Indistinguishability obfuscation for quantum circuits of low T-gate complexity

Anne Broadbent[1] and Raza Ali Kazmi[2]

[1]Anne affiliation
[2]Raza affiliation

October 13, 2019

Abstract

We initiate the study of constructions for indistinguishability obfuscation for quantum circuits. In particular, we construct an indistinguishability obfuscator that takes as input a quantum circuit, and outputs a quantum state and a quantum circuit, which together can be used to evaluate the original quantum circuit, on any quantum input. In our construction, the size of the output of the obfuscator is exponential in the number of non-Clifford gates, which means that the construction is efficient as long as the number of non-Clifford gates is logarithmic.

1 Introduction

Indistinguishability obfuscation ($i\mathcal{O}$) was first proposed by Barak, Goldreich, Impagliazzo, Rudich, Sahai, Vadhan and Yang [**?**]. Among other things, it has been shown to enable digital signatures, public key encryption [**?**], multiparty key agreement, broadcast encryption [**?**], fully homomorphic encryption [**?**] and zero knowledge [**?**] etc. In this work, we continue the study of computational indistinguishable obfuscation in the quantum world. The main contribution of this paper is to provide a new definition of quantum indistinguishability obfuscation $Qi\mathcal{O}$ and show how to construct a $Qi\mathcal{O}$ for certain families of quantum circuits. The first construction is based on the canonical representation of Clifford circuits [**?**], while the second construction is based on the principle of gate teleportation [**?**]. The two constructions present different advantages: the technique using the canonical form is straightforward and does not require any computational assumption. Moreover, the obfuscated circuits are classical, and hence can be easily communicated, stored, used and copied. In contrast, the gate-teleportation scheme requires the assumption of quantum-secure classical $i\mathcal{O}$ for a certain family of functions (section 2.3) and the obfuscated circuits are quantum. While this presents a technological challenge to communication, storage and also usage, this methodology

allow us to obfuscate a more general set of quantum circuit than the canonical base contruction. Moreover the gate-teleportation methodology could also enable a new functionality related to the *unclonability* of quantum states. (Anne need to fill in)

1.1 Related Work

The quantum obfuscation was first studied in [], where a new notion called (G, Γ)-*indistinguishability obfuscation* was proposed. Where G is a set of gates and Γ is a set of relations satisfied by the elements of G. In this notion any two circuits over the set of gates G are perfectly indistinguishable if they differ by some sequence of applications of the relations in Γ. One of the motivations of their work was to provide a weaker definition of perfectly indistinguishable obfuscation, which is shown to be impossible under certain complexity-theoretic assumptions []. However, (G, Γ)-*indistinguishability obfuscation* appears to be incomparable with the computational indistinguishability obfuscation [], which is the topic of this paper.

The quantum obfuscation is studied more rigorously in [], where the following notions of quantum obfuscation are defined.

1. Quantum black-box obfuscation.
2. Quantum information-theoretic black-box obfuscation.
3. Quantum indistinguishability obfuscation (perfect, statistical, computational).
4. Quantum Best-Possible obfuscation (perfect, statistical, computational).

The main contribution of their work was to extend the classical impossibility results to the quantum settings such as a generic transformation of quantum circuits into black-box-obfuscated quantum circuits is impossible [], statistical indistinguishability obfuscation is impossible, up to an unlikely complexity-theoretic collapse []. However, no concrete instantiation was provided in their paper for any of type quantum obfuscations. They also discussed a number of applications of quantum black-box obfuscation such as CPA-secure quantum encryption, quantum fully-homomorphic encryption, and public-key quantum money, however it is not clear what impact these impossibility results have on these applications. They also showed that an existence of a computational quantum indistinguishability obfuscation would imply a witness encryption scheme for all languages in QMA [].

In this work we define a new definition of computational quantum obfuscation $Qi\mathcal{O}$ and provide two concrete instantiation of it. The first instantiation is based on the work of Aronson and Gottesman [**?**], In this paper, an efficient algorithm to compute a canonical form of any Clifford circuit was describe. However, the canonical form was not guaranteed to be unique, so we slightly modified their algorithm so that it always outputs a unique canonical form for any Clifford circuit. The second instantiation is based on gate-teleportation [] and assume an existence of a quantum-secure classical $i\mathcal{O}$ for certain class of functions (section 2.3). Using this technique we can obfuscate any n-qubit quantum circuit as far as the number of T gates are in $O(\log(n))$.

NOTE[1]

2 Preliminaries

2.1 Basic Classical Cryptographic Notions

Let $\mathbb{N}$ be the set of positive integers. For $n \in \mathbb{N}$, we set $[n] = \{1, \cdots, n\}$. We denote the set of all binary strings of length n by $\{0,1\}^n$. An element $s \in \{0,1\}^n$ is called a bitstring, and $|s| = n$ denotes its length. We reserve the notation 0^n (resp., 1^n) to denote the n-bit string with all zeroes (resp., all ones). We denote an arbitrary polynomial from the set $\mathbb{N}$ to $\mathbb{N}$ by $poly()$.

A function $\text{negl} : \mathbb{N} \to \mathbb{R}^+ \cup \{0\}$ is negligible if for every positive polynomial $p(n)$ there exists a positive integer n_0 such that for all $n > n_0$, $\text{negl}(n) < 1/p(n)$. A typical use of negligible functions is to indicate that the probability of success of some algorithm is too small to be amplified to a constant by a feasible (*i.e.*, polynomial) number of repetitions. Given two bit strings x and y of equal length, we denote their bitwise XOR by $x \oplus y$.

Classical Circuits and Algorithms

For $n, m \in \mathbb{N}$ let $f : \{0,1\}^n \to \{0,1\}^m$ be a function. We say a circuit C computes f if for every $s \in \{0,1\}^n$, $C(s) = f(s)$. We define the size of a circuit C as the number of gates in it and is denoted by $|C|$. A set of gates for classical computation are universal if, for all $n, m \in \mathbb{N}$, and for every function $f : \{0,1\}^n \to \{0,1\}^m$ a circuit can be constructed for computing f using only gates from that set. It is a well known fact that {AND, OR, NOT} is a set of universal gates for classical circuits. A family of circuits $\mathcal{F} = \{C_n \mid n \in \mathbb{N}\}$, one for each input size $n \in \mathbb{N}$ is called uniform if there exists a deterministic Turing machine M, such that

- For each $n \in \mathbb{N}$, M outputs a description of $C_n \in \mathcal{F}$ on input 1^n.
- For each $n \in \mathbb{N}$, M runs in $poly(n)$.

Definition 1. (**Quantum Secure Indistinguishability Obfuscation** $i\mathcal{O}$) *A probabilistic polynomial-time algorithm is a quantum secure computational indistinguishability obfuscator $i\mathcal{O}$, for a class of circuits $\mathcal{C}$, if the following conditions hold:*

1. `Functionality:` *For any circuit $C \in \mathcal{C}$, and for all inputs x*

$$i\mathcal{O}(C)(x) = C(x).$$

2. `Polynomial Slowdown:` *For every $C \in \mathcal{C}$, $|i\mathcal{O}(C)| \in poly(|C|)$.*

[1] ANNE: Is there an advantage in using quantum states to obfuscate programs? I would suspect that one big advantage would be unclonable programs (they cannot be copied). Is this too ambitious to look at? What does it even mean to have unclonable programs? (this links with work that I am currently doing with Sébastien Lord, a PhD student).

3. `Indistinguishability:` *For any two circuits $C_0, C_1 \in \mathcal{C}$, of the same size that compute the same function and for every polynomial time quantum distinguisher $\mathcal{D}_q$, there exists a negligible function* negl *such that:*

$$\left|\Pr[\mathcal{D}_q(i\mathcal{O}(C_0)) = 1] - \Pr[\mathcal{D}_q(i\mathcal{O}(C_1)) = 1]\right| \leq \text{negl}(|C_0|).$$

2.2 Basic Quantum Notions

[**?**] Given an n-bit string x, the corresponding quantum-computational n-qubit basis state is denoted $|x\rangle$. The 2^n-dimensional Hilbert space spanned by n-qubit basis states is denoted

$$\mathcal{H}_n := \mathbf{span}\left\{|x\rangle : x \in \{0,1\}^n\right\} .$$

We denote by $\mathcal{D}(\mathcal{H}_n)$ the set of density operators (i.e., valid quantum states) on $\mathcal{H}_n$. These are linear operators on $\mathcal{D}(\mathcal{H}_n)$ which are positive-semidefinite and have trace equal to 1. When considering different physical subsystems, we will denote them with uppercase Latin letters; when a Hilbert space corresponds to a subsystem, we will place the subsystem label in the subscript. For instance, if $F \cup G \cup H = [n]$ then $\mathcal{H}_n = \mathcal{H}_F \otimes \mathcal{H}_G \otimes \mathcal{H}_H$. Sometimes we will write explicitly the subsystems a state belongs to as subscripts; this will be useful when considering, *e.g.*, the reduced state on some of the subspaces. For example, we will sometimes express the statement $\rho \in \mathcal{D}(\mathcal{H}_F \otimes \mathcal{H}_G \otimes \mathcal{H}_H)$ simply by calling the state ρ_{FGH}; in that case, the state obtained by tracing out the subsystem H will be denoted ρ_{FG}.

Given $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, the trace distance between ρ and σ is given by half the trace norm $\|\rho - \sigma\|_1$ of their difference. When ρ and σ are classical probability distributions, the trace distance reduces to the total variation distance. Physically realizable maps from a state space $\mathcal{D}(\mathcal{H})$ to another state space $\mathcal{D}(\mathcal{H}')$ are called *admissible*—these are the completely positive trace-preserving (CPTP) maps. For the purpose of distinguishability via input/output operations, the appropriate norm for CPTP maps is the diamond norm, denoted $\|\cdot\|_\diamond$. The set of admissible maps coincides with the set of all maps realizable by composing (i.) addition of ancillas, (ii.) unitary evolutions, (iii.) measurements in the computational basis, and (iv.) tracing out subspaces. We remark that unitaries $U \in U(\mathcal{H}_n)$ act on $\mathcal{D}(\mathcal{H}_n)$ by conjugation: $\rho \mapsto U\rho U^\dagger$. The identity operator $\mathbb{1}_n \in U(\mathcal{H}_n)$ is thus both a valid map, and (when normalized by 2^{-n}) a valid state in $\mathcal{D}(\mathcal{H}_n)$—corresponding to the classical uniform distribution.

Quantum Gates

Recall the single-qubit Pauli operators defined as:

$$\mathsf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \mathsf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \mathsf{Y} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \qquad \mathsf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The Pauli operators are Hermitian and unitary quantum gates, i.e. $P^\dagger = P$ and $P^\dagger P = PP^\dagger = P^2 = I$ for all $P \in \{\mathsf{I}, \mathsf{X}, \mathsf{Y}, \mathsf{Z}\}$. It is easy to check that applying a uniformly random Pauli operator to any single-qubit density operator results in the maximally mixed state:

$$\frac{1}{4}\left(\rho + \mathsf{X}\rho\mathsf{X} + \mathsf{Y}\rho\mathsf{Y} + \mathsf{Z}\rho\mathsf{Z}\right) = \frac{\mathbb{1}_1}{2} \qquad \text{for all } \rho \in \mathcal{D}(\mathcal{H}_1)\,.$$

Since the Pauli operators are self-adjoint, we may implement the above map by choosing two bits s and t uniformly at random and then applying

$$\rho \mapsto \mathsf{X}^s\mathsf{Z}^t\rho\mathsf{Z}^t\mathsf{X}^s\,.$$

To observers with no knowledge of s and t, the resulting state is information-theoretically indistinguishable from $\mathbb{1}_1/2$. Of course, if we know s and t, we can invert the above map and recover ρ completely.

The above map can be straightforwardly extended to the n-qubit case in order to obtain an elementary *quantum encryption scheme* called the *quantum one-time pad*. We first set $\mathsf{X}_j = \mathbb{1}^{\otimes j-1} \otimes \mathsf{X} \otimes \mathbb{1}^{\otimes n-j}$ and likewise for Y_j and Z_j. We define the n-qubit Pauli group $\mathcal{P}_n$ to be the subgroup of $\mathrm{SU}(\mathcal{H}_n)$ generated by $\{\mathsf{X}_j, \mathsf{Y}_j, \mathsf{Z}_j : j = 1, \ldots, n\}$. Note that Hermiticity is inherited from the single-qubit case, i.e. $P^\dagger = P$ for every $P \in \mathcal{P}_n$.

Definition 2. Clifford Group: *The set of gates* $\{\mathsf{X}, \mathsf{Z}, \mathsf{P}, \mathsf{CNOT}, \mathsf{H}\}$ *applied to arbitrary wires (redundantly) generates the Clifford group, where*

$$\mathsf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathsf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \mathsf{P} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad \mathsf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \textit{and} \quad \mathsf{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

We note the following relations between these gates:

$$\mathsf{XZ} = -\mathsf{ZX}, \quad \mathsf{T}^2 = \mathsf{P}, \quad \mathsf{P}^2 = \mathsf{Z}, \quad \mathsf{HXH} = \mathsf{Z}, \quad \mathsf{TP} = \mathsf{PT}, \quad \mathsf{PZ} = \mathsf{ZP}.$$

Also, for any $a, b \in \{0, 1\}$ we have $\mathsf{HX}^b\mathsf{Z}^a = \mathsf{X}^a\mathsf{Z}^b\mathsf{H}$

Quantum Circuits and Algorithm

For $n \in \mathbb{N}$, the set of all $n \times n$ unitary matrix is denoted by $O(n, \mathbb{C}) = \{U \in \mathbb{C}^{n\times n} \mid U \cdot U^\dagger = \mathbf{I}\}$. We say a quantum circuit C_q computes $U \in O(n, \mathbb{C})$ if for every quantum state $|\psi\rangle \in Q(n)$,

$$U(|\psi\rangle) = C_q(|\psi\rangle),$$

where $Q(n)$ denote the set of all n-qubit states.

A quantum circuit that computes unitary matrix is called a reversible quantum circuit, i.e it always possible to uniquely recover the input, given the output. A set of gates are said to be universal if, for any a unitary matrix U a quantum circuit can be constructed for computing U using only gates from that set. It is a well known fact that Clifford gates are not universal, but adding any non-Clifford gate, such as T, gives a universal set of gates. The

$$\mathsf{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix},$$

A family of quantum circuit $C = \{C_n \in \mathbb{N} \mid\}$ one for each input size $n \in \mathbb{N}$ is called uniform if there exists a deterministic Turing machine M, such that

- For each $n \in \mathbb{N}$, M outputs a description of $C_n \in \mathcal{F}$ on input 1^n.
- For each $n \in \mathbb{N}$, M runs in $poly(n)$.

All quantum operations are not unitary (reversible), nevertheless a general (possibly irreversible) quantum operation also called superoperator can efficiently simulated by a reversible quantum operations by adding ancilla states to the original system, then perform a unitary operation on the joint system, and then tracing out Tr some subsystem []. More precisely, this can be described as the map:

$$\rho_{in} \xmapsto{\text{superoperator}} \rho_{out} = Tr_B(U(\rho_{in} \oplus |00\cdots0\rangle\langle 00\cdots0|)U^\dagger)$$

where $\rho_{in} \in \mathcal{H}_n$, is the original state and $|00\cdots0\rangle$ is an ancilla state of dimension at most n^2. A circuit that computes a general quantum operation is called a general quantum circuit. Therefore, general quantum circuit can refer to both reversible or irreversible circuits. A polynomial-time quantum algorithm is a uniform family of general quantum circuits.

Remark: From now we use the term quantum circuits to refer to reversible quantum circuits only and the term quantum algorithm is reserved for some family of general quantum circuits.

2.3 Correction and Update Functions for Clifford Circuits

For any Clifford gate $U \in \{\mathsf{X}, \mathsf{Z}, \mathsf{P}, \mathsf{CNOT}, \mathsf{H}\}$ we define a correction function f_U that relates U and the Pauli's X and Z matrices in the following manner.

$$\mathsf{X}(\mathsf{X}^b\mathsf{Z}^a) = (-1)^a(\mathsf{X}^b\mathsf{Z}^a)\mathsf{X}, \quad \text{where } f_{\mathsf{H}}(a,b) = (a,b), \text{ for any } a,b \in \{0,1\}.$$
$$\mathsf{Z}(\mathsf{X}^b\mathsf{Z}^a) = (-1)^b(\mathsf{X}^b\mathsf{Z}^a)\mathsf{Z}, \quad \text{where } f_{\mathsf{H}}(a,b) = (a,b), \text{ for any } a,b \in \{0,1\}.$$
$$\mathsf{H}(\mathsf{X}^b\mathsf{Z}^a) = (\mathsf{X}^a\mathsf{Z}^b)\mathsf{H}, \quad \text{where } f_{\mathsf{H}}(a,b) = (b,a), \text{ for any } a,b \in \{0,1\}.$$
$$\mathsf{P}(\mathsf{X}^b\mathsf{Z}^a) = ((-i)^b\mathsf{X}^a\mathsf{Z}^{a\oplus b})\mathsf{P}, \quad \text{where } f_{\mathsf{P}}(a,b) = (a, a\oplus b), \text{ for any } a,b \in \{0,1\}.$$
$$\mathsf{CNOT}(\mathsf{X}^{b_1}\mathsf{Z}^{a_1}\otimes\mathsf{X}^{b_2}\mathsf{Z}^{a_2}) = (\mathsf{X}^{b_1}\mathsf{Z}^{a_1\oplus a_2}\otimes\mathsf{X}^{b_1\oplus b_2}\mathsf{Z}^{a_2})\mathsf{CNOT}, \text{ where } f_{\mathsf{CNOT}}(a_1,b_1,a_2,b_2) = (a_1\oplus a_2, b_1, a_2, b_1\oplus b_2).$$

Similarly for any n-qubit Clifford Circuit[2] $\mathcal{C}_q$ we define an update function $F_{c_q} : \mathbb{F}_2^n \to \mathbb{F}_2^n$, that

[2] A Clifford circuit is a quantum circuit in which every gate is from the Clifford group.

relates $\mathcal{C}_q$ and a unitary $(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})$ in the following manner,

$$(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})\mathcal{C}_q = \mathcal{C}_q(\mathsf{X}^{\otimes_{i=1}^n b'_i} \cdot \mathsf{X}^{\otimes_{i=1}^n a'_i})$$

where $a_i, b_i, a'_i, b'_i \in \{0,1\}$ for all integers $1 \leq i \leq n$ and $F_{c_q}(a_1, b_1, a_2, b_2, \ldots a_n, b_n) = (a'_1, b'_1, \ldots, a'_n, b'_n)$. The update function F_{c_q} is computed by the composition of the correction functions of the gates in the circuit $\mathcal{C}_q$. For example consider a 2 qubit circuit Let $C_q = ((\mathrm{I} \otimes \mathsf{H}) \cdot (\mathsf{CNOT})$. The update function for this circuit is computed by first applying the f_{H} to the first two input bits and then f_{CNOT} to all four bits.

$$F_{C_q} = f_{\mathrm{CNOT}} \circ f_{\mathrm{H}}(a_1, b_1, a_2, b_2) = f_{\mathrm{CNOT}}(b_1, a_1, a_2, b_2) = (b_1 \oplus a_2, a_1, a_2, a_1 \oplus b_2).$$

And we have

$$(\mathsf{X}^{b_1} \otimes \mathsf{X}^{b_2})(\mathsf{Z}^{a_1} \otimes \mathsf{Z}^{a_2})C_q = C_q(\mathsf{X}^{a_1} \otimes \mathsf{X}^{a_1 \oplus b_2})(\mathsf{Z}^{b_1 \oplus a_2} \otimes \mathsf{Z}^{a_2}).$$

Bell Basis

We denote the four Bell states as $|\beta_{00}\rangle$, $|\beta_{01}\rangle$, $|\beta_{10}\rangle$ and $|\beta_{11}\rangle$.

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

2.4 Gate Teleportation

Suppose we want to evaluate a single qubit gate $U \in \{\mathsf{X}, \mathsf{Z}, \mathsf{P}, \mathsf{CNOT}, \mathsf{H}\}$ on some qubit $|\phi\rangle$. Then using gate teleportation we can compute $U(|\phi\rangle)$ as follows.

Algorithm 1 Gate Teleportation Protocol for Clifford Gates.

1. Prepare a 2 qubit Bell state $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle)}{\sqrt{2}}$.
2. Write the joint system as

$$|\phi\rangle|\beta_{00}\rangle = \frac{1}{2}|\beta_{00}\rangle|\phi\rangle + \frac{1}{2}|\beta_{01}\rangle(\mathsf{X}(|\phi\rangle)) + \frac{1}{2}|\beta_{10}\rangle(\mathsf{Z}(|\phi\rangle)) + \frac{1}{2}|\beta_{11}\rangle(\mathsf{XZ}(|\phi\rangle)).$$

   Where β_{ij}, denotes the 2 qubit Bell basis.

3. Apply U on the second qubit of the Bell state

$$\mathbb{I}\otimes\mathbb{I}\otimes U(|\phi\rangle|\beta_{00}\rangle) = \frac{1}{2}|\beta_{00}\rangle U(|\phi\rangle) + \frac{1}{2}|\beta_{01}\rangle U(\mathsf{X}(|\phi\rangle)) + \frac{1}{2}|\beta_{10}\rangle U(\mathsf{Z}(|\phi\rangle)) + \frac{1}{2}|\beta_{11}\rangle U(\mathsf{XZ}(|\phi\rangle)).$$

4. Measure the first two qubits in the Bell basis and obtain the classical bits (a, b). The system now in the state Z

$$|\psi\rangle_{AB} = |\beta_{ab}\rangle \otimes U(\mathsf{X}^b\mathsf{Z}^a(|\phi\rangle)). \tag{1}$$

5. Compute the correction function $f_U(a, b) = (a', b')$ (see section 2.3).
6. Apply the correction unitary $\mathsf{Z}^{a'}\mathsf{X}^{b'}$ to the system $Tr_A(|\psi\rangle_{AB})$ and recover $U(|\phi\rangle)$.

$$\mathsf{Z}^{a'}\mathsf{X}^{b'}(Tr_A(|\psi\rangle_{AB})) = \mathsf{Z}^{a'}\mathsf{X}^{b'}U(\mathsf{X}^b\mathsf{Z}^a(|\phi\rangle)) = (\mathsf{Z}^{a'}\mathsf{X}^{b'})(\mathsf{X}^{b'}\mathsf{Z}^{a'})U(|\phi\rangle) = U(|\phi\rangle)$$

Remark. *Using gate teleportation we can also evaluate any non Clifford gates such as* T*, however, the correction unitary becomes more complicated.*

$$\mathsf{T}\mathsf{Z}^a\mathsf{X}^b = \mathsf{X}^b\mathsf{Z}^{a\oplus}\mathsf{P}^b\mathsf{T}$$

3 Quantum Indistinguishability Obfuscation

3.1 Definitions

Definition 3. (Equivalent Quantum Circuits): *Let C_{q_0} and C_{q_1} be two n-qubit quantum circuits. We say C_{q_0} and C_{q_1} are equivalent if for every state $|\psi\rangle \in Q(n)$*

$$C_{q_1}(|\psi\rangle) = C_{q_2}(|\psi\rangle).$$

Definition 4. (Quantum Indistinguishability Obfuscation) *A polynomial-time quantum algorithm for a class of quantum circuits $\mathcal{C}_Q$ is a quantum (computational) indistinguishability obfuscator $Qi\mathcal{O}$ if the following conditions hold:*

1. `Functionality:` *For every* $C_q \in \mathcal{C}_Q$ *and every quantum state* $|\phi\rangle$,

$$(\rho, C'_q) \leftarrow Qi\mathcal{O}(C_q) \quad \textit{and} \quad C'_q(\rho, |\phi\rangle) = C_q(|\phi\rangle)$$

2. `Polynomial Slowdown:` *For every* $C_q \in \mathcal{C}_Q$,

   - $\rho \in Q(poly(|C_q|))$, *i.e.* ρ *is at most a* $poly(|C_q|)$ *qubit state.*
   - $|C'_q| \in poly(|C_q|)$.

3. `Indistinguishability:` *For any two equivalent quantum circuits* $C_{q_1}, C_{q_2} \in \mathcal{C}_Q$, *of the same size and for every polynomial-time quantum distinguisher* $\mathcal{D}_q$, *there exists a negligible function* negl *such that:*

$$\left|\Pr[\mathcal{D}_q(Qi\mathcal{O}(C_{q_1})) = 1] - \Pr[\mathcal{D}_q(Qi\mathcal{O}(C_{q_2})) = 1]\right| \leq \text{negl}(k).$$

Where $k = |C_{q_1}| = |C_{q_2}|$.

3.2 Quantum Indistinguishability Obfuscation for Clifford Circuits

In this section we present two methods to obfuscate any Clifford circuit, one using a canonical form and the other using the gate teleportation.

3.2.1 Quantum Indistinguishability Obfuscation using Canonical Form

Aronson and Gottesman invented a polynomial-time algorithm that computed a canonical form of any Clifford circuit [**?**]. Their algorithm (we denote as `AG-Canonical`, page 8 - 9 [**?**]) takes a tabula (binary matrix) related to a Clifford circuit as an input and output its canonical form. Unfortunately, this canonical form may not always be unique. To see this we briefly recap the idea behind their algorithm. An n qubit state can be represented by a binary tableau consist of $2n$ rows and $2n + 1$ columns, where $x_{i,j}, z_{i,j} \in \{0, 1\}$.

$$\left(\begin{array}{ccc|ccc|c} z_{11} & \cdots & z_{1n} & x_{11} & \cdots & x_{1n} & r_1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ z_{n1} & \cdots & z_{nn} & x_{n1} & \cdots & x_{nn} & r_n \\ \hline z_{(n+1)1} & \cdots & z_{(n+1)n} & x_{(n+1)1} & \cdots & x_{(n+1)n} & r_{n+1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ z_{(2n)1} & \cdots & z_{(2n)n} & x_{(2n)1} & \cdots & x_{(2n)n} & r_{2n} \end{array}\right)$$

Each row of the tableau $R_i = \pm(P_1 \otimes \cdots \otimes P_n) \in \mathcal{P}_n$, for $1 \leq i \leq 2n$, where bits (x_{ij}, z_{ij}) determine the j^{th} Pauli gate P_j: 00 means I, 01 means X, 11 means Y, and 10 means Z and r_i is 1 if R_i has negative phase and 0 if r_i has positive phase. Rows 1 to n of the tableau represent

the destabilizer generators $R_1, \ldots, R_n$ and rows $n+1$ to $2n$ represent the stabilizer generators $R_{n+1}, \ldots, R_{2n}$ of the state it represents.

For example for the 2-qubit state $|00\rangle$ a possible tableau is

$$\left(\begin{array}{cc|cc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

and the stabilizers for the state are $R_3 = +(\mathsf{Z} \otimes \mathsf{I})$ and $R_4 = +(\mathsf{I} \otimes \mathsf{Z})$. Note if we swap row 3 with row 4, then we get another tableau for the state $|00\rangle$, therefore a quantum state can be represented by more than one tableau. Now suppose we want to compute a canonical form of an n qubit Clifford circuit C_q. Let $\mathcal{T}_i$ be a initial tableau representing the state $|0\rangle^{\otimes n}$. As we proceeds through the gates in C_q; we update $\mathcal{T}_i$ according to the following rules [**?**].

CNOT from control a to target b. For all $i \in \{1, \ldots, 2n\}$, set $r_i := r_i \oplus x_{ia} z_{ib} \, (x_{ib} \oplus z_{ia} \oplus 1)$, $x_{ib} := x_{ib} \oplus x_{ia}$, and $z_{ia} := z_{ia} \oplus z_{ib}$.

Hadamard on qubit a. For all $i \in \{1, \ldots, 2n\}$, set $r_i := r_i \oplus x_{ia} z_{ia}$ and swap x_{ia} with z_{ia}.

Phase on qubit a. For all $i \in \{1, \ldots, 2n\}$, set $r_i := r_i \oplus x_{ia} z_{ia}$ and then set $z_{ia} := z_{ia} \oplus x_{ia}$.

Let $\mathcal{T}_f$ be the final tableau representing the state $C_q(|0\rangle^{\otimes n})$. Note the state $|0\rangle^{\otimes n}$ can be represented by more than one possible initial tableaus. Now suppose we have another circuit C_q' that is equivalent to C_q. Let $\mathcal{T}_i' \neq \mathcal{T}_i$ be a initial tableau representing the state $|0\rangle^{\otimes n}$. Let $\mathcal{T}_f'$ be the final tableau representing the state $C_q'(|0\rangle^{\otimes n})$. Then it is possible that $\mathcal{T}_f \neq \mathcal{T}_f'$. Moreover, the algorithm `AG-Canonical` takes $\mathcal{T}_f$ as a input and compute a canonical form as follows: First apply $\mathsf{CNOT}, \mathsf{H}$ and P to $\mathcal{T}_f$ in a sequence (denoted by S_G) to obtain standard initial tableau $[\mathbf{I}_{2n}|\mathbf{0}]$. Then the canonical form of C_q is given by the sequence S_G. This means, the output of `AG-Canonical` may be different for C_q from C_q' if $\mathcal{T}_f \neq \mathcal{T}_f'$. For example, $C_q = \mathsf{I} \otimes \mathsf{I}$ and $C_q' = (\mathsf{I} \otimes \mathsf{H}) \cdot (\mathsf{I} \otimes \mathsf{H})$ are equivalent circuits. Let Let $\mathcal{T}_i$ and $\mathcal{T}_i'$ denote initial tableaus for the state $|0\rangle^{\otimes 2}$.

$$\mathcal{T}_i = \left(\begin{array}{cc|cc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right) \quad \text{and} \quad \mathcal{T}_i' = \left(\begin{array}{cc|cc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right)$$

After running C_q and C_q' on the state $|0\rangle^{\otimes 2}$ and updating their initial tableaus according to the above rules, we have $\mathcal{T}_f = \mathcal{T}_i \neq \mathcal{T}_f' = \mathcal{T}_i'$. Then we calculate the canonical form of using `AG-Canonical` on input $\mathcal{T}_f$ and $\mathcal{T}_f'$, then we cannot possibly apply to both final tableau the same sequence of $\mathsf{CNOT}, \mathsf{H}$ and P to obtain the initial tableau, therefore the output of `AG-Canonical` is a different canonical form for C_q from C_q'.

However, one can trivially modified the algorithm (`AG-Canonical`) [**?**] so that it always outputs a unique canonical form. We add the following initial lines of code to `AG-Canonical` and called

this new algorithm `AG-Canonical-Unique`. The main difference between two algorithms is that `AG-Canonical-Unique` takes a circuit as an input instead of a tableau (see below).

Algorithm 1 Unique Canonical form for Clifford Circuits (`AG-Canonical-Unique`)

Input: A n qubit Clifford Circuit C_q.

1. Set $\mathcal{T}_i = [\mathbf{I}_{2n}|\mathbf{0}] \in \{0,1\}^{2n\times 2n+1}$ be the standard initial tableau representing the state $|0\rangle^{\otimes n}$.
2. Compute the final tableau $\mathcal{T}_f$ by running $\mathcal{T}_i$ on C_q.
3. Compute and output `AG-Canonical`$(\mathcal{T}_f)$.

Lemma 3.1. *The* `AG-Canonical-Unique` *computes a unique canonical form for Clifford Circuits in polynomial-time.*

Proof. The cost of computing the final tableau for any n qubit Clifford circuit is a $O(poly(n|C_q|))$ ([**?**]) and the cost of `AG-Canonical` is also $O(poly(n|C_q|))$ ([**?**]). Therefore, `AG-Canonical-Unique` runs in polynomial-time. Moreover, Aronson and Gottesman proved in [**?**] that if C_{q_1} and C_{q_2} are two Clifford circuits and $\mathcal{T}_{f_1}$ and $\mathcal{T}_{f_2}$ are their final tableaus obtained by running them on the standard initial tableau, then C_{q_1} and C_{q_2} are equivalent if and only if $\mathcal{T}_{f_1} = \mathcal{T}_{f_2}$. This means the final tableau $\mathcal{T}_f$ obtain in `AG-Canonical-Unique` is the same for every equivalent Clifford circuit. Therefore, the output of `AG-Canonical` is the same for every equivalent circuit. Therefore `AG-Canonical-Unique` computes a unique canonical form for Clifford circuits. □

Quantum Indistinguishability Obfuscator: The quantum indistinguishability obfuscator $Qi\mathcal{O}$ for Clifford circuits is a pair of polynomial-time algorithm $(\mathcal{O}, \mathcal{T})$ such that

$$(|\rho\rangle, C'_q) \leftarrow (\mathcal{O}(C_q)),$$

Where $|\rho\rangle$, is an empty register and $C'_q \leftarrow$ `AG-Canonical-Unique`(C_q). The algorithm $\mathcal{T}$ takes C'_q and $|\phi\rangle$ as an input and compute the C'_q on $|\phi\rangle$. Note the canonical form reveals no knowledge about the input circuit, therefore this $Qi\mathcal{O}$ is perfectly secure against any quantum adversary for Clifford circuits.

3.2.2 Using Gate Teleportation

In this section we will show that how gate teleportation can be used to obfuscate Clifford circuits. Our protocol relies on the assumption that there exists a quantum secure $i\mathcal{O}$, but to this date there is no known provably quantum secure $i\mathcal{O}$ exists for general circuits. However, our protocol

relies on the assumption that a quantum secure $i\mathcal{O}$ exists for a very specific class of functions (update functions). In fact, a provably quantum secure $i\mathcal{O}$ for the update functions corresponding to Clifford circuits can easily be constructed (see section 3.3). We assume that a quantum secure $i\mathcal{O}$ is hard coded in the algorithm $\mathcal{O}$.

Algorithm 2 $\mathcal{O}$ of $Qi\mathcal{O}_{\text{Clifford}}$

- Input: A n qubit Clifford Circuit C_q.
  1. Prepare $2n$ qubit Bell state $|\beta^{2n}\rangle = |\beta_{00}\rangle \otimes \cdots \otimes |\beta_{00}\rangle$.
  2. Apply the circuit C_q on the lower half of the qubits $|\psi\rangle = (I \otimes C_q)|\beta^{2n}\rangle$.
  3. Compute the circuit C of update function F_{C_q}.
  4. Output $(|\psi\rangle, i\mathcal{O}(C))$.

Algorithm 3 $\mathcal{T}$ of $Qi\mathcal{O}_{\text{Clifford}}$

- Input $\left(|\psi\rangle, i\mathcal{O}(F_{C_q}), n\right)$, where $\left(|\psi\rangle, i\mathcal{O}(F_{C_q})\right) = \mathcal{O}(C_q, 1^n)$.
  1. Measure the first $2n$ qubits of the system $|\phi\rangle \otimes |\psi\rangle$ in the Bell basis and obtain the classical output $(a_1, b_1, \ldots, a_n, b_n)$.
  2. Now last n qubits are in the state $C_q(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})(|\phi\rangle) = (\mathsf{X}^{\otimes_{i=1}^n b'_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a'_i})C_q(|\phi\rangle)$.
  3. Compute the correction bits $(a'_1, b'_1, \ldots, a'_n, b'_n) = i\mathcal{O}(F_{C_q})(a_1, b_1, \ldots, a_n, b_n)$.
  4. Apply $(\mathsf{X}^{\otimes_{i=1}^n b'_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a'_i})$ to the system $C_q(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})(|\phi\rangle)$ and obtain $C_q(|\phi\rangle)$.

Theorem 3.2. *If $i\mathcal{O}$ is a quantum secure classical indistinguishability obfuscation, then $Qi\mathcal{O}_{\text{Clifford}}$ is a quantum Indistinguishability Obfuscation for all Clifford Circuits.*

Proof:

- `Functionality:` The functionality $Qi\mathcal{O}_{\text{Clifford}}$ is followed from the gate teleportation.
- `Polynomial Slowdown:` We first show that $\mathcal{O}$ and $\mathcal{T}$ runs in polynomial-time. Note step 1 and Step 2 of $\mathcal{O}$ cost at most $O(n|C_q|)$. The function F_{C_q} takes $2n$ bits as an input and outputs $2n$ by only performing **XOR** or **Swap** operations on the input bits as its passes through each layer of the gates in C_q. There can be at most $|C_q|$ layers, so the total number of **XOR** or **Swap** operations required to compute F_{C_q} are in $O(n|C_q|)$. Therefore, F_{C_q} can be computed by a circuit C of size at most $poly(n|C_q|)$ and $\mathcal{O}$ runs in polynomial-time. Moreover, $|\psi\rangle$ is a $2n$ qubit quantum state and the output of $i\mathcal{O}$ is by definition a polynomial in the input size.

- `Indistinguishability:` Let C_{q_1} and C_{q_2} be two n qubits equivalent Clifford circuits and

$$\big(|\psi_1\rangle, i\mathcal{O}(F_{C_{q_1}})\big) = Qi\mathcal{O}_{\text{Clifford}}(C_{q_2}) \text{ and } \big(|\psi_2\rangle, i\mathcal{O}(F_{C_{q_2}})\big) = Qi\mathcal{O}_{\text{Clifford}}(C_{q_2})$$

Note

$$|\psi_1\rangle = (I \otimes C_{q_1})|\beta^{2n}\rangle = (I \otimes C_{q_2})|\beta^{2n}\rangle = |\psi_2\rangle.$$

And from Theorem 3.3 we have $F_{C_{q_1}} = F_{C_{q_2}}$ therefore if $i\mathcal{O}$ is a quantum indistinguishability obfuscation then the output of al is a quantum Indistinguishability Obfuscation for all Clifford Circuits.

Theorem 3.3. *Let C_{q_1} and C_{q_2} be two equivalent Clifford circuits and $F_{C_{q_1}}$ and $F_{C_{q_2}}$ denote the update functions for the circuits C_{q_1} and C_{q_2}, then $F_{C_{q_1}} = F_{C_{q_2}}$.*

Proof: For any n-qubit state $|\psi\rangle$ we have $C_{q_1}(|\psi\rangle) = C_{q_2}(|\psi\rangle)$. If we use Circuit teleportation protocol to compute $C_1(|\psi\rangle)$ and $C_{q_2}(|\psi\rangle)$, After measurement and tracing out the bell states the system corresponding to the circuit C_{q_1} and C_{q_2} are in the states.

$$C_{q_1}(\mathrm{U}|\psi\rangle) = \mathrm{U}_{C_{q_1}} C_{q_1}(|\psi\rangle)(\text{ and } C_{q_2}(\mathrm{U}|\psi\rangle) = \mathrm{U}_{C_{q_2}}(C_{q_2}(|\psi\rangle)))$$

Where

$$\mathrm{U} = (X^{\otimes_{i=1}^n b_i} \cdot Z^{\otimes_{i=1}^n a_i}),$$
$$\mathrm{U}_{C_{q_1}} = (X^{\otimes_{i=1}^n b'_i} \cdot Z^{\otimes_{i=1}^n a'_i}),$$
$$\mathrm{U}_{C_{q_2}} = (X^{\otimes_{i=1}^n e'_i} \cdot Z^{\otimes_{i=1}^n d'_i}).$$
$$F_{C_{q_1}}(a_1, b_1, \ldots, a_n, b_n) = (a'_1, b'_1, \ldots, a'_n, b'_n) \text{ and } F_{C_{q_2}}(d_1, e_1, \ldots, d_n, e_n) = (d'_1, e'_1, \ldots, d'_n, e'_n)$$

We have

$$C_{q_1}(|\psi\rangle) = (\mathrm{U}^\dagger_{C_{q_1}} \mathrm{U}_{C_{q_1}}) C_{q_1}(|\psi\rangle) = \mathrm{U}^\dagger_{C_{q_1}}(C_{q_1}(\mathrm{U}(|\psi\rangle))$$
$$= \mathrm{U}^\dagger_{C_{q_1}}(C_{q_2}(\mathrm{U}(|\psi\rangle))), [C_{q_1} \text{ and } C_{q_2} \text{ are equivalent }]$$
$$= \mathrm{U}^\dagger_{C_{q_1}} \mathrm{U}_{C_{q_2}}(C_{q_2}(|\psi\rangle)) = C_{q_2}(|\psi\rangle)$$
$$\implies \mathrm{U}^\dagger_{C_{q_1}} \mathrm{U}_{C_{q_2}} = \mathbf{I} \iff \mathrm{U}_{C_{q_1}} = \mathrm{U}_{C_{q_2}}$$

By Lemma 3.4 (next page) we have that $F_{C_{q_1}} = F_{C_{q_2}}$.

Lemma 3.4. *Let C_{q_1} and C_{q_2} be two equivalent Clifford circuits, then $F_{C_{q_1}} = F_{C_{q_2}}$ if and only if $\mathrm{U}_{C_{q_1}} = \mathrm{U}_{C_{q_2}}$.*

Proof: ($p \Rightarrow q$) Suppose $F_{C_{q_1}} = F_{C_{q_2}}$ then clearly $\mathrm{U}_{C_{q_1}} = \mathrm{U}_{C_{q_2}}$.

Now to proof ($q \Rightarrow p$) Suppose $\mathrm{U}_{C_{q_1}} = \mathrm{U}_{C_{q_2}}$ and $F_{C_{q_1}} \neq F_{C_{q_2}}$, then there exists a binary string $(a_1, b_1, \ldots, a_n, b_n)$ such that

$$F_{C_{q_1}}(a_1, b_1, \ldots, a_n, b_n) \neq F_{C_{q_2}}(a_1, b_1, \ldots, a_n, b_n)$$

Since $\mathrm{U}_{C_{q_1}}(|\psi\rangle) = \mathrm{U}_{C_{q_2}}(|\psi\rangle)$ for every n-qubit state $|\psi\rangle$. Let

$$|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle$$

where $|\phi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$, $\alpha_i \neq 0$ and $\beta_i \neq 0$, for every integer $1 \leq i \leq n$.

$$\mathrm{U}_{C_{q_1}}(|\psi\rangle) = \Big(\alpha_1|0 + a'_1\rangle + (-1)^{b'_1}(i)^{c'_1}\beta_1|1\rangle\Big) \otimes \cdots \otimes \Big(\alpha_n|0 + a'_n\rangle + (-1)^{b'_n}(i)^{c'_i}\beta_n|1\rangle\Big)$$

$$\mathrm{U}_{C_{q_2}}(|\psi\rangle) = \Big(\alpha_1|0 + d'_1\rangle + (-1)^{e'_1}(i)^{f'_1}\beta_1|1\rangle\Big) \otimes \cdots \otimes \Big(\alpha_n|0 + d'_n\rangle + (-1)^{e'_n}(i)^{f'_i}\beta_n|1\rangle\Big)$$

For any i if $a'_i \neq d'_i$ or $b'_i \neq e'_i$ or $c'_i \neq f'_i$ then the output $\mathrm{U}_{C_{q_1}}(|\psi\rangle)$ will differ from $\mathrm{U}_{C_{q_2}}(|\psi\rangle)$ on the i-th qubit. Which is a contraction to the assumption that $\mathrm{U}_{C_{q_1}} = \mathrm{U}_{C_{q_2}}$. Therefore $F_{C_{q_1}} = F_{C_{q_2}}$.

3.3 Indistinguishability Obfuscation for the Clifford Update Functions

In this section we present a (classical) $i\mathcal{O}$ that can obfuscate the update function F_{C_q}, for any n qubit Clifford circuit C_q.

Algorithm 4 $i\mathcal{O}$ for Clifford update Functions $F_{\texttt{Clifford}}$

- Input: A n qubit Clifford Circuit C_q, a security parameter 1^n.
  1. Compute $C_{q_c} \leftarrow \texttt{Canonical}(C_q)$.
  2. Compute the update function $F_{C_{q_c}}$.
  3. Output $F_{C_{q_c}}$.

4 Obfuscating Beyond Clifford Circuits

Here, we show how to build iO for quantum circuit families that satisfy Definition 2.

4.0.1 Using a Canonical Form

Main idea: Each Clifford layer is obfuscated using the canonical form. The T gate layers are given in the clear. The result is a canonical form, since the family is selected such that the description just given will be a canonical form.

4.0.2 Using Gate Teleportation

As mentioned in the section2 that adding a non-Clifford gates such as T to Clifford gates gives us a generating set for all quantum circuits. The T relates to the X, Z

$$\mathsf{T}\mathsf{X}^b\mathsf{Z}^a = \mathsf{X}^b\mathsf{Z}^{a\oplus b}\mathsf{P}^b$$

Now suppose we want evaluate the circuit HT on some qubit $|\phi\rangle$ using gate teleportation, then

$$\mathsf{HT}\mathsf{X}^b\mathsf{Z}^a(|\phi\rangle) = \mathsf{X}^{b\oplus a}\mathsf{Z}^b\mathsf{H}\mathsf{P}^b\mathsf{T}(|\phi\rangle)$$

If $b = 0$, then we don't have to worry about P correction, otherwise we have to perform a P correction which is a problem since H and P does not compute. However we can write $\mathsf{P} = (\frac{1+i}{2})\mathsf{I} + (\frac{1-i}{2})\mathsf{Z}$

$$\begin{aligned}
\mathsf{HT}\mathsf{X}^b\mathsf{Z}^a(|\phi\rangle) &= \mathsf{X}^{a\oplus b}\mathsf{Z}^b\left(\left(\frac{1+i}{2}\right)\mathsf{H} + \left(\frac{1-i}{2}\right)\mathsf{H}\mathsf{Z}^b\right)\mathsf{T}(|\phi\rangle) \\
&= \mathsf{X}^{a\oplus b}\mathsf{Z}^b\left(\left(\frac{1+i}{2}\right)\mathsf{I} + \left(\frac{1-i}{2}\right)\mathsf{X}^b\right)\mathsf{H}\mathsf{T}(|\phi\rangle) \\
&= \left(\alpha_1\mathsf{X}^{a\oplus b}\mathsf{Z}^b + \alpha_2\mathsf{X}^a\mathsf{Z}^b\right)\mathsf{H}\mathsf{T}(|\phi\rangle),
\end{aligned}$$

where $\alpha_1 = \left(\frac{1+i}{2}\right)$ and $\alpha_2 = (-1)^b\left(\frac{1-i}{2}\right)$. For this particular our correction unitary requited at most two complex numbers and four bits. In fact for any 1-qubit the correction need to store at most fours complex numbers and eights bits. Therefore, the update function for any 1-qubit quantum circuit is

$$F_{C_q} : \mathbb{F}_2^2 \longrightarrow \mathbb{C}^4 \times \mathbb{F}_2^8, \qquad (a, b) \longrightarrow ((\alpha_1, \alpha_2, \alpha_3, \alpha_4), (a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4)).$$

and corresponds to the correction unitary $\sum_{i=1}^{4} \alpha_i\mathsf{X}^{b_i}\mathsf{Z}^{a_i}$. In general, to evaluate a n-qubit quantum circuit C_q with k number of T, the update function is

$$F_{C_q} : \mathbb{F}_2^n \longrightarrow \mathbb{C}^{l_1} \times \mathbb{F}_2^{l_2}, \text{ where } l_1 = n \cdot 4^k,\ l_2 = 2n \cdot 4^k,$$

$$\sum_{j=1}^{4^k}\left(\alpha_{1j}\mathsf{X}^{b_{1j}}\mathsf{Z}^{a_{1j}} \otimes \alpha_{2j}\mathsf{X}^{b_{2j}}\mathsf{Z}^{a_{2j}} \otimes \cdots \otimes \alpha_{nj}\mathsf{X}^{b_{nj}}\mathsf{Z}^{a_{nj}}\right)$$

where $a_{ij}, b_{ij} \in \mathbb{F}_2, \alpha_{ij} \in \mathbb{C}$ and $\frac{1}{2^k} \leq |\alpha_{ij}| \leq k$. Therefore, we can efficiently obfuscate any quantum circuit as far as the number of T gates in it are at most $O(\log(n))$.

Here we use an idea related to [**?**, **?**]. See Figure 8 in [**?**]. We leave EPR pairs at each T-gate layer, and after the gate teleportation, use iO on a program that will decide whether or not the P-gate correction needs to be applied. Have to ask Anne about the relevance of [**?**]

5 Conclusion and Open Questions

The main open questions related to this work are:

$i\mathcal{O}$ obfuscation for general quantum circuits

applications of gate-teleportation based quantum $i\mathcal{O}$ (for instance, to unclonable programs [**?**]).

Acknowledgements

This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-17-1-0083, Canada's NSERC, an Ontario ERA, and the University of Ottawa's Research Chairs program.

References

References

References