Quantum Security of TNT

Shuping Mao[1,2], Zhiyu Zhang[1,2], Lei Hu[1,2], Luying Li[1,2] and Peng Wang[1,2](✉)

[1] State Key Laboratory of Information Security, Institute of Information Engineering, CAS
[2] School of Cyber Security, University of Chinese Academy of Sciences
w.rocking@gmail.com

Abstract. With the development of quantum attacks, many classical-secure structures are not secure in quantum. How to evaluate the quantum security of structure and give a tight security bound becomes a challenging research topic. As a tweakable block cipher structure based on block ciphers, TNT was proven to be of classical beyond-birthday-bound $O(2^{3n/4})$ security. We prove that TNT is a quantum-secure tweakable block cipher with a bound of $O(2^{n/6})$. In addition, we show the tight quantum PRF security bound of $O(2^{n/3})$ when TNT is based on random functions, which is better than $O(2^{n/4})$ given by Bhaumik et al. and solves their open problem. Our proof uses the recording standard oracle with errors technique of Hosoyamada and Iwata based on Zhandry's compressed oracle technique.

Keywords: TNT · qPRF · q$\widetilde{\text{PRP}}$ · Quantum proof · Quantum attack.

1 Introduction

The notion of *tweakable block cipher* (TBC for short) proposed by Liskov et al. [23] has become a popular symmetric primitive. Compared to block ciphers, TBCs have an extra input named "tweak". TNT (Tweak-aNd-Tweak) proposed at Eurocrypt 2020 by Bao et al. [2] is a TBC based on three block ciphers:

$$\mathsf{TNT}[E_{K_0}, E_{K_1}, E_{K_2}](M, T) = E_{K_2}(T \oplus E_{K_1}(T \oplus E_{K_0}(M))),$$

where E is the block cipher and T is the tweak. For a secure TBC, each tweak induces an independent pseudorandom permutation (PRP), making the design and security proof of the above mode much easier. So, Liskov et al. [23] suggested two stages to design block cipher modes: first design TBCs based on block ciphers, and second design modes based on TBCs.

Early TBCs based on block ciphers such as LRW1, LRW2 [23] and XEX [29], have birthday-bound classic security, which can be broken by $2^{n/2}$ queries where n is the block length. Unfortunately, none of these constructions is quantum secure when the attacker queries TBC's quantum oracles $O(n)$ times [13].

If the underlying component is lightweight block ciphers with a typical block length of 64 bits, Beyond-Birthday-Bound (BBB) security is an essential requirement for the above TBCs. A large number of TBCs with BBB security have been proposed, including CLRW2 [20], r-CLRW [19], $\widetilde{F}[1]$ and $\widetilde{F}[2]$ [26], $\widetilde{E1}, ..., \widetilde{E32}$ [31], TEM [6], XTX [27], XKX [28], XHX [16], XHX2 [22] and TNT [2], etc.

TNT is an elegant TBC with BBB security. It has been proven to be secure up to $O(2^{2n/3})$ queries (later, we abbreviate as "$O(2^{2n/3})$ security"). Then Guo et al. [9] improved the bound to $O(2^{3n/4})$, and gave a distinguishing attack with $O(\sqrt{n}2^{3n/4})$ queries. Early birthday-bound TBCs are vulnerable to quantum attacks, which raises natural questions.

Whether TNT ***is secure in quantum?*** or even ***Whether*** TNT ***is beyond-birthday-bound secure in quantum?***

Note that since the quantum collision bound is $O(2^{n/3})$ [32], we refer to the birthday bound in quantum as $O(2^{n/3})$. We call the bound beyond $O(2^{n/3})$ as beyond-birthday bound in quantum.

We can also view TNT as a pseudorandom function (PRF). Bhaumik et al. [4] have recently proved that the quantum security bound of TNT as a PRF is $O(2^{n/4})$ while leaving the task of improving the bound to $O(2^{n/3})$ as an open problem.

Can we find the tight bound of TNT ***as a quantum PRF?***

Security analysis can be divided into two categories, namely proofs and attacks. When the proof bound and attacking bound coincide with each other, it is referred to as a tight bound. In the case of proofs of modes that are based on block ciphers, it is customary to assess the proof bound by substituting the underlying block ciphers idealized as random permutations with random functions, so as to simplify the proof. As to TNT, the PRP security bound can be assessed in the case of $\mathsf{TNT}[\pi_0, \pi_1, \pi_2]$ where $\pi_i, i = 1, 2, 3$ are three independent random permutations. We only consider the PRF security bound of $\mathsf{TNT}[f_0, f_1, f_2]$ where $f_i, i = 1, 2, 3$ are three independent random functions, and then transform it to PRP bound by the PRP/PRF-switching lemma which measures the distance between a random permutation and a random function. In the classical literature [3], the typical birthday bound is $O(2^{n/2})$, while in the quantum literature [32], it is $O(2^{n/3})$. Consequently, this lemma is mostly utilized in birthday-bound proofs. In the case of tweakable block ciphers, the corresponding $\widetilde{\text{PRP}}$/PRF-switching lemma (Here the PRF has two inputs: message and tweak) that measures the distance between a tweakable random permutation and a random function is also $O(2^{n/2})$ in the classic literature [29]. However, in the quantum literature [11,13], it is $O(2^{n/6})$, which is not expected to be tight [13].

From the perspective of quantum attacks, many classical-secure constructions are not secure in quantum. Quantum algorithms such as Simon's algorithm [30], Grover's algorithm [8], Grover-meet-Simon algorithm [21] etc. can effectively accelerate attacks to some classical structures. For example, TBCs such as LRW1, LRW2 [13] and XEX, block-cipher structures such as 3-round [18], 4-round [14] Feistel structure, 3-round MISTY-L structure, 3-round MISTY-R structure [24], 3-round, 4-round Lai-Massey structure [25] and Even-Mansour structure [17] are not secure by using Simon's algorithm with polynomial quantum queries. FX construction [21], 5-round Feistel structure [7], 7-round Feistel-KF structure and 9-round Feistel-FK structure [14] can be attacked with less queries using the Grover-meet-Simon algorithm. Quantum attacks have a great impact on cryptographic constructions, and how to find quantum-secure constructions and how to prove them is also a hot topic of research.

From the perspective of quantum proofs, in 2019, Zhandry [33] proposed "compressed oracle" to record quantum queries, which solved the quantum recording problem and greatly advanced quantum proof technology. Then Hosoyamada and Iwata proposed "Recording Standard Oracle with Errors" (RstOE for short) based on Zhandry's technique. By using the RstOE technique, they show the tight quantum security bound of 4-round Feistel structure [10,11], the quantum security of LRWQ [13] and the tight quantum security bound of HMAC and NMAC [12] in the Quantum Random Oracle Model.

Table 1. Security results of TNT, where f_0, f_1, f_2 are random functions and π_0, π_1, π_2 are random permutations.

	Security goal	Proof bound	Attacking bound	Reference
$\mathsf{TNT}[f_0, f_1, f_2]$	qPRF	$O(2^{n/4})$	-	[4]
	qPRF	$O(2^{n/3})$	$O(2^{n/3})$	Section 3
$\mathsf{TNT}[\pi_0, \pi_1, \pi_2]$	$\widetilde{\text{PRP}}$	$O(2^{2n/3})$	-	[2]
	$\widetilde{\text{PRP}}$	$O(2^{3n/4})$	$O(\sqrt{n}2^{3n/4})$	[9]
	qPRF	$O(2^{n/4})$	-	[4]
	qPRF	$O(2^{n/3})$	-	Section 3
	q$\widetilde{\text{PRP}}$	$O(2^{n/6})$	$O(2^{n/2})$	Section 4

Our contributions Our contributions are related to the three questions mentioned above: we answer two questions and give the corresponding attack for the other one. The contributions of this paper are listed as follows and summarized in Table 1:

1. We show the tight quantum PRF security bound of $\mathsf{TNT}[f_0, f_1, f_2]$ is $O(2^{n/3})$ by a proof and an attack. Our proof bound is better than $O(2^{n/4})$ by Bhaumik et al. [4] and solves their open problem. The quantum attack we use for $\mathsf{TNT}[f_0, f_1, f_2]$ requires that the underlying components be random functions, so it is not possible to transform it directly into a quantum attack on $\mathsf{TNT}[\pi_0, \pi_1, \pi_2]$.
2. We prove the $O(2^{n/6})$ quantum $\widetilde{\text{PRP}}$ security of $\mathsf{TNT}[\pi_0, \pi_1, \pi_2]$, where n is the block length. Without considering the effect of the q$\widetilde{\text{PRP}}$/qPRF switching lemma, the bound is $O(2^{n/3})$. So TNT is still secure in quantum.
3. We give a cross-road distinguisher on TNT with $O(2^{n/2})$ quantum queries and a Grover-meet-Simon attack with $O(n2^{k/2})$ quantum queries, where k is the length of key.

2 Preliminaries

2.1 (Tweakable) Block Ciphers

Block Ciphers. A block cipher (or BC for short) $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a map with key space $\{0,1\}^k$ and message space $\{0,1\}^n$ such that for every key $K \in \{0,1\}^k$, $M \mapsto E(K, M)$ is a permutation of $\{0,1\}^n$. We let E_K denote the map

$M \mapsto E(K, M)$. The inverse of a block cipher E is the map $E^{-1} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ defined by $E^{-1}(K, C) = E_K^{-1}(C)$.

Tweakable Block Ciphers. A tweakable block cipher (or TBC for short) $\tilde{E} : \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$ is a map with key space $\{0,1\}^k$, tweak space $\{0,1\}^t$, and message space $\{0,1\}^n$ such that for every key $K \in \{0,1\}^k$ and every tweak $T \in \{0,1\}^t$, $M \mapsto \tilde{E}(K, M, T)$ is a permutation of $\{0,1\}^n$. We let $\tilde{E}_K$ denote the map $(M, T) \mapsto \tilde{E}(K, M, T)$. The inverse of a TBC $\tilde{E}$ is the map $\tilde{E}_K^{-1} : \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$ defined by $\tilde{E}^{-1}(K, C, T)$ being the unique M such that $\tilde{E}(K, M, T) = C$.

2.2 Quantum Security Advantages

Let H denote the Hadamard operator in the 1-qubit state. Let the identity operator for an n-qubit quantum system be I_n or I.

Quantum distinguishing advantage. O_1, O_2 are two oracles. Let $\mathcal{A}$ be an adversary querying the corresponding quantum oracles U_{O_i}, defined as $U_{O_i} |x\rangle |y\rangle = |x\rangle |y \oplus O_i(x)\rangle$, $i = 1, 2$. The quantum distinguishing advantage of $\mathcal{A}$ is defined as:

$$\mathrm{Adv}^{\text{dist}}_{O_1,O_2}(\mathcal{A}) := \left|\Pr\left[\mathcal{A}^{U_{O_1}} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{U_{O_2}} \Rightarrow 1\right]\right|.$$

Quantum PRF advantage. Let $F : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^n$ is a function. $\mathsf{RF} : \{0,1\}^* \to \{0,1\}^n$ is a random function. Let $\mathcal{A}$ be an adversary querying the quantum oracle U_F or U_{RF}. The quantum pseudorandom function advantage (or qPRF advantage for short) of $\mathcal{A}$ is defined as:

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

Quantum PRP advantage. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. $\mathsf{RP} : \{0,1\}^n \to \{0,1\}^n$ is a random permutation. Let $\mathcal{A}$ be an adversary querying the quantum oracle U_E or U_{RP}. The quantum pseudorandom permutation advantage (or qPRP advantage for short) of $\mathcal{A}$ is defined as:

$$\mathrm{Adv}^{\text{qPRP}}_{E}(\mathcal{A}) = \mathrm{Adv}^{\text{dist}}_{E,\mathsf{RP}}(\mathcal{A}).$$

Quantum $\widetilde{\textbf{PRP}}$ advantage. Let $\tilde{E} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ be a tweakable block cipher. $\widetilde{\mathsf{RP}} : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ is a tweakable random permutation, i.e. $\widetilde{\mathsf{RP}}(T, \cdot)$ is an independent random permutation for each $T \in \{0,1\}^t$. Let $\mathcal{A}$ be an adversary querying the quantum oracle $U_{\tilde{E}}$ or $U_{\widetilde{\mathsf{RP}}}$. The quantum tweakable pseudorandom permutation advantage (or q$\widetilde{\text{PRP}}$ advantage for short) of $\mathcal{A}$ is defined as:

$$\mathrm{Adv}^{\text{q}\widetilde{\text{PRP}}}_{\tilde{E}}(\mathcal{A}) = \mathrm{Adv}^{\text{dist}}_{\tilde{E},\widetilde{\mathsf{RP}}}(\mathcal{A}).$$

Proposition 1 (qPRP/qPRF switching lemma [32]). *Let $\mathcal{A}$ be an adversary making at most q quantum queries to a random permutation RP or a random function RF from $\{0,1\}^n$ to $\{0,1\}^n$. Then* $\mathrm{Adv}^{\textit{dist}}_{\mathsf{RP},\mathsf{RF}}(\mathcal{A}) \leq O\left(\frac{q^3}{2^n}\right)$.

Proposition 2 (q$\widetilde{\mathrm{PRP}}$/qPRF switching lemma [13] Proposition 4). *Let $\mathcal{A}$ be an adversary making at most q quantum queries to a random tweakable permutation $\widetilde{\mathsf{RP}}$ or a random function RF from $\{0,1\}^t \times \{0,1\}^n$ to $\{0,1\}^n$. Then* $\mathrm{Adv}^{dist}_{\widetilde{\mathsf{RP}},\mathsf{RF}}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^6}{2^n}}\right)$.

Note that the bound in Proposition 2 is not expected to be tight [13].

2.3 Proof Techniques

Recording standard oracle with errors (RstOE for short) [13] is proposed by Hosoyamada and Iwata and based on Zhandry's compressed oracle technique [33], which can approximately record transcripts of quantum queries of random oracles.

In the classical setting, some proof techniques require the simulator to remember the queries that the adversary has made. However, in the quantum setting, recording a query is equivalent (from the adversary's point of view) to measuring the query, which will disturb the quantum system and could be detectable by the adversary. Thus, we cannot make quantum queries to oracles and record transcripts directly. Zhandry's compressed oracle technique solves this problem by concentrating on the Fourier domain: by doing queries in the Fourier basis, the data will be written to the oracle's registers, instead of adding data from the oracle's registers to the adversary's registers. So, the simulator will get some information about the adversary's queries. For the superposition of oracles, first look at the Fourier domain, query, and compress, then revert back to the Primal domain. This process is roughly analogous to classical on-the-fly simulation. Recording standard oracle with errors is similar to Zhandry's technique with no compressed step, it uses the Hadamard transform $H^{\otimes n}|u\rangle = \frac{1}{2^{n/2}}\sum_x (-1)^{u\cdot x}|x\rangle$ to transform quantum states into the Fourier domain. It enables us to record transcripts of queries made to random functions with some errors. We first introduce some definitions.

Definition 1 (Standard oracle). *Let $x \in \{0,1\}^m, y \in \{0,1\}^n$. Let $S : \{0,1\}^m \to \{0,1\}^n$ be represented as its truth table $S = (b_0||s_0)||(b_1||s_1)||\cdots(b_{2^m-1}||s_{2^m-1})$, where $b_i \in \{0,1\}$ and $s_i \in \{0,1\}^n$ for $i \in \{0,1\}^m$. b_is are the flag bits. Then the standard oracle* stO *is defined by:*

$$\mathsf{stO} : |x\rangle|y\rangle|S\rangle \mapsto |x\rangle|y \oplus s_x\rangle|S\rangle.$$

Definition 2 (Recording Standard Oracle with Errors [13]). $\mathsf{IH}, \mathsf{CH}, U_{toggle}$ *are unitary operators act on $(n+1)2^m$-qubit states. Let $CH^{\otimes n} := |1\rangle\langle 1| \otimes H^{\otimes n} + |0\rangle\langle 0| \otimes I_n$ is the controlled n-qubit Hadamard operator. $X|b\rangle = |b \oplus 1\rangle$ is a "NOT" operator. And*

$$\mathsf{IH} := \left(I_1 \otimes H^{\otimes n}\right)^{\otimes 2^m}, \mathsf{CH} := \left(CH^{\otimes n}\right)^{\otimes 2^m}, \text{ and}$$
$$U_{toggle} := \left(I_1 \otimes |0^n\rangle\langle 0^n| + X \otimes (I_n - |0^n\rangle\langle 0^n|)\right)^{\otimes 2^m}.$$

Let $U_{enc} := \mathsf{CH} \cdot U_{toggle} \cdot \mathsf{IH}$. Then U_{enc} and its conjugate U^*_{enc} are called encoding and decoding, respectively. The recording standard oracle with errors RstOE *is a stateful quantum oracle with $(n+1)2^m$-qubit states and* $\mathsf{RstOE} := (I \otimes U_{enc}) \cdot \mathsf{stO} \cdot (I \otimes U^*_{enc})$.

Data will be written from the adversary's registers to the oracle's registers when doing queries in the Fourier basis. Databases will store information about adversary's queries. Here we show the definition of database D.

Definition 3 (Database D [13]). *Let D be a string $(b_0||d_0)||\cdots||(b_{2^m-1}||d_{2^m-1})$ with $(n+1)2^m$-bit. D is a valid database if there is no x such that $d_x \neq 0^n \wedge b_x = 0$. D is an invalid database otherwise. For a valid database D, we write $D(x) = y$ to denote $b_x = 1$ and $d_x = y$, and $D(x) = \perp$ to denote $b_x = 0$. For $\alpha \neq \perp$ and $x \neq x'$, if two different valid databases $D \neq D'$ satisfy $D(x) = \perp \wedge D'(x) = \alpha$ and $D(x') = D'(x')$, then $D' = D \cup (x, \alpha)$ and $D = D' \backslash (x, \alpha)$.*

Let $\mathcal{A}$ be a quantum algorithm, let $|\psi_i\rangle$ be the quantum state before the i-th query, let $|\psi_{q+1}\rangle$ be the quantum state after all unitary processes. Then we have the following proposition.

Proposition 3 (Proposition 1 in [13]). *For $i \geq 1$, if we measure the oracle states' register of $|\psi_{i+1}\rangle$ and obtained a database D, then D is valid and contains at most i entries.*

The core technical properties of RstOE technique are as follows, it realizes on-the-fly in quantum with some errors, where case 1 in Proposition 4 describes the data x that was asked again, and case 2 in Proposition 4 describes the first query for x.

Proposition 4 (Proposition 1 in [10] and [11]). *. Let D be a valid database and $D(x) = \perp$. Then, the following properties hold.*

1. $\mathsf{RstOE}|x, y\rangle \otimes |D \cup (x, \alpha)\rangle = |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle + |\epsilon_1\rangle$, *where* $\||\epsilon_1\rangle\| \leq 5\sqrt{2^n}$. *More precisely,*

$$
\begin{aligned}
|\epsilon_1\rangle = & \frac{1}{\sqrt{2^n}}|x, y \oplus \alpha\rangle(|D\rangle - (\sum_{\gamma \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}|D \cup (x, \gamma)\rangle))) \\
& - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}}|x, y \oplus \gamma\rangle \otimes (|D \cup (x, \gamma)\rangle - |D_\gamma^{\mathit{invalid}}\rangle) \\
& + \frac{1}{2^n}|x\rangle|\widehat{0^n}\rangle \otimes (2 \sum_{\delta \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}|D \cup (x, \delta)\rangle - |D\rangle),
\end{aligned}
$$

where $|\widehat{0^n}\rangle := H^{\otimes n}|0^n\rangle$ *and* $\left|D_\gamma^{\mathsf{invalid}}\right\rangle$ *is a superposition of invalid databases that depend on* γ *defined by* $|D_\gamma^{\mathsf{invalid}}\rangle := \sum_{\delta \neq 0^n} \frac{(-1)^{\gamma \cdot \delta}}{\sqrt{2^n}}|D \cup (x, \gamma)\rangle$.

2. $\mathsf{RstOE}|x, y\rangle \otimes |D\rangle = \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}|x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle + |\epsilon_2\rangle$, *where* $\||\epsilon_2\rangle\| \leq 2\sqrt{2^n}$. *More precisely, let* $|\widehat{0^n}\rangle := H^{\otimes n}|0^n\rangle$, *we have*

$$
|\epsilon_2\rangle = \frac{1}{\sqrt{2^n}}|x\rangle|\widehat{0^n}\rangle \otimes (|D\rangle - \sum_{\gamma \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}|D \cup (x, \gamma)\rangle).
$$

Let $f_0, ..., f_l$ be random functions. F is a function with the ability to access $f_0, ..., f_l$ in a black-box manner. We denote O_F as the quantum oracle of F. Let D_i be the database of $f_i, i = 0, ...l$ and we write $\mathbb{D}_F = (D_0, ..., D_l)$ as the combined database of F. Correspondingly, we define O_G (G is a function with the ability to access random functions $g_0, ..., g_s$) and $\mathbb{D}_G = (D_0, ..., D_s)$.

Definition 4 (Good and bad (combined) database of Oracle [13]). *Valid databases can be divided into good databases and bad databases, which correspond to good and bad transcripts in classical. For two oracles O_F and O_G, a one-to-one correspondence between good databases of O_F and O_G is expected. In this way, we can write the good database of O_G as $[\mathbb{D}_F]_G$ when the good database of O_F is $\mathbb{D}_F$. Or write the good database of O_F as $[\mathbb{D}_G]_F$ when the good database of O_G is $\mathbb{D}_G$.*

2.4 Quantum algorithms

Simon's problem [30]: Given a Boolean function $f : \{0,1\}^n \to \{0,1\}^m$, $x, y \in \{0,1\}^n$. x, y satisfied the condition $[f(x) = f(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}]$, s is non-zero and $s \in \{0,1\}^n$, the goal is to find s.
Simon's Algorithm [30] is a quantum algorithm to recover the period of the periodic function f in Simon's problem with polynomial queries. Here we show the step:

1. Initialize the state of $n+m$ qubits to $|0\rangle^{\otimes n}|0\rangle^{\otimes m}$;
2. Apply Hadamard transformation $H^{\otimes n}$ to the first n qubits to obtain quantum superposition $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle^{\otimes m}$;
3. Make a quantum query to the function f and get the state: $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$;
4. Measure the last m qubits to get the output z of $f(x)$, and the first n qubits collapse to $\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)$;
5. Apply Hadamard transform to the first n qubits, we have $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{y\cdot z}(1+(-1)^{y\cdot s})|y\rangle$. If $y \cdot s = 1$ then the amplitude of $|y\rangle$ is 0. So measuring the state in the computational basis yields a random vector y such that $y \cdot s = 0$, which means that y must be orthogonal to s.

By repeating this step $O(n)$ times, $n-1$ independent vectors y orthogonal to s can be obtained with high probability, then we can recover s by using linear algebra.
The Search problem: Consider a Boolean function $f : \{0,1\}^n \to \{0,1\}$ that partitions set $\{0,1\}^n$ between its good and bad elements, where x is good if $f(x) = 1$ and bad otherwise. Find a good element x_{good} that $f(x_{good}) = 1$.

If there is only one good element x_{good}, the problem could be solved using Grover's Algorithm.
Grover's Algorithm [8] is a quantum algorithm to find the marked element x_{good} from $\{0,1\}^n$ with $O(2^{n/2})$ quantum queries. Here we show the step:

1. Initializing a n-bit register $|0\rangle^{\otimes n}$;
2. Apply Hadamard transformation $H^{\otimes n}$ to the first register to obtain quantum superposition $H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle = \frac{1}{\sqrt{2^n}}|x_{good}\rangle + \sqrt{\frac{2^n-1}{2^n}}|x_{bad}\rangle = |\varphi\rangle$;
3. Construct an Oracle $O : |x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$, if x is the correct state then $f(x) = 1$, otherwise $f(x) = 0$;
4. Apply Grover iteration for $R \approx \frac{\pi}{4}\sqrt{2^n}$ times: $[(2|\varphi\rangle\langle\varphi| - I)O]^R|\varphi\rangle \approx |x_{good}\rangle$;
5. Return x_{good}.

Brassard et. al. [5] generalized Grover's algorithm and proposed the quantum amplitude amplification to solve a more general quantum search problem. Assume that for a random x, the probability of $f(x) = 1$ is p, then the quantum amplitude amplification could find a good solution after several iterations that is proportional to $\frac{1}{\sqrt{p}}$ in the worst case.

Quantum Amplitude Amplification [5], abbreviated QAA in this paper, is a generalization of Grover search which allows to increase the success probability of any measurement-free quantum algorithm by iterating it. Let $\mathcal{A}$ be a quantum circuit such that

$$\mathcal{A}|0\rangle = (\sum_{x\in G} \alpha_x|x\rangle)|0\rangle + (\sum_{x\in B} \beta_x|x\rangle)|1\rangle = \sqrt{p}\,|\psi_G\rangle + \sqrt{1-p}\,|\psi_B\rangle\,,$$

where p is the success probability of $\mathcal{A}$ (real and positive); $|\psi_G\rangle$ is a superposition (not necessarily uniform) of good outcomes (the set G) and $|\psi_B\rangle$ of bad outcomes (the set B), marked by their respective flags 1 and 0. Let O_0 be the inversion around zero operator that flips the phase of the basis vector $|0\rangle$: it does $O_0|y\rangle = -1|y\rangle$ if and only if $y = 0$; and O be the operator that flips the phase of all basis vectors $|x, b\rangle$ such that $b = 1$. The QAA computes a sequence of states $|\psi_i\rangle$ defined by the following iterative process (we denote $\mathcal{A}^\dagger$ as the inverse of $\mathcal{A}$):

1. $|\psi_0\rangle = \mathcal{A}|0\rangle$;
2. for $i = 1$ to m : $|\psi_{i+1}\rangle = \mathcal{A}O_0\mathcal{A}^\dagger O\,|\psi_i\rangle$.

Let $\theta = \arcsin(\sqrt{p})$, then we have $|\psi_0\rangle = \sin(\theta)\,|\psi_G\rangle + \cos(\theta)\,|\psi_B\rangle$, and $|\psi_i\rangle = \sin((2i+1)\theta)\,|\psi_G\rangle + \cos((2i+1)\theta)\,|\psi_B\rangle$. If we measure the state $|\psi_i\rangle$, we could get a good state x_{good} with probability $\sin^2((2i+1)\theta)$. Thus, after $t = \lfloor \frac{\pi}{4} \times \frac{1}{\sqrt{p}} \rfloor$ times iterations of QAA ($p = \theta$ when p is small, $\lfloor\cdot\rfloor$ is the floor function), the probability of success is almost 1.

Grover-meet-Simon Algorithm [21] is a quantum combined algorithm, it uses Grover's algorithm to search the marked element, by running many independent Simon's algorithms to check whether the function is periodic or not, and recover both the marked element and period in the end.

In addition, there is a single-collision quantum algorithm Ambainis's Theorem, which gives the bound on quantum single-collision.

Ambainis's Theorem (Theorem 3 in [1]) Let $f : \mathcal{X} \to \mathcal{Y}$ be a function, where $\mathcal{X}$, $\mathcal{Y}$ be finite sets. Then there exists a quantum algorithm that judges if distinct elements $x_1, x_2 \in \mathcal{X}$ exist such that $f(x_1) = f(x_2)$ with probability at least $1-\epsilon$ with bounded error $\epsilon < 1/2$ by making $O\left(|\mathcal{X}|^{2/3}\right)$ quantum queries to f.

3 Tight Quantum Security of $\mathsf{TNT}[f_0, f_1, f_2]$

3.1 Main Results

TNT built on three independent random functions $f_0, f_1, f_2 : \{0,1\}^n \to \{0,1\}^n$ is defined as

$$\mathsf{TNT}[f_0, f_1, f_2](M, T) = f_2(T \oplus f_1(T \oplus f_0(M))),$$

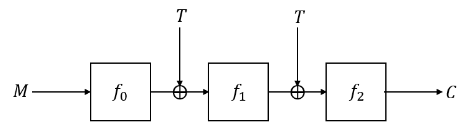

Fig. 1. The $\mathsf{TNT}[f_0, f_1, f_2]$ structure.

where $M, T \in \{0,1\}^n$. Figure 1 shows the $\mathsf{TNT}[f_0, f_1, f_2]$ structure.

Theorem 1 (Section 3.2). *Let $\mathcal{A}$ be a quantum adversary that makes at most q quantum queries. Then we have* $\mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[f_0,f_1,f_2]}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^3}{2^n}}\right)$.

Theorem 2 (Section 3.3). *There exists a quantum adversary $\mathcal{A}$ making $O(2^{n/3})$ quantum queries such that* $\mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[f_0,f_1,f_2]}(\mathcal{A}) = \frac{2}{125}$.

3.2 qPRF Security Proofs for $\mathsf{TNT}[f_0, f_1, f_2]$

In Asiacrypt 2019, Hosoyamada and Iwata [10] prove the qPRF security for 4-round Feistel structure by using the RstOE technique, which is excellent for proving quantum security with more precise bounds. Here, we apply this technique to prove the security bound for $\mathsf{TNT}[f_0, f_1, f_2]$.

To prove the qPRF security of $\mathsf{TNT}[f_0, f_1, f_2]$, that is, to prove that $\mathsf{TNT}[f_0, f_1, f_2]$ is indistinguishable from RF. For convenience, we denote $\mathsf{TNT}[f_0, f_1, f_2]$ as TNT_s, then $\mathsf{TNT}_s(M,T) = f_2(T \oplus f_1(T \oplus f_0(M)))$. Now let $f_2' : \{0,1\}^{3n} \to \{0,1\}^n$ be a random function, we define $\mathsf{TNT}_b(M,T) = f_2'(M, T, T \oplus f_1(T \oplus f_0(M)))$. Then $\mathsf{TNT}_b(M,T)$ is indistinguishable from a random function because if one of the inputs of $\mathsf{TNT}_b(M,T)$, M and T, changes, the inputs of f_2' must change, which guarantees the randomness of $\mathsf{TNT}_b(M,T)$.

In this way, we transform the qPRF security proof for $\mathsf{TNT}[f_0, f_1, f_2]$ into an indistinguishability proof for TNT_s and TNT_b. To facilitate the subsequent proof, we define the intermediate state $M_1 = f_0(M) \oplus T$ and $M_2 = f_1(M_1) \oplus T$. Then $\mathsf{TNT}_s(M,T) = f_2(M_2)$ and $\mathsf{TNT}_b(M,T) = f_2'(M, T, M_2)$.

In the following, we use the RstOE technique to prove the indistinguishability of TNT_s and TNT_b. Before the formal proofs begin, we first show the quantum oracles and quantum implementations of TNT_s and TNT_b, which help us to understand the quantum encryption process.

Quantum oracle of $\mathsf{TNT}[f_0, f_1, f_2]$. We define the unitary operators $O_i, i = 0, 1, 2$ and O_2' as follows.

$$
\begin{aligned}
O_0 :& |M,T\rangle|y\rangle \mapsto |M,T\rangle|y \oplus M_1\rangle, \\
O_1 :& |M,T\rangle|M_1\rangle|y\rangle \mapsto |M,T\rangle|M_1\rangle|y \oplus M_2\rangle, \\
O_2 :& |M,T\rangle|M_1\rangle|M_2\rangle|y\rangle \mapsto |M,T\rangle|M_1\rangle|M_2\rangle|y \oplus f_2(M_2)\rangle, \\
O_2' :& |M,T\rangle|M_1\rangle|M_2\rangle|y\rangle \mapsto |M,T\rangle|M_1\rangle|M_2\rangle|y \oplus f_2'(M,T,M_2)\rangle.
\end{aligned}
$$

Quantum implementations of TNT_s (TNT_b) .

1. Take $|M, T\rangle$ as an input.
2. Query $|M, T\rangle|0^n\rangle$ to O_0 to obtain the state ($|Y\rangle$ is the register to which the answer from the oracle will be added)

$$|M, T\rangle|Y\rangle \otimes |M_1\rangle \, . \tag{1}$$

3. Query $|M, T\rangle|M_1\rangle|0^n\rangle$ to O_1 to obtain the state

$$|M, T\rangle|Y\rangle \otimes |M_1\rangle \otimes |M_2\rangle. \tag{2}$$

4. Query $|M, T\rangle|M_1\rangle|M_2\rangle|Y\rangle$ to O_2 (O_2') to obtain the state

$$|M, T\rangle|Y \oplus \mathsf{TNT}_s(M, T)\rangle \otimes |M_1\rangle \otimes |M_2\rangle. \tag{3}$$

$$(|M, T\rangle|Y \oplus \mathsf{TNT}_b(M, T)\rangle \otimes |M_1\rangle \otimes |M_2\rangle.) \tag{4}$$

5. Uncompute Steps $2 - 4$ to obtain

$$|M, T\rangle|Y \oplus \mathsf{TNT}_s(M, T)\rangle. \tag{5}$$

$$(|M, T\rangle|Y \oplus \mathsf{TNT}_b(M, T)\rangle.) \tag{6}$$

From (1) to (6) we have

$$O_{\mathsf{TNT}_s} = O_0^* \cdot O_1^* \cdot O_2 \cdot O_1 \cdot O_0,$$
$$O_{\mathsf{TNT}_b} = O_0^* \cdot O_1^* \cdot O_2' \cdot O_1 \cdot O_0.$$

Proof ideas Valid databases consist of good databases and bad databases. For O_{TNT_s} and O_{TNT_b}, the behavior of good databases for O_{TNT_s} should be the same as good databases for O_{TNT_b} such that the adversary cannot distinguish O_{TNT_s} and O_{TNT_b} in the presence of good databases. In this way, the distinguishing advantage is determined by the bad databases.

In addition, there is another situation that we must consider: when performing queries, a good database may become a bad database. Thus, the bad databases in the ith query consist of two parts: databases that were bad before the $(i-1)$th query, and databases that went from good to bad at the $(i-1)$th query. The fact that there are no bad databases in the initial state ($i = 0$). Thus, the core of our proof actually lies in proving that each query of good databases going bad has very little effect on the adversary's ability to distinguish.

Let D_0, D_1, D_2 and D_2' be (valid) databases for f_0, f_1, f_2 and f_2', respectively. If $D_i(x) = y$, we write $(x, y) \in D_i, i = 0, 1, 2$ and if $D_2'(x_1, x_2, x_3) = y$, we write $(x_1||x_2||x_3, y) \in D_2'$. We define the combined database of TNT_s as $\mathbb{D}_s = (D_0, D_1, D_2)$ and TNT_b as $\mathbb{D}_b = (D_0, D_1, D_2')$.

Good and bad database of TNT_s and TNT_b. For $(W_0, Z_0) \in D_0$, $(Z_0 \oplus W_1, Z_1) \in D_1$, $(V, C) \in D_2$, $(W_0||W_1||V, C) \in D_2'$, let $\varepsilon = (W_0, W_1, Z_0, Z_1, V, C)$. We say $\mathbb{D}_s$ ($\mathbb{D}_b$) is good if and only if: For every $(V, C) \in D_2((W_0||W_1||V, C) \in D_2')$, there exists a unique $\varepsilon = (W_0, W_1, Z_0, Z_1, V, C)$ with $V = Z_1 \oplus W_1$ such that $(W_0, Z_0) \in D_0$ and $(Z_0 \oplus W_1, Z_1) \in D_1$. $\mathbb{D}_s$ ($\mathbb{D}_b$) is bad when it is not good. Simply put, just as in classical, V does not collide in good databases (One V can only correspond to one (W_0, W_1)).

Now, if $\mathbb{D}_b$ is a good database, then for $(W_0||W_1||V,C) \in D_2'$ there is a unique $\varepsilon = (W_0, W_1, Z_0, Z_1, V, C)$ with $V = Z_1 \oplus W_1$. This means that for inputs (W_0, W_1) of queries to TNT_b, V does not collide. So, for such inputs (W_0, W_1) of queries to TNT_s, V does not collide, too. Thus, for such $(V,C) \in D_2$, there is a unique $\varepsilon = (W_0, W_1, Z_0, Z_1, V, C)$ with $V = Z_1 \oplus W_1$ and $\mathbb{D}_s$ is a good database or vice versa. So, there is a one-to-one correspondence between good databases of TNT_s and TNT_b. For D_2' for f_2' and $(W_0||W_1||V,C) \in D_2'$, we write $[D_2']_2$ as the database for f_2 and $(V,C) \in [D_2']_2$. (Or we can also write $[D_2]_2'$ as the database for f_2' and $(W_0||W_1||V,C) \in [D_2]_2'$ when D_2 for f_2 and $(V,C) \in D_2$.) And for $\mathbb{D}_b$ for $\mathsf{TNT}_b = (D_0, D_1, D_2')$, we write $[\mathbb{D}_b]_s = [D_0, D_1, D_2']_2$ as the database for TNT_s. (Or for $\mathbb{D}_s$, we write $[\mathbb{D}_s]_b = [D_0, D_1, D_2]_2'$ as the database for TNT_b.) Then the mapping $\mathbb{D}_b \mapsto [\mathbb{D}_b]_s$ ($\mathbb{D}_s \mapsto [\mathbb{D}_s]_b$) gives a one-to-one correspondence between good databases for TNT_b and those for TNT_s: We take $\mathbb{D}_s$ as an example and the opposite direction similarly. For a (combined) good database $\mathbb{D}_s$ for TNT_s, let $[\mathbb{D}_s]_b$ be the database for f_2' such that $(W_0||W_1||V,C) \in [D_2]_2'$ if and only if $(V,C) \in D_2$ and $(W_0, W_1, Z_0, Z_1, V, C)$ is unique with $V = Z_1 \oplus W_1$ for some Z_1. Then the (combined) database $[\mathbb{D}_s]_b = (D_0, D_1, [D_2]_2')$ is a good database for TNT_b, and vice versa.

Indistinguishability proof for TNT_s and TNT_b. Let $\mathcal{A}$ be a quantum adversary that makes at most q quantum queries. Let $|\psi_i\rangle$ and $|\psi_i'\rangle$ denote the whole quantum states of $\mathcal{A}$ and the oracle just before the i-th query when $\mathcal{A}$ runs relative to TNT_s and TNT_b, respectively. Let $(M,T), Y$, and Z correspond to $\mathcal{A}$'s register to send queries to oracles, register to receive answers from oracles, and register for offline computation, respectively.

For each $1 \le i \le q+1$, since oracle's databases can be divided into good databases and bad databases, the corresponding whole quantum states of $\mathcal{A}$ and the oracle $|\psi_i\rangle$ and $|\psi_i'\rangle$ can also be divided into good parts and bad parts. We write $|\psi_i'\rangle = |\psi_i'^{\mathsf{good}}\rangle + |\psi_i'^{\mathsf{bad}}\rangle$ and $|\psi_i\rangle = |\psi_i^{\mathsf{good}}\rangle + |\psi_i^{\mathsf{bad}}\rangle$. Since there is a one-to-one correspondence between good databases of TNT_s and TNT_b, we write $|\psi_i^{\mathsf{good}}\rangle$ and $|\psi_i'^{\mathsf{good}}\rangle$ in the following form:

$$|\psi_i'^{\,\text{good}}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid and good}}} a^{(i)}_{M,T,Y,Z,(D_0,D_1,D_2')} |M,T\rangle|Y\rangle|Z\rangle \otimes |D_0, D_1, D_2'\rangle\,, \tag{7}$$

and

$$|\psi_i^{\text{good}}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{:valid and good}}} a^{(i)}_{M,T,Y,Z,(D_0,D_1,D_2')} |M,T\rangle|Y\rangle|Z\rangle \otimes |[D_0, D_1, D_2']_2\rangle\,, \tag{8}$$

where $a^{(i)}_{M,T,Y,Z,(D_0,D_1,D_2')}$ is complex number and for each database (D_0, D_1, D_2') in $|\psi_i'^{\mathsf{good}}\rangle$ (resp., (D_0, D_1, D_2) in $|\psi_i^{\mathsf{good}}\rangle$) with non-zero quantum amplitude, $|D_i| \le 2(i-1), 1 \le i \le 2$, and $|D_2'| \le i-1$ (resp., $|D_2| \le i-1$).

Next, as we mentioned in the proof idea, bad databases at the ith query consist of two parts: databases that were bad before the $(i-1)$th query, and databases that changed from good to bad at the $(i-1)$th query. And the effect of bad databases on an adversary's ability to distinguish is an important question. Proposition 3 in [13] gives a generalized conclusion of this question, which we specify for TNT_s and TNT_b.

Proposition 5 (Proposition 3 in [13]). *Suppose that there exist vectors* $|\psi_i'^{good}\rangle$, $|\psi_i'^{bad}\rangle$, $|\psi_i^{good}\rangle$ *and* $|\psi_i^{bad}\rangle$ *that satisfy* $|\psi_i'\rangle = |\psi_i'^{\mathsf{good}}\rangle + |\psi_i'^{\mathsf{bad}}\rangle$ *and* $|\psi_i\rangle = |\psi_i^{\mathsf{good}}\rangle + |\psi_i^{\mathsf{bad}}\rangle$, $|\psi_i'^{\mathsf{good}}\rangle$ *and* $|\psi_i^{\mathsf{good}}\rangle$ *satisfy equation (7) and (8),* $\||\psi_i'^{\mathsf{bad}}\rangle\| \leq \||\psi_{i-1}'^{\mathsf{bad}}\rangle\| + \epsilon_i'^{bad}$ *and* $\||\psi_i^{\mathsf{bad}}\rangle\| \leq \||\psi_{i-1}^{\mathsf{bad}}\rangle\| + \epsilon_i^{bad}$. *Then,*

$$\mathrm{Adv}^{\mathrm{dist}}_{\mathsf{TNT}_s,\mathsf{TNT}_b}(\mathcal{A}) \leq \sum_{1\leq i\leq q} \epsilon_i^{bad} + \sum_{1\leq i\leq q} \epsilon_i'^{bad}.$$

Return to our proof. The core of qPRF security proofs for $\mathsf{TNT}[f_0, f_1, f_2]$ is the indistinguishability of TNT_s and TNT_b, and by Proposition 5 the core of the distinction between TNT_s and TNT_b lies in $\||\psi_i'^{\mathsf{bad}}\rangle\|$ and $\||\psi_i^{\mathsf{bad}}\rangle\|$. More precisely, it depends on $\epsilon_i'^{\mathsf{bad}}$ and $\epsilon_i^{\mathsf{bad}}$.

In Proposition 6 we show $\||\psi_i'^{\mathsf{bad}}\rangle\|$ and $\||\psi_i^{\mathsf{bad}}\rangle\|$ of TNT_b and TNT_s.

Proposition 6 (Core proposition). *For* $|\psi_i'^{\mathsf{bad}}\rangle$ *and* $|\psi_i^{\mathsf{bad}}\rangle$ *of* TNT_b *and* TNT_s*, we have*

$$\||\psi_i'^{\mathsf{bad}}\rangle\| \leq \||\psi_{i-1}'^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right), \||\psi_i^{\mathsf{bad}}\rangle\| \leq \||\psi_{i-1}^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right).$$

Proof. From (1) to (6) we have $O_{\mathsf{TNT}_s} = O_0^* \cdot O_1^* \cdot O_2 \cdot O_1 \cdot O_0$ and $O_{\mathsf{TNT}_b} = O_0^* \cdot O_1^* \cdot O_2' \cdot O_1 \cdot O_0$. Therefore, when we do a new query, what we are actually looking at is the bad parts of quantum states $O_0^* \cdot O_1^* \cdot O_2' \cdot O_1 \cdot O_0|\psi_i'\rangle$ and $O_0^* \cdot O_1^* \cdot O_2 \cdot O_1 \cdot O_0|\psi_i\rangle$. So we will start with $|\psi_i'\rangle$ (and $|\psi_i\rangle$) and go step by step to calculate $O_0|\psi_i'\rangle$, $O_1 \cdot O_0|\psi_i'\rangle$, $O_2' \cdot O_1 \cdot O_0|\psi_i'\rangle$, $O_1^* \cdot O_2' \cdot O_1 \cdot O_0|\psi_i'\rangle$ and $O_0^* \cdot O_1^* \cdot O_2' \cdot O_1 \cdot O_0|\psi_i'\rangle$ ($|\psi_i\rangle$ ditto). For completeness, we provide concrete computations in Appendix A.

Proof (proof of Theorem 1). From Proposition 5 we have

$$\begin{aligned}\mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[f_0,f_1,f_2]}(\mathcal{A}) &= \mathrm{Adv}^{\mathsf{dist}}_{\mathsf{TNT}_s,\mathsf{TNT}_b}(\mathcal{A}) \\ &\leq \sum_{1\leq i\leq q} O\left(\sqrt{\frac{i}{2^n}}\right) + \sum_{1\leq i\leq q} O\left(\sqrt{\frac{i}{2^n}}\right) \leq O\left(\sqrt{\frac{q^3}{2^n}}\right).\end{aligned}$$

Applying qPRP/qPRF switching lemma, we can also prove the qPRF security of $\mathsf{TNT}[\pi_0, \pi_1, \pi_2]$.

Theorem 3. *Let $\mathcal{A}$ be a quantum adversary makes at most q quantum queries. Then we have* $\mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[\pi_0,\pi_1,\pi_2]}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^3}{2^n}}\right) + O\left(\frac{q^3}{2^n}\right)$*, where π_0, π_1 and π_2 are independent random permutations.*

Proof. From Proposition 1 and Theorem 1, there exists quantum adversaries $\mathcal{B}_i, i = 0, 1, 2$ and $\mathcal{C}$ such that

$$\mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[\pi_0,\pi_1,\pi_2]}(\mathcal{A}) = \sum_{0\leq i\leq 2} \mathrm{Adv}^{\mathsf{dist}}_{\pi_i,f_i}(\mathcal{B}_i) + \mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[f_0,f_1,f_2]}(\mathcal{C}) \leq O(\sqrt{\frac{q^3}{2^n}}) + O(\frac{q^3}{2^n}).$$

3.3 qPRF Attack for $\mathsf{TNT}[f_0, f_1, f_2]$

For $\mathsf{TNT}[f_0, f_1, f_2](M,T) = f_2(T \oplus f_1(T \oplus f_0(M)))$, let $M = x, T = 0$, then we have $\mathsf{TNT}[f_0, f_1, f_2](x, 0) = f_2(f_1(f_0(x)))$, where f_0, f_1, f_2 are independent random functions. Further, we can simplify the qPRF attack on $\mathsf{TNT}[f_0, f_1, f_2]$ as a qPRF attack on $f_2 \circ f_1 \circ f_0$. In the full version of [10], Hosoyamada and Iwata performed a qPRF attack on RF $\circ$ RF (Lemma 3 in [11]), which gave us the inspiration. Along the same lines as in [11], we also consider Ambainis's Theorem. Before proving Theorem 2, we first prove the following proposition.

Proposition 7. *Let $f_2 \circ f_1 \circ f_0$ be the composition of three independent random functions $f_2, f_1, f_0 : \{0,1\}^n \to \{0,1\}^n$. There exists a quantum adversary $\mathcal{A}$ that makes $O(2^{n/3})$ quantum queries, such that* $\mathrm{Adv}^{\mathsf{qPRF}}_{f_2\circ f_1\circ f_0}(\mathcal{A}) = \frac{2}{125}$.

Proof. Let $f : \{0,1\}^n \to \{0,1\}^n$ is an independent random function. For $1 \le N \le 2^n$, let the subset $\{0, 1, \ldots, N-1\}$ as $[N]$. To use Ambainis's Theorem, let quantum algorithm $\mathcal{D}_N^f$ with $O\left(|N|^{2/3}\right)$ quantum queries and an error $\epsilon < 1/25$ and:

$$\mathcal{D}_N^f = \begin{cases} 1, \exists x_1, x_2 \in [N] \text{ s.t. } f(x_1) = f(x_2) \\ 0, \qquad\qquad \text{otherwise.} \end{cases}$$

Let $\mathrm{coll}^f_{[N]}$ denote that f has a collision in $[N]$ and let $p = \Pr_f\left[\neg\, \mathrm{coll}^f_{[N]}\right]$. In [11], equation (86) shows that $p = \prod_{j=1}^{N-1}\left(1 - \frac{j}{2^n}\right)$, and (87) shows that $\Pr_{f_0,f_1}\left[\neg\, \mathrm{coll}^{f_1\circ f_0}_{[N]}\right] = p^2$. Then we have

$$\begin{aligned} \Pr_{f_0,f_1,f_2}\left[\neg\, \mathrm{coll}^{f_2\circ f_1\circ f_0}_{[N]}\right] =& \Pr_{f_0,f_1,f_2}\left[\neg\, \mathrm{coll}^{f_2}_{f_1\circ f_0([N])} \mid \neg\, \mathrm{coll}^{f_1\circ f_0}_{[N]}\right] \cdot \Pr_{f_0,f_1}\left[\neg\, \mathrm{coll}^{f_1\circ f_0}_{[N]}\right] \\ =& p^3. \end{aligned}$$

And with the error $\epsilon < 1/25$ we have

$$\begin{aligned} \mathrm{Adv}^{\mathsf{qPRF}}_{f_2\circ f_1\circ f_0}(\mathcal{D}_N) =& \left| \Pr_f\left[\mathcal{D}_N^f() \Rightarrow 1\right] - \Pr_{f_0,f_1,f_2}\left[\mathcal{D}_N^{f_2\circ f_1\circ f_0}() \Rightarrow 1\right] \right| \\ \ge& \left| \Pr_f\left[\mathrm{coll}^f_{[N]}\right] - \Pr_{f_0,f_1,f_2}\left[\mathrm{coll}^{f_2\circ f_1\circ f_0}_{[N]}\right] \right| - \frac{2}{25} \\ =& (1-p^3) - (1-p) - \frac{2}{25} = (p+p^2)(1-p) - \frac{2}{25}. \end{aligned}$$

The claim in [11] shows that there exist $N_0 = O\left(2^{n/2}\right)$ and $p_0 = \prod_{j=1}^{N_0-1}\left(1 - \frac{j}{2^n}\right)$, $\frac{1}{5} \le p_0 \le \frac{3}{5}$ holds for sufficiently large n. Here sufficiently large n means n satisfying $e^{-\frac{N_0(N_0-1)}{2\cdot 2^{n/2}}} \le 3/5$ where $N_0 = 2^{n/4}\sqrt{2\log 2}$. So there exists a parameter N_0 in $O\left(2^{n/2}\right)$, and $\frac{1}{5} \le p_0 \le \frac{3}{5}$ holds for sufficiently large n. And

$$\mathrm{Adv}^{\mathsf{qPRF}}_{f_2\circ f_1\circ f_0}(\mathcal{D}_{N_0}) \ge \left(\frac{1}{5} + \frac{1}{5^2}\right)\left(1 - \frac{3}{5}\right) - \frac{2}{25} = \frac{2}{125}.$$

By Ambainis' theorem, $\mathcal{D}_{N_0}$ makes at most $O((N_0)^{2/3}) = O((2^{n/2})^{2/3}) = O(2^{n/3})$ quantum queries. Then Proposition 7 is proved.

Proof. (Proof of Theorem 2) From Proposition 7, there exists a quantum adversary $\mathcal{A}$ that makes $O(2^{n/3})$ quantum queries, such that

$$\mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[f_0,f_1,f_2](x,0)}(\mathcal{A}) = \mathrm{Adv}^{\mathsf{qPRF}}_{f_2\circ f_1\circ f_0}(\mathcal{D}_{N_0}) = \frac{2}{125}.$$

4 Quantum Security of $\mathsf{TNT}[\pi_0, \pi_1, \pi_2]$

4.1 Main Results

TNT built on three random permutations π_0, π_1 and π_2 is defined as

$$\mathsf{TNT}[\pi_0, \pi_1, \pi_2](M, T) = \pi_2(T \oplus \pi_1(T \oplus \pi_0(M))).$$

Theorem 4 (Section 4.2). *Let $\mathcal{A}$ be a quantum algorithm that makes at most q quantum queries and $q \leq 2^{n/3}$. Then there exist a quantum algorithm $\mathcal{D}$ that make at most $O(q)$ quantum queries, such that*

$$\mathrm{Adv}^{\mathsf{q}\widetilde{\mathsf{PRP}}}_{\mathsf{TNT}[\pi_0,\pi_1,\pi_2]}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^3}{2^n}}\right) + \mathrm{Adv}^{dist}_{\widetilde{\mathsf{RP}},\mathsf{RF}}(\mathcal{D}).$$

Note. In fact, if we apply the q$\widetilde{\text{PRP}}$/qPRF switching lemma (Proposition 2), we will get $\mathrm{Adv}^{\mathsf{q}\widetilde{\mathsf{PRP}}}_{\mathsf{TNT}[\pi_0,\pi_1,\pi_2]}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^6}{2^n}}\right)$. But the bound of the switching lemma may not be tight [13], so we list it separately.

Theorem 5 (Quantum crossroad distinguisher on TNT, Section 4.3). *Let $M^0, M^1, T^0, T^1, x \in \{0,1\}^n$, let Q be either TNT or a tweakable random permutation. Assume that we have $\left(M^0, T^0\right)$ and $\left(M^1, T^1\right)$ such that $Q\left(M^0, T^0\right) = Q\left(M^1, T^1\right)$. Let*

$$f(x) = \begin{cases} 1, \text{ if } Q\left(M^0, x\right) = Q\left(M^1, x \oplus T^0 \oplus T^1\right) \text{ and } x \neq T^0; \\ 0, \text{ otherwise}. \end{cases}$$

Let $\mathcal{A}$ be a quantum algorithm such that $\mathcal{A}|0\rangle = \sqrt{p}\,|\psi_G\rangle + \sqrt{1-p}\,|\psi_B\rangle$, where G is the kernel of f and B is the support of f. We run QAA on f with $t = \lfloor \frac{\pi}{8} \times 2^{\frac{n}{2}} \rfloor$ iterations, then measure the state. If Q is TNT, then the probability of obtaining a good result is at least $0.8 - 2^{-\frac{n-5}{2}}$. If Q is a tweakable random permutation, then the probability of obtaining a good result is at most $\frac{1}{2}$.

Theorem 6 (Quantum Grover-meet-Simon attack on TNT, Section 4.4). *If $E_{K_i}, i = 0, 1, 2$ are block ciphers, the length of the key K_2 of E_{K_2} is k bits. We can give a quantum Grover-meet-Simon attack on $\mathsf{TNT}[E_{K_0}, E_{K_1}, E_{K_2}]$ with $O(n2^{k/2})$ queries.*

4.2 q$\widetilde{\text{PRP}}$ Security Proof for $\mathsf{TNT}[\pi_0, \pi_1, \pi_2]$

Proposition 8. *Let $\mathcal{A}$ be a quantum algorithm that makes at most q quantum queries. Then there exist quantum algorithms $\mathcal{C}, \mathcal{D}$ that make at most $O(q)$quantum queries, such that*

$$\mathrm{Adv}^{\mathsf{q}\widetilde{\mathsf{PRP}}}_{\mathsf{TNT}[\pi_0,\pi_1,\pi_2]}(\mathcal{A}) \leq \mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[f_0,f_1,f_2]}(\mathcal{C}) + \mathrm{Adv}^{\mathsf{dist}}_{\mathsf{RF},\widetilde{\mathsf{RP}}}(\mathcal{D}) + O\left(\frac{q^3}{2^n}\right).$$

Proof. First we change π_2 to f_2, from Proposition 1 we have

$$\mathrm{Adv}^{\mathsf{dist}}_{\mathsf{TNT}[\pi_0,\pi_1,\pi_2],\mathsf{TNT}_{[\pi_0,\pi_1,f_2]}}(\mathcal{A}) \leq O\left(\frac{q^3}{2^n}\right).$$

The same applies to $\mathrm{Adv}^{\mathsf{dist}}_{\mathsf{TNT}[\pi_0,\pi_1,f_2],\mathsf{TNT}[\pi_0,f_1,f_2]}(\mathcal{A})$ and $\mathrm{Adv}^{\mathsf{dist}}_{\mathsf{TNT}[\pi_0,f_1,f_2],\mathsf{TNT}[f_0,f_1,f_2]}(\mathcal{A})$. And we have $\mathrm{Adv}^{\mathsf{dist}}_{\mathsf{TNT}[f_0,f_1,f_2],\mathsf{RF}}(\mathcal{A}) = \mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[f_0,f_1,f_2]}(\mathcal{A})$. So

$$\mathrm{Adv}^{\mathsf{q}\widetilde{\mathsf{PRP}}}_{\mathsf{TNT}[\pi_0,\pi_1,\pi_2]}(\mathcal{A}) \leq \mathrm{Adv}^{\mathsf{qPRF}}_{\mathsf{TNT}[f_0,f_1,f_2]}(\mathcal{C}) + \mathrm{Adv}^{\mathsf{dist}}_{\mathsf{RF},\widetilde{\mathsf{RP}}}(\mathcal{D}) + O\left(\frac{q^3}{2^n}\right).$$

Proof. (Proof of Theorem 4) From Theorem 1 and Proposition 8, when $q \leq 2^{n/3}$ we have $\mathrm{Adv}^{\mathsf{q}\widetilde{\mathsf{PRP}}}_{\mathsf{TNT}[\pi_0,\pi_1,\pi_2]}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^3}{2^n}}\right) + \mathrm{Adv}^{\mathsf{dist}}_{\widetilde{\mathsf{RP}},\mathsf{RF}}(\mathcal{D})$.

4.3 Quantum Cross-Road Distinguisher on TNT

At Asiacrypt 2020, Guo et. al. [9] proposed a cross-road distinguisher on TNT in classical setting. Though their attack could not be converted to a quantum attack, we propose a quantum cross-road distinguisher utilizing the same property. Let Q be either TNT or a tweakable random permutation. For four pairs $(M^i, T^j) \in \{0,1\}^{2n}$, where $i \in \{0,1\}, j \in \{0,1,2,3\}$, $Q\left(M^0, T^0\right) = Q\left(M^1, T^1\right)$ and $Q\left(M^0, T^2\right) = Q\left(M^1, T^3\right)$ are independent if Q is a tweakable random permutation, and dependent otherwise.

Proposition 9. *Let $M^i, T^j \in \{0,1\}^n, i \in \{0,1\}, j \in \{0,1,2,3\}$, let Q be TNT. Assume that $\left(M^0, T^0\right)$ and $\left(M^1, T^1\right)$ satisfy $Q\left(M^0, T^0\right) = Q\left(M^1, T^1\right)$. There exist T^2 and $T^3 = T^2 \oplus (T^0 \oplus T^1)$ that satisfy $Q\left(M^0, T^2\right) = Q\left(M^1, T^3\right)$.*

Proof. If Q is TNT, for two randomly chosen pairs (M^0, T^0) and (M^1, T^1), there are another two pairs (M^0, T^2) and (M^1, T^3) that satisfy

$$\begin{aligned} T^2 &= \pi_0(M^0) \oplus \pi_0(M^1) \oplus T^1, \\ T^3 &= T^2 \oplus (T^0 \oplus T^1) = \pi_0(M^0) \oplus \pi_0(M^1) \oplus T^0. \end{aligned}$$

Then we have

$$\begin{aligned}
& Q(M^0, T^0) = Q(M^1, T^1) \\
\iff\ & \pi_2(T^0 \oplus \pi_1(T^0 \oplus \pi_0(M^0))) = \pi_2(T^1 \oplus \pi_1(T^1 \oplus \pi_0(M^1))) \\
\iff\ & T^0 \oplus \pi_1(T^0 \oplus \pi_0(M^0)) = T^1 \oplus \pi_1(T^1 \oplus \pi_0(M^1)) \\
\iff\ & T^0 \oplus \pi_1(T^3 \oplus \pi_0(M^0) \oplus \pi_0(M^1) \oplus \pi_0(M^0)) = \\
& T^1 \oplus \pi_1(T^2 \oplus \pi_0(M^0) \oplus \pi_0(M^1) \oplus \pi_0(M^1)) \\
\iff\ & T^3 \oplus \pi_1((T^3 \oplus \pi_0(M^1))) = T^2 \oplus \pi_1(T^2 \oplus \pi_0(M^0)) \\
\iff\ & \pi_2(T^3 \oplus \pi_1((T^3 \oplus \pi_0(M^1)))) = \pi_2(T^2 \oplus \pi_1(T^2 \oplus \pi_0(M^0))) \\
\iff\ & Q\left(M^1, T^3\right) = Q\left(M^0, T^2\right).
\end{aligned}$$

Thus, $Q(M^0, T^2) = Q(M^1, T^3)$ if and only if $Q(M^0, T^0) = Q(M^1, T^1)$. According to the above relation, for randomly chosen pairs (M^0, T^0) and (M^1, T^1), if $\left(M^0, T^0\right)$ and $\left(M^1, T^1\right)$ satisfy $Q\left(M^0, T^0\right) = Q\left(M^1, T^1\right)$, then for $T^2 = \pi_0(M^0) \oplus \pi_0(M^1) \oplus T^1$ and $T^3 = T^2 \oplus (T^0 \oplus T^1)$, $Q\left(M^0, T^2\right) = Q\left(M^1, T^3\right)$ is satisfied.

The quantum algorithm distinguishing TNT and a tweakable random permutation in Theorem 5 is based on proposition 9.

Proof. (Proof of Theorem 5) If Q is a tweakable random permutation, for a random x the probability that $f(x) = 1$ is 2^{-n}. Thus, for QAA on a tweakable random permutation, $\theta = 2^{-\frac{n}{2}}$, and

$$\begin{aligned}
|\psi_t\rangle &= \sin((2t+1)\theta) |\psi_G\rangle + \cos((2t+1)\theta) |\psi_B\rangle \\
&= \sin(\lfloor \frac{\pi}{4} \times 2^{\frac{n}{2}} - 1 \rfloor \times 2^{-\frac{n}{2}}) |\psi_G\rangle + \cos(\lfloor \frac{\pi}{4} \times 2^{\frac{n}{2}} - 1 \rfloor \times 2^{-\frac{n}{2}}) |\psi_B\rangle .
\end{aligned}$$

where $\sin(\lfloor \frac{\pi}{4} \times 2^{\frac{n}{2}} - 1 \rfloor \times 2^{-\frac{n}{2}}) \leq \sin(\frac{\pi}{4} \times 2^{\frac{n}{2}} \times 2^{-\frac{n}{2}}) = \sin(\frac{\pi}{4}) = \frac{\sqrt{2}}{2}$. Thus, the probability of getting a good result is at most $\frac{1}{2}$.

If Q is TNT then :

1. If $x = \pi_1(M^0) \oplus \pi_1(M^1) \oplus T^1$, then (proposition 9)
$$Q\left(M^0, x\right) = Q\left(M^1, x \oplus T^0 \oplus T^1\right);$$
2. If $x \neq \pi_1(M^0) \oplus \pi_1(M^1) \oplus T^1$, the probability that $f(x) = 1$ is 2^{-n}.

As a result, for a random x the probability that $f(x) = 1$ is 2^{-n+1}. Therefore $\theta = 2^{-\frac{n-1}{2}}$, and

$$\begin{aligned}
|\psi_t\rangle &= \sin((2t+1)\theta) |\psi_G\rangle + \cos((2t+1)\theta) |\psi_B\rangle \\
&= \sin(\lfloor \frac{\pi}{4} \times 2^{\frac{n}{2}} - 1 \rfloor \times 2^{-\frac{n-1}{2}}) |\psi_G\rangle + \cos(\lfloor \frac{\pi}{4} \times 2^{\frac{n}{2}} - 1 \rfloor \times 2^{-\frac{n-1}{2}}) |\psi_B\rangle .
\end{aligned}$$

Since the derivative of $\sin x$ is $(\sin x)' = \cos x$, and $0 < (\sin x)' < 1$ for $0 < x < \frac{\pi}{2}$, we have

$$\begin{aligned}
&\sin^2(\lfloor \frac{\pi}{4} \times 2^{\frac{n}{2}} - 1 \rfloor \times 2^{-\frac{n-1}{2}}) \geq \sin^2((\frac{\pi}{4} \times 2^{\frac{n}{2}} - 2) \times 2^{-\frac{n-1}{2}}) \\
&\geq (\sin(\frac{\pi}{4} \times \sqrt{2}) - 2^{-\frac{n-3}{2}})^2 > \sin^2(\frac{\pi}{4} \times \sqrt{2}) - 2 \times 2^{-\frac{n-3}{2}} > 0.8 - 2^{-\frac{n-5}{2}} .
\end{aligned}$$

Thus, the probability of getting a good result is at least $0.8 - 2^{-\frac{n-5}{2}}$.

4.4 Grover-meet-Simon attack on TNT

If E is a block cipher, K_0, K_1, K_2 are three independent keys and the length of the key is k bits. Let $M, T \in \{0,1\}^n, b \in \{0,1\}, x \in \{0,1\}^n, K \in \{0,1\}^k$ and α_0, α_1 be arbitrarily two different fixed numbers in $\{0,1\}^n$. Let $(M,T)=(\alpha_b,x)$ be the input of $\mathsf{TNT}[E_{K_0},E_{K_1},E_{K_2}]$. We construct a function g based on TNT:

$$\begin{aligned} g(K,x) =& E_K^{-1}(\mathsf{TNT}[E_{K_0},E_{K_1},E_{K_2}](\alpha_0,x))\oplus \\ & E_K^{-1}(\mathsf{TNT}[E_{K_0},E_{K_1},E_{K_2}](\alpha_1,x)). \end{aligned}$$

When $K = K_2$, we have $g(K_2,x) = E_{K_1}(x \oplus E_{K_0}(\alpha_0)) \oplus E_{K_1}(x \oplus E_{K_0}(\alpha_1))$. Therefore $g(K_2,\cdot)$ is a periodic function with period $s = E_{K_0}(\alpha_0) \oplus E_{K_0}(\alpha_1)$.

Proof. (Proof of Theorem 6) We use Grover's algorithm to search key K_2, by running many independent Simon's algorithms to check whether the function g is periodic or not. If k is guessed right, g is a periodic function with period $s = E_{K_0}(\alpha_0) \oplus E_{K_0}(\alpha_1)$. Given quantum oracle to g, K_2 and $E_{K_0}(\alpha_0) \oplus E_{K_0}(\alpha_1)$ could be computed with $O(n2^{k/2})$ quantum queries.

5 Conclusions and Discussions

TNT is a concise structure with classical BBB security. In fact, the way it incorporates the tweak avoids quantum attacks by Simon's algorithm using the construction of periodic functions. We prove that TNT is quantum secure against chosen plaintext attacks up to $O(2^{n/6})$ queries. Without considering the bound of $O(2^{n/6})$ induced by the $\widetilde{\text{qPRP}}$/qPRF switching lemma, which is thought to be not tight [13], TNT is secure up to $O(2^{n/3})$ quantum queries. Neither attacks with $O(2^{n/6})$ quantum queries have been found yet, nor with $O(2^{n/3})$. We give a distinguishing attack with $O(2^{n/2})$ quantum queries and a Grover-meet-Simon attack with $O(n2^{k/2})$ quantum queries. What is the tight bound for TNT as $\widetilde{\text{qPRP}}$? We leave it as an open problem.

We show that the tight quantum PRF security bound of $\mathsf{TNT}[f_0,f_1,f_2]$ is $O(2^{n/3})$. Our proof bound is better than the $O(2^{n/4})$ quantum queries by Bhaumik et al. [4]. We also give a matching attack with $O(2^{n/3})$ quantum queries, therefore, resolving their open problem. But it is not possible to transform it directly into a quantum attack against $\mathsf{TNT}[\pi_0,\pi_1,\pi_2]$ as $\widetilde{\text{qPRP}}$. We show that $\mathsf{TNT}[\pi_0,\pi_1,\pi_2]$ is a quantum-secure TBC against chosen plaintext attacks. In [15], Ashwin Jha et al. gave a tight security bound in CCA on $\mathsf{TNT}[\pi_0,\pi_1,\pi_2]$ with $O(2^{n/2})$ queries in classical. We conjecture that it is also quantum secure against chosen ciphertext attacks, which is another open problem.

References

1. Ambainis, A.: Quantum walk algorithm for element distinctness. SIAM J. Comput. **37**(1), 210–239 (2007). https://doi.org/10.1137/S0097539705447311 8
2. Bao, Z., Guo, C., Guo, J., Song, L.: TNT: how to tweak a block cipher. In: Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques. vol. 12106, pp. 641–673. Springer (2020). https://doi.org/10.1007/978-3-030-45724-2_22 1, 3

3. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption. In: 38th Annual Symposium on Foundations of Computer Science, FOCS '97. pp. 394–403. IEEE Computer Society (1997). https://doi.org/10.1109/SFCS.1997.646128 2
4. Bhaumik, R., Cogliati, B., Ethan, J., Jha, A.: On quantum secure compressing pseudorandom functions. IACR Cryptol. ePrint Arch. p. 207 (2023), https://eprint.iacr.org/2023/207 2, 3, 17
5. Brassard, G., Hoyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. Contemporary Mathematics **305**, 53–74 (2002) 8
6. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking even-mansour ciphers. In: Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference. vol. 9215, pp. 189–208. Springer (2015). https://doi.org/10.1007/978-3-662-47989-6_9 1
7. Dong, X., Wang, X.: Quantum key-recovery attack on Feistel structures. Sci. China Inf. Sci. **61**(10), 102501:1–102501:7 (2018). https://doi.org/10.1007/s11432-017-9468-y 2
8. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing. pp. 212–219. ACM (1996). https://doi.org/10.1145/237814.237866 2, 7
9. Guo, C., Guo, J., List, E., Song, L.: Towards closing the security gap of tweak-and-tweak (TNT). In: Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security. vol. 12491, pp. 567–597. Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_19 2, 3, 15
10. Hosoyamada, A., Iwata, T.: 4-round luby-rackoff construction is a qPRP. In: Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security. vol. 11921, pp. 145–174. Springer (2019). https://doi.org/10.1007/978-3-030-34578-5_6 3, 6, 9, 13
11. Hosoyamada, A., Iwata, T.: 4-round luby-rackoff construction is a qPRP: Tight quantum security bound. IACR Cryptol. ePrint Arch. p. 243 (2019), https://eprint.iacr.org/2019/243 2, 3, 6, 13
12. Hosoyamada, A., Iwata, T.: On tight quantum security of HMAC and NMAC in the quantum random oracle model. In: Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021. vol. 12825, pp. 585–615. Springer (2021). https://doi.org/10.1007/978-3-030-84242-0_21 3
13. Hosoyamada, A., Iwata, T.: Provably quantum-secure tweakable block ciphers. IACR Trans. Symmetric Cryptol. **2021**(1), 337–377 (2021). https://doi.org/10.46586/tosc.v2021.i1.337-377 1, 2, 3, 5, 6, 7, 12, 14, 17
14. Ito, G., Hosoyamada, A., Matsumoto, R., Sasaki, Y., Iwata, T.: Quantum chosen-ciphertext attacks against Feistel ciphers. In: Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019. vol. 11405, pp. 391–411. Springer (2019). https://doi.org/10.1007/978-3-030-12612-4_20 2
15. Jha, A., Khairallah, M., Nandi, M., Saha, A.: Tight security of tnt and beyond: Attacks, proofs and possibilities for the cascaded lrw paradigm. Cryptology ePrint Archive, Paper 2023/1272 (2023), https://eprint.iacr.org/2023/1272, https://eprint.iacr.org/2023/1272 17
16. Jha, A., List, E., Minematsu, K., Mishra, S., Nandi, M.: XHX - A framework for optimally secure tweakable block ciphers from classical block ciphers and universal hashing. In: Progress in Cryptology - LATINCRYPT 2017 - 5th International Conference on Cryptology and Information Security in Latin America. vol. 11368, pp. 207–227. Springer (2017). https://doi.org/10.1007/978-3-030-25283-0_12 1
17. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference. vol. 9815, pp. 207–237. Springer (2016). https://doi.org/10.1007/978-3-662-53008-5_8 2

18. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: IEEE International Symposium on Information Theory, ISIT 2010. pp. 2682–2685. IEEE (2010). https://doi.org/10.1109/ISIT.2010.5513654 2
19. Lampe, R., Seurin, Y.: Tweakable blockciphers with asymptotically optimal security. In: Fast Software Encryption - 20th International Workshop, FSE 2013. vol. 8424, pp. 133–151. Springer (2013). https://doi.org/10.1007/978-3-662-43933-3_8 1
20. Landecker, W., Shrimpton, T., Terashima, R.S.: Tweakable blockciphers with beyond birthday-bound security. In: Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference. vol. 7417, pp. 14–30. Springer (2012). https://doi.org/10.1007/978-3-642-32009-5_2 1
21. Leander, G., May, A.: Grover meets simon - quantumly attacking the FX-construction. In: Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security. vol. 10625, pp. 161–178. Springer (2017). https://doi.org/10.1007/978-3-319-70697-9_6 2, 8
22. Lee, B., Lee, J.: Tweakable block ciphers secure beyond the birthday bound in the ideal cipher model. In: Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security. vol. 11272, pp. 305–335. Springer (2018). https://doi.org/10.1007/978-3-030-03326-2_11 1
23. Liskov, M.D., Rivest, R.L., Wagner, D.A.: Tweakable block ciphers. J. Cryptol. **24**(3), 588–613 (2011). https://doi.org/10.1007/s00145-010-9073-y 1
24. Luo, Y., Yan, H., Wang, L., Hu, H., Lai, X.: Study on block cipher structures against simon's quantum algorithm (in chinese). Journal of Cryptologic Research **6**(5), 561–573 (2019) 2
25. Mao, S., Guo, T., Wang, P., Hu, L.: Quantum attacks on lai-massey structure. In: Post-Quantum Cryptography - 13th International Workshop, PQCrypto 2022. vol. 13512, pp. 205–229. Springer (2022). https://doi.org/10.1007/978-3-031-17234-2_11 2
26. Mennink, B.: Optimally secure tweakable blockciphers. In: Fast Software Encryption - 22nd International Workshop, FSE 2015. vol. 9054, pp. 428–448. Springer (2015). https://doi.org/10.1007/978-3-662-48116-5_21 1
27. Minematsu, K., Iwata, T.: Tweak-length extension for tweakable blockciphers. In: Cryptography and Coding - 15th IMA International Conference, IMACC 2015. vol. 9496, pp. 77–93. Springer (2015). https://doi.org/10.1007/978-3-319-27239-9_5 1
28. Naito, Y.: Tweakable blockciphers for efficient authenticated encryptions with beyond the birthday-bound security. IACR Trans. Symmetric Cryptol. **2017**(2), 1–26 (2017). https://doi.org/10.13154/tosc.v2017.i2.1-26 1
29. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security. vol. 3329, pp. 16–31. Springer (2004). https://doi.org/10.1007/978-3-540-30539-2_2 1, 2
30. Simon, D.R.: On the power of quantum computation. SIAM J. Comput. **26**(5), 1474–1483 (1997). https://doi.org/10.1137/S0097539796298637 2, 7
31. Wang, L., Guo, J., Zhang, G., Zhao, J., Gu, D.: How to build fully secure tweakable blockciphers from classical blockciphers. In: Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security. vol. 10031, pp. 455–483 (2016). https://doi.org/10.1007/978-3-662-53887-6_17 1
32. Zhandry, M.: A note on the quantum collision and set equality problems. Quantum Inf. Comput. **15**(7&8), 557–567 (2015). https://doi.org/10.26421/QIC15.7-8-2 2, 4
33. Zhandry, M.: How to record quantum queries, and applications to quantum indifferentiability. In: Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference. vol. 11693, pp. 239–268. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_9 2, 5

A Proof of Proposition 6

First, let's review the implementation of O_{TNT_s} and O_{TNT_b}. From (1) to (6) we have

$$O_{\mathsf{TNT}_s} = O_0^* \cdot O_1^* \cdot O_2 \cdot O_1 \cdot O_0,$$
$$O_{\mathsf{TNT}_b} = O_0^* \cdot O_1^* \cdot O_2' \cdot O_1 \cdot O_0.$$

For $|\psi_i'\rangle = |\psi_i'^{\mathsf{good}}\rangle + |\psi_i'^{\mathsf{bad}}\rangle$ and $|\psi_i\rangle = |\psi_i^{\mathsf{good}}\rangle + |\psi_i^{\mathsf{bad}}\rangle$, where $|\psi_i'^{\mathsf{good}}\rangle$ and $|\psi_i^{\mathsf{good}}\rangle$ satisfy equation (7) and (8), We first consider the action of O_0.

From (1) we query $|M,T\rangle|0^n\rangle$ to O_0 and get $|M,T\rangle \otimes |M_1\rangle$. Accordingly, after acting on O_0, the quantum state can be divided into good and bad parts with $O_0|\psi_i'\rangle = |\psi_i'^{\mathsf{good},1}\rangle + |\psi_i'^{\mathsf{bad},1}\rangle$ and $O_0|\psi_i\rangle = |\psi_i^{\mathsf{good},1}\rangle + |\psi_i^{\mathsf{bad},1}\rangle$. And from (1), (7) and (8) there exists complex number $a^{(i),1}_{M,T,Y,Z,(D_0,D_1,D_2')}$ such that

$$|\psi_i'^{\mathsf{good},1}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid and good}\\ D_0(M)\neq\perp}} \begin{array}{c} a^{(i),1}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \otimes |D_0,D_1,D_2'\rangle \\ \otimes|M_1\rangle \end{array} \tag{9}$$

and

$$|\psi_i^{\mathsf{good},1}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid and good}\\ D_0(M)\neq\perp}} \begin{array}{c} a^{(i),1}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \otimes |[D_0,D_1,D_2']_2\rangle \\ \otimes|M_1\rangle \end{array}. \tag{10}$$

Now we consider the bad part below.

Lemma 1 (Action of O_0). *For $|\psi_i'^{\mathsf{bad},1}\rangle$ and $|\psi_i^{\mathsf{bad},1}\rangle$, we have*

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

Proof. Let $\mathbf{\Pi}_{\mathsf{valid}}$ denote the projection onto the space spanned by the vectors that correspond to valid databases. Then, by applying Proposition 4 to O_0, we have that

$$\begin{aligned}
&\mathbf{\Pi}_{\mathsf{valid}}O_0|\psi_i'^{\mathsf{good}}\rangle \\
=&\mathbf{\Pi}_{\mathsf{valid}}O_0 \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid and good}}} a^i_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \otimes |D_0,D_1,D_2'\rangle \\
=&\mathbf{\Pi}_{\mathsf{valid}}O_0 \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_2')\text{:good}}} \begin{array}{c} a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \\ \otimes|D_0\cup(M,\alpha),D_1,D_2'\rangle \end{array}
\end{aligned}$$

$$
\begin{aligned}
&+ \mathbf{\Pi}_{\mathsf{valid}} O_0 \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid}\\ D_0(M)=\perp\\ (D_0,D_1,D_2')\text{:good}}} \begin{array}{c} a^i_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \\ \otimes|D_0,D_1,D_2'\rangle \end{array}\\
=& \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_2')\text{:good}}} \begin{array}{c} a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \\ \otimes|D_0\cup(M,\alpha),D_1,D_2'\rangle\otimes|\alpha\oplus T\rangle \end{array} \qquad (11)\\
&- \sum_{\substack{M,T,Y,\alpha,\gamma,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_2')\text{:good}}} \begin{array}{c} \frac{1}{2^n} a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \\ \otimes|D_0\cup(M,\gamma),D_1,D_2'\rangle\otimes|\gamma\oplus T\rangle \end{array} \qquad (12)\\
&+ \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid}\\ D_0(M)=\perp\\ (D_0,D_1,D_2')\text{:good}}} \begin{array}{c} \frac{1}{\sqrt{2^n}} a^i_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \\ \otimes|D_0\cup(M,\alpha),D_1,D_2'\rangle\otimes|\alpha\oplus T\rangle \end{array} \qquad (13)\\
&+|\epsilon'\rangle.
\end{aligned}
$$

Where

$$
\begin{aligned}
&|\epsilon'\rangle\\
=& \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_2')\text{:good}}} \begin{array}{c} \frac{1}{\sqrt{2^n}} a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ \left(|D_0\rangle - \left(\sum_\gamma \frac{1}{\sqrt{2^n}}|D_0\cup(M,\gamma)\rangle\right)\right)|D_1 D_2'\rangle\otimes|\alpha\oplus T\rangle \end{array} \qquad (14)\\
&+ \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_2')\text{:good}}} \begin{array}{c} \frac{1}{2^n} a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ \left(2\sum_\gamma \frac{1}{\sqrt{2^n}}|D_0\cup(M,\gamma)\rangle - |D_0\rangle\right)|D_1,D_2'\rangle\otimes|\widehat{0^n}\rangle \end{array} \qquad (15)\\
&+ \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid}\\ D_0(M)=\perp\\ (D_0,D_1,D_2')\text{:good}}} \begin{array}{c} \frac{1}{\sqrt{2^n}} a^i_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ \left(|D_0\rangle - \left(\sum_\gamma \frac{1}{\sqrt{2^n}}|D_0\cup(M,\gamma)\rangle\right)\right)|D_1,D_2'\rangle\otimes|\widehat{0^n}\rangle \end{array} \qquad (16)
\end{aligned}
$$

$$
\||(14)\rangle\|^2 = \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1,D_2')\text{: valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_2')\text{:good}}} \frac{1}{2^n}\left|a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}\right|^2
$$

$$+\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\(D_0,D_1,D_2')\text{: valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_2')\text{:good}}}\frac{1}{2^{2n}}\left|a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}\right|^2\le O\left(\frac{1}{2^n}\right).$$

Similarly we have $\||(15)\rangle\|^2 \le O\left(\frac{1}{2^n}\right)$ and $\||(16)\rangle\|^2 \le O\left(\frac{1}{2^n}\right)$. So we have $\||\epsilon'\rangle\| \le O(\sqrt{\frac{1}{2^n}})$. The same goes for $\mathbf{\Pi}_{\mathsf{valid}}O_0|\psi_i^{\mathsf{good}}\rangle$ and $\||\epsilon\rangle\|$. And we set

$$|\psi_i^{\mathsf{good},1}\rangle := \mathbf{\Pi}_{\mathsf{good}}(\mathbf{\Pi}_{\mathsf{valid}}O_0|\psi_i^{\mathsf{good}}\rangle - |\epsilon\rangle), \tag{17}$$

$$|\psi_i^{\mathsf{bad},1}\rangle := O_0|\psi_i\rangle - |\psi_i^{\mathsf{good},1}\rangle. \tag{18}$$

The same goes for $|\psi_i'^{\mathsf{good},1}\rangle$ and $|\psi_i'^{\mathsf{bad},1}\rangle$. Where $\mathbf{\Pi}_{\mathsf{good}}$ denotes the projection onto the space spanned by the vectors that correspond to good databases. Let $\mathbf{\Pi}_{\mathsf{bad}}$ denotes the projection onto the space spanned by the vectors that correspond to bad databases.

$$\mathbf{\Pi}_{\mathsf{bad}}|(11)\rangle = 0 \tag{19}$$

$$\mathbf{\Pi}_{\mathsf{bad}}|(12)\rangle = -\sum_{\substack{M,T,Y,\alpha,\gamma,(D_0,D_1,D_2');\\(D_0,D_1,D_2')\text{: valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_2')\text{:good}\\(D_0\cup(M,\gamma),D_1,D_2')\text{:bad}}}\begin{matrix}\frac{1}{2^n}a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\\ \otimes|D_0\cup(M,\gamma),D_1,D_2'\rangle\otimes|\gamma\oplus T\rangle\end{matrix}$$

$$= -\sum_{\substack{M,T,Y,\alpha,\gamma,(D_0,D_1,D_2');\\(D_0,D_1,D_2')\text{: valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_2')\text{:good}\\(D_0\cup(M,\gamma),D_1,D_2')\text{:bad}\\D_1(M_1)\neq\perp\wedge D_2'(M_2)\neq\perp}}\begin{matrix}\frac{1}{2^n}a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\\ \otimes|D_0\cup(M,\gamma),D_1,D_2'\rangle\otimes|\gamma\oplus T\rangle\end{matrix} \tag{20}$$

$$-\sum_{\substack{M,T,Y,\alpha,\gamma,(D_0,D_1,D_2');\\(D_0,D_1,D_2')\text{: valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_2')\text{:good}\\(D_0\cup(M,\gamma),D_1,D_2')\text{:bad}\\D_1(M_1)=\perp\vee(D_1(M_1)\neq\perp\wedge D_2'(M_2)=\perp)}}\begin{matrix}\frac{1}{2^n}a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\\ \otimes|D_0\cup(M,\gamma),D_1,D_2'\rangle\otimes|\gamma\oplus T\rangle\end{matrix} \tag{21}$$

For the upper bound of (20), if a tuple $(M, D_0\cup(M,\gamma), D_1, D_2')$ satisfies the conditions: $D_0(M) =\perp$ and $(D_0\cup(M,\gamma), D_1, D_2')$ is bad. Then the number of α satisfies the bellow conditions is at most $|D_1| \le 2(i-1)$.

1. $D_0\cup(M,\alpha), D_1, D_2')$ is good.
2. $D_1(M_1) \neq\perp$ $(M_1 = \alpha\oplus T)$.
3. $D_2'(M_2) \neq\perp$ $(M_2 = D_1(M_1)\oplus T)$.

And we have

$$\begin{aligned}
\||(20)\rangle\|^2 &= \frac{1}{2^{2n}}\left|\sum_{\substack{M,T,Y,\alpha,\gamma,(D_0,D_1,D_2');\\(D_0,D_1,D_2'):\text{ valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_2'):\text{good}\\(D_0\cup(M,\gamma),D_1,D_2'):\text{bad}\\D_1(M_1)\neq\perp\wedge D_2'(M_2)\neq\perp}} \begin{matrix}\frac{1}{2^n}a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\\ \otimes|D_0\cup(M,\gamma),D_1,D_2'\rangle\otimes|\gamma\oplus T\rangle\end{matrix}\right|^2\\
&\leq \sum_{\substack{M,T,Y,\gamma,(D_0,D_1,D_2');\\(D_0,D_1,D_2'):\text{ valid}\\D_0(M)=\perp\\(D_0\cup(M,\gamma),D_1,D_2'):\text{bad}}} \frac{1}{2^{2n}}\cdot 2(i-1)\cdot \sum_{\substack{\alpha;\\(D_0\cup(M,\alpha),D_1,D_2'):\text{good}\\D_1(M_1)\neq\perp\wedge D_2'(M_2)\neq\perp}} \left|a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}\right|^2\\
&\leq \sum_{\gamma}\frac{2(i-1)}{2^{2n}} = \frac{2(i-1)}{2^n}. \qquad (22)
\end{aligned}$$

For the upper bound of (21), if a tuple (M,α,D_0,D_1,D_2') satisfies the conditions: $D_0(M)=\perp$, and $D_1(M_1)=\perp$ or $D_1(M_1)\neq\perp\wedge D_2'(M_2)=\perp$ ($M_1=\alpha\oplus T, M_2=D_1(M_1)\oplus T$). Then the number of γ satisfies $(D_0\cup(M,\gamma),D_1,D_2')$ becomes bad is at most $D_2'\leq i-1$. So we have

$$\begin{aligned}
&\||(21)\rangle\|^2\\
=&\frac{1}{2^{2n}}\left|\sum_{\substack{M,T,Y,\alpha,\gamma,(D_0,D_1,D_2');\\(D_0,D_1,D_2'):\text{ valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_2'):\text{good}\\(D_0\cup(M,\gamma),D_1,D_2'):\text{bad}\\D_1(M_1)=\perp\vee(D_1(M_1)\neq\perp\wedge D_2'(M_2)=\perp)}} \begin{matrix}a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\\ \otimes|D_0\cup(M,\gamma),D_1,D_2'\rangle\otimes|\gamma\oplus T\rangle\end{matrix}\right|^2\\
\leq&\sum_{\substack{M,T,Y,\gamma,(D_0,D_1,D_2');\\(D_0,D_1,D_2'):\text{ valid}\\D_0(M)=\perp\\(D_0\cup(M,\gamma),D_1,D_2'):\text{bad}}}\ \sum_{\substack{\alpha;\\(D_0\cup(M,\alpha),D_1,D_2'):\text{good}\\D_1(M_1)=\perp\vee(D_1(M_1)\neq\perp\wedge D_2'(M_2)=\perp)}} \frac{|a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|^2}{2^n}\\
\leq&\sum_{\substack{M,T,Y,(D_0,D_1,D_2');\\(D_0,D_1,D_2'):\text{ valid}\\D_0(M)=\perp\\(D_0\cup(M,\gamma),D_1,D_2'):\text{bad}}}\ \sum_{\substack{\alpha;\\(D_0\cup(M,\alpha),D_1,D_2'):\text{good}}} |a^i_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D_2')}|^2\cdot\frac{i-1}{2^n}
\end{aligned}$$

$$\leq \frac{i-1}{2^n}. \tag{23}$$

From (19) to (23), we have

$$\|\mathbf{\Pi}_{\mathsf{bad}}|(12)\rangle\| \leq O\left(\sqrt{\frac{i}{2^n}}\right). \tag{24}$$

In addition,

$$\|\mathbf{\Pi}_{\mathsf{bad}}|(13)\rangle\|^2 = \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2'); \\ (D_0,D_1,D_2'):\text{ valid} \\ D_1(P_1)=\perp \\ (D_1,\ldots,D_m,D_2'):\text{bad}}} \frac{\left|a^i_{M,T,Y,Z,(D_0,D_1D_2')}\right|^2}{2^n} \leq O\left(\frac{i}{2^n}\right). \tag{25}$$

So

$$\|\mathbf{\Pi}_{\mathsf{bad}}|(13)\rangle\| \leq O\left(\sqrt{\frac{i}{2^n}}\right). \tag{26}$$

From (19),(24) and (26), we have

$$\|\mathbf{\Pi}_{\mathsf{bad}}(\mathbf{\Pi}_{\mathsf{valid}}O_0|\psi_i^{'\mathsf{good}}\rangle - |\epsilon'\rangle)\| \leq O\left(\sqrt{\frac{i}{2^n}}\right). \tag{27}$$

So

$$\begin{aligned}
\||\psi_i^{'\mathsf{bad},1}\rangle\| =& \|O_0|\psi_i'\rangle - |\psi_i^{'\mathsf{good},1}\rangle\| \\
=& \|\mathbf{\Pi}_{\mathsf{valid}}O_0|\psi_i'\rangle - \mathbf{\Pi}_{\mathsf{good}}(\mathbf{\Pi}_{\mathsf{valid}}O_0|\psi_i^{'\mathsf{good}}\rangle - |\epsilon'\rangle)\| \\
=& \|\mathbf{\Pi}_{\mathsf{bad}}(\mathbf{\Pi}_{\mathsf{valid}}O_0|\psi_i^{'\mathsf{good}}\rangle - |\epsilon'\rangle) + \mathbf{\Pi}_{\mathsf{valid}}O_0|\psi_i^{'\mathsf{bad}}\rangle + |\epsilon'\rangle\| \\
\leq& \|\mathbf{\Pi}_{\mathsf{bad}}(\mathbf{\Pi}_{\mathsf{valid}}O_0|\psi_i^{'\mathsf{good}}\rangle - |\epsilon'\rangle)\| + \||\psi_i^{'\mathsf{bad}}\rangle\| + \||\epsilon'\rangle\| \\
\leq& \||\psi_i^{'\mathsf{bad}}\rangle\| + O(\sqrt{\frac{i}{2^n}}).
\end{aligned} \tag{28}$$

The same goes for $\||\psi_i^{\mathsf{bad},1}\rangle\|$.

Similarly, we can show the action of O_1 in the same way. From (2), we query $|M,T\rangle|M_1\rangle|0^n\rangle$ to O_1 and get $|M,T\rangle\otimes|M_1\rangle\otimes|M_2\rangle$. Similarly, we have $O_1 \cdot O_0|\psi_i'\rangle = |\psi_i^{'\mathsf{good},2}\rangle + |\psi_i^{'\mathsf{bad},2}\rangle$ and $O_1 \cdot O_0|\psi_i\rangle = |\psi_i^{\mathsf{good},2}\rangle + |\psi_i^{\mathsf{bad},2}\rangle$. And from (2), (9) and (10) there exists complex number $a^{(i),2}_{M,T,Y,Z,(D_0,D_1,D_2')}$ such that

$$|\psi_i^{'\mathsf{good},2}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2'); \\ (D_0,D_1,D_2'):\text{ valid and good} \\ D_0(M)\neq\perp,D_1(M_1)\neq\perp}} a^{(i),2}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \otimes |D_0,D_1,D_2'\rangle \otimes|M_1\rangle\otimes|M_2\rangle \tag{29}$$

and

$$|\psi_i^{\mathsf{good},2}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2'):\text{ valid and good}\\ D_0(M)\neq\perp,D_1(M_1)\neq\perp}} \begin{array}{c} a^{(i),2}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ \big|[D_0,D_1,D_2']_2\big\rangle\otimes|M_1\rangle\otimes|M_2\rangle \end{array} \tag{30}$$

Lemma 2 (Action of O_1). *For $|\psi_i'^{\mathsf{bad},2}\rangle$ and $|\psi_i^{\mathsf{bad},2}\rangle$, we have*

$$\||\psi_i'^{\mathsf{bad},2}\rangle\| \le \||\psi_i'^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right), \||\psi_i^{\mathsf{bad},2}\rangle\| \le \||\psi_i^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right).$$

Proof. The proof is similar to Lemma 1, which we omit here.

From (3) and (4), we query $|M,T\rangle|M_1\rangle|M_2\rangle|Y\rangle$ to O_2 (O_2') and obtain the state $|M,T\rangle|Y\oplus\mathsf{TNT}_s(M,T)\rangle\otimes|M_1\rangle\otimes|M_2\rangle$ ($|M,T\rangle|Y\oplus\mathsf{TNT}_b(M,T)\rangle\otimes|M_1\rangle\otimes|M_2\rangle$). Similarly, we have $O_2'\cdot O_1\cdot O_0|\psi_i'\rangle = |\psi_i'^{\mathsf{good},3}\rangle + |\psi_i'^{\mathsf{bad},3}\rangle$ and $O_2\cdot O_1\cdot O_0|\psi_i\rangle = |\psi_i^{\mathsf{good},3}\rangle + |\psi_i^{\mathsf{bad},3}\rangle$. And from (3), (4), (29) and (30) there exists complex number $a^{(i),3}_{M,T,Y,Z,(D_0,D_1,D_2')}$ such that

$$|\psi_i'^{\mathsf{good},3}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2'):\text{ valid and good}\\ D_0(M)\neq\perp,D_1(M_1)\neq\perp}} \begin{array}{c} a^{(i),3}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes|D_0,D_1,D_2'\rangle \\ \otimes|M_1\rangle\otimes|M_2\rangle \end{array} \tag{31}$$

and

$$|\psi_i^{\mathsf{good},3}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2'):\text{ valid and good}\\ D_0(M)\neq\perp,D_1(M_1)\neq\perp}} \begin{array}{c} a^{(i),3}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ \big|[D_0,D_1,D_2']_2\big\rangle\otimes|M_1\rangle\otimes|M_2\rangle \end{array} \tag{32}$$

Lemma 3 (Action of O_2 and O_2'). *For $|\psi_i'^{\mathsf{bad},3}\rangle$ and $|\psi_i^{\mathsf{bad},3}\rangle$, we have*

$$\||\psi_i'^{\mathsf{bad},3}\rangle\| \le \||\psi_i'^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right), \||\psi_i^{\mathsf{bad},3}\rangle\| \le \||\psi_i^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right).$$

Proof. Let

$$\begin{aligned} |\psi_i^{'\mathsf{good},3}\rangle &:= \mathbf{\Pi}_{\mathsf{valid}}O_2'|\psi_i^{'\mathsf{good},2}\rangle, \\ |\psi_i^{'\mathsf{bad},3}\rangle &:= O_2'\cdot O_1\cdot O_0|\psi_i'\rangle - |\psi_i^{'\mathsf{good},3}\rangle. \end{aligned}$$

And we have

$$\||\psi_i^{'\mathsf{bad},3}\rangle\| = \|O_2'\cdot O_1\cdot O_0|\psi_i'\rangle - \mathbf{\Pi}_{\mathsf{valid}}O_2'|\psi_i^{'\mathsf{good},2}\rangle\|$$

$$=\|\mathbf{\Pi}_{\mathsf{valid}} O_2'(|\psi_i^{'\mathsf{good},2}\rangle + |\psi_i^{'\mathsf{bad},2}\rangle) - \mathbf{\Pi}_{\mathsf{valid}} O_2' |\psi_i^{'\mathsf{good},2}\rangle\|$$
$$\leq \||\psi_i^{\prime\mathsf{bad},2}\rangle\| \leq \||\psi_i^{\prime\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i^m}{2^n}}\right).$$

The same goes for $|\psi_i^{\mathsf{good},3}\rangle$, $|\psi_i^{\mathsf{bad},3}\rangle$ and $\||\psi_i^{\mathsf{bad},3}\rangle\|$.

From (5) and (6), we uncompute steps to O_1^*. We have $O_1^* \cdot O_2' \cdot O_1 \cdot O_0|\psi_i'\rangle = |\psi_i^{\prime\mathsf{good},4}\rangle + |\psi_i^{\prime\mathsf{bad},4}\rangle$ and $O_1^* \cdot O_2 \cdot O_1 \cdot O_0|\psi_i\rangle = |\psi_i^{\mathsf{good},4}\rangle + |\psi_i^{\mathsf{bad},4}\rangle$. And from (31) and (32) there exists complex number $a^{(i),4}_{M,T,Y,Z,(D_0,D_1,D_2')}$ such that

$$|\psi_i^{\prime\mathsf{good},4}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2'):\text{ valid and good}\\ D_0(M)\neq\perp}} \begin{aligned} a^{(i),4}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \otimes |D_0,D_1,D_2'\rangle \\ \otimes|M_1\rangle \end{aligned} \tag{33}$$

and

$$|\psi_i^{\mathsf{good},4}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2'):\text{ valid and good}\\ D_0(M)\neq\perp}} \begin{aligned} a^{(i),4}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ \big|[D_0,D_1,D_2']_2\big\rangle \otimes |M_1\rangle \end{aligned} \tag{34}$$

Lemma 4 (Action of O_1^*). *For $|\psi_i^{\prime\mathsf{bad},4}\rangle$ and $|\psi_i^{\mathsf{bad},4}\rangle$, we have*

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

Proof. Before proving it, we first give some definitions. A state vector $|D_0,D_1,D_2'\rangle \otimes |Y\rangle\,|Z\rangle$ for O_{TNT_b}, where $|Y\rangle\,|Z\rangle$ is the ancillary $2n$ qubits, is regular if $|Y\rangle = |0^n\rangle$, $|Z\rangle = |0^n\rangle$ and the database is valid. Similarly. A state vector $|D_0,D_1,D_2'\rangle \otimes |Y\rangle\,|Z\rangle$ is preregular if $|Z\rangle = |0^n\rangle$ and the database is valid. O_{TNT_s} is similarly.

Let $\mathbf{\Pi}_{\mathsf{prereg}}$ denote the projection onto the space spanned by the vectors that correspond to preregular databases. Let

$$|\psi_i^{'\mathsf{good},4}\rangle := \mathbf{\Pi}_{\mathsf{good}}\mathbf{\Pi}_{\mathsf{prereg}} O_1^* |\psi_i^{'\mathsf{good},3}\rangle,$$
$$|\psi_i^{'\mathsf{bad},4}\rangle := O_1^* \cdot O_2' \cdot O_1 \cdot O_0|\psi_i'\rangle - |\psi_i^{'\mathsf{good},4}\rangle.$$

The same goes for $|\psi_i^{\mathsf{good},4}\rangle$ and $|\psi_i^{\mathsf{bad},4}\rangle$.

$$\mathbf{\Pi}_{\mathsf{prereg}} O_1^* |\psi_i^{'\mathsf{good},3}\rangle$$
$$=\mathbf{\Pi}_{\mathsf{prereg}} O_1^* \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2'):\text{ valid and good}\\ D_0(M)\neq\perp, D_1(M_1)\neq\perp}} \begin{aligned} a^{i,3}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \otimes |D_0,D_1,D_2'\rangle \\ \otimes|M_1\rangle\otimes|M_2\rangle \end{aligned}$$

$$=\mathbf{\Pi}_{\mathsf{prereg}} O_1^* \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2'): \text{ valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp}} \begin{array}{c} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ |D_0,D_1\cup(M_1,\alpha),D_2'\rangle\otimes|M_1\rangle\otimes|M_2\rangle \end{array}$$

$$= \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2'): \text{ valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp}} \begin{array}{c} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ |D_0,D_1\cup(M_1,\alpha),D_2'\rangle\otimes|M_1\rangle \end{array} \tag{35}$$

$$+ \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2'): \text{ valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp}} \begin{array}{c} \frac{1}{\sqrt{2^n}} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes|D_0\rangle \\ \left(|D_1\rangle - \left(\sum_\gamma \frac{1}{\sqrt{2^n}}|D_1\cup(M_1,\gamma)\rangle\right)\right)|D_2'\rangle\otimes|M_1\rangle \end{array} \tag{36}$$

$$- \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2'): \text{ valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp}} \begin{array}{c} \frac{1}{2^n} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ |D_0,D_1\cup(M_1,\alpha),D_2'\rangle\otimes|M_1\rangle \end{array} \tag{37}$$

$$+ \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2'): \text{ valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp}} \begin{array}{c} \frac{1}{2^{3n/2}} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes|D_0\rangle \\ \left(2\sum_\delta \frac{1}{\sqrt{2^n}}|D_1\cup(M_1,\delta)\rangle - |D_1\rangle\right)|D_2'\rangle\otimes|M_1\rangle. \end{array} \tag{38}$$

Then

$$\mathbf{\Pi}_{\mathsf{bad}}|(35)\rangle = \mathbf{\Pi}_{\mathsf{bad}}|(37)\rangle = 0. \tag{39}$$

For $|(36)\rangle$ we have:

$$\mathbf{\Pi}_{\mathsf{bad}}\,|(36)\rangle$$

$$=\mathbf{\Pi}_{\mathsf{bad}} \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2'): \text{ valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp}} \begin{array}{c} \frac{1}{\sqrt{2^n}} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ |D_0,D_1,D_2'\rangle\otimes|M_1\rangle \end{array} \tag{40}$$

$$-\mathbf{\Pi}_{\mathsf{bad}} \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2'): \text{ valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp}} \begin{array}{c} \frac{1}{2^n} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ |D_0,D_1\cup(M_1,\gamma),D_2'\rangle\otimes|M_1\rangle \end{array}. \tag{41}$$

For the upper bound of (40), if a tuple (M, T, D_0, D_1, D_2') satisfies the conditions: $D_0(M) \neq\perp$ and $D_1(M_1) =\perp$ ($M_1 = D_0(M) \oplus T$). Then the nember of α satisfies the bellow conditions is at most $|D_2'| \leq i$.

1. $(D_0, D_1 \cup (M_1, \alpha), D_2')$ is good.
2. $D_2'(M_2) \neq \perp$ $(M_2 = D_1(M_1) \oplus T)$.

So we have:

$$
\begin{aligned}
&\| |(40)\rangle \|^2 \\
=& \left\| \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2')\text{: valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp\\ D_2'(M_2)\neq\perp}} \begin{matrix} \frac{1}{\sqrt{2^n}} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')} |M,T\rangle|Y\rangle|Z\rangle\otimes \\ |D_0, D_1, D_2'\rangle \otimes |M_1\rangle \end{matrix} \right\|^2 \\
=& \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ D_0(M)\neq\perp, D_1(M_1)=\perp}} \frac{1}{2^n} \left\| \sum_{\substack{\alpha;\\ (D_0,D_1\cup(M_1,\alpha),D_2')\text{: valid and good}\\ D_2'(M_2)\neq\perp}} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')} \right\|^2 \\
\leq& \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ D_0(M)\neq\perp, D_1(M_1)=\perp}} \frac{i}{2^n} \sum_{\substack{\alpha;\\ (D_0,D_1\cup(M_1,\alpha),D_2')\text{: valid and good}\\ D_2'(M_2)\neq\perp}} \left| a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')} \right|^2 \\
\leq& O\left(\frac{i}{2^n}\right).
\end{aligned}
\tag{42}
$$

For the upper bound of (41) we have:

$$
\begin{aligned}
&\| |(41)\rangle \|^2 \\
=& \left\| \mathbf{\Pi}_{\mathsf{bad}} \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2')\text{: valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp\\ D_2'(M_2)\neq\perp}} \begin{matrix} \frac{1}{2^n} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')} |M,T\rangle|Y\rangle|Z\rangle\otimes \\ |D_0, D_1\cup(M_1,\gamma), D_2'\rangle \otimes |M_1\rangle \end{matrix} \right\|^2
\end{aligned}
\tag{43}
$$

$$
+ \left\| \mathbf{\Pi}_{\mathsf{bad}} \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2')\text{: valid and good}\\ D_0(M)\neq\perp, D_1(M_1)=\perp\\ D_2'(M_2)=\perp}} \begin{matrix} \frac{1}{2^n} a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')} |M,T\rangle|Y\rangle|Z\rangle\otimes \\ |D_0, D_1\cup(M_1,\gamma), D_2'\rangle \otimes |M_1\rangle \end{matrix} \right\|^2
\tag{44}
$$

For the upper bound of (43), if a tuple $(M,(D_0,D_1\cup(M_1,\gamma),D_2'))$ satisfies the conditions: $D_0(M)\neq\perp$ and $(D_0,D_1\cup(M_1,\gamma),D_2')$ is bad. Then the nember of α satisfies the bellow conditions is at most $|D_2'|\leq i$.

1. $(D_0,D_1\cup(M_1,\alpha),D_2')$ is good.
2. $D_1(M_1)=\perp$.
3. $D_2'(M_2)\neq\perp$ ($M_2=D_1(M_1)\oplus T$).

So we have:

$$\begin{aligned}
&\||(43)\rangle\|^2\\
=&\left\|\sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2')\text{: valid and good}\\ D_0(M)\neq\perp,D_1(M_1)=\perp\\ D_2'(M_2)\neq\perp\\ (D_0,D_1\cup(M_1,\gamma),D_2')\text{: bad}}}\begin{array}{c}\frac{1}{2^n}a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes\\ |D_0,D_1\cup(M_1,\gamma),D_2'\rangle\otimes|M_1\rangle\end{array}\right\|^2\\
\leq& O\left(\frac{i}{2^n}\right).
\end{aligned}\tag{45}$$

For the upper bound of (44), if a tuple $(M,\alpha,(D_0,D_1,D_2'))$ satisfies the conditions: $D_0(M)\neq\perp$, $(D_0,D_1\cup(M_1,\alpha),D_2')$ is good and $D_2'(M_2)=\perp$ ($M_2=D_1(M_1)\oplus T$). Then the nember of γ satisfies the bellow conditions is at most $|D_2'|\leq i$.

1. $(D_0,D_1\cup(M_1,\gamma),D_2')$ is bad.
2. $D_1(M_1)=\perp$.

So we have:

$$\begin{aligned}
&\||(44)\rangle\|^2\\
=&\left\|\sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_2');\\ (D_0,D_1\cup(M_1,\alpha),D_2')\text{: valid and good}\\ D_0(M)\neq\perp,D_1(M_1)=\perp\\ D_2'(M_2)=\perp\\ (D_0,D_1\cup(M_1,\gamma),D_2')\text{: bad}}}\begin{array}{c}\frac{1}{2^n}a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes\\ |D_0,D_1\cup(M_1,\gamma),D_2'\rangle\otimes|M_1\rangle\end{array}\right\|^2\\
\leq&\sum_{\substack{M,T,Y,Z,\gamma,(D_0,D_1,D_2');\\ D_0(M)\neq\perp,D_1(M_1)=\perp\\ (D_0,D_1\cup(M_1,\gamma),D_2')\text{: bad}}}\sum_{\substack{\alpha;\\ (D_0,D_1\cup(M_1,\alpha),D_2')\text{: valid and good}\\ D_2'(M_2)=\perp}}\frac{\left|a^{i,3}_{M,T,Y,Z,(D_0,D_1\cup(M_1,\alpha),D_2')}\right|^2}{2^n}
\end{aligned}$$

$$\leq O\left(\frac{i}{2^n}\right). \tag{46}$$

From (45) and (46), we have

$$\mathbf{\Pi}_{\mathsf{bad}}\left|(41)\right\rangle \leq O\left(\sqrt{\frac{i}{2^n}}\right). \tag{47}$$

From (42) and (47), we have $\mathbf{\Pi}_{\mathsf{bad}}|(36)\rangle \leq O\left(\sqrt{\frac{i}{2^n}}\right)$. Similarly, $\mathbf{\Pi}_{\mathsf{bad}}|(38)\rangle \leq O\left(\sqrt{\frac{i}{2^n}}\right)$. So $\|\mathbf{\Pi}_{\mathsf{bad}}\mathbf{\Pi}_{\mathsf{prereg}}O_1^*|\psi_i^{'\mathsf{good},3}\rangle\| \leq O\left(\sqrt{\frac{i}{2^n}}\right)$. And

$$\begin{aligned}\||\psi_i^{'\mathsf{bad},4}\rangle\| =&\|O_1^* \cdot O_2' \cdot O_1 \cdot O_0|\psi_i'\rangle - |\psi_i^{'\mathsf{good},4}\rangle\| \\ =&\|\mathbf{\Pi}_{\mathsf{prereg}}O_1^*(|\psi_i^{'\mathsf{good},3}\rangle + |\psi_i^{'\mathsf{bad},3}\rangle) - \mathbf{\Pi}_{\mathsf{good}}\mathbf{\Pi}_{\mathsf{prereg}}O_1^*|\psi_i^{'\mathsf{good},3}\rangle\| \\ \leq&\|\mathbf{\Pi}_{\mathsf{bad}}\mathbf{\Pi}_{\mathsf{prereg}}O_1^*|\psi_i^{'\mathsf{good},3}\rangle\| + \||\psi_i^{'\mathsf{bad},3}\rangle\| \\ \leq&\||\psi_i^{'\mathsf{bad},3}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right) \leq \||\psi_i^{'\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right).\end{aligned}$$

The same goes for $\||\psi_i^{\mathsf{bad},4}\rangle\|$.

Finally, we uncompute steps to O_0^*. We have $O_0^* \cdot O_1^* \cdot O_2' \cdot O_1 \cdot O_0|\psi_i'\rangle = |\psi_i^{'\mathsf{good},5}\rangle + |\psi_i^{'\mathsf{bad},5}\rangle$ and $O_0^* \cdot O_1^* \cdot O_2 \cdot O_1 \cdot O_0|\psi_i\rangle = |\psi_i^{\mathsf{good},5}\rangle + |\psi_i^{\mathsf{bad},5}\rangle$. And from (33) and (34) there exists complex number $a^{(i),5}_{M,T,Y,Z,(D_0,D_1,D_2')}$ such that

$$|\psi_i^{'\mathsf{good},5}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2'):\text{ valid and good}\\ D_0(M)\neq\perp}} a^{(i),5}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle \otimes |D_0,D_1,D_2'\rangle \tag{48}$$

and

$$|\psi_i^{\mathsf{good},5}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_2');\\ (D_0,D_1,D_2'):\text{ valid and good}\\ D_0(M)\neq\perp}} \begin{array}{c} a^{(i),5}_{M,T,Y,Z,(D_0,D_1,D_2')}|M,T\rangle|Y\rangle|Z\rangle\otimes \\ \left|[D_0,D_1,D_2']_2\right\rangle \end{array} \tag{49}$$

Lemma 5 (Action of O_0^*). *For $|\psi_i^{'\mathsf{bad},5}\rangle$ and $|\psi_i^{\mathsf{bad},5}\rangle$, we have*

$$\||\psi_i^{'\mathsf{bad},5}\rangle\| \leq \||\psi_i^{'\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right), \||\psi_i^{\mathsf{bad},5}\rangle\| \leq \||\psi_i^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right).$$

Proof. The proof is similar to Lemma 4, which we omit here.

Proof. (proof of Proposition 6) Let $|\psi_1^{'\mathsf{bad}}\rangle = |\psi_1^{\mathsf{bad}}\rangle = 0$. For $|\psi_{i+1}^{'\mathsf{good}}\rangle, |\psi_{i+1}^{'\mathsf{bad}}\rangle, |\psi_{i+1}^{\mathsf{good}}\rangle$ and $|\psi_{i+1}^{\mathsf{bad}}\rangle$, from Lemma 5 we have $\||\psi_{i+1}^{'\mathsf{bad}}\rangle\| \leq \||\psi_i^{'\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right)$ and $\||\psi_{i+1}^{\mathsf{bad}}\rangle\| \leq \||\psi_i^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{i}{2^n}}\right)$.