Quantum Security of TNT

Shuping Mao¹, Zhiyu Zhang¹, Lei Hu¹, Luying Li¹ and Peng Wang¹(✉)

¹ State Key Laboratory of Information Security, Institute of Information Engineering, CAS, China
² School of Cyber Security, University of Chinese Academy of Sciences, China

w.rocking@gmail.com

Abstract. Many classical secure structures are broken by quantum attacks. Evaluating the quantum security of a structure and providing a tight security bound is a challenging research area. As a tweakable block cipher structure based on block ciphers, TNT was proven to have $O(2^{3n/4})$ CPA and $O(2^{n/2})$ CCA security in the classical setting. 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 · q̃PRP · Quantum proof · Quantum attack.

1 Introduction

The notion of tweakable block cipher (TBC for short) proposed by Liskov et al. [LRW11] has become a popular symmetric crypto primitive. Compared to block ciphers, TBCs have an extra input named “tweak”. TNT (Tweak-aNd-Tweak) proposed at Eurocrypt 2020 by Bao et al. [BGGS20] is a TBC based on three block ciphers:

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

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. [LRW11] 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 [LRW11] and XEX [Rog04], 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 [HI21b].

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 [LST12], r-CLRW [LS13], $\tilde{F}[1]$ and $\tilde{F}[2]$ [Men15], $\tilde{E}1, \ldots, \tilde{E}32$ [WGZ+16], TEM [CLS15], XTX [MI15], XKK [Nai17], XHX [JLM+17], XHX2 [LL18] and TNT [BGGS20], etc.

TNT is an elegant TBC. It has been proven to be secure up to $O(2^{2n/3})$ chosen plaintext or ciphertext queries. (Later, we abbreviate this as “$O(2^{2n/3})$ security”). Then Guo et al. [GGLS20] improved the CPA (chosen plaintext attack) bound to $O(2^{3n/4})$, and gave a distinguishing attack with $O(\sqrt{2^{3n/4}})$ CPA queries. Recently, Khairallah [Kha23] gave a distinguishing attack with $O(2^{n/2})$ CCA (chosen ciphertext attack) queries showing flaws in previous CPA security proofs, and Jha et al. [JNS23] further proved that the bound is tight. They merged the attacking and
proving results into a single paper [JKNS23]. Therefore, TNT is BBB CPA secure, but birthday-bound CCA secure. Early birthday-bound TBCs are vulnerable to quantum attacks, which raises natural questions.

**Whether TNT is secure in quantum? or even Whether TNT is BBB CPA secure in quantum?**
Note that since the quantum collision bound is \(O(2^{n/3})\) [Zha15], we refer to the birthday bound in quantum as \(O(2^{n/3})\). We call the bound beyond \(O(2^{n/3})\) the beyond-birthday bound in quantum.

We can also view TNT as a pseudorandom function (PRF). Bhaumik et al. [BCEJ23] have recently proved that the quantum security bound of TNT as a PRF is \(O(2^{n/3})\) 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, in order to simplify the proof. As to TNT, the PRP security bound can be assessed in the case of \(|\pi_0, \pi_1, \pi_2|\) where \(\pi_i, i = 1, 2, 3\) are three independent random permutations. We only consider the PRF security bound of \(f_0, f_1, f_2\) 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 classical literature [BDJR97], the typical birthday bound is \(O(2^{n/2})\), while in the quantum literature [Zha15], 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 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 [Rog04]. However, in the quantum literature [HI19b, HI21b], it is \(O(2^{n/6})\), which is not expected to be tight [HI21b].

From the perspective of quantum attacks, many classical secure constructions are no longer secure. Quantum algorithms such as Simon’s algorithm [Sim97], Grover’s algorithm [Gro96], Grover-meet-Simon algorithm [LM17] etc. can effectively accelerate attacks to some classical structures. For example, TBCs such as LRW1, LRW2 [HI21b] and XEX, block-cipher structures such as 3-round [KM10], 4-round [IHM’19] Feistel structure, 3-round MISTY-L structure, 3-round MISTY-R structure [LYW’19], 3-round, 4-round Lai-Massey structure [MGWH22] and Even-Mansour structure [KLLN16] are not secure by using Simon’s algorithm with polynomial quantum queries. FX construction [LM17], 5-round Feistel structure [DW18], 7-round Feistel-KF structure and 9-round Feistel-FK structure [IHM’19] 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 [Zha19] 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 [HI19a, HI19b], the quantum security of LRWQ [HI21b] and the tight quantum security bound of HMAC and NMAC [HI21a] in the Quantum Random Oracle Model.

### 1.1 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 \(f_0, f_1, f_2\) is \(O(2^{n/3})\) by a proof and an attack, where \(n\) is the block length. Our proof bound is better than \(O(2^{n/3})\) by Bhaumik et
Table 1: Security results of TNT, where \( f_0, f_1, f_2 \) are random functions and \( \pi_0, \pi_1, \pi_2 \) are random permutations.

<table>
<thead>
<tr>
<th>Security goal</th>
<th>Proof bound</th>
<th>Attacking bound</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>TNT[( f_0, f_1, f_2 )]</td>
<td>qPRF ( O(2^{n/3}) )</td>
<td>-</td>
<td>[BCEJ23] Section 3</td>
</tr>
<tr>
<td></td>
<td>qPRF ( O(2^{n/3}) )</td>
<td>( O(2^{n/3}) )</td>
<td>[BCEJ23] Section 3</td>
</tr>
<tr>
<td>PRP (CPA)</td>
<td>( O(2^{3n/4}) )</td>
<td>( O(\sqrt{2^{3n/4}}) )</td>
<td>[BGGS20]</td>
</tr>
<tr>
<td>PRP (CCA)</td>
<td>( O(2^{n/2}) )</td>
<td>( O(2^{n/2}) )</td>
<td>[JKNS23]</td>
</tr>
<tr>
<td>qPRF ( \pi_0, \pi_1, \pi_2 )</td>
<td>qPRF ( O(2^{n/4}) )</td>
<td>-</td>
<td>[BCEJ23] Section 3</td>
</tr>
<tr>
<td>qPRF ( \pi_0, \pi_1, \pi_2 )</td>
<td>qPRF ( O(2^{n/3}) )</td>
<td>-</td>
<td>Section 3</td>
</tr>
<tr>
<td>qPRF (CPA) ( \pi_0, \pi_1, \pi_2 )</td>
<td>qPRF ( O(2^{n/6}) )</td>
<td>( O(2^{n/2}) )</td>
<td>Section 4</td>
</tr>
<tr>
<td>qPRF (CCA) ( \pi_0, \pi_1, \pi_2 )</td>
<td>-</td>
<td>( O(2^{n/3}) )</td>
<td>Section 4</td>
</tr>
</tbody>
</table>

al. [BCEJ23] and solves their open problem. The quantum attack on 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 TNT[\( \pi_0, \pi_1, \pi_2 \)].

2. We prove the \( O(2^{n/6}) \) quantum PRP security of TNT[\( \pi_0, \pi_1, \pi_2 \)]. Without considering the effect of the qPRP/qPRF switching lemma, the bound is \( O(2^{n/3}) \).

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 the key. And we give a quantum attack with \( O(2^{n/3}) \) chosen ciphertext queries at the same time.

2 Preliminaries

2.1 (Tweakable) Block Ciphers

**Block Ciphers.** A block cipher (or BC for short) \( E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n \) is a map with key space \( \{0, 1\}^k \) and message space \( \{0, 1\}^n \) such that for every key \( K \in \{0, 1\}^k \), \( M \rightarrow E(K, M) \) is a permutation of \( \{0, 1\}^n \). We let \( E_K \) denote the map \( M \rightarrow E(K, M) \). The inverse of a block cipher \( E \) is the map \( E^{-1} : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n \) defined by \( E^{-1}(K, C) = E_K^{-1}(C) \).

**Tweakable Block Ciphers.** A tweakable block cipher (or TBC for short) \( E' : \{0, 1\}^k \times \{0, 1\}^n \times \{0, 1\}^t \rightarrow \{0, 1\}^n \) 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 \( T \in \{0, 1\}^t \), \( M \rightarrow E'(K, M, T) \) is a permutation of \( \{0, 1\}^n \). We let \( E_K \) denote the map \( (M, T) \rightarrow E'(K, M, T) \). The inverse of a TBC \( E \) is the map \( E_K^{-1} : \{0, 1\}^k \times \{0, 1\}^n \times \{0, 1\}^t \rightarrow \{0, 1\}^n \) defined by \( E_K^{-1}(K, C, T) \) being the unique \( M \) such that \( E(K, M, T) = C \).

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

\[
\text{Adv}_{O_1, O_2}^{\text{dist}}(A) := \Pr[A^{U_{O_1}} = 1] - \Pr[A^{U_{O_2}} = 1].
\]

**Quantum PRF advantage.** Let \( F : \{0, 1\}^k \times \{0, 1\}^* \rightarrow \{0, 1\}^n \) is a function. \( RF : \{0, 1\}^* \rightarrow \{0, 1\}^n \) is a random function. Let \( A \) 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:

$$\text{Adv}^{\text{qPRF}}_E(\mathcal{A}) = \text{Adv}^{\text{dist}}_{E,\mathcal{R}F}(\mathcal{A}).$$

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

$$\text{Adv}^{\text{qPRP}}_E(\mathcal{A}) = \text{Adv}^{\text{dist}}_{E,\mathcal{R}P}(\mathcal{A}).$$

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

$$\text{Adv}^{\text{qPRP}}_{E}(\mathcal{A}) = \text{Adv}^{\text{dist}}_{E,\mathcal{R}P}(\mathcal{A}).$$

**Proposition 1** (qPRP/qPRF switching lemma [Zha15]). Let $\mathcal{A}$ be an adversary making at most $q$ quantum queries to a random permutation $\mathcal{R}P$ or a random function $\mathcal{R}F$ from $\{0,1\}^n$ to $\{0,1\}^n$. Then $\text{Adv}^{\text{dist}}_{\mathcal{R}P,\mathcal{R}F}(\mathcal{A}) \leq O\left(\frac{\sqrt{q}}{\sqrt{n}}\right)$.

**Proposition 2** (qPRP/qPRF switching lemma [HI21b] Proposition 4). Let $\mathcal{A}$ be an adversary making at most $q$ quantum queries to a random tweakable permutation $\mathcal{R}P$ or a random function $\mathcal{R}F$ from $\{0,1\}^t \times \{0,1\}^n$ to $\{0,1\}^n$. Then $\text{Adv}^{\text{dist}}_{\mathcal{R}P,\mathcal{R}F}(\mathcal{A}) \leq O\left(\sqrt{\frac{q}{\sqrt{t}}}\right)$.

Note that the bound in Proposition 2 is not expected to be tight [HI21b].

### 2.3 Proof Techniques

Recording standard oracle with errors (RstOE for short) [HI21b] is proposed by Hosoyamada and Iwata and based on Zhandry’s compressed oracle technique [Zha19], 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 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 $H^{|u|} = \frac{1}{\sqrt{|u|}} \sum_{x} (-1)^{u \cdot x} |x\rangle$ 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 $S : \{0,1\}^m \rightarrow \{0,1\}^n$ 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 $i \in \{0,1\}^m$. $b_i$s are the flag bits. Then the standard oracle $stO$ is defined by:

$$stO : |x\rangle |y\rangle |S\rangle \mapsto |x\rangle |y \oplus s_x\rangle |S\rangle.$$. 
Definition 2 (Recording Standard Oracle with Errors [HI21b]). Let, CH, U_{\text{toggle}} are unitary operators act on $(n+1)2^m$-qubit states. Let $CH^{\otimes n} := |1\rangle \langle 1| \otimes H \otimes |0\rangle \otimes I_1$ be the controlled n-qubit Hadamard operator. $X|b\rangle = |b \oplus 1\rangle$ is a “NOT” operator. And
\[
I\text{H} := (I_1 \otimes H^{\otimes n}) \otimes 2^m, \quad \text{CH} := (CH^{\otimes n}) \otimes 2^m, \quad \text{and}
\]
\[
U_{\text{toggle}} := (I_1 \otimes |0\rangle \langle 0| + X \otimes (I_1 - |0\rangle \langle 0|)) \otimes 2^m.
\]
Let $U_{\text{enc}} := \text{CH} \cdot U_{\text{toggle}} \cdot \text{IH}$. Then $U_{\text{enc}}$ and its conjugate $U_{\text{enc}}^*$ 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 $\text{RstOE} := (I \otimes U_{\text{enc}}) \cdot \text{stO} \cdot (I \otimes U_{\text{enc}}^*)$.

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 $D$ [HI21b]). Let $D$ be a string $(b_0||d_0)|| \cdots ||(d_{2^n-1}||d_{2^n-1})$ with $(n+1)2^m$-bit. $D$ is a valid database if there is no $x$ such that $d_x \neq 0^n$ and $b_x = 0$. $D$ 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 $\alpha \neq \beta$ and $x \neq x'$, if two different valid databases $D \neq D'$ satisfy $D(x) = \perp \land D'(x) = \alpha$ and $D(x') = D'(x')$, then $D' = D \cup (x, \alpha)$ and $D = D' \setminus (x, \alpha)$.

Let $A$ 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 [HI21b]). 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 [HI19a] and [HI19b]). Let $D$ be a valid database and $D(x) = \perp$. Then, the following properties hold.

1. $\text{RstOE}|x, y\rangle \otimes |D \cup (x, \alpha)\rangle = |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle + |e_1\rangle$, where $||e_1\rangle|| \leq 5\sqrt{2^n}$.

More precisely,
\[
|e_1\rangle = \frac{1}{\sqrt{2^n}}|x, y \oplus \alpha\rangle(|D\rangle - (\sum_{\gamma \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}|D \cup (x, \gamma)\rangle))
\]
\[= - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}}|x, y \oplus \gamma\rangle \otimes (|D \cup (x, \gamma)\rangle - |D_{\text{valid}}\rangle)
\]
\[+ \frac{1}{\sqrt{2^n}}|x\rangle|0^n\rangle \otimes (2 \sum_{\delta \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}|D \cup (x, \delta)\rangle - |D\rangle),
\]
where $|\bar{0}\rangle := H^{\otimes n}|0^n\rangle$ and $|D_{\text{valid}}\rangle$ is a superposition of invalid databases that depend on $\gamma$ defined by $|D_{\text{valid}}\rangle := \sum_{\gamma \neq 0^n} \frac{(-1)^{\gamma \cdot x}}{\sqrt{2^n}}|D \cup (x, \gamma)\rangle$.

2. $\text{RstOE}|x, y\rangle \otimes |D\rangle = \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}|x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle + |e_2\rangle$, where $||e_2\rangle|| \leq 2\sqrt{2^n}$.

More precisely, let $|\bar{0}\rangle := H^{\otimes n}|0^n\rangle$, we have
\[
|e_2\rangle = \frac{1}{\sqrt{2^n}}|x\rangle|\bar{0}\rangle \otimes (|D\rangle - \sum_{\gamma \in \{0,1\}^n} \frac{1}{\sqrt{2^n}}|D \cup (x, \gamma)\rangle).
\]
Let \( f_0, \ldots, f_l \) be random functions. \( F \) is a function with the ability to access \( f_0, \ldots, f_l \) in a black-box manner. We denote \( O_F \) as the quantum oracle of \( F \). Let \( D_i \) be the database of \( f_i, i = 0, \ldots, l \) and we write \( \mathbb{D}_F = (D_0, \ldots, D_l) \) as the combined database of \( F \). Correspondingly, we define \( O_G \) (\( G \) is a function with the ability to access random functions \( g_0, \ldots, g_s \) and \( \mathbb{D}_G = (D_0, \ldots, D_s) \).

**Definition 4** (Good and bad (combined) database of Oracle \([HI21b]\)). 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** \([Sim97]\): Given a Boolean function \( f : \{0, 1\}^n \to \{0, 1\}^m \), \( x, y \in \{0, 1\}^n \), \( x, y \) satisfied the condition \( f(x) = f(y) \iff x \oplus y \in \{0^n, s\} \), \( s \) is non-zero and \( s \in \{0, 1\}^n \), the goal is to find \( s \).

**Simon’s Algorithm** \([Sim97]\) 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 \( x_{\text{good}} \) that \( f(x_{\text{good}}) = 1 \).

If there is only one good element \( x_{\text{good}} \), the problem could be solved using Grover’s Algorithm.

**Grover’s Algorithm** \([Gro96]\) is a quantum algorithm to find the marked element \( x_{\text{good}} \) 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 \( H^\otimes n |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x\rangle = \frac{1}{\sqrt{2^n}} |x_{\text{good}}\rangle + \sqrt{\frac{2^n - 1}{2^n}} |x_{\text{bad}}\rangle = |\varphi\rangle \);  
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: \([|0\rangle\langle 0| - I] O^R |\varphi\rangle \approx |x_{\text{good}}\rangle\);  
5. Return \( x_{\text{good}} \).
Ambainis’s Theorem (Theorem 3 in [Amb07]) with probability $\sin \frac{\theta}{M, T}$ where $\theta$ is built on three independent random functions.  

3.1 Main Results

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

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

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

Brassard et. al. [BHMT02] 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 [BHMT02], 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

$$\mathcal{A}[0] = \left( \sum_{x \in G} \alpha_x \ket{x} \right) \ket{0} + \left( \sum_{x \in B} \beta_x \ket{x} \right) \ket{1} = \sqrt{p} \ket{\psi_G} + \sqrt{1 - p} \ket{\psi_B},$$

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

1. $\ket{\psi_0} = \mathcal{A}[0]$;
2. for $i = 1$ to $m: \ket{\psi_{i+1}} = \mathcal{A} O_0^{i} O \ket{\psi_i}.$

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

Grover-meet-Simon Algorithm [LM17] 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 [Amb07]) Let $f : \mathcal{X} \rightarrow \mathcal{Y}$ 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 $\text{TNT}[f_0, f_1, f_2]$

3.1 Main Results

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

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

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

In Asiacrypt 2019, Hosoyamada and Iwata [HI19a] 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 $\text{TNT}[f_0, f_1, f_2]$.

To prove the qPRF security of $\text{TNT}[f_0, f_1, f_2]$, that is, to prove that $\text{TNT}[f_0, f_1, f_2]$ is indistinguishable from RF. For convenience, we denote $\text{TNT}[f_0, f_1, f_2]$ as $\text{TNT}_s$, then $\text{TNT}_s(M, T) = f_2(T \oplus f_1(T \oplus f_0(M)))$. Now let $f'_2 : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a random function, we define $\text{TNT}_b(M, T) = f'_2(M, T \oplus f_1(T \oplus f_0(M)))$. Then $\text{TNT}_b(M, T)$ is indistinguishable from a random function because if one of the inputs of $\text{TNT}_b(M, T)$, $M$ and $T$, changes, the inputs of $f'_2$ must change, which guarantees the randomness of $\text{TNT}_b(M, T)$.

In this way, we transform the qPRF security proof for $\text{TNT}[f_0, f_1, f_2]$ into an indistinguishability proof for $\text{TNT}_s$ and $\text{TNT}_b$. 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 $\text{TNT}_s(M, T) = f_2(M_2)$ and $\text{TNT}_b(M, T) = f'_2(M_2, T, M_2)$.

In the following, we use the RstOE technique to prove the indistinguishability of $\text{TNT}_s$ and $\text{TNT}_b$. Before the formal proofs begin, we first show the quantum oracles and quantum implementations of $\text{TNT}_s$ and $\text{TNT}_b$, which help us to understand the quantum encryption process.

Quantum oracle of $\text{TNT}[f_0, f_1, f_2]$. We define the unitary operators $O_i, i = 0, 1, 2$ and $O'_2$ as follows.

$O_0 : |M, T\rangle |y\rangle \mapsto |M, T\rangle |y \oplus M_1\rangle$,

$O_1 : |M, T\rangle |M_1\rangle |y\rangle \mapsto |M, T\rangle |M_1\rangle |y \oplus M_2\rangle$,

$O_2 : |M, T\rangle |M_1\rangle |M_2\rangle |y\rangle \mapsto |M, T\rangle |M_1\rangle |M_2\rangle |y \oplus f_2(M_2)\rangle$,

$O'_2 : |M, T\rangle |M_1\rangle |M_2\rangle |y\rangle \mapsto |M, T\rangle |M_1\rangle |M_2\rangle |y \oplus f'_2(M_2, M, T)\rangle$.

Quantum implementations of $\text{TNT}_s$ ($\text{TNT}_b$).

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)

\[ |M, T\rangle |Y\rangle \otimes |M_1\rangle. \] (1)

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

\[ |M, T\rangle |Y\rangle \otimes |M_1\rangle \otimes |M_2\rangle. \] (2)

4. Query $|M, T\rangle |M_1\rangle |M_2\rangle |Y\rangle$ to $O_2 (O'_2)$ to obtain the state

\[ |M, T\rangle |Y \oplus \text{TNT}_s(M, T)\rangle \otimes |M_1\rangle \otimes |M_2\rangle. \] (3)

\[ (|M, T\rangle |Y \oplus \text{TNT}_b(M, T)\rangle \otimes |M_1\rangle \otimes |M_2\rangle). \] (4)

5. Uncompute Steps 2 – 4 to obtain

\[ |M, T\rangle |Y \oplus \text{TNT}_s(M, T)\rangle. \] (5)

\[ (|M, T\rangle |Y \oplus \text{TNT}_b(M, T)\rangle). \] (6)
From (1) to (6) we have
\[ O_{\text{TNT}_s} = O_0^s \cdot O_1^s \cdot O_2^s \cdot O_1 \cdot O_0, \]
\[ O_{\text{TNT}_b} = O_0^s \cdot O_1^s \cdot O_2^b \cdot O_1 \cdot O_0. \]

**Proof ideas** Valid databases consist of good databases and bad databases. For \( O_{\text{TNT}_s} \) and \( O_{\text{TNT}_b} \), the behavior of good databases for \( O_{\text{TNT}_s} \) should be the same as good databases for \( O_{\text{TNT}_b} \), such that the adversary cannot distinguish \( O_{\text{TNT}_s} \) and \( O_{\text{TNT}_b} \) 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 \( i \)th 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 \( \text{TNT}_s \) as \( \mathcal{D}_s = (D_0, D_1, D_2) \) and \( \text{TNT}_b \) as \( \mathcal{D}_b = (D_0, D_1, D_2') \).

**Good and bad database of \( \text{TNT}_s \) and \( \text{TNT}_b \).** 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 \( \epsilon = (W_0, W_1, Z_0, Z_1, V, C) \). We say \( \mathcal{D}_s (\mathcal{D}_b) \) 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 \( \epsilon = (W_0, W_1, Z_0, Z_1, V, C) \) with \( V = Z_1 \oplus W_1 \) such that \((W_0, Z_0) \in D_0 \) and \((Z_0 \oplus W_1, Z_1) \in D_1, D_s (D_b) \) 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 \( \mathcal{D}_b \) is a good database, then for \((W_0 || W_1 || V, C) \in D_2' \) there is a unique \( \epsilon = (W_0, W_1, Z_0, Z_1, V, C) \) with \( V = Z_1 \oplus W_1 \). This means that for inputs \((W_0, W_1) \) of queries to \( \text{TNT}_b, V \) does not collide. So, for such inputs \((W_0, W_1) \) of queries to \( \text{TNT}_s \), \( V \) does not collide, too. Thus, for such \((V, C) \in D_2 \), there is a unique \( \epsilon = (W_0, W_1, Z_0, Z_1, V, C) \) with \( V = Z_1 \oplus W_1 \) and \( \mathcal{D}_s \) is a good database or vice versa. So, there is a one-to-one correspondence between good databases of \( \text{TNT}_s \) and \( \text{TNT}_b \). 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 \( \mathcal{D}_b \) for \( \text{TNT}_b = (D_0, D_1, D_2') \), we write \([\mathcal{D}_b]_2 = [D_0, D_1, D_2']_2 \) as the database for \( \text{TNT}_s \). (Or for \( \mathcal{D}_b \), we write \([\mathcal{D}_b]_2 \) as the database for \( \text{TNT}_b \).) Then the mapping \( \mathcal{D}_b \to [\mathcal{D}_b]_2 \) gives a one-to-one correspondence between good databases for \( \text{TNT}_b \) and those for \( \text{TNT}_s \). We take \( \mathcal{D}_s \) as an example and the opposite direction similarly. For a (combined) good database \( \mathcal{D}_s \) for \( \text{TNT}_s \), let \( [\mathcal{D}_s]_2 \) 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 \([\mathcal{D}_s]_2 \) is a good database for \( \text{TNT}_b \), and vice versa.

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

For each \( 1 \leq i \leq q + 1 \), since oracle’s databases can be divided into good databases and bad databases, the corresponding whole quantum states of \( A \) and the oracle \( \ket{\psi_i} \) and \( \ket{\psi'_i} \) can also be divided into good parts and bad parts. We write \( \ket{\psi'_i} = \ket{\psi'^{\text{good}}_i} + \ket{\psi'^{\text{bad}}_i} \) and \( \ket{\psi_i} = \ket{\psi^{\text{good}}_i} + \ket{\psi^{\text{bad}}_i} \). Since there is a one-to-one correspondence between good databases of \( \text{TNT}_s \) and \( \text{TNT}_b \), we write \( \ket{\psi'^{\text{good}}_i} \) and \( \ket{\psi^{\text{good}}_i} \) in the following form:

\[
\ket{\psi'^{\text{good}}_i} = \sum_{M, T, Y, Z, (D_0, D_1, D_2)} a^{(i)}_{M, T, Y, Z, (D_0, D_1, D_2)} \ket{M, T, Y} \otimes |D_0, D_1, D_2'>, \quad (7)
\]
and

$$|\psi^\text{good}_i\rangle = \sum_{M, T, Y, Z, (D_0, D_1, D_2'), (D_0', D_1, D_2':) \text{valid and good}} a^{(i)}_{M, T, Y, Z, (D_0, D_1, D_2')} |M, T, Y\rangle |Z\rangle \otimes |D_0, D_1, D_2\rangle |Z\rangle,$$  \hspace{1cm} (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 $|\psi^\text{good}_i\rangle$ (resp., $(D_0, D_1, D_2')$ in $|\psi^\text{bad}_i\rangle$) with non-zero quantum amplitude, $|D_1| \leq 2(i - 1), 1 \leq i \leq 2$, and $|D_2'| \leq i - 1$ (resp., $|D_2| \leq i - 1$).

Next, as we mentioned in the proof idea, bad databases at the $i$th 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 [HI21b] gives a generalized conclusion of this question, which we specify for TNT$_a$ and TNT$_b$.

**Proposition 5** (Proposition 3 in [HI21b]). Suppose that there exist vectors $|\psi_i^\text{good}\rangle$, $|\psi_i^\text{bad}\rangle$, $|\psi_i^\text{good}'\rangle$ and $|\psi_i^\text{bad}'\rangle$ that satisfy $|\psi_i^\text{good}\rangle = |\psi_i^\text{good}'\rangle + |\psi_i^\text{bad}\rangle$ and $|\psi_i^\text{bad}\rangle = |\psi_i^\text{good}\rangle + |\psi_i^\text{bad}'\rangle$, $|\psi_i^\text{good}\rangle$ and $|\psi_i^\text{good}'\rangle$ satisfy equation (7) and (8). $|||\psi_i^\text{bad}\rangle||| \leq |||\psi_i^\text{bad}'\rangle||| + t^\text{bad}$ and $|||\psi_i^\text{bad}\rangle||| \leq |||\psi_i^\text{bad}'\rangle||| + t^\text{bad}$. Then,

$$\text{Adv}_{\text{dist}}^{\text{TNT}_a, \text{TNT}_b} (A) \leq \sum_{1 \leq i \leq q} e_i^\text{bad} + \sum_{1 \leq i \leq q} e_i^\text{bad}.$$

Return to our proof. The core of qPRF security proofs for TNT$_{f_0, f_1, f_2}$ is the indistinguishability of TNT$_a$ and TNT$_b$, and by Proposition 5 the core of the distinction between TNT$_a$ and TNT$_b$ lies in $|||\psi_i^\text{bad}\rangle|||$ and $|||\psi_i^\text{bad}\rangle|||$. More precisely, it depends on $e_i^\text{bad}$ and $e_i^\text{bad}$.

In Proposition 6 we show $|||\psi_i^\text{bad}\rangle|||$ and $|||\psi_i^\text{bad}\rangle|||$ of TNT$_b$ and TNT$_a$.

**Proposition 6** (Core proposition). For $|\psi_i^\text{bad}\rangle$ and $|\psi_i^\text{bad}\rangle$ of TNT$_b$ and TNT$_a$, we have

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

**Proof.** From (1) to (6) we have $O_{\text{TNT}_a} = O_0^a \cdot O_1^a \cdot O_2 \cdot O_3 \cdot O_0$ and $O_{\text{TNT}_b} = O_0^b \cdot O_1^b \cdot O_2 \cdot O_3 \cdot O_1 \cdot O_0$. Therefore, when we do a new query, what we are actually looking at is the bad parts of quantum states $O_0^a \cdot O_1^a \cdot O_2 \cdot O_3 \cdot O_0$ and $O_0^b \cdot O_1^b \cdot O_2 \cdot O_3 \cdot O_1 \cdot O_0$. So we will start with $|\psi_i^\text{bad}\rangle$ (and $|\psi_i^\text{bad}\rangle$) and go step by step to calculate $O_0^a|\psi_i^\text{bad}\rangle$, $O_1^a|\psi_i^\text{bad}\rangle$, $O_2^b|\psi_i^\text{bad}\rangle$, $O_1^b|\psi_i^\text{bad}\rangle$, $O_0^b|\psi_i^\text{bad}\rangle$, and $O_0^b|\psi_i^\text{bad}\rangle$ ($|\psi_i^\text{bad}\rangle$ ditto). For completeness, we provide concrete computations in Appendix A. \hfill \Box

**proof of Theorem 1.** From Proposition 5 we have

$$\text{Adv}^{\text{qPRF}}_{\text{TNT}_{f_0, f_1, f_2}} (A) = \text{Adv}^{\text{dist}}_{\text{TNT}_a, \text{TNT}_b} (A) \leq \sum_{1 \leq i \leq q} O \left( \sqrt{\frac{i}{2^n}} \right) + \sum_{1 \leq i \leq q} O \left( \sqrt{\frac{i}{2^n}} \right) \leq O \left( \sqrt{\frac{q^2}{2^n}} \right).$$

\hfill \Box

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

**Theorem 3.** Let $A$ be a quantum adversary makes at most $q$ quantum queries. Then we have

$$\text{Adv}^{\text{qPRF}}_{\text{TNT}_{\pi_0, \pi_1, \pi_2}} (A) \leq O \left( \sqrt{\frac{q^2}{2^n}} \right) + O \left( \frac{q^3}{2^n} \right),$$

where $\pi_0, \pi_1$ and $\pi_2$ are independent random permutations.
Proof. From Proposition 1 and Theorem 1, there exists quantum adversaries $B_i, i = 0, 1, 2$ and $C$ such that
\[
\text{Adv}^{\text{PRF}}_{TNT[\sigma_0, \pi_1, \pi_2]}(A) = \sum_{0 \leq i \leq 2} \text{Adv}^{\text{dist}}_{\pi_i, f_i}(B_i) + \text{Adv}^{\text{PRF}}_{TNT[f_0, f_1, f_2]}(C) \leq O\left(\sqrt{2^n} + O\left(\frac{q^3}{2^n}\right)\right).
\]

3.3 qPRF Attack for $TNT[f_0, f_1, f_2]$

For $TNT[f_0, f_1, f_2](M, T) = f_2(T \oplus f_1(T \oplus f_0(M)))$, let $M = x, T = 0$, then we have $TNT[f_0, f_1, f_2](x, 0) = f_2(f_1(f_0(x)))$, where $f_0, f_1, f_2$ are independent random functions. Further, we can simplify the qPRF attack on $TNT[f_0, f_1, f_2]$ as a qPRF attack on $f_2 \circ f_1 \circ f_0$. In the full version of [HI19a], Hosoyama and Iwata performed a qPRF attack on $RF \circ RF$ (Lemma 3 in [HI19b]), which gave us the inspiration. Along the same lines as in [HI19b], 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 $f_2, f_1, f_0 : \{0, 1\}^n \rightarrow \{0, 1\}^n$. There exists a quantum adversary $A$ that makes $O(2^n/3)$ quantum queries, such that $\text{Adv}^{\text{PRF}}_{f_2 \circ f_1 \circ f_0}(A) = \frac{2}{125}$.

Proof. Let $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be an independent random function. For $1 \leq N \leq 2^n$, let the subset $\{0, 1, \ldots, N-1\}$ as $[N]$. To use Ambainis’s Theorem, let quantum algorithm $D_N^f$ with $O(|[N]|^{2/3})$ quantum queries and an error $\epsilon < 1/25$ and:
\[
D_N^f = \begin{cases} 1, & \exists x_1, x_2 \in [N] \text{ s.t. } f(x_1) = f(x_2) \\ 0, & \text{otherwise} \end{cases}
\]

Let $\text{coll}^{|[N]|}_f$ denote that $f$ has a collision in $[N]$ and let $p = \Pr_f[\neg \text{coll}^{|[N]|}_f]$. In [HI19b], equation (86) shows that $p = \prod_{i=1}^{N-1} (1 - \frac{1}{2^n})$, and (87) shows that $\Pr_{f_0, f_1}[\neg \text{coll}^{|[N]|}_{f_0} \circ f | \neg \text{coll}^{|[N]|}_f] = p^2$. Then we have
\[
\Pr_{f_0, f_1, f_2}[\neg \text{coll}^{|[N]|}_{f_0 \circ f_1 \circ f_2} | \neg \text{coll}^{|[N]|}_{f_0}] = \Pr_{f_0, f_1, f_2}[\neg \text{coll}^{|[N]|}_{f_0} \circ f | \neg \text{coll}^{|[N]|}_f] \cdot \Pr_{f_0, f_1, f_2}[\neg \text{coll}^{|[N]|}_f]
\]
\[
= p^3.
\]

And with the error $\epsilon < 1/25$ we have
\[
\text{Adv}^{\text{PRF}}_{f_2 \circ f_1 \circ f_0}(D_N^f) = \left| \Pr_f[D_N^f(\epsilon) \Rightarrow 1] - \Pr_{f_0, f_1, f_2}[D_N^{{f_2 \circ f_1 \circ f_0}}(\epsilon) \Rightarrow 1] \right|
\]
\[
\geq \left| \Pr_f[\text{coll}^{|[N]|}_f] - \Pr_{f_0, f_1, f_2}[\text{coll}^{|[N]|}_{f_2 \circ f_1 \circ f_0}] \right| - \frac{2}{25}
\]
\[
= (1 - p^3) - (1 - p) - \frac{2}{25} = (p + p^2)(1 - p) - \frac{2}{25}.
\]

The claim in [HI19b] shows that there exist $N_0 = O\left(2^{n/2}\right)$ and $p_0 = \prod_{j=1}^{N_0-1} (1 - \frac{1}{2^n}) \cdot \frac{1}{5} \leq p_0 \leq \frac{2}{5}$ holds for sufficiently large $n$. Here sufficiently large $n$ means $n$ satisfies $e^{-\frac{1}{2} \frac{3}{2} \sqrt{n \log 2}} \leq 3/5$ 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 $\frac{1}{5} \leq p_0 \leq \frac{3}{5}$ holds for sufficiently large $n$. And
\[
\text{Adv}^{\text{PRF}}_{f_2 \circ f_1 \circ f_0}(D_{N_0}) \geq \left( \frac{1}{5} + \frac{1}{5^2} \right) \left( 1 - \frac{3}{5} \right) - \frac{2}{25} = \frac{2}{125}.
\]

By Ambainis’ theorem, $D_{N_0}$ 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. $\square$
Quantum Security of TNT

4 Quantum Security of TNT[\pi_0, \pi_1, \pi_2]

4.1 Main Results

TNT built on three random permutations \(\pi_0, \pi_1\) and \(\pi_2\) is defined as

\[
TNT[\pi_0, \pi_1, \pi_2](M, T) = \pi_2(T \oplus \pi_1(T \oplus \pi_0(M))).
\]

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

\[
\text{Adv}^{\text{qPRF}}_{\text{TNT}[\pi_0, \pi_1, \pi_2]}(A) \leq O\left(\frac{q^3}{2^n}\right) + \text{Adv}^{\text{qPRF}}_{\text{RF}}(D).
\]

**Note.** In fact, if we apply the qPRF/qPRF switching lemma (Proposition 2), we will get

\[
\text{Adv}^{\text{qPRF}}_{\text{TNT}[\pi_0, \pi_1, \pi_2]}(A) \leq O\left(\sqrt{\frac{q^3}{2^n}}\right). 
\]

But the bound of the switching lemma may not be tight [HI21b], so we list it separately.

**Theorem 4** (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 \((M^0, T^0)\) and \((M^1, T^1)\) such that \(Q(M^0, T^0) = Q(M^1, T^1)\). Let

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

Let \(A\) be a quantum algorithm such that \(A|0\rangle = \sqrt{p}|\psi_G\rangle + \sqrt{1-p}|\psi_B\rangle\), where \(G\) is the kernel of \(f\) and \(B\) is the support of \(f\). We run QAA on \(f\) with \(t = [\frac{q}{2} \times 2^n]\) iterations, then measure the state. If \(Q\) is TNT, then the probability of obtaining a good result is at least \(0.8 - 2^{-\frac{2n}{3}}\). If \(Q\) is a tweakable random permutation, then the probability of obtaining a good result is at most \(\frac{1}{2}\).

**Theorem 5** (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 TNT\([E_{K_0}, E_{K_1}, E_{K_2}]\) with \(O(n^{2k/2})\) queries.

**Theorem 6** (Quantum chosen ciphertext attack on TNT, Section 4.5). For fixed \(M\) and \(\Delta\), we define

\[
F(T) = Q^{-1}(Q(M, T), T \oplus \Delta),
\]

where \(Q\) is either TNT or a tweakable random permutation, and \(Q^{-1}\) is its inverse. We pick a subset \(S \subset [2^\Delta]\) of cardinality \(2^\Delta\). Construct a table \(L\) of size \(2^\Delta\) where each item in \(L\) holds a distinct pair \((x, F(x))\) with \(x \in S\). Let

\[
f(x) = \begin{cases} 
1, & \text{if there exists a pair } (x_0, F(x_0)) \text{ in } L \text{ that } F(x) = F(x_0); \\
0, & \text{otherwise.} 
\end{cases}
\]
Let $A$ be a quantum algorithm such that $A|0\rangle = \sqrt{p}|\psi(G)\rangle + \sqrt{1-p}|\psi_B\rangle$, where $G$ is the kernel of $f$ and $B$ is the support of $f$. We run $QAA$ on $f$ with $t = \lfloor \frac{n}{3} \times 2^\frac{n}{3} \rfloor$ iterations, then measure the state. If $Q$ is TNT, then the probability of obtaining a good result is at least $0.8 - 2^{-\frac{n}{3} + \frac{2}{3}}$. If $Q$ is a tweakable random permutation, then the probability of obtaining a good result is at most $\frac{1}{2}$.

### 4.2 $qPRP$ Security Proof for TNT[$\pi_0, \pi_1, \pi_2$]

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

$$Adv^{qPRP}_{TNT[\pi_0, \pi_1, \pi_2]}(A) \leq Adv^{qPRF}_{TNT[\pi_0, \pi_1, \pi_2]}(C) + Adv^{dist}_{RF,RP}(D) + O\left(\frac{q^4}{2^n}\right).$$

**Proof.** First we change $\pi_2$ to $f_2$, from Proposition 1 we have

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

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

$$Adv^{qPRP}_{TNT[\pi_0, \pi_1, \pi_2]}(A) \leq Adv^{qPRF}_{TNT[\pi_0, f_1, f_2]}(C) + Adv^{dist}_{RF,RP}(D) + O\left(\frac{q^4}{2^n}\right).$$

\[\square\]

**Proof.** (Proof of Theorem 4) From Theorem 1 and Proposition 8, when $q \leq 2^{n/3}$ we have

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

\[\square\]

### 4.3 Quantum Cross-Road Distinguisher on TNT

At Asiacrypt 2020, Guo et. al. [GGLS20] 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 $(M^i, T^j) \in \{0, 1\}^2$, where $i \in \{0, 1\}, j \in \{0, 1, 2, 3\}$, $Q(M^0, T^0) = Q(M^1, T^1)$ and $Q(M^0, T^2) = Q(M^1, T^3)$ 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 $(M^0, T^0)$ and $(M^1, T^1)$ satisfy $Q(M^0, T^0) = Q(M^1, T^1)$. There exist $T^2$ and $T^3 = T^2 \oplus (T^0 \oplus T^1)$ that satisfy $Q(M^0, T^2) = Q(M^1, T^3)$.

**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

$$T^2 = \pi_0(M^0) \oplus \pi_0(M^1) \oplus T^1,$$

$$T^3 = T^2 \oplus (T^0 \oplus T^1) = \pi_0(M^0) \oplus \pi_0(M^1) \oplus T^0.$$

Then we have

$$Q(M^0, T^0) = Q(M^1, T^1)$$

$$\iff \pi_2(T^0 \oplus \pi_1(T^0 \oplus \pi_0(M^0))) = \pi_2(T^1 \oplus \pi_1(T^1 \oplus \pi_0(M^1)))$$

$$\iff T^0 \oplus \pi_1(T^0 \oplus \pi_0(M^0)) = T^1 \oplus \pi_1(T^1 \oplus \pi_0(M^1))$$
\[ T^0 \oplus \pi_1(T^3 \oplus \pi_0(M^0) \oplus \pi_0(M^1) \oplus \pi_0(M^0)) = T^1 \oplus \pi_1(T^2 \oplus \pi_0(M^0) \oplus \pi_0(M^1) \oplus \pi_0(M^1)) \]

\[ T^0 \oplus \pi_1((T^3 \oplus \pi_0(M^1))) = T^2 \oplus \pi_1(T^2 \oplus \pi_0(M^0)) \]

\[ Q(T^1, T^3) = Q(M^0, T^2) . \]

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 \( (M^0, T^0) \) and \( (M^1, T^1) \) satisfy \( Q(M^0, T^0) = Q(M^1, T^1) \), then for \( T^2 = \pi_0(M^0) \oplus \pi_0(M^1) \oplus T^1 \) and \( T^3 = T^2 \oplus (T^0 \oplus T^1) \), \( Q(M^0, T^2) = Q(M^1, T^3) \) 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

\[ |\psi_1\rangle = \sin((2t + 1)\theta)|\psi_G\rangle + \cos((2t + 1)\theta)|\psi_B\rangle = \sin((\frac{\pi}{4} \times 2^2 - 1) \times 2^{-\frac{n}{2}}) |\psi_G\rangle + \cos((\frac{\pi}{4} \times 2^{-\frac{n}{2}} - 1) \times 2^{-\frac{n}{2}}) |\psi_B\rangle . \]

where \( \sin((\frac{\pi}{4} \times 2^2 - 1) \times 2^{-\frac{n}{2}}) \leq \sin(\frac{\pi}{4} \times 2^2) = \sin(\frac{\pi}{4}) = \frac{1}{\sqrt{2}} \). 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)
   \[ Q(M^0, x) = Q(M^1, x \oplus T^0 \oplus T^1) ; \]

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

\[ |\psi_1\rangle = \sin((2t + 1)\theta)|\psi_G\rangle + \cos((2t + 1)\theta)|\psi_B\rangle = \sin((\frac{\pi}{4} \times 2^2 - 1) \times 2^{-\frac{n-1}{2}}) |\psi_G\rangle + \cos((\frac{\pi}{4} \times 2^{-\frac{n-1}{2}} - 1) \times 2^{-\frac{n-1}{2}}) |\psi_B\rangle . \]

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

\[ \sin^2((\frac{\pi}{4} \times 2^2 - 1) \times 2^{-\frac{n-1}{2}}) \geq \sin^2((\frac{\pi}{4} \times 2^2 - 2) \times 2^{-\frac{n-1}{2}}) \]

\[ > (\sin(\frac{\pi}{4} \times \sqrt{2}) - 2 \times 2^{-\frac{n-1}{2}})^2 > \sin^2(\frac{\pi}{4} \times \sqrt{2}) - 2 \times 2^{-\frac{n-1}{2}} - 0.8 - 2^{-\frac{n}{2}} \]

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

**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 \( M, T \in \{0, 1\}^k, b \in \{0, 1\}, x \in \{0, 1\}^n, K \in \{0, 1\}^k \) and \( \alpha_0, \alpha_1 \) be arbitrarily two different fixed numbers in \( \{0, 1\}^n \). Let \( (M, T) = (\alpha_0, x) \) be the input of \( \text{TNT}[E_{K_0}, E_{K_1}, E_{K_2}] \). We construct a function \( g \) based on TNT:

\[ g(K, x) = E_{K_1}^{-1}(\text{TNT}[E_{K_0}, E_{K_1}, E_{K_2}](\alpha_0, x)) \oplus E_{K_1}^{-1}(\text{TNT}[E_{K_0}, E_{K_1}, E_{K_2}](\alpha_1, x)) . \]

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 $s = E_{K_0}(α_0) + E_{K_0}(α_1)$. Given quantum oracle to $g$, $K_2$ and $E_{K_0}(α_0) + E_{K_0}(α_1)$ could be computed with $O(n2^{n/2})$ quantum queries.

4.5 Quantum Chosen Ciphertext Attack on TNT

Jha et al. [JKNS23] proposed a chosen ciphertext attack on TNT with time complexity $O(2^{n/2})$. For fixed $M$ and $Q$, we define

$$F(T) = Q^{-1}(Q(M,T), T \oplus \Delta),$$

where $Q$ is either TNT or a tweakable random permutation, and $Q^{-1}$ is its inverse. Jha et al. shows when $Q$ is TNT, one could find twice as many as collision than when $Q$ is a tweakable random permutation.

Proposition 10 (From [JKNS23]). We randomly chosen $T_0, T_1$ from $\mathbb{F}_2^n$. For fixed $M$ and $\Delta$, we have

$$\Pr[F(T_0) = F(T_1)] = \begin{cases} 2^{-n}, & \text{if } Q \text{ is a tweakable random permutation}, \\ 2^{-n+1}, & \text{if } Q \text{ is TNT}. \end{cases} \quad (9)$$

For further details, we refer to [JKNS23] section 3.1. Utilizing proposition 10, we could mount a quantum chosen ciphertext attack on TNT.

Proof. (Proof of Theorem 7) If $Q$ is a tweakable random permutation, for a random $x$ the probability that $f(x) = 1$ is $2^{-n} \times 2^\frac{3}{2} = 2^{-\frac{n+3}{2}}$. Thus, for QAA on a tweakable random permutation, $\theta = 2^{-\frac{n}{2}}$, and

$$|\psi_i\rangle = \sin((2t+1)\theta)|\psi_G\rangle + \cos((2t+1)\theta)|\psi_B\rangle = \sin(\frac{\pi}{4} \times 2^\frac{3}{2} - 1] \times 2^{-\frac{3}{2}}) |\psi_G\rangle + \cos(\frac{\pi}{4} \times 2^\frac{3}{2} - 1] \times 2^{-\frac{3}{2}}) |\psi_B\rangle.$$

where $\sin(\frac{\pi}{4} \times 2^\frac{3}{2} - 1] \times 2^{-\frac{3}{2}}) \leq \sin(\frac{\pi}{4} \times 2^\frac{3}{2}) = \sin(\frac{\pi}{2}) = \frac{\sqrt{2}}{2}$. Thus, the probability of getting a good result is at most $\frac{1}{2}$.

If $Q$ is TNT, for a random $x$ the probability that $f(x) = 1$ is $2^{-n+1} \times 2^\frac{3}{2} = 2^{-\frac{n+1}{2}}$. Therefore $\theta = 2^{-\frac{n+1}{2}}$, and

$$|\psi_i\rangle = \sin((2t+1)\theta)|\psi_G\rangle + \cos((2t+1)\theta)|\psi_B\rangle = \sin(\frac{\pi}{4} \times 2^\frac{3}{2} - 1] \times 2^{-\frac{n+1}{2}}) |\psi_G\rangle + \cos(\frac{\pi}{4} \times 2^\frac{3}{2} - 1] \times 2^{-\frac{n+1}{2}}) |\psi_B\rangle.$$

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

$$\sin^2(\frac{\pi}{4} \times 2^\frac{3}{2} - 1] \times 2^{-\frac{n+1}{2}}) \geq \sin^2((\frac{\pi}{4} \times 2^\frac{3}{2} - 2) \times 2^{-\frac{n+1}{2}}) \geq (\sin(\frac{\pi}{4} \times \sqrt{2}) - 2^{-\frac{n+1}{2}})^2 > \sin^2(\frac{\pi}{4} \times \sqrt{2}) - 2 \times 2^{-\frac{n+1}{2}} > 0.8 - 2^{-\frac{n+1}{2}}.$$

Thus, the probability of getting a good result is at least $0.8 - 2^{-\frac{n+1}{2}}$.\qed

5 Conclusions and Discussions

TNT is a concise structure that incorporates the tweak to avoid simple quantum attacks by Simon’s algorithm. 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 qPRP/qPRF switching lemma, which is thought to be not tight [HI21b], 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 $O(n2^{n/2})$ quantum queries. We also give a chosen ciphertext attack with $O(2^{n/3})$ quantum queries based on the work of Khairallah et al. [Kha23, JNS23, JKNS23]. What is the tight bound for TNT as qPRP? We leave it as an open problem.

We show that the tight quantum PRF security bound of 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. [BCEJ23]. We also give a matching attack with $O(2^{n/3})$ quantum queries, therefore, resolving their open problem.

References


A Proof of Proposition 6

First, let’s review the implementation of $O_{\text{TNT}_s}$ and $O_{\text{TNT}_b}$. From (1) to (6) we have

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

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

From (1) we query $|M, T\rangle^{0n}$ 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 $O_0|\psi_i'\rangle = |\psi_i^{\text{good,1}}\rangle + |\psi_i^{\text{bad,1}}\rangle$. 

\[\text{[Nai17]}\quad \text{Yusuke Naito. Tweakable blockciphers for efficient authenticated encryptions with beyond the birthday-bound security. IACR Trans. Symmetric Cryptol., 2017(2):1–26, 2017.} \]
and \( O_0|\psi_i\rangle = |\psi_i^{\text{good},1}\rangle + |\psi_i^{\text{bad},1}\rangle \). And from (1), (7) and (8) there exists complex number \( a_{M,T,Y,Z,\{D_0, D_1, D_2\}}^{(i),1} \) such that

\[
|\psi_i^{\text{good},1}\rangle = \sum_{M,T,Y,Z,\{D_0, D_1, D_2\}; \ (D_0, D_1, D_2') : \text{valid and good}} a_{M,T,Y,Z,\{D_0, D_1, D_2\}}^{(i),1} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0, D_1, D_2'\rangle \otimes |M_1\rangle
\]  

(10)

and

\[
|\psi_i^{\text{good},1}\rangle = \sum_{M,T,Y,Z,\{D_0, D_1, D_2\}; \ (D_0, D_1, D_2') : \text{valid and good}} a_{M,T,Y,Z,\{D_0, D_1, D_2\}}^{(i),1} |M, T\rangle |Y\rangle |Z\rangle \otimes |[D_0, D_1, D_2']\rangle \otimes |M_1\rangle
\]  

(11)

Now we consider the bad part below.

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

\[
\| |\psi_i^{\text{bad},1}\rangle \| \leq \| |\psi_i^{\text{bad}}\rangle \| + O \left( \sqrt{\frac{1}{2^n}} \right), \quad \| |\psi_i^{\text{bad}}\rangle \| \leq \| |\psi_i^{\text{bad}}\rangle \| + O \left( \sqrt{\frac{1}{2^n}} \right).
\]

**Proof.** Let \( \Pi_{\text{valid}} \) 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

\[
\Pi_{\text{valid}} O_0 |\psi_i^{\text{good}}\rangle
\]

\[
= \Pi_{\text{valid}} O_0 \sum_{M,T,Y,Z,\{D_0, D_1, D_2\}; \ (D_0, D_1, D_2') : \text{valid and good}} a_{M,T,Y,Z,\{D_0, D_1, D_2\}}^{(i),1} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0, D_1, D_2'\rangle
\]

\[
= \Pi_{\text{valid}} O_0 \sum_{M,T,Y,Z,\{D_0, D_1, D_2\}; \ (D_0, D_1, D_2') : \text{valid and good}} a_{M,T,Y,Z,\{D_0, D_1, D_2\}}^{(i),1} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0 \cup (M, \alpha), D_1, D_2'\rangle
\]

\[
+ \Pi_{\text{valid}} O_0 \sum_{M,T,Y,Z,\{D_0, D_1, D_2\}; \ (D_0, D_1, D_2') : \text{valid and good}} a_{M,T,Y,Z,\{D_0, D_1, D_2\}}^{(i),1} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0 \cup (M, \alpha), D_1, D_2'\rangle \otimes |\alpha \oplus T\rangle
\]

\[
= \sum_{M,T,Y,Z,\{D_0, D_1, D_2\}; \ (D_0, D_1, D_2') : \text{valid and good}} a_{M,T,Y,Z,\{D_0, D_1, D_2\}}^{(i),1} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0 \cup (M, \alpha), D_1, D_2'\rangle \otimes |\alpha \oplus T\rangle
\]  

(12)

\[
- \sum_{M,T,Y,Z,\{D_0, D_1, D_2\}; \ (D_0, D_1, D_2') : \text{valid and good}} \frac{1}{\sqrt{2^m}} a_{M,T,Y,Z,\{D_0, D_1, D_2\}}^{(i),1} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0 \cup (M, \gamma), D_1, D_2'\rangle \otimes |\gamma \oplus T\rangle
\]  

(13)

\[
+ \sum_{M,T,Y,Z,\{D_0, D_1, D_2\}; \ (D_0, D_1, D_2') : \text{valid and good}} \frac{1}{\sqrt{2^m}} a_{M,T,Y,Z,\{D_0, D_1, D_2\}}^{(i),1} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0 \cup (M, \alpha), D_1, D_2'\rangle \otimes |\alpha \oplus T\rangle
\]  

(14)
+ |\epsilon\rangle.

Where

\[ |\epsilon\rangle = \sum_{M,T,Y,Z, (D_0, D_1, D_2)} \frac{1}{\sqrt{2^n}} a_{M,T,Y,Z, (D_0, D_1, D_2)}^i |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0\cup (M, \gamma)\rangle |D_1\rangle |D_2\rangle \]  

(15)

\[ = \sum_{M,T,Y,Z, (D_0, D_1, D_2)} \frac{1}{\sqrt{2^n}} a_{M,T,Y,Z, (D_0, D_1, D_2)}^i \left(|D_0\rangle - \sum_{\gamma} \frac{1}{\sqrt{2^n}} |D_0 \cup (M, \gamma)\rangle \right) |D_1\rangle |D_2\rangle \otimes |\alpha \oplus T\rangle \]

(16)

\[ = \sum_{M,T,Y,Z, (D_0, D_1, D_2)} \frac{1}{\sqrt{2^n}} a_{M,T,Y,Z, (D_0, D_1, D_2)}^i \left(|D_0\rangle - \sum_{\gamma} \frac{1}{\sqrt{2^n}} |D_0 \cup (M, \gamma)\rangle \right) |D_1\rangle |D_2\rangle \otimes |\alpha \oplus T\rangle \]

(17)

\[ \| (15) \|^2 = \sum_{M,T,Y,Z, (D_0, D_1, D_2)} \frac{1}{2^n} \left| a_{M,T,Y,Z, (D_0, D_1, D_2)}^i \right|^2 \]

\[ + \sum_{M,T,Y,Z, (D_0, D_1, D_2)} \frac{1}{2^n} \left| a_{M,T,Y,Z, (D_0, D_1, D_2)}^i \right|^2 \leq O \left( \frac{1}{2^n} \right). \]

Similarly we have \( \| (16) \|^2 \leq O \left( \frac{1}{2^n} \right) \) and \( \| (17) \|^2 \leq O \left( \frac{1}{2^n} \right). \) So we have \( \| |\epsilon\rangle\| \leq O(\sqrt{2^n}). \)

The same goes for \( \Pi_{\text{valid}} O_0 |\psi_i^{\text{good}}\rangle \) and \( \| |\epsilon\rangle\|. \) And we set

\[ |\psi_i^{\text{good,1}}\rangle := \Pi_{\text{good}} (\Pi_{\text{valid}} O_0 |\psi_i^{\text{good}}\rangle - |\epsilon\rangle), \]

(18)

\[ |\psi_i^{\text{bad,1}}\rangle := O_0 |\psi_i\rangle - |\psi_i^{\text{good,1}}\rangle. \]

(19)

The same goes for \( |\psi_i^{\text{good,1}}\rangle \) and \( |\psi_i^{\text{bad,1}}\rangle. \) Where \( \Pi_{\text{good}} \) denotes the projection onto the space spanned by the vectors that correspond to good databases. Let \( \Pi_{\text{bad}} \) denotes the projection onto the space spanned by the vectors that correspond to bad databases.

\[ \Pi_{\text{bad}} |(12)\rangle = 0 \]

(20)
And we have

\begin{align}
\text{For the upper bound of (21), if a tuple } (M, D_0 \cup (M, \gamma), D_1, D'_2) \text{ satisfies the conditions: } D_0(M) = \bot \text{ and } (D_0 \cup (M, \gamma), D_1, D'_2) \text{ is bad. Then the number of } \alpha \text{ satisfies the bellow conditions is at most } |D_1| \leq 2(i - 1).

1. \( D_0 \cup (M, \alpha), D_1, D'_2 \) is good.

2. \( D_1(M_1) \neq \bot (M_1 = \alpha \oplus T).\)

3. \( D'_2(M_2) \neq \bot (M_2 = D_1(M_1) \oplus T). \)

And we have

\begin{align}
\|\|21\|2^2 &= \frac{1}{2^{2n}} \sum_{M,T,Y,\alpha,\gamma,(D_0,D_1,D'_2)} \left| \frac{1}{n} a_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D'_2)}(M,T)\gamma(Z) \right|^2 \\
&\quad \otimes \left| D_0 \cup (M, \gamma), D_1, D'_2 \right| |\gamma \oplus T \right) \\
&\leq \frac{1}{2^{2n}} \sum_{M,T,Y,\alpha,\gamma,(D_0,D_1,D'_2)} \left| \frac{1}{n} a_{M,T,Y,Z,(D_0\cup(M,\alpha),D_1,D'_2)}(M,T)\gamma(Z) \right|^2 \\
&\quad \otimes \left| D_0 \cup (M, \gamma), D_1, D'_2 \right| |\gamma \oplus T \right) \\
&\leq \sum_{\gamma} \frac{2(i - 1)}{2^{2n}} = \frac{2(i - 1)}{2^{2n}}.
\end{align}

\begin{align}
\|\|22\|2^2
\end{align}

For the upper bound of (22), if a tuple \((M, \alpha, D_0, D_1, D'_2)\) satisfies the conditions: \(D_0(M) = \bot\), and \(D_1(M_1) = \bot\) or \(D_1(M_1) \neq \bot \land D'_2(M_2) = \bot (M_1 = \alpha \oplus T, M_2 = D_1(M_1) \oplus T).\) Then the number of \(\gamma\) satisfies \((D_0 \cup (M, \gamma), D_1, D'_2)\) becomes bad is at most \(D'_2 \leq i - 1\). So we have

\begin{align}
\|\|22\|2^2
\end{align}
\[\frac{1}{2^n} \sum_{M, Y, \alpha, \gamma, \delta_0, \delta_1, \delta_2} a_i^{M, Y, Z, \delta_0^i, \delta_1^i, \delta_2^i} |M, T, Y \rangle |Z\rangle \otimes | \delta_0^i \cup \{ \delta_1^i, \delta_2^i \} \rangle \leq 1 \]

\[\sum_{\alpha} \sum_{M, Y, \alpha, \delta_0, \delta_1, \delta_2} |a_i^{M, Y, Z, \delta_0^i, \delta_1^i, \delta_2^i}|^2 \cdot \frac{i - 1}{2^n} \]

From (20) to (24), we have

\[||\Pi_{\text{bad}}||_2 \leq O\left(\sqrt{\frac{i}{2^n}}\right).\]  

In addition,

\[||\Pi_{\text{bad}}||_1 = \sum_{M, Y, Z, \delta_0, \delta_1, \delta_2} |a_i^{M, Y, Z, \delta_0^i, \delta_1^i, \delta_2^i}|^2 \leq O\left(\frac{i}{2^n}\right).\]  

So

\[||\Pi_{\text{bad}}||_1 = O\left(\sqrt{\frac{i}{2^n}}\right).\]  

From (20), (25) and (27), we have

\[||\Pi_{\text{bad}}(I)_{\text{valid}}|\psi_i^{\text{good}, 1}\rangle - |\psi_i^{\text{bad}, 1}\rangle|| \leq O\left(\sqrt{\frac{i}{2^n}}\right).\]  

So

\[|||\psi_i^{\text{bad}, 1}\rangle|| = ||O_0|\psi_i^{\text{bad}, 1}\rangle - |\psi_i^{\text{good}, 1}\rangle||

\[= ||\Pi_{\text{valid}}O_0|\psi_i^{\text{good}, 1}\rangle - \Pi_{\text{good}}(I)_{\text{valid}}O_0|\psi_i^{\text{good}, 1}\rangle - |\psi_i^{\text{bad}, 1}\rangle||

\[= ||\Pi_{\text{bad}}(I)_{\text{valid}}O_0|\psi_i^{\text{good}, 1}\rangle - |\psi_i^{\text{bad}, 1}\rangle + \Pi_{\text{valid}}O_0|\psi_i^{\text{bad}, 1}\rangle + |\psi_i^{\text{bad}, 1}\rangle||\]
And from (2), (10) and (11) there exists complex number $a \in \mathbb{C}$. Similarly, we have $O_1 \cdot O_0 |\psi_i\rangle = |\psi^{\text{good}, 2}_i\rangle + |\psi^{\text{bad}, 2}_i\rangle$ and $O_1 \cdot O_0 |\psi_i\rangle = |\psi^{\text{good}, 2}_i\rangle + |\psi^{\text{bad}, 2}_i\rangle$.

And from (2), (10) and (11) there exists complex number $a_{M,T,Y,Z,(D_0,D_1,D_2)}^{(i),2}$ such that

$$|\psi^{\text{good}, 2}_i\rangle = \sum_{M,T,Y,Z,(D_0,D_1,D_2): \text{valid and good } D_0(M) \neq \perp, D_1(M) \neq \perp} a_{M,T,Y,Z,(D_0,D_1,D_2)}^{(i),2} |M,T,Y,Z\rangle \otimes |D_0,D_1,D_2\rangle$$

and

$$|\psi^{\text{bad}, 2}_i\rangle = \sum_{M,T,Y,Z,(D_0,D_1,D_2): \text{valid and good } D_0(M) \neq \perp, D_1(M) \neq \perp} a_{M,T,Y,Z,(D_0,D_1,D_2)}^{(i),2} |M,T,Y,Z\rangle \otimes |D_0,D_1,D_2\rangle$$

Similarly, we have $O_2 \cdot O_1 |\psi_i\rangle = |\psi^{\text{good}, 3}_i\rangle + |\psi^{\text{bad}, 3}_i\rangle$ and $O_2 \cdot O_1 |\psi_i\rangle = |\psi^{\text{good}, 3}_i\rangle + |\psi^{\text{bad}, 3}_i\rangle$.

And from (3), (4), (30) and (31) there exists complex number $a_{M,T,Y,Z,(D_0,D_1,D_2)}^{(i),3}$ such that

$$|\psi^{\text{good}, 3}_i\rangle = \sum_{M,T,Y,Z,(D_0,D_1,D_2): \text{valid and good } D_0(M) \neq \perp, D_1(M) \neq \perp} a_{M,T,Y,Z,(D_0,D_1,D_2)}^{(i),3} |M,T,Y,Z\rangle \otimes |D_0,D_1,D_2\rangle$$

and

$$|\psi^{\text{bad}, 3}_i\rangle = \sum_{M,T,Y,Z,(D_0,D_1,D_2): \text{valid and good } D_0(M) \neq \perp, D_1(M) \neq \perp} a_{M,T,Y,Z,(D_0,D_1,D_2)}^{(i),3} |M,T,Y,Z\rangle \otimes |D_0,D_1,D_2\rangle.$$
And we have
\[
\| |\psi_i^{\text{bad,3}}\| = \|O_1^2 \cdot O_1 \cdot O_0 |\psi_i^0\| - \Pi_{\text{valid}} O_1^2 |\psi_i^{\text{good,2}}\| = \|\Pi_{\text{valid}} O_1^2 (|\psi_i^{\text{good,2}}\| + |\psi_i^{\text{bad,2}}\|) - \Pi_{\text{valid}} O_1^2 |\psi_i^{\text{good,2}}\| \| \leq \| |\psi_i^{\text{bad,2}}\| \| + \Pi_{\text{valid}} O_1^2 \| + O \left( \sqrt{\frac{1}{2^n}} \right).
\]

The same goes for \( |\psi_i^{\text{good,3}}\|, |\psi_i^{\text{bad,3}}\| \) and \( \| |\psi_i^{\text{bad,3}}\| \|.

From (5) and (6), we uncompute steps to \( O_1^2 \). We have \( O_1^2 \cdot O_1 \cdot O_0 |\psi_i^0\| = |\psi_i^{\text{good,4}}\| + |\psi_i^{\text{bad,4}}\| \) and \( O_1^2 \cdot O_1 \cdot O_0 |\psi_i^0\| = |\psi_i^{\text{good,4}}\| + |\psi_i^{\text{bad,4}}\| \). And from (32) and (33) there exists complex number \( a_{M,T,Y,Z,(D_0,D_1,D'_2)}^{(i),4} \) such that
\[
|\psi_i^{\text{good,4}}\| = \sum_{M,T,Y,Z,(D_0,D_1,D'_2): (D_0,D_1,D'_2) \text{ valid and good } D_0(M) \neq \perp} a_{M,T,Y,Z,(D_0,D_1,D'_2)}^{(i),4} |M,T\rangle |Y\rangle |Z\rangle \odot |D_0,D_1,D'_2\rangle \odot |M_1\rangle \tag{34}
\]
and
\[
|\psi_i^{\text{good,4}}\| = \sum_{M,T,Y,Z,(D_0,D_1,D'_2): (D_0,D_1,D'_2) \text{ valid and good } D_0(M) \neq \perp} a_{M,T,Y,Z,(D_0,D_1,D'_2)}^{(i),4} |M,T\rangle |Y\rangle |Z\rangle \odot \left| [D_0,D_1,D'_2]_2 \right| \odot |M_1\rangle \tag{35}
\]

**Lemma 4 (Action of \( O_1^2 \)).** For \( |\psi_i^{\text{bad,4}}\| \) and \( |\psi_i^{\text{bad,4}}\| \), we have
\[
\| |\psi_i^{\text{bad,4}}\| \| \leq \| |\psi_i^{\text{bad,3}}\| \| + O \left( \sqrt{\frac{1}{2^n}} \right), \quad \| |\psi_i^{\text{bad,4}}\| \| \leq \| |\psi_i^{\text{bad,3}}\| \| + O \left( \sqrt{\frac{1}{2^n}} \right).
\]

**Proof.** Before proving it, we first give some definitions. A state vector \( |D_0,D_1,D'_2\rangle \odot |Y\rangle |Z\rangle \) for \( O_{\text{TNT}}^1 \), 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 \( |D_0,D_1,D'_2\rangle \odot |Y\rangle |Z\rangle \) is preregular if \( |Z\rangle = |0^n\rangle \) and the database is valid. \( O_{\text{TNT}} \) is similarly.

Let \( \Pi_{\text{prereg}} \) denote the projection onto the space spanned by the vectors that correspond to preregular databases. Let
\[
|\psi_i^{\text{good,4}}\| := \Pi_{\text{good}} \Pi_{\text{prereg}} O_1^2 |\psi_i^{\text{good,3}}\|,
\]
\[
|\psi_i^{\text{bad,4}}\| := O_1^2 \cdot O_1 \cdot O_0 |\psi_i^0\| - |\psi_i^{\text{good,4}}\|.
\]

The same goes for \( |\psi_i^{\text{good,4}}\| \) and \( |\psi_i^{\text{bad,4}}\| \).

\[
\Pi_{\text{prereg}} O_1^2 |\psi_i^{\text{good,3}}\| = \sum_{M,T,Y,Z,(D_0,D_1,D'_2): (D_0,D_1,D'_2) \text{ valid and good } D_0(M) \neq \perp} a_{M,T,Y,Z,(D_0,D_1,D'_2)}^{(i),3} |M,T\rangle |Y\rangle |Z\rangle \odot |D_0,D_1,D'_2\rangle \odot |M_1\rangle \tag{36}
\]
and
\[
\Pi_{\text{prereg}} O_1^2 |\psi_i^{\text{good,3}}\| = \sum_{M,T,Y,Z,(D_0,D_1,D'_2), (D_0,D_1,D'_2) \cup (M_1,\alpha), D'_2 \text{ valid and good } D_0(M) \neq \perp} a_{M,T,Y,Z,(D_0,D_1,D'_2)}^{(i),3} |M,T\rangle |Y\rangle |Z\rangle \odot \left| D_0,D_1 \cup (M_1,\alpha), D'_2 \right| \odot |M_1\rangle \odot |M_2\rangle \tag{37}
\]
\[\begin{align*}
= & \sum_{M, T, Y, Z, \alpha, (D_0, D_1, D_2)} a_{i, 3, M, T, Y, Z, (D_0, D_1 \cup (M_1, \alpha), D_2')} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0, D_1 \cup (M_1, \alpha), D_2'\rangle \otimes |M_1\rangle \\
+ & \sum_{M, T, Y, Z, \alpha, (D_0, D_1, D_2')} \frac{1}{\sqrt{2^n}} a_{i, 3, M, T, Y, Z, (D_0, D_1 \cup (M_1, \alpha), D_2')} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0\rangle \\
- & \sum_{M, T, Y, Z, \alpha, (D_0, D_1, D_2')} \frac{1}{\sqrt{2^n}} a_{i, 3, M, T, Y, Z, (D_0, D_1 \cup (M_1, \alpha), D_2')} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0\rangle \\
+ & \sum_{M, T, Y, Z, \alpha, (D_0, D_1, D_2')} \left( 2 \sum_{\delta} \frac{1}{\sqrt{2^n}} |D_1 \cup (M_1, \delta)\rangle - |D_1\rangle \right) |D_2'\rangle \otimes |M_1\rangle .
\end{align*}\]

Then
\[\Pi_{\text{bad}}(|36\rangle) = \Pi_{\text{bad}}(|38\rangle) = 0.\] (40)

For \(|37\rangle\), we have:
\[\Pi_{\text{bad}}(|37\rangle) = 0.\]

For the upper bound of (41), 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 number of \(\alpha\) satisfies the below conditions is at most \(|D_2'| \leq \delta\).

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:
\[\left\| (41) \right\|^2 = \sum_{M, T, Y, Z, \alpha, (D_0, D_1, D_2')} \frac{1}{\sqrt{2^n}} a_{i, 3, M, T, Y, Z, (D_0, D_1 \cup (M_1, \alpha), D_2')} |M, T\rangle |Y\rangle |Z\rangle \otimes |D_0, D_1 \cup (M_1, \alpha), D_2'\rangle \otimes |M_1\rangle \]

\]
So we have:

\[
\begin{align*}
&= \sum_{M,T,Y,Z, (D_0, D_1, D_2'); D_0(M) \neq \perp, D_1(M_1) = \perp} \frac{1}{2^n} a_{M,T,Y,Z, (D_0, D_1; (M_1, \alpha), D_2')}^i, \quad \sum_{\alpha, i} a_{M,T,Y,Z, (D_0, D_1; (M_1, \alpha), D_2'); \text{valid and good}}^i, \\
&\leq \sum_{M,T,Y,Z, (D_0, D_1, D_2'); D_0(M) \neq \perp, D_1(M_1) = \perp} \frac{i}{2^n} a_{M,T,Y,Z, (D_0, D_1; (M_1, \alpha), D_2'); \text{valid and good}}^i, \\
&\leq O\left(\frac{i}{2^n}\right). 
\end{align*}
\]

For the upper bound of (42) we have:

\[
\|\| (42)\| \|^2
\]

\[
\begin{align*}
&= \Pi_{\text{bad}} \sum_{M,T,Y,Z, \alpha, \gamma, (D_0, D_1, D_2')}; (D_0, D_1; (M_1, \alpha), D_2')': \text{valid and good} \\
&\quad \quad \quad \quad \quad \quad \quad D_0(M) \neq \perp, D_1(M_1) = \perp \\
&\quad \quad \quad \quad \quad \quad \quad D_2'(M_2) \neq \perp \\
&\quad \quad \quad \quad \quad \quad \quad |D_0, D_1; (M_1, \gamma), D_2'; \otimes |M_1\rangle |
\end{align*}
\]

\[
\begin{align*}
&= \Pi_{\text{bad}} \sum_{M,T,Y,Z, \alpha, \gamma, (D_0, D_1, D_2')}; (D_0, D_1; (M_1, \gamma), D_2'); \text{valid and good} \\
&\quad \quad \quad \quad \quad \quad \quad D_0(M) \neq \perp, D_1(M_1) = \perp \\
&\quad \quad \quad \quad \quad \quad \quad D_2'(M_2) = \perp \\
&\quad \quad \quad \quad \quad \quad \quad |D_0, D_1; (M_1, \gamma), D_2'; \otimes |M_1\rangle |
\end{align*}
\]

For the upper bound of (44), if a tuple \((M, (D_0, D_1; (M_1, \gamma), D_2'))\) satisfies the conditions: \(D_0(M) \neq \perp\) and \((D_0, D_1; (M_1, \gamma), D_2')\) is bad. Then the number of \(\alpha\) satisfies the below conditions is at most \(|D_2'| \leq i\).

1. \((D_0, D_1; (M_1, \alpha), D_2')\) 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:

\[
\|\| (44)\| \|^2
\]

\[
\begin{align*}
&= \sum_{M,T,Y,Z, \alpha, \gamma, (D_0, D_1, D_2')}; (D_0, D_1; (M_1, \gamma), D_2')': \text{valid and good} \\
&\quad \quad \quad \quad \quad \quad \quad D_0(M) \neq \perp, D_1(M_1) = \perp \\
&\quad \quad \quad \quad \quad \quad \quad D_2'(M_2) \neq \perp \\
&\quad \quad \quad \quad \quad \quad \quad (D_0, D_1; (M_1, \gamma), D_2'); \text{bad} \\
&\quad \quad \quad \quad \quad \quad \quad |D_0, D_1; (M_1, \gamma), D_2'; \otimes |M_1\rangle |
\end{align*}
\]
\[ \leq O \left( \frac{i}{2^n} \right). \quad (46) \]

For the upper bound of (45), if a tuple \((M, \alpha, (D_0, D_1, D_2'))\) satisfies the conditions: \(D_0(M) \neq \perp\), \((D_0, D_1 \cup (M, \alpha), D_2)\) is good and \(D_2'(M_2) = \perp (M_2 = D_1(M_1) \oplus T)\). Then the number of \(\gamma\) satisfies the below conditions is at most \(|D_2'| \leq i^2\).

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

So we have:

\[
\leq \sum_{M,T,Y,Z,\alpha,\gamma, (D_0, D_1, D_2') :}
\sum_{(D_0, D_1 \cup (M_1, \alpha), D_2') :}
\sum_{\alpha, D_0(M) \neq \perp, D_1(M_1) = \perp, D_2'(M_2) = \perp}
\sum_{\alpha, D_0(D_1 \cup (M_1, \gamma), D_2') :}
\leq O \left( \frac{i}{2^n} \right).
\quad (47)
\]

From (46) and (47), we have

\[
\Pi_{\text{bad}} \langle (42) \rangle \leq O \left( \frac{i}{2^n} \right). \quad (48)
\]

From (43) and (48), we have \(\Pi_{\text{bad}} \langle (37) \rangle \leq O \left( \frac{i}{2^n} \right). \) Similarly, \(\Pi_{\text{bad}} \langle (39) \rangle \leq O \left( \frac{i}{2^n} \right). \)

So \(\|\Pi_{\text{bad}} \Pi'_{\text{prereg}} \Omega(\psi^{\text{good},4}_i)\| \leq O \left( \frac{i}{2^n} \right)\). And

\[
\|\psi^{\text{bad},4}_i\| = \|O^*_1 \cdot O^*_2 \cdot O_0 |\psi^0_i\| - |\psi^{\text{good},4}_i\|
\leq \|\Pi'_{\text{prereg}} \Omega(\psi^{\text{good},4}_i) + |\psi^{\text{bad},3}_i\| - \Pi_{\text{good}} \Pi'_{\text{prereg}} \Omega(\psi^{\text{good},4}_i)\|
\leq \|\Pi_{\text{bad}} \Pi_{\text{prereg}} \Omega(\psi^{\text{good},4}_i)\| + \|\psi^{\text{bad},3}_i\|
\leq \|\psi^{\text{bad},3}_i\| + O \left( \frac{i}{2^n} \right) \leq \|\psi^{\text{bad},4}_i\| + O \left( \frac{i}{2^n} \right).
\]

The same goes for \(\|\psi^{\text{bad},4}_i\|\).

Finally, we uncompute steps to \(O^*_5\). We have \(O^*_0 \cdot O^*_1 \cdot O^*_2 \cdot O_1 \cdot O_0 |\psi_i\| = |\psi^{\text{good},5}_i\| + |\psi^{\text{bad},5}_i\|\) and \(O^*_0 \cdot O^*_1 \cdot O_2 \cdot O_1 \cdot O_0 |\psi_i\| = |\psi^{\text{good},5}_i\| + |\psi^{\text{bad},5}_i\|. \) And from (34) and (35) there exists complex
number \( a^{(i),5}_{M,T,Y,Z,(D_0,D_1,D'_2)} \) such that
\[
|\psi^{\text{good},5}_i\rangle = \sum_{M,T,Y,Z,(D_0,D_1,D'_2); \text{valid and good}} a^{(i),5}_{M,T,Y,Z,(D_0,D_1,D'_2)} |M,T,Y,Z\rangle \otimes |D_0,D_1,D'_2\rangle
\]
and
\[
|\psi^{\text{good},5}_i\rangle = \sum_{M,T,Y,Z,(D_0,D_1,D'_2); \text{valid and good}} a^{(i),5}_{M,T,Y,Z,(D_0,D_1,D'_2)} |M,T,Y,Z\rangle \otimes |D_0,D_1,D'_2\rangle
\]

**Lemma 5 (Action of \( O^*_0 \)).** For \( |\psi^{\text{bad},5}_i\rangle \) and \( |\psi^{\text{bad},5}_i\rangle \), we have
\[
\| |\psi^{\text{bad},5}_i\rangle \| \leq \| |\psi^{\text{bad}}_i\rangle \| + O \left( \sqrt{\frac{i}{2n}} \right), \| |\psi^{\text{bad},5}_i\rangle \| \leq \| |\psi^{\text{bad}}_i\rangle \| + O \left( \sqrt{\frac{i}{2n}} \right).
\]

**Proof.** The proof is similar to Lemma 4, which we omit here. \( \square \)

**Proof. (proof of Proposition 6)** Let \( |\psi^{\text{bad}}_i\rangle = |\psi^{\text{bad}}_i\rangle = 0 \). For \( |\psi^{\text{good},5}_{i+1}\rangle, |\psi^{\text{bad},5}_{i+1}\rangle, |\psi^{\text{good}}_{i+1}\rangle \) and \( |\psi^{\text{bad}}_{i+1}\rangle \), from Lemma 5 we have \( \| |\psi^{\text{bad},5}_{i+1}\rangle \| \leq \| |\psi^{\text{bad}}_{i+1}\rangle \| + O \left( \sqrt{\frac{i}{2n}} \right) \) and \( \| |\psi^{\text{bad},5}_{i+1}\rangle \| \leq \| |\psi^{\text{bad}}_{i+1}\rangle \| + O \left( \sqrt{\frac{i}{2n}} \right) \). \( \square \)