{(j),1}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\otimes|D_1,D_2,D_F\rangle\\ &\quad\otimes|x_{LR}\oplus D_{1R}(x'),x_{LL}\oplus x_{LR}\oplus D_{1L}(x')\oplus D_{1R}(x'),x_{RL}\oplus D_{1L}(x'),x_{RR}\oplus D_{1R}(x')\rangle\\ &=0. \end{aligned}\tag{47}$$

On the second term of right-hand side of (46), we have

$$\begin{aligned}\Pi_{\mathsf{bad}} &\sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F\\(D_1,D_2,D_F)\text{: good},D_1(x')\neq\perp}} \frac{1}{2^{n/2}}a^{(j)}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\\ &\qquad\otimes|D_1\backslash(x',D_1(x'))\cup(x',\gamma),D_2,D_F\rangle\\ &\qquad\otimes|x_{LR}\oplus\gamma_2,x_{LL}\oplus x_{LR}\oplus\gamma_1\oplus\gamma_2,x_{RL}\oplus\gamma_1,x_{RR}\oplus\gamma_2\rangle\\ &= \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F\\(D_1\cup(x',\alpha),D_2,D_F)\text{: good},D_1(x')=\perp\\(D_1\cup(x',\gamma),D_2,D_F)\text{: bad}}} \frac{1}{2^{n/2}}a^{(j)}_{x,y,z,D_1\cup(x',\alpha),D_2,D_F}\,|x,y,z\rangle\\ &\qquad\otimes|D_1\cup(x',\gamma),D_2,D_F\rangle\\ &\qquad\otimes|x_{LR}\oplus\gamma_2,x_{LL}\oplus x_{LR}\oplus\gamma_1\oplus\gamma_2,x_{RL}\oplus\gamma_1,x_{RR}\oplus\gamma_2\rangle\\ &= \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F\\(D_1\cup(x',\alpha),D_2,D_F)\text{: good},D_1(x')=\perp\\(D_1\cup(x',\gamma),D_2,D_F)\text{: bad}\\D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)\neq\perp}} \frac{1}{2^{n/2}}a^{(j)}_{x,y,z,D_1\cup(x',\alpha),D_2,D_F}\,|x,y,z\rangle\\ &\qquad\otimes|D_1\cup(x',\gamma),D_2,D_F\rangle\\ &\qquad\otimes|x_{LR}\oplus\gamma_2,x_{LL}\oplus x_{LR}\oplus\gamma_1\oplus\gamma_2,x_{RL}\oplus\gamma_1,x_{RR}\oplus\gamma_2\rangle \qquad (48)\\ &\quad+ \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F\\(D_1\cup(x',\alpha),D_2,D_F)\text{: good},D_1(x')=\perp\\(D_1\cup(x',\gamma),D_2,D_F)\text{: bad}\\D_2(x'_1)=\perp\vee\left(D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)=\perp\right)}} \frac{1}{2^{n/2}}a^{(j)}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\\ &\qquad\otimes|D_1\cup(x',\gamma),D_2,D_F\rangle\\ &\qquad\otimes|x_{LR}\oplus\gamma_2,x_{LL}\oplus x_{LR}\oplus\gamma_1\oplus\gamma_2,x_{RL}\oplus\gamma_1,x_{RR}\oplus\gamma_2\rangle, \qquad (49)\end{aligned}$$

where $x_{1LL}:=\alpha_2\oplus x_{LR}$, $x_{1LR}:=\alpha_1\oplus\alpha_2\oplus x_{LL}\oplus x_{LR}$, $x_{1RL}:=\alpha_1\oplus x_{RL}$, $x_{1RR}:=\alpha_2\oplus x_{RR}$, and $x_{2LL}:=D_{2R}(x'_1)\oplus x_{1LR}$, $x_{2LR}:=D_{2L}(x'_1)\oplus D_{2R}(x'_1)\oplus x_{1LL}\oplus x_{1LR}$, $x_{2RL}:=D_{2L}(x'_1)\oplus x_{2RL}$, $x_{2RR}:=D_{2R}(x'_1)\oplus x_{1RR}$ when $D_2(x'_1)\neq\perp$.

Next, we give an upper bound of the norm of the term (48). Note that if a tuple $(x,(D_1\cup(x',\gamma),D_2,D_F))$ satisfies the conditions

(1) $D_1(x')=\perp$, and (2) $(D_1\cup(x',\gamma),D_2,D_F))$ is bad,

the number of α such that

(1) $(D_1\cup(x',\alpha),D_2,D_F))$ becomes good, (2) $D_2(x'_1)\neq\perp$, and (3) $[D_F]_3(x'_2)\neq\perp$,

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

$$\begin{aligned}
&\Bigg\| \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1\cup(x',\alpha),D_2,D_F)\text{: good} \\ D_1(x')=\perp \\ (D_1\cup(x',\gamma),D_2,D_F)\text{: bad} \\ D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x',\alpha),D_2,D_F} |x,y,z\rangle \otimes |D_1\cup(x',\gamma),D_2,D_F\rangle \\
&\qquad\qquad \otimes |x_{LR}\oplus\gamma_2, x_{LL}\oplus x_{LR}\oplus\gamma_1\oplus\gamma_2, x_{RL}\oplus\gamma_1, x_{RR}\oplus\gamma_2\rangle \Bigg\|^2 \\
&= \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x')=\perp \\ (D_1\cup(x',\gamma),D_2,D_F)\text{: bad}}} \frac{1}{2^n} \cdot \Bigg| \sum_{\substack{\alpha:(D_1\cup(x',\alpha),D_2,D_F)\text{ is good} \\ D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)\neq\perp}} a^{(j)}_{x,y,z,D_1\cup(x',\alpha),D_2,D_F} \Bigg|^2 \\
&\leq \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x')=\perp \\ (D_1\cup(x',\gamma),D_2,D_F)\text{: bad}}} \frac{1}{2^n} \cdot 2(j-1) \cdot \sum_{\substack{\alpha:(D_1\cup(x',\alpha),D_2,D_F)\text{ is good} \\ D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)\neq\perp}} \left| a^{(j)}_{x,y,z,D_1\cup(x',\alpha),D_2,D_F} \right|^2 \\
&= \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1\cup(x',\alpha),D_2,D_F)\text{: good},D_1(x')=\perp \\ (D_1\cup(x',\gamma),D_2,D_F)\text{: bad} \\ D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)\neq\perp}} \frac{2(j-1)}{2^n} \\
&\leq \sum_{\gamma} \frac{2(j-1)}{2^n} = \frac{2(j-1)}{2^{n/2}} \qquad (50)
\end{aligned}$$

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

Next, we give an upper bound of the norm of the term (49). Note that if a tuple $(x,\alpha,D_1,D_2,D_F))$ satisfies the conditions

(1) $D_1(x') = \perp$, (2) $(D_1\cup(x',\alpha),D_2,D_F))$ is good, and

(3) $D_2(x'_1) = \perp$, or $D_2(x'_1) \neq \perp \wedge [D_F]_3(x'_2) = \perp$,

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

$$\begin{aligned}
&\Bigg\| \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1\cup(x',\alpha),D_2,D_F)\text{: good},D_1(x')=\perp \\ (D_1\cup(x',\gamma),D_2,D_F)\text{: bad} \\ D_2(x'_1)=\perp\vee\left(D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)=\perp\right)}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x',\alpha),D_2,D_F} |x,y,z\rangle \otimes |D_1\cup(x',\gamma),D_2,D_F\rangle \\
&\qquad\qquad \otimes |x_{LR}\oplus\gamma_2, x_{LL}\oplus x_{LR}\oplus\gamma_1\oplus\gamma_2, x_{RL}\oplus\gamma_1, x_{RR}\oplus\gamma_2)\rangle \Bigg\|^2 \\
&= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x')=\perp}} \sum_{\substack{\gamma \\ (D_1\cup(x',\gamma),D_2,D_F)\text{: bad}}} \Bigg| \sum_{\substack{\alpha \\ (D_1\cup(x',\alpha),D_2,D_F)\text{: good} \\ D_2(x'_1)=\perp\vee\left(D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)=\perp\right)}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x',\alpha),D_2,D_F} |x,y,z\rangle \Bigg|^2
\end{aligned}$$

$$\leq \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x')=\perp}} \sum_{\substack{\gamma \\ (D_1\cup(x',\gamma),D_2,D_F)\text{: bad} \\ D_2(x'_1)=\perp\vee\left(D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)=\perp\right)}} \sum_{\substack{\alpha \\ (D_1\cup(x',\alpha),D_2,D_F)\text{: good} \\ D_2(x'_1)=\perp\vee\left(D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)=\perp\right)}} \frac{\left|a^{(j)}_{x,y,z,D_1,D_2,D_F}\left|x,y,z\right\rangle\right|^2}{2^{n/2}}$$

$$= \sum_{\substack{x,y,z,D_1\cup(x',\alpha),D_2,D_F \\ D_1(x')=\perp}} \sum_{\substack{\alpha \\ (D_1\cup(x',\alpha),D_2,D_F)\text{: good} \\ D_2(x'_1)=\perp\vee\left(D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)=\perp\right)}} \left|a^{(j)}_{x,y,z,D_1\cup(x',\alpha),D_2,D_F}\left|x,y,z\right\rangle\right|^2 \sum_{\substack{\gamma \\ (D_1\cup(x',\gamma),D_2,D_F)\text{: bad}}} \frac{1}{2^{n/2}}$$

$$\leq \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x')=\perp}} \sum_{\substack{\alpha \\ (D_1\cup(x',\alpha),D_2,D_F)\text{: good} \\ D_2(x'_1)=\perp\vee\left(D_2(x'_1)\neq\perp\wedge[D_F]_3(x'_2)=\perp\right)}} \left|a^{(j)}_{x,y,z,D_1\cup(x',\alpha),D_2,D_F}\left|x,y,z\right\rangle\right|^2 \sum_{\substack{\gamma \\ (D_1\cup(x',\gamma),D_2,D_F)\text{: bad}}} \frac{(j-1)}{2^{n/2}}$$

$$\leq \frac{(j-1)}{2^{n/2}}, \tag{51}$$

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

From (48)-(51), we have

$$\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F \\ (D_1,D_2,D_F)\text{: good} \\ D_1(x')\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1,D_2,D_F}\left|x,y,z\right\rangle \otimes \left|D_1\backslash(x',D_1(x'))\cup(x',\gamma),D_2,D_F\right\rangle \right.$$
$$\left. \otimes \left|x_{LR}\oplus\gamma_2, x_{LL}\oplus x_{LR}\oplus\gamma_1\oplus\gamma_2, x_{RL}\oplus\gamma_1, x_{RR}\oplus\gamma_2\right\rangle \right\|$$
$$\leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \tag{52}$$

follows.

In addition, on the third term of the right-hand side of (46), we have

$$\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,D_1,D_2,D_F,\alpha \\ (D_1,D_2,D_F)\text{: good},D_1(x')=\perp}} \sqrt{\frac{1}{2^{n/2}}} a^{(j)}_{x,y,z,D_1,D_2,D_F}\left|x,y,z\right\rangle \otimes \left|D_1\cup(x',\alpha),D_2,D_F\right\rangle \right.$$
$$\left. \otimes \left|x_{LR}\oplus\alpha_2, x_{LL}\oplus x_{LR}\oplus\alpha_1\oplus\alpha_2, x_{RL}\oplus\alpha_1, x_{RR}\oplus\alpha_2\right\rangle \right\|^2$$
$$= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\text{: good},D_1(x')=\perp}} \left|a^{(j)}_{x,y,z,D_1,D_2,D_F}\right|^2 \sum_{\alpha:(D_1\cup(x',\alpha),D_2,D_F)\text{ is bad}} \frac{1}{2^{n/2}}$$
$$= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\text{: good},D_1(x')=\perp}} \left|a^{(j)}_{x,y,z,D_1,D_2,D_F}\right|^2 \cdot O\left(\frac{j}{2^{n/2}}\right)$$
$$\leq O\left(\frac{j}{2^{n/2}}\right). \tag{53}$$

From (47), (52), (53), we have

$$\left\| \Pi_{\mathsf{bad}} \left(\Pi_{\mathsf{valid}} O_{\mathsf{UP}.1} \left|\psi_j^{'\mathsf{good}}\right\rangle - \left|\epsilon'\right\rangle \right) \right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{54}$$

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

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

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

The following lemma shows how the states $O_{\mathsf{UP}.1} |\psi_j\rangle$ and $O_{\mathsf{UP}.1} |\psi'_j\rangle$ change when $O_{\mathsf{UP}.2}$ acts on them.

Lemma 5 (Action of the first $O_{\mathsf{UP}.2}$)**.** *Suppose that there exist j and vectors $|\psi_i^{\mathsf{good}}\rangle$, $|\psi_i^{\mathsf{bad}}\rangle$, $|\psi_i^{'\mathsf{good}}\rangle$ and $|\psi_i^{'\mathsf{bad}}\rangle$ that satisfy Proposition 7 for $i = 1, \ldots, j$. Then, there exists vectors $|\psi_j^{\mathsf{good},2}\rangle$, $|\psi_j^{\mathsf{bad},2}\rangle$, $|\psi_j^{'\mathsf{good},2}\rangle$ and $|\psi_j^{'\mathsf{bad},2}\rangle$ that satisfy the following properties:*

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

$$\begin{aligned}
|\psi_j^{\mathsf{good},2}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x')\neq\perp, D_2(x'_1)\neq\perp}} & a^{(j),2}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \\
& \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}\rangle , \\
|\psi_j^{'\mathsf{good},2}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x')\neq\perp, D_2(x'_1)\neq\perp}} & a^{(j),2}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \\
& \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}\rangle .
\end{aligned}$$

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

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

where $x_{1LL} = D_{1R}(x') \oplus x_{LR}$, $x_{1LR} = D_{1L}(x') \oplus D_{1R}(x') \oplus x_{LL} \oplus x_{LR}$, $x_{1RL} = D_{1L}(x') \oplus x_{RL}$, $x_{1RR} = D_{1R}(x') \oplus x_{RR}$, $x_{2LL} = D_{2R}(x'_1) \oplus x_{1LR}$, $x_{2LR} = D_{2L}(x'_1) \oplus D_{2R}(x'_1) \oplus x_{1LL} \oplus x_{1LR}$, $x_{2RL} = D_{2L}(x'_1) \oplus x_{1RL}$, and $x_{2RR} = D_{2R}(x'_1) \oplus x_{1RR}$ for each summand of $|\psi_j^{\mathsf{good},2}\rangle$ and $|\psi_j^{'\mathsf{good},2}\rangle$.

This lemma can be proved in the same manner as Lemma 4, and hence we skip the details of the proof.

The next lemma shows how the states changes when $O_{\mathsf{UP}.3}$ and $O'_{\mathsf{UP}.3}$ act on the states $O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.1} |\psi_j\rangle$ and $O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.1} |\psi'_j\rangle$, respectively.

Lemma 6 (Action of $O_{\mathsf{UP}.3}$ and $O'_{\mathsf{UP}.3}$)**.** *Suppose that there exist j and vectors $|\psi_i^{\mathsf{good}}\rangle$, $|\psi_i^{\mathsf{bad}}\rangle$, $|\psi_i^{'\mathsf{good}}\rangle$ and $|\psi_i^{'\mathsf{bad}}\rangle$ that satisfy Proposition 7 for $i = 1, \ldots, j$. Then, there exists vectors $|\psi_j^{\mathsf{good},3}\rangle$, $|\psi_j^{\mathsf{bad},3}\rangle$, $|\psi_j^{'\mathsf{good},3}\rangle$ and $|\psi_j^{'\mathsf{bad},3}\rangle$ that satisfy following properties:*

1. $O_{UP.3} \cdot O_{UP.2} \cdot O_{UP.1} |\psi_j\rangle = |\psi_j^{\mathsf{good},2}\rangle + |\psi_j^{\mathsf{bad},2}\rangle$, *and*
   $O'_{UP.3} \cdot O_{UP.2} \cdot O_{UP.1} |\psi'_j\rangle = |\psi_j^{'\mathsf{good},2}\rangle + |\psi_j^{'\mathsf{bad},2}\rangle$.

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

$$|\psi_j^{\mathsf{good},3}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x')\neq\perp, D_2(x'_1)\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}\rangle ,$$

$$|\psi_j^{'\mathsf{good},3}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x')\neq\perp, D_2(x'_1)\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}\rangle .$$

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

4. *$\| |\psi_j^{\mathsf{bad},3}\rangle \|$ and $\| |\psi_j^{'\mathsf{bad},3}\rangle \|$ are upper bounded as*

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

where $x_{1LL} = D_{1R}(x') \oplus x_{LR}$, $x_{1LR} = D_{1L}(x') \oplus D_{1R}(x') \oplus x_{LL} \oplus x_{LR}$, $x_{1RL} = D_{1L}(x') \oplus x_{RL}$, $x_{1RR} = D_{1R}(x') \oplus x_{RR}$, $x_{2LL} = D_{2R}(x'_1) \oplus x_{1LR}$, $x_{2LR} = D_{2L}(x'_1) \oplus D_{2R}(x'_1) \oplus x_{1LL} \oplus x_{1LR}$, $x_{2RL} = D_{2L}(x'_1) \oplus x_{1RL}$, and $x_{2RR} = D_{2R}(x'_1) \oplus x_{1RR}$ for each summand of $|\psi_j^{\mathsf{good},3}\rangle$ and $|\psi_j^{'\mathsf{good},3}\rangle$.

Proof. From Lemma 5, it follows that there exists vectors $|\psi_j^{\mathsf{good},2}\rangle$, $|\psi_j^{\mathsf{bad},2}\rangle$, $|\psi_j^{'\mathsf{good},2}\rangle$ and $|\psi_j^{'\mathsf{bad},2}\rangle$ that satisfy the four properties in Lemma 5.

Define $|\psi_j^{\mathsf{good},3}\rangle := \Pi_{\mathsf{valid}} O_{\mathsf{UP}.3} |\psi_j^{\mathsf{good},2}\rangle$, $|\psi_j^{\mathsf{bad},3}\rangle := O_{\mathsf{UP}.3} O_{\mathsf{UP}.2} O_{\mathsf{UP}.1} |\psi_j\rangle - |\psi_j^{\mathsf{good},2}\rangle$, $|\psi_j^{'\mathsf{good},3}\rangle := \Pi_{\mathsf{valid}} O'_{\mathsf{UP}.3} |\psi_j^{'\mathsf{good},2}\rangle$, and $|\psi_j^{'\mathsf{bad},3}\rangle := O'_{\mathsf{UP}.3} O_{\mathsf{UP}.2} O_{\mathsf{UP}.1} |\psi'_j\rangle - |\psi_j^{'\mathsf{good},2}\rangle$.

Note that, for each summand $|x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}\rangle$ of $|\psi_j^{'\mathsf{good},2}\rangle$, we have that

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

by definition of good databases. Therefore, we have

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

which implies $|\psi_j^{'\mathsf{good},3}\rangle = \Pi_{\mathsf{good}} |\psi_j^{'\mathsf{good},3}\rangle$.

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

Now the first property obviously holds. The second property immediately follows from Lemma 3 and the second property in Lemma 5. Third property follows from the third property in Lemma 5. For the fourth property, we have

$$\begin{aligned}
\left\| |\psi_j^{\mathsf{bad},3}\rangle \right\| &= \left\| O_{\mathsf{UP}.3} O_{\mathsf{UP}.2} O_{\mathsf{UP}.1} |\psi_j\rangle - |\psi_j^{\mathsf{good},3}\rangle \right\| \\
&= \left\| \Pi_{\mathsf{valid}} O_{\mathsf{UP}.3} O_{\mathsf{UP}.2} O_{\mathsf{UP}.1} |\psi_j\rangle - \Pi_{\mathsf{valid}} O_{\mathsf{UP}.2} |\psi_j^{\mathsf{good},2}\rangle \right\| \\
&= \left\| \Pi_{\mathsf{valid}} O_{\mathsf{UP}.3} |\psi_j^{\mathsf{bad},2}\rangle \right\| \\
&\leq \left\| |\psi_j^{\mathsf{bad},2}\rangle \right\| \\
&\leq \left\| |\psi_j^{\mathsf{bad}}\rangle \right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right). \qquad (55)
\end{aligned}$$

Similarly, $\left\| |\psi_j^{'\mathsf{bad},3}\rangle \right\| \leq \left\| |\psi_j^{'\mathsf{bad}}\rangle \right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right)$ follows. Therefore, the fourth property of the lemma holds. □

The next lemma shows how the states $O_{\mathsf{UP}.3} \cdot O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.1} |\psi_j\rangle$ and $O'_{\mathsf{UP}.3} \cdot O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.1} |\psi'_j\rangle$ change when $O_{\mathsf{UP}.2}$ acts on them.

Lemma 7 (Action of the second $O_{\mathsf{UP}.2}$)**.** *Suppose that there exist j and vectors $|\psi_i^{\mathsf{good}}\rangle$, $|\psi_i^{\mathsf{bad}}\rangle$, $|\psi_i^{'\mathsf{good}}\rangle$ and $|\psi_i^{'\mathsf{bad}}\rangle$ that satisfy Proposition 7 for $i = 1, \ldots, j$. Then, there exists vectors $|\psi_j^{\mathsf{good},4}\rangle$, $|\psi_j^{\mathsf{bad},4}\rangle$, $|\psi_j^{'\mathsf{good},4}\rangle$ and $|\psi_j^{'\mathsf{bad},4}\rangle$ that satisfy following properties:*

1. $O_{UP.2} \cdot O_{UP.3} \cdot O_{UP.2} \cdot O_{UP.1} |\psi_j\rangle = |\psi_j^{\mathsf{good},4}\rangle + |\psi_j^{\mathsf{bad},4}\rangle$, *and*
   $O_{UP.2} \cdot O'_{UP.3} \cdot O_{UP.2} \cdot O_{UP.1} |\psi'_j\rangle = |\psi_j^{'\mathsf{good},4}\rangle + |\psi_j^{'\mathsf{bad},4}\rangle$.

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

$$\begin{aligned}
|\psi_j^{\mathsf{good},4}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x')\neq\perp}} & a^{(j),4}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \\
& \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle, \\
|\psi_j^{'\mathsf{good},4}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x')\neq\perp}} & a^{(j),4}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1, D_2, D_F\rangle \\
& \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle.
\end{aligned}$$

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

4. *$\| |\psi_j^{\mathsf{bad},4}\rangle \|$ and $\| |\psi_j^{'\mathsf{bad},4}\rangle \|$ are upper bounded as*

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

where $x_{1LL} = D_{1R}(x') \oplus x_{LR}$, $x_{1LR} = D_{1L}(x') \oplus D_{1R}(x') \oplus x_{LL} \oplus x_{LR}$, $x_{1RL} = D_{1L}(x') \oplus x_{RL}$, $x_{1RR} = D_{1R}(x') \oplus x_{RR}$ *for each summand of* $|\psi_j^{\mathsf{good},4}\rangle$ *and* $|\psi_j^{'\mathsf{good},4}\rangle$.

Proof. From Lemma 6, it follows that there exists vectors $|\psi_j^{\mathsf{good},3}\rangle$, $|\psi_j^{\mathsf{bad},3}\rangle$, $|\psi_j^{'\mathsf{good},3}\rangle$ and $|\psi_j^{'\mathsf{bad},3}\rangle$ that satisfy the four properties in Lemma 6.

Let Π_{prereg} denote the projection onto the space spanned by the vectors that correspond to preregular states. Note that, when we measure the states $O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.3} \cdot O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.1} |\psi_j\rangle$ and $O_{\mathsf{UP}.2} \cdot O'_{\mathsf{UP}.3} \cdot O_{\mathsf{UP}.2} \cdot O_{\mathsf{UP}.1} |\psi'_j\rangle$, we always obtain preregular states.

Define $|\psi_j^{\mathsf{good},4}\rangle := \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} |\psi_j^{\mathsf{good},3}\rangle$, $|\psi_j^{\mathsf{bad},4}\rangle := O_{\mathsf{UP}.2}O_{\mathsf{UP}.3}O_{\mathsf{UP}.2}O_{\mathsf{UP}.1} |\psi_j\rangle - |\psi_j^{\mathsf{good},4}\rangle$. Similarly, we define $|\psi_j^{'\mathsf{good},4}\rangle := \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} |\psi_j^{'\mathsf{good},3}\rangle$, and $|\psi_j^{'\mathsf{bad},4}\rangle := O_{\mathsf{UP}.2}O'_{\mathsf{UP}.3}O_{\mathsf{UP}.2}O_{\mathsf{UP}.1} |\psi'_j\rangle - |\psi_j^{'\mathsf{good},4}\rangle$. Then the first property obviously holds. In addition, the second and third properties follows from the second and third properties of Lemma 6. Below we show the fourth property.

Furthermore, let $\Pi_{D_3:\not\perp}$ and $\Pi_{D_3:\perp}$ be the projections onto the spaces spanned by the vectors $|x,y,z\rangle \otimes |D_1,D_2,D_3\rangle \otimes |x_{1LL},x_{1LR},x_{1RL},x_{1RR}\rangle \otimes |x_{2LL},x_{2LR},x_{2RL},x_{2RR}\rangle$ such that $D_3(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}) \neq \perp$ and $D_3(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}) = \perp$, respectively. Then, we have

$$
\begin{aligned}
&\Pi_{D_3:\not\perp} |\psi_j^{\mathsf{good},3}\rangle \\
&\quad = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)\neq\perp, [D_F]_3(x'_2)\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1,D_2,[D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{1LL},x_{1LR},x_{1RL},x_{1RR}\rangle \otimes |x_{2LL},x_{2LR},x_{2RL},x_{2RR}\rangle \\
&\quad = \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)=\perp, [D_F]_3(x'_2)\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \otimes |D_1,D_2\cup(x'_1,\alpha),[D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{1LL},x_{1LR},x_{1RL},x_{1RR}\rangle \otimes |x_{2LL},x_{2LR},x_{2RL},x_{2RR}\rangle
\end{aligned}
$$

where $x_{1LL} := D_{1R}(x') \oplus x_{LR}$, $x_{1LR} := D_{1L}(x') \oplus D_{1R}(x') \oplus x_{LL} \oplus x_{LR}$, $x_{1RL} := D_{1L}(x') \oplus x_{RL}$, and $x_{1RR} := D_{1R}(x') \oplus x_{RR}$ for each summand in the right hand side.

By applying the first property of Proposition 4 to f_2, we have

$$
\begin{aligned}
&\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} \Pi_{D_3:\not\perp} |\psi_j^{\mathsf{good},3}\rangle \\
&\quad = \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)=\perp, [D_F]_3(x'_2)\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \otimes |D_1,D_2\cup(x'_1,\alpha),[D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{1LL},x_{1LR},x_{1RL},x_{1RR}\rangle \otimes |x_{2LL},x_{2LR},x_{2RL},x_{2RR}\rangle \\
&\quad = \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)=\perp, [D_F]_3(x'_2)\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \otimes |D_1,D_2\cup(x'_1,\alpha),[D_F]_3\rangle \\
&\qquad\qquad \otimes |x_{1LL},x_{1LR},x_{1RL},x_{1RR}\rangle \otimes |0^{n/4},0^{n/4},0^{n/4},0^{n/4}\rangle \\
&\quad + \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)=\perp, [D_F]_3(x'_2)\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \\
&\qquad\qquad \otimes |D_1\rangle, \left(|D_2\rangle - \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |D_2\cup(x'_1,\gamma)\rangle \right), |[D_F]_3\rangle
\end{aligned}
$$

$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle$$

$$- \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1')=\perp, [D_F]_3(x_2')\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle$$

$$\otimes |D_1\rangle, \left(|D_2\cup(x_1',\gamma)\rangle - |D_\gamma^{\mathsf{invalid}}\rangle\right), |[D_F]_3\rangle$$

$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, \alpha_1\oplus\gamma_1, \alpha_2\oplus\gamma_2\rangle$$

$$+ \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1')=\perp, [D_F]_3(x_2')\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle$$

$$\otimes |D_1\rangle, \left(2\sum_\delta \frac{1}{\sqrt{2^{n/2}}} |D_2\cup(x_1',\delta)\rangle - |D_2\rangle\right), |[D_F]_3\rangle$$

$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, \widehat{0^{n/4}}, \widehat{0^{n/4}}\rangle$$

$$= \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1')=\perp, [D_F]_3(x_2')\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle \otimes |D_1, D_2\cup(x_1',\alpha), [D_F]_3\rangle$$

$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \tag{56}$$

$$+ \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1')=\perp, [D_F]_3(x_2')\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle$$

$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \tag{57}$$

$$- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1')=\perp, [D_F]_3(x_2')\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle \otimes |D_1, D_2\cup(x_1',\gamma), [D_F]_3\rangle$$

$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \tag{58}$$

$$- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1')=\perp, [D_F]_3(x_2')\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle \otimes |D_1, D_2\cup(x_1',\alpha), [D_F]_3\rangle$$

$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \tag{59}$$

$$+ \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1')=\perp, [D_F]_3(x_2')\neq\perp}} \frac{1}{2^{3n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle$$

$$\otimes |D_1\rangle \left(2\sum_\delta \frac{1}{\sqrt{2^{n/2}}} |D_2\cup(x_1',\delta)\rangle - |D_2\rangle\right), |[D_F]_3\rangle$$

$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \tag{60}$$

On the term (56), we have

$$\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1')=\perp, [D_F]_3(x_2')\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle$$

$$\otimes |D_1, D_2 \cup (x'_1, \alpha), [D_F]_3\rangle$$
$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle$$
$$= 0 \tag{61}$$

since all databases are good.

On the term (57), we have

$$\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)=\perp, [D_F]_3(x'_2)\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \right.$$
$$\left. \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \right\|^2$$
$$= \left\| \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x')\neq\perp, D_2(x'_1)=\perp}} \sum_{\substack{\alpha \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ [D_F]_3(x'_2)\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \right.$$
$$\otimes |D_1, D_2, [D_F]_3\rangle$$
$$\left. \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \right\|^2$$
$$= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x')\neq\perp, D_2(x'_1)=\perp}} \frac{1}{2^{n/2}} \cdot \left| \sum_{\substack{\alpha \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ [D_F]_3(x'_2)\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \right|^2$$

Now, for each (x, y, z, D_1, D_2, D_F) such that $D_1(x') \neq \perp$ and $D_2(x'_1) = \perp$ (recall that $x_{1LL} := x_{LR} \oplus D_{1R}(x')$, $x_{1LR} := x_{LL} \oplus x_{LR} \oplus D_{1L}(x') \oplus D_{1R}(x')$, $x_{1RL} := x_{RL} \oplus D_{1L}(x')$, $x_{1RR} := x_{RR} \oplus D_{1R}(x')$), the number of α such that $[D_F]_3(x'_2) \neq \perp$ (recall that $x_{2LL} := x_{1LR} \oplus D_{2R}(x'_1)$, $x_{2LR} := x_{1LL} \oplus x_{1LR} \oplus D_{2L}(x'_1) \oplus D_{2R}(x'_1)$, $x_{2RL} := x_{1RL} \oplus D_{2L}(x_1)$, $x_{2RR} := x_{1RR} \oplus D_{2R}(x'_1)$), and $(D_1, D_2 \cup (x'_1, \alpha), D_F)$ becomes good is at most $|D_F| \leq j$. Hence, from the convexity of the function $X \mapsto X^2$, we have

$$\left| \sum_{\substack{\alpha \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ [D_F]_3(x'_2)\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \right|^2$$
$$\leq j \cdot \sum_{\substack{\alpha \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ [D_F]_3(x'_2)\neq\perp}} \left| a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \right|^2$$

holds, which further implies that following holds:

$$\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)=\perp, [D_F]_3(x'_2)\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \right.$$
$$\left. \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \right\|^2$$

$$= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x')\neq\perp, D_2(x'_1)=\perp}} \frac{j}{2^{n/2}} \cdot \left| \sum_{\substack{\alpha \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ [D_F]_3(x'_2)\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \right|^2$$

$$\leq O\left(\frac{j}{2^{n/2}}\right). \tag{62}$$

We now give an upper bound of the norm of the term (58). Note that, if a tuple $(x,(D_1,D_2\cup((x'_1),\gamma),D_F))$ satisfies the conditions

(1) $D_1(x')\neq\perp$, (2) $(D_1,D_2\cup(x'_1,\gamma),D_F)$ is bad,

then the number of α such that

(1) $(D_1,D_2\cup(x'_1,\alpha),D_F)$ becomes good, (2) $D_2(x'_1)=\perp$, and (3) $[D_F]_3(x'_2)\neq\perp$,

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

$$\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)=\perp, [D_F]_3(x'_2)\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \otimes |D_1,D_2\cup(x'_1,\gamma),[D_F]_3\rangle \right.$$
$$\left. \otimes |x_{1LL},x_{1LR},x_{1RL},x_{1RR}\rangle \otimes |0^{n/4},0^{n/4},0^{n/4},0^{n/4}\rangle \right\|^2$$

$$= \left\| \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)=\perp, [D_F]_3(x'_2)\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \right.$$
$$\otimes |D_1,D_2\cup(x'_1,\gamma),[D_F]_3\rangle$$
$$\left. \otimes |x_{1LL},x_{1LR},x_{1RL},x_{1RR}\rangle \otimes |0^{n/4},0^{n/4},0^{n/4},0^{n/4}\rangle \right\|^2$$

$$\leq O\left(\frac{j}{2^{n/2}}\right) \tag{63}$$

in the same way as we showed (51).

On the term (58), we have

$$\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x'_1,\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x'_1)=\perp, [D_F]_3(x'_2)\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x'_1,\alpha),D_F} |x,y,z\rangle \right.$$
$$\otimes |D_1,D_2\cup(x'_1,\alpha),[D_F]_3\rangle$$
$$\left. \otimes |x_{1LL},x_{1LR},x_{1RL},x_{1RR}\rangle \otimes |0^{n/4},0^{n/4},0^{n/4},0^{n/4}\rangle \right\|^2$$

$$= 0, \tag{64}$$

since all databases are good.

On the term (59), we have

$$\Bigg\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\bot, D_2(x_1')=\bot, [D_F]_3(x_2')\neq\bot}} \frac{1}{2^{3n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle$$
$$\otimes |D_1\rangle \left(2\sum_{\delta} \frac{1}{\sqrt{2^{n/2}}} |D_2\cup(x_1',\delta)\rangle - |D_2\rangle \right), |[D_F]_3\rangle$$
$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \Bigg\|^2$$
$$= O\left(\frac{j}{2^{n/2}}\right) \tag{65}$$

follows from (62) and (63).

From (56)-(65),

$$\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} \Pi_{D_3:\not\perp} |\psi_j^{\mathsf{good},3}\rangle \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{66}$$

follows.

In the same way as we obtained (56)-(60), by applying the first property of Proposition 4 to f_2, we have

$$\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} \Pi_{D_3:\bot} |\psi_j^{\mathsf{good},3}\rangle$$
$$= \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\bot, D_2(x_1')=\bot, [D_F]_3(x_2')=\bot}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle \otimes |D_1, D_2\cup(x_1',\alpha), [D_F]_3\rangle$$
$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \tag{67}$$
$$+ \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\bot, D_2(x_1')=\bot, [D_F]_3(x_2')=\bot}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle \otimes |D_1, D_2, [D_F]_3\rangle$$
$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \tag{68}$$
$$- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\bot, D_2(x_1')=\bot, [D_F]_3(x_2')=\bot}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle$$
$$\otimes |D_1, D_2\cup(x_1',\gamma), [D_F]_3\rangle$$
$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \tag{69}$$
$$- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\bot, D_2(x_1')=\bot, [D_F]_3(x_2')=\bot}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle$$
$$\otimes |D_1, D_2\cup(x_1',\alpha), [D_F]_3\rangle$$
$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \tag{70}$$
$$+ \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\bot, D_2(x_1')=\bot, [D_F]_3(x_2')=\bot}} \frac{1}{2^{3n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle$$

$$\otimes |D_1\rangle \left(2 \sum_{\delta} \frac{1}{\sqrt{2^{n/2}}} |D_2 \cup (x_1', \delta)\rangle - |D_2\rangle \right), |[D_F]_3\rangle$$
$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \quad (71)$$

On the term (67), we have

$$\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1, D_2 \cup (x_1', \alpha), D_F)\text{: good} \\ D_1(x') \neq \perp, D_2(x_1') = \perp, [D_F]_3(x_2') = \perp}} a^{(j),3}_{x,y,z,D_1,D_2 \cup (x_1', \alpha), D_F} |x, y, z\rangle \otimes |D_1, D_2 \cup (x_1', \alpha), [D_F]_3\rangle$$
$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle$$
$$= 0, \quad (72)$$

since all databases are good.

On the term (68), we have

$$\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1, D_2 \cup (x_1', \alpha), D_F)\text{: good} \\ D_1(x') \neq \perp, D_2(x_1') = \perp, [D_F]_3(x_2') = \perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2 \cup (x_1', \alpha), D_F} |x, y, z\rangle \otimes |D_1, D_2, [D_F]_3\rangle$$
$$\otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle$$
$$= 0, \quad (73)$$

since all databases are good.

Next, we give an upper bound of the norm of the term (69). Note that, for each tuple $(x, \alpha, (D_1, D_2, D_F))$ that satisfies

(1) $D_1(x') \neq \perp$, (2) $(D_1, D_2 \cup (x_1', \alpha), D_F)$ is good, and (3) $[D_F]_3(x_2') \neq \perp$,

the number of γ such that $(D_1, D_2 \cup (x_1', \gamma), D_F)$ becomes bad is at most $|D_F| \leq j$. Therefore, we have

$$\left\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1, D_2 \cup (x_1', \alpha), D_F)\text{: good} \\ D_1(x') \neq \perp, D_2(x_1') = \perp, [D_F]_3(x_2') = \perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2 \cup (x_1', \alpha), D_F} |x, y, z\rangle \otimes |D_1, D_2 \cup (x_1', \gamma), [D_F]_3\rangle \right.$$
$$\left. \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \right\|^2$$
$$= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x') \neq \perp, D_2(x_1') = \perp}} \sum_{\substack{\gamma \\ (D_1, D_2 \cup (x_1', \alpha), D_F)\text{: bad}}} \cdot \left| \sum_{\substack{\alpha \\ (D_1, D_2 \cup (x_1', \alpha), D_F)\text{: good} \\ [D_F]_3(x_2') = \perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2 \cup (x_1', \alpha), D_F} |x, y, z\rangle \right|^2$$
$$= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ D_1(x') \neq \perp, D_2(x_1') = \perp}} \sum_{\substack{\gamma \\ (D_1, D_2 \cup (x_1', \alpha), D_F)\text{: bad}}} \frac{1}{2^{n/2}} \cdot \sum_{\substack{\alpha \\ (D_1, D_2 \cup (x_1', \alpha), D_F)\text{: good} \\ [D_F]_3(x_2') = \perp}} \left| a^{(j),3}_{x,y,z,D_1,D_2 \cup (x_1', \alpha), D_F} |x, y, z\rangle \right|^2$$

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

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

On the term (70), we have

$$\begin{aligned}\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1)=\perp, [D_F]_3(x_2)=\perp}} & \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle \otimes |D_1, D_2\cup(x_1',\alpha), [D_F]_3\rangle \\ & \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \\ = 0, & \end{aligned} \tag{75}$$

since all databases are good.

On the term (71), we have

$$\begin{aligned}\Bigg\| \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ (D_1,D_2\cup(x_1',\alpha),D_F)\text{: good} \\ D_1(x')\neq\perp, D_2(x_1)=\perp, [D_F]_3(x_2)=\perp}} & \frac{1}{2^{3n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_1',\alpha),D_F} |x,y,z\rangle \\ & \otimes |D_1\rangle \left(2\sum_{\delta}\frac{1}{\sqrt{2^{n/2}}} |D_2\cup(x_1',\delta)\rangle - |D_2\rangle\right), |[D_F]_3\rangle \\ & \otimes |x_{1LL}, x_{1LR}, x_{1RL}, x_{1RR}\rangle \otimes |0^{n/4}, 0^{n/4}, 0^{n/4}, 0^{n/4}\rangle \Bigg\|^2 \\ \leq O\left(\frac{j}{2^{n/2}}\right) & \end{aligned} \tag{76}$$

follows from (73) and (74).

From (67)-(74), it follows that

$$\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2}\Pi_{D_3:\perp} |\psi_j^{\mathsf{good},3}\rangle \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right). \tag{77}$$

Therefore, we have

$$\begin{aligned}\left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} |\psi_j^{\mathsf{good},3}\rangle\right\| & \\ \leq \left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2}\Pi_{D_F:\not\perp} |\psi_j^{\mathsf{good},3}\rangle\right\| + \left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2}\Pi_{D_F:\perp} |\psi_j^{\mathsf{good},3}\rangle\right\| & \\ \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) & \end{aligned} \tag{78}$$

follows from (66) and (77).

Since we have

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

which implies that

$$\begin{aligned}\left\|\psi_j^{\mathsf{bad},4}\right\| &= \left\|O_{\mathsf{UP}.2}O_{\mathsf{UP}.3}O_{\mathsf{UP}.2}O_{\mathsf{UP}.1} |\psi_j\rangle - \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} |\psi_j^{\mathsf{good},3}\rangle\right\| \\ &= \left\|\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2}O_{\mathsf{UP}.3}O_{\mathsf{UP}.2}O_{\mathsf{UP}.1} |\psi_j\rangle - \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} |\psi_j^{\mathsf{good},3}\rangle\right\|\end{aligned}$$

$$
\begin{aligned}
&= \left\| \Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} \left(|\psi_j^{\mathsf{good},3}\rangle + |\psi_j^{\mathsf{bad},3}\rangle \right) - \Pi_{\mathsf{good}} \Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} |\psi_j^{\mathsf{good},3}\rangle \right\| \\
&= \left\| \Pi_{\mathsf{bad}} \Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} |\psi_j^{\mathsf{good},3}\rangle \right\| + \left\| \Pi_{\mathsf{prereg}} O_{\mathsf{UP}.2} |\psi_j^{\mathsf{bad},3}\rangle \right\| \\
&\leq O\left(\sqrt{\frac{j}{2^{n/2}}} \right) + \left\| |\psi_j^{\mathsf{bad},3}\rangle \right\| \\
&\leq O\left(\sqrt{\frac{j}{2^{n/2}}} \right) + \left\| |\psi_j^{\mathsf{bad}}\rangle \right\| \qquad (79)
\end{aligned}
$$

follows from Lemma 6 on the action of $O_{\mathsf{UP}.3}$ and $O'_{\mathsf{UP}.3}$. Similarly, we can show

$$
\left\| |\psi_j^{'\mathsf{bad},4}\rangle \right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}} \right) + \left\| |\psi_j^{'\mathsf{bad}}\rangle \right\| \qquad (80)
$$

in the same way, and the fourth property of the lemma also holds. □

Action of the second $O_{\mathsf{UP}.1}$: Let $|\psi_{j+1}^{\mathsf{good}}\rangle := \Pi_{\mathsf{good}} \Pi_{\mathsf{reg}} O_{\mathsf{UP}.1} |\psi_j^{\mathsf{good},4}\rangle$, $|\psi_{j+1}^{\mathsf{bad}}\rangle := |\psi_{j+1}\rangle - |\psi_{j+1}^{\mathsf{good}}\rangle$, $|\psi_{j+1}^{'\mathsf{good}}\rangle := \Pi_{\mathsf{good}} \Pi_{\mathsf{reg}} O_{\mathsf{UP}.1} |\psi_j^{'\mathsf{good},4}\rangle$, $|\psi_{j+1}^{'\mathsf{bad}}\rangle := |\psi'_{j+1}\rangle - |\psi_{j+1}^{'\mathsf{good}}\rangle$. Then we can show the desired properties in Proposition 7, in the same way as we showed Lemma 7 on the action of the second $O_{\mathsf{UP}.2}$. □

Finishing the Proof of Proposition 6. Let $|\psi_j^{\mathsf{good}}\rangle$, $|\psi_j^{\mathsf{bad}}\rangle$, $|\psi_j^{'\mathsf{good}}\rangle$, and $|\psi_j^{'\mathsf{bad}}\rangle$ be the vectors as defined in the Proposition 7. From (44) of Proposition 7, it follows that

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

Similarly, it holds that $\| |\psi_{q+1}^{'\mathsf{bad}}\rangle \| \leq O\left(\sqrt{q^3/2^{n/2}} \right)$.

Now, let $\mathsf{tr}_{\mathcal{D}_{123}}$ and $\mathsf{tr}_{\mathcal{D}_{12F}}$ be the partial trace operations over the databases for FOX_3 and FOX'_3, respectively. From (42) and (43) of Proposition 7, it follows that

$$
\mathsf{td}\left(\mathsf{tr}_{\mathcal{D}_{123}} \left(|\psi_{q+1}^{\mathsf{good}}\rangle, \langle \psi_{q+1}^{\mathsf{good}}| \right), \mathsf{tr}_{\mathcal{D}_{12F}} \left(|\psi_{q+1}^{'\mathsf{good}}\rangle, \langle \psi_{q+1}^{'\mathsf{good}}| \right) \right) = 0.
$$

Therefore, we have that

$$
\begin{aligned}
\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}_3, \mathsf{FOX}'_3}(\mathcal{A}) &\leq \mathsf{td}\left(\mathsf{tr}_{\mathcal{D}_{123}} \left(|\psi_{q+1}\rangle, \langle \psi_{q+1}| \right), \mathsf{tr}_{\mathcal{D}_{12F}} \left(|\psi_{q+1}\rangle, \langle \psi_{q+1}| \right) \right) \\
&\leq \mathsf{td}\left(\mathsf{tr}_{\mathcal{D}_{123}} \left(|\psi_{q+1}^{\mathsf{good}}\rangle, \langle \psi_{q+1}^{\mathsf{good}}| \right), \mathsf{tr}_{\mathcal{D}_{12F}} \left(|\psi_{q+1}^{'\mathsf{good}}\rangle, \langle \psi_{q+1}^{'\mathsf{good}}| \right) \right) \\
&\quad + 2\| |\psi_{q+1}^{\mathsf{bad}}\rangle \| + 2\| |\psi_{q+1}^{'\mathsf{bad}}\rangle \| \\
&\leq O\left(\sqrt{q^3/2^{n/2}} \right),
\end{aligned}
$$

which completes the proof of Proposition 6. □

6.2 Hardness of Distinguishing FOX'_2 from RF

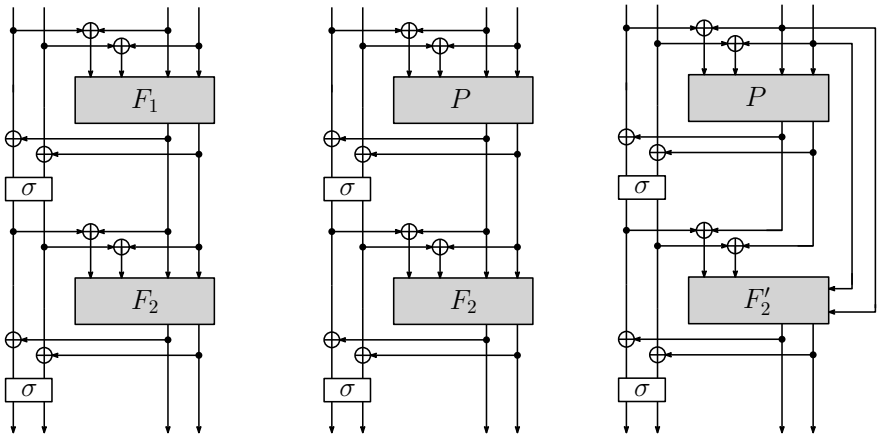
Proposition 8. *Let $\mathcal{A}$ be an adversary that makes at most q quantum queries. Then, it holds that $\mathbf{Adv}^{dist}_{FOX'_2, RF}(\mathcal{A}) \leq O(\sqrt{q^6/2^{n/2}})$.*

Let us modify $\mathsf{FOX}'_2(F_1, F_2)$ in such a way that F_1 is replaced with a family of random permutations P, and denote the resulting function by $\mathsf{FOX}'_2(P, F_2)$ (see Figure 7b).

Further, let us modify $\mathsf{FOX}'_2(P, F_2)$ again in such a way that F_2 is replaced with a new random function F'_2, and denote the resulting function by RF' (see Figure 7c). The random function $F'_2 : \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \to \{0,1\}^{n/2}$ is defined as follows:

$$(x_{1LL} \oplus x_{1RL}, x_{1LR} \oplus x_{1RR}, x_{1RL}, x_{1RR}, x_{RL}, x_{RR}) \mapsto (x_{2LL}, x_{2LR}, x_{2RL}, x_{2RR}),$$

where $x_{1LL} := x_{LR} \oplus P_{1R}(x_{LL} \oplus x_{RL}, x_{LR} \oplus x_{RR})$, $x_{1LR} := x_{LL} \oplus x_{LR} \oplus P_{1L}(x_{LL} \oplus x_{RL}, x_{LR} \oplus x_{RR}) \oplus P_{1R}(x_{LL} \oplus x_{RL}, x_{LR} \oplus x_{RR})$, $x_{1RL} := P_{1L}(x_{LL} \oplus x_{RL}, x_{LR} \oplus x_{RR})$, and $x_{1RR} := P_{1R}(x_{LL} \oplus x_{RL}, x_{LR} \oplus x_{RR})$.



(a) $\mathsf{FOX}'_2(F_1, F_2)$. (b) $\mathsf{FOX}'_2(P, F_2)$. (c) $\mathsf{RF}' := \mathsf{FOX}'_2(P, F'_2)$.

Figure 7: The modified versions of FOX_2.

Our goal is confined to show the following 2 properties:

- $\mathsf{FOX}'_2(F_1, F_2)$ is hard to distinguish from $\mathsf{FOX}'_2(P, F_2)$, and
- $\mathsf{FOX}'_2(P, F_2)$ is hard to distinguish from RF' .

In what follows, we show

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}'_2(F_1,F_2),\mathsf{RF}'}(\mathcal{A}) \leq O\left(\sqrt{q^6/2^{n/2}}\right)$$

instead of showing $\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}'_2(F_1,F_2),\mathsf{RF}}(\mathcal{A}) \leq O\left(\sqrt{q^6/2^{n/2}}\right)$.

Hardness of Distinguishing $\mathsf{FOX}'_2(F_1, F_2)$ from $\mathsf{FOX}'_2(P, F_2)$. This can be shown by using Proposition 2 which says that it is hard to distinguish FRP from RF. Note that in $\mathsf{FOX}'_2(F_1, F_2)$, F_1 and F_2 are independent random functions, whereas in $\mathsf{FOX}'_2(P, F_2)$, P is a FRP. Hence, using Proposition 2, it follows that

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}'_2(F_1,F_2),\mathsf{FOX}'_2(P,F_2)}(q) \leq O(\sqrt{q^6/2^{n/2}}). \tag{81}$$

Hardness of Distinguishing $\mathsf{FOX}'_2(P, F_2)$ from RF'. Observe that the function distribution of $\mathsf{FOX}_2(P, F'_2)$ is same as that of RF'. (Note that $P(x_{LL} \oplus x_{RL}, x_{LR} \oplus x_{RR}, x_{RL}, x_{RR}) \neq P(x_{LL} \oplus x'_{RL}, x_{LR} \oplus x'_{RR}, x'_{RL}, x'_{RR})$ always holds if $x_{RL} \neq x'_{RL}$ and $x_{RR} \neq x'_{RR}$. Thus, if $(x_{LL}, x_{LR}, x_{RL}, x_{RR}) \neq (x'_{LL}, x'_{LR}, x'_{RL}, x'_{RR})$, then the corresponding inputs to F'_2 will be distinct.) Therefore, we have that

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}'_2(P,F'_2),\mathsf{RF}'}(q) = 0. \tag{82}$$

Finally, by combining the results given in Equations (81) and (82), it follows that

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}'_2(F_1,F_2),\mathsf{RF}'}(q) \leq O\left(\sqrt{q^6/2^{n/2}}\right), \tag{83}$$

which completes the proof of Proposition 8. □

6.3 Proof of Theorem 1

We are in a position to complete the proof for Theorem 1, by using the results presented in Subsection 6.1 and Subsection 6.2.

Proof of Theorem 1. First, we modify FOX_4 in such a way that the state update operation of the third round is modified as

$$\begin{aligned}(x_{3LL}, x_{3LR}, x_{3RL}, x_{3RR}) := \big(&x_{2LR} \oplus F_R(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}),\\ &x_{2LL} \oplus x_{2LR} \oplus F_L(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR})\\ &\qquad \oplus F_R(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}),\\ &F_L(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR}),\\ &F_R(x_{2LL} \oplus x_{2RL}, x_{2LR} \oplus x_{2RR}, x_{2RL}, x_{2RR})\big)\end{aligned}$$

and the state update operation of fourth round is modified as

$$\begin{aligned}(x_{4LL}, x_{4LR}, x_{4RL}, x_{4RR}) := \big(&x_{3LR} \oplus F'_R(x_{3LL} \oplus x_{3RL}, x_{3LR} \oplus x_{3RR}, x_{3RL}, x_{3RR}),\\ &x_{3LL} \oplus x_{3LR} \oplus F'_L(x_{3LL} \oplus x_{3RL}, x_{3LR} \oplus x_{3RR}, x_{3RL}, x_{3RR})\\ &\qquad \oplus F'_R(x_{3LL} \oplus x_{3RL}, x_{3LR} \oplus x_{3RR}, x_{3RL}, x_{3RR}),\\ &F'_L(x_{3LL} \oplus x_{3RL}, x_{3LR} \oplus x_{3RR}, x_{3RL}, x_{3RR}),\\ &F'_R(x_{3LL} \oplus x_{3RL}, x_{3LR} \oplus x_{3RR}, x_{3RL}, x_{3RR})\big),\end{aligned}$$

where $F, F' : \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \times \{0,1\}^{n/4} \to \{0,1\}^{n/2}$ are random functions. Let us denote the modified function by FOX''_4. In addition, let FOX'''_4 be the composition of FOX_2 with a random function $\mathsf{RF} : \{0,1\}^n \to \{0,1\}^n$ (see Figure 8).

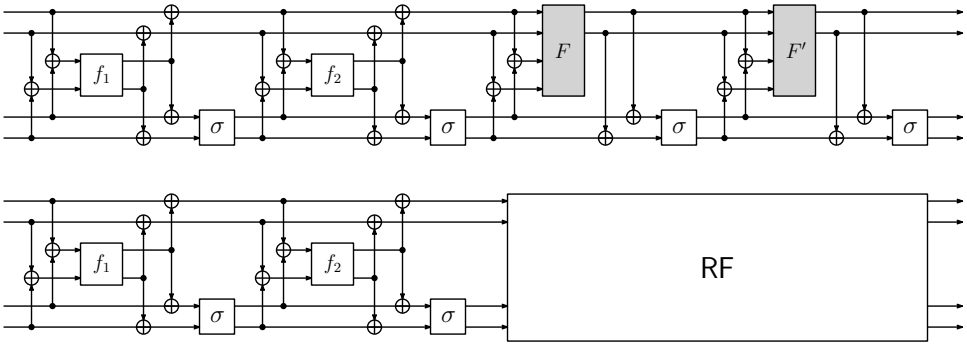


Figure 8: FOX''_4 and FOX'''_4

Then, by applying Proposition 6 twice, it follows that

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}_4,\mathsf{FOX}''_4}(q) \leq O\left(\sqrt{q^3/2^{n/2}}\right). \tag{84}$$

In addition, by applying Proposition 8, it holds that

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}''_4,\mathsf{FOX}'''_4}(q) \leq O\left(\sqrt{q^6/2^{n/2}}\right). \tag{85}$$

Furthermore, it holds that $\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}'''_4,\mathsf{RF}}(q) = 0$ since FOX_2 is a permutation. From the quantum version of the PRP-PRF switching lemma (Proposition 1) and all the above inequalities (84)-(85), we have

$$\begin{aligned}\mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}_4,\mathsf{RP}}(q) &\leq \mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}_4,\mathsf{FOX}''_4}(q) + \mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}''_4,\mathsf{FOX}'''_4}(q) + \mathbf{Adv}^{\mathsf{dist}}_{\mathsf{FOX}'''_4,\mathsf{RF}}(q) + \mathbf{Adv}^{\mathsf{dist}}_{\mathsf{RF},\mathsf{RP}}(q) \\ &\leq O\left(\sqrt{\frac{q^6}{2^{n/2}}}\right),\end{aligned}$$

which completes the proof of Theorem 1. □

7 Conclusions

We showed that the 3- and 4-round FOX constructions are not PRP against qCPAs, and qCCAs, respectively. We also showed that $O(2^{n/12})$ quantum queries are required to distinguish the 4-round FOX construction with block size n bits from a random permutation by qCPAs. That is, the 4-round FOX construction becomes a quantumly secure PRP against qCPAs if the round functions are quantumly secure PRFs. We used an alternative formalization of Zhandry's compressed oracle technique introduced by Hosoyamada and Iwata for the security proofs.

As a future work, it would be interesting to derive tighter security bounds for the 4-round FOX construction against qCPAs. Another important future work would be to analyze the security of FOX construction against qCCAs. Since the compressed oracle technique can be used for random functions but cannot be used for random permutations that allow inverse queries, qCCA security remains a challenging problem.

Acknowledgment

We would like to thank the anonymous reviewers for their insightful comments and suggestions, which has significantly improved the presentation and technical quality of this work. The second author would also like to thank MATRICS grant 2019/1514 by the Science and Engineering Research Board (SERB), Dept. of Science and Technology, Govt. of India for supporting the research carried out in this work.

Timeline

This version of the manuscript was submitted to a venue on April 8, 2022. A previous version of the manuscript, which was submitted earlier on March 1, 2022, had a minor flaw in the proof of Proposition 8 which has been rectified in the current version.

References

[AG07] MediaCrypt AG. IDEA-NXT description. `http://www.mediacrypt.com`, 2007.

[BBC+21] Ritam Bhaumik, Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, and Yannick Seurin. QCB: efficient quantum-secure authenticated encryption. In *Advances in Cryptology - ASIACRYPT*, volume 13090, pages 668–698. Springer, 2021.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Advances in Cryptology - ASIACRYPT*, volume 7073, pages 41–69. Springer, 2011.

[BGLP21] Zhenzhen Bao, Jian Guo, Shun Li, and Phuong Pham. Quantum multi-collision distinguishers. Cryptology ePrint Archive, Report 2021/703, 2021. `https://ia.cr/2021/703`.

[BNS19] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. On quantum slide attacks. In *Selected Areas in Cryptography - SAC*, volume 11959, pages 492–519. Springer, 2019.

[Bon17] Xavier Bonnetain. Quantum key-recovery on full AEZ. In *Selected Areas in Cryptography - SAC*, volume 10719, pages 394–406. Springer, 2017.

[CKS21] Amit Kumar Chauhan, Abhishek Kumar, and Somitra Kumar Sanadhya. Quantum free-start collision attacks on double block length hashing with round-reduced AES-256. *IACR Trans. Symmetric Cryptol.*, 2021(1):316–336, 2021.

[DDW20] Xiaoyang Dong, Bingyou Dong, and Xiaoyun Wang. Quantum attacks on some Feistel block ciphers. *Des. Codes Cryptography*, 88(6):1179–1203, 2020.

[DSS+20] Xiaoyang Dong, Siwei Sun, Danping Shi, Fei Gao, Xiaoyun Wang, and Lei Hu. Quantum collision attacks on AES-like hashing with low quantum random access memories. In *Advances in Cryptology - ASIACRYPT*, volume 12492, pages 727–757. Springer, 2020.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *ACM Symposium on the Theory of Computing*, pages 212–219. ACM, 1996.

[HI19] Akinori Hosoyamada and Tetsu Iwata. 4-Round Luby-Rackoff Construction is a qPRP. In *Advances in Cryptology - ASIACRYPT*, pages 145–174. Springer, 2019.

[HI20] Akinori Hosoyamada and Tetsu Iwata. Tight quantum security bound of the 4-round Luby-Rackoff construction. *IACR Cryptol. ePrint Arch.*, 2019:243, 2020.

[HS18] Akinori Hosoyamada and Yu Sasaki. Quantum demiric-selçuk meet-in-the-middle attacks: Applications to 6-round generic feistel constructions. In *Security and Cryptography for Networks - SCN*, volume 11035, pages 386–403. Springer, 2018.

[HS20] Akinori Hosoyamada and Yu Sasaki. Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound. In *Advances in Cryptology - EUROCRYPT*, volume 12106, pages 249–279. Springer, 2020.

[IHM+19] Gembu Ito, Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki, and Tetsu Iwata. Quantum chosen-ciphertext attacks against Feistel ciphers. In *Topics in Cryptology - CT-RSA*, volume 11405, pages 391–411. Springer, 2019.

[JV04] Pascal Junod and Serge Vaudenay. FOX : A new family of block ciphers. In *SAC*, volume 3357, pages 114–129. Springer, 2004.

[KLLN16a] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In *CRYPTO*, volume 9815, pages 207–237. Springer, 2016.

[KLLN16b] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(1):71–94, 2016.

[KM10] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In *IEEE International Symposium on Information Theory*, pages 2682–2685. IEEE, 2010.

[LLH15] Yiyuan Luo, Xuejia Lai, and Jing Hu. The pseudorandomness of many-round lai-massey scheme. *J. Inf. Sci. Eng.*, 31(3):1085–1096, 2015.

[LM90] Xuejia Lai and James L. Massey. A proposal for a new block encryption standard. In *EUROCRYPT*, volume 473, pages 389–404. Springer, 1990.

[LM17] Gregor Leander and Alexander May. Grover meets Simon - quantumly attacking the FX-construction. In *Advances in Cryptology - ASIACRYPT*, volume 10625, pages 161–178. Springer, 2017.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Edition.* Cambridge University Press, USA, 2011.

[NDJY21] Boyu Ni, Xiaoyang Dong, Keting Jia, and Qidi You. (quantum) collision attacks on reduced simpira v2. *IACR Trans. Symmetric Cryptol.*, 2021(2):222–248, 2021.

[Sho94] Peter W. Shor. Polynominal time algorithms for discrete logarithms and factoring on a quantum computer. In *Algorithmic Number Theory, ANTS-I*, volume 877, page 289. Springer, 1994.

[Sim97] Daniel R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997.

[SS17] Thomas Santoli and Christian Schaffner. Using simon's algorithm to attack symmetric-key cryptographic primitives. *Quantum Inf. Comput.*, 17(1&2):65–78, 2017.

[Vau99] Serge Vaudenay. On the Lai-Massey scheme. In *Advances in Cryptology - ASIACRYPT*, volume 1716, pages 8–19. Springer, 1999.

[WLLZ09] Zhongming Wu, Yiyuan Luo, Xuejia Lai, and Bo Zhu. Improved cryptanalysis of the FOX block cipher. In *Trusted Systems INTRUST*, volume 6163, pages 236–249. Springer, 2009.

[Zha15] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Inf. Comput.*, 15(7&8):557–567, 2015.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *Advances in Cryptology - CRYPTO*, volume 11693, pages 239–268. Springer, 2019.

Appendices

A Detailed View of qCPA Distinguisher against FOX_3

This section provides a detailed view of quantum CPA distinguisher against FOX_3, which is given in Section 4. In Figure 9, we give details of all intermediate calculations for an easy verification of the given qCPA attack against FOX_3.

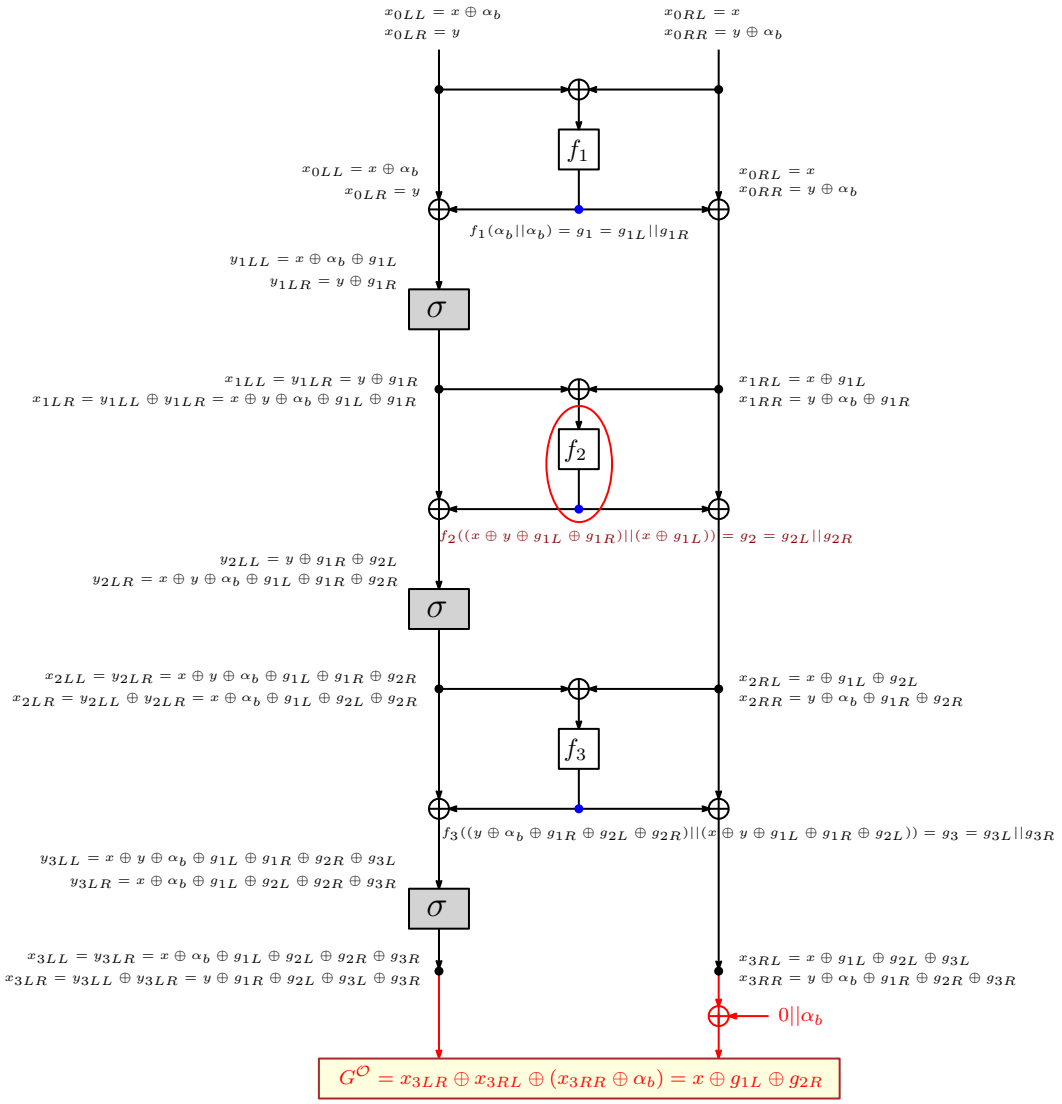


Figure 9: A detailed view of $G^{\mathcal{O}}$ with $\mathcal{O} = \mathsf{FOX}_3$, and $f_i \in \mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$.

B Detailed View of qCCA Distinguishers against FOX_4

This section provides a detailed view of quantum CCA distinguisher against FOX_4. In Figure 10, we give details of all intermediate calculations for FOX_4.

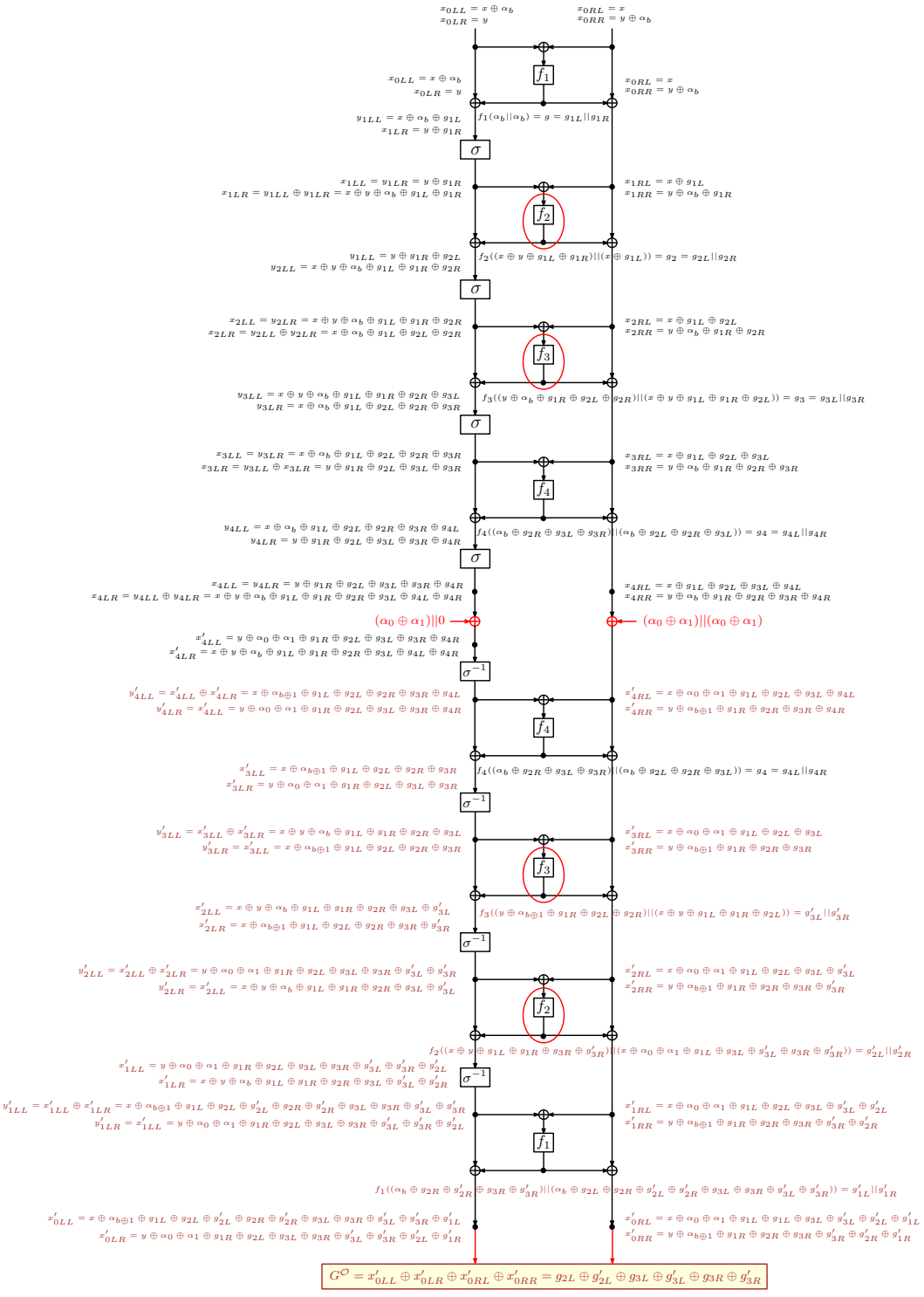


Figure 10: A detailed view of $G^{\mathcal{O}}$ with $\mathcal{O} = \mathsf{FOX}_4$, and $f_i \in \mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$.