# Constructions for Quantum Indistinguishability Obfuscation

Anne Broadbent * Raza Ali Kazmi, †

**Abstract**

An *indistinguishability obfuscator* is a probabilistic polynomial-time algorithm that takes a circuit as input and outputs a new circuit that has the same functionality as the input circuit, such that for any two circuits of the same size that compute the *same* function, the outputs of the indistinguishability obfuscator are indistinguishable. Here, we study schemes for indistinguishability obfuscation for *quantum* circuits. We present two definitions for indistinguishability obfuscation: in our first definition ($qi\mathcal{O}$) the outputs of the obfuscator are required to be indistinguishable if the input circuits are perfectly equivalent, while in our second definition ($qi\mathcal{O}_{\mathbf{D}}$), the outputs are required to be indistinguishable as long as the input circuits are approximately equivalent with respect to a pseudo-distance $\mathbf{D}$. Our main results provide (1) a computationally-secure scheme for $qi\mathcal{O}$ where the size of the output of the obfuscator is exponential in the number of non-Clifford ($\mathsf{T}$ gates), which means that the construction is efficient as long as the number of $\mathsf{T}$ gates is logarithmic in the circuit size and (2) a statistically-secure $qi\mathcal{O}_{\mathbf{D}}$, for circuits that are close to the $k$th level of the Gottesman-Chuang hierarchy (with respect to $\mathbf{D}$); this construction is efficient as long as $k$ is small and fixed.

## 1 Introduction

At the intuitive level, an *obfuscator* is a probabilistic polynomial-time algorithm that transforms a circuit $C$ into another circuit $C'$ that has the same functionality as $C$ but that does not reveal anything about $C$, except its functionality *i.e.*, anything that can be learned from $C'$ about $C$ can also be learned from black-box access to the input-output functionality of $C$. This concept is formalized in terms of *virtual black-box obfuscation*, and was shown [12] to be unachievable in general. Motivated by this impossibility result, the same work proposed a weaker notion called *indistinguishability obfuscation* ($i\mathcal{O}$).

*University of Ottawa, Department of Mathematics and Statistics, abroadbe@uottawa.ca
†Fintech Reseach, Bank of Canada RKazmi@bank-banque-canada.ca

In the classical case, an *indistinguishability obfuscator* is a probabilistic polynomial-time algorithm that takes a circuit $C$ as input and outputs a circuit $i\mathcal{O}(C)$ such that $i\mathcal{O}(C)(x) = C(x)$ for all inputs $x$ and the size of $i\mathcal{O}(C)$ is at most polynomial in the size of $C$. Moreover, it must be that for any two circuits $C_1$ and $C_2$ of the same size and that compute the same function, their obfuscations are computationally indistinguishable. It is known that $i\mathcal{O}$ achieves the notion of *best possible obfuscation*, which states that any information that is not hidden by the obfuscated circuit is also not hidden by any circuit of similar size computing the same functionality [30]. Indistinguishability obfuscation is a very powerful cryptographic tool which is known to enable, among others: digital signatures, public key encryption [40], multiparty key agreement, broadcast encryption [15], fully homomorphic encryption [20] and witness-indistinguishable proofs [14]. Notable in the context of these applications is the *punctured programming technique* [40] which manages to render an $i\mathcal{O}(C)$ into an intriguing cryptographic building block, and this, despite that fact that the security guarantees of $i\mathcal{O}(C)$ appear quite weak as they are applicable only if the two original circuits have *exactly* the same functionality.

The first candidate construction of $i\mathcal{O}$ was published in [26], with security relying on the presumed hardness of multilinear maps [22, 28, 36]. Unfortunately, there have been many quantum attacks on multilinear maps [6, 21, 23]. Recently, new $i\mathcal{O}$ schemes were proposed under different assumptions [10, 27, 34]. Whether or not these schemes are resistant against quantum attacks remains to be determined.

Indistinguishability obfuscation has been studied for *quantum* circuits in [4, 5]. In a nutshell (see Section 1.2 for more details), [5] shows a type of obfuscation for quantum circuits, but without a security reduction. On the other hand, the focus of [4] is on impossibility of obfuscation for quantum circuits in a variety of scenarios. Thus, despite these works, until now, the achievability of indistinguishability obfuscation for quantum circuits has remained wide open.

## 1.1 Overview of Results and Techniques

Our contribution establishes indistinguishability obfuscation for certain families of quantum circuits. Below we overview each of our two main definitions, and methods to achieve them. We then compare the two approaches:

### 1.1.1 Indistinguishability obfuscation for quantum circuits

First, we define indistinguishability obfuscation for quantum circuits ($qi\mathcal{O}$) (Section 3) as an extension of the conventional classical definition. This definition specifies that on input a classical description of a quantum circuit $C_q$, the obfuscator outputs a *pair* $(|\phi\rangle, C'_q)$, where $|\phi\rangle$ is an auxiliary quantum state and $C'_q$ is a quantum circuit. For correctness, we require that $||C'_q(|\phi\rangle, \cdot) - C_q(\cdot)||_\diamond = 0$, whereas for security, we require that, on input two functionally equivalent quantum circuits, the outputs of $qi\mathcal{O}$ are indistinguishable. As a straightforward extension of the classical results, we then argue that *inefficient* indistinguishability

obfuscation exists.

In terms of constructing $qi\mathcal{O}$, we first focus on the family of *Clifford* circuits and show two methods of obfuscation: one straightforward method based on the canonical representation of Cliffords, and another based on the principle of gate teleportation [32]. Clifford circuits are quantum circuits that are built from the gate-set $\{\mathsf{X}, \mathsf{Z}, \mathsf{P}, \mathsf{CNOT}, \mathsf{H}\}$. They are known not to be universal for quantum computation and are, in a certain sense, the quantum equivalent of classical *linear circuits*. It is known that Clifford circuits can be efficiently simulated on a classical computer [31]; however, note that this simulation is with respect to a *classical* distribution, hence for a purely quantum computation, quantum circuits are required, which motivates the obfuscation of this circuit class. Furthermore, Clifford circuits are an important building block for fault-tolerant quantum computing, for instance, due to the fact that Cliffords admit transversal computations in many fault-tolerant codes. We provide two methods to achieve $qi\mathcal{O}$ for Clifford circuits.

**Obfuscating Cliffords using a canonical form.** Our first construction of $qi\mathcal{O}$ for Clifford circuits starts with the well-known fact that a canonical form is an $i\mathcal{O}$. We point out that a canonical form for Clifford circuits was presented in [2]; this completes this construction (we also note that an alternative canonical form was also presented in [41]). This canonical form technique does not require any computational assumptions. Moreover, the obfuscated circuits are classical, and hence can be easily communicated, stored, used and copied.

**Obfuscating Cliffords using gate teleportation.** Our second construction of $qi\mathcal{O}$ for Clifford circuits takes a very different approach. We start with the gate teleportation scheme [32]: according to this, it is possible to *encode* a quantum computation $C_q$ into a quantum state (specifically, by preparing a collection of entangled qubit pairs, and applying $C_q$ to half of this preparation). Then, in order to perform a quantum computation on a target input $|\psi\rangle$, we *teleport* $|\psi\rangle$ *into* the prepared entangled state. This causes the state $|\psi\rangle$ to undergo the evolution of $C_q$, *up to some corrections*, based on the teleportation outcome. If $C_q$ is chosen from the Clifford circuits, these corrections are relatively simple[1] and thus we can use a classical $i\mathcal{O}$ to provide the correction function. In contrast to the previous scheme, the gate teleportation scheme requires the assumption of quantum-secure classical $i\mathcal{O}$ for a certain family of functions (Section 2.14) and the obfuscated circuits include a quantum system. While this presents a technological challenge to communication, storage and also usage, there could be advantages to storing quantum programs into quantum states, for instance to take advantage of their *uncloneability* [1, 19].

**Obfuscating Beyond Cliffords.** Next, in our main result for Section 5, we generalize the gate teleportation scheme for Clifford circuits, and show a $qi\mathcal{O}$

[1]The correction is a tensor products of *Pauli* operators, which is computed as a function of $C_q$ and of the teleportation outcome.

obfuscator for all quantum circuits where the number of non-Clifford gates is at most logarithmic in the circuit size. For this, we consider the commonly-used Clifford+$\mathsf{T}$ gate-set, and we note that the $\mathsf{T}$ relates to the $\mathsf{X}, \mathsf{Z}$ as: $\mathsf{T}\mathsf{X}^b\mathsf{Z}^a = \mathsf{X}^b\mathsf{Z}^{a\oplus b}\mathsf{P}^b\mathsf{T}$. This means that, if we implement a circuit $C$ with $\mathsf{T}$ gates as in the gate teleportation scheme above, then the *correction* function is no longer a simple Pauli update (as in the case for Cliffords). However, this is only partially true: since the Paulis form a basis, there is always a way to represent an update as a complex, linear combination of Pauli matrices. In particular, for the case of a $\mathsf{T}$, we note that $\mathsf{P} = (\frac{1+i}{2})\mathsf{I} + (\frac{1-i}{2})\mathsf{Z}$. Hence, it *is* possible to produce an update function for general quantum circuits that are encoded via gate teleportation. To illustrate this, we first analyze the case of a general Clifford+$\mathsf{T}$ quantum circuit on a *single* qubit (Section 5.1). Here, we are able to provide $qi\mathcal{O}$ for all circuits. Next, for general quantum circuits, (Section 5.2), we note that the update function exists for all circuits, but becomes more and more complex as the number of $\mathsf{T}$ gates increases. We show that if we limit the number of $\mathsf{T}$ gates to be logarithmic in the circuit size, we can reach an efficient construction. Both of these constructions assume a quantum-secure, classical indistinguishability obfuscation.

To the best of our knowledge, our gate teleportation provides the first method for indistinguishability obfuscation that is efficient for a large class of quantum circuits, beyond Clifford circuits. Note, however that canonical forms (also called *normal* forms) are known for *single*-qubits universal quantum circuits [29,38]. We note that, for many other quantum cryptographic primitives, it is the case that the $\mathsf{T}$-gate is the bottleneck (somewhat akin to a *multiplication* in the classical case). This has been observed, *e.g.*, in the context of *homomorphic quantum encryption* [17,25], and instantaneous quantum computation [43]. Because of these applications, and since the $\mathsf{T}$ is also typically also the bottleneck for fault-tolerant quantum computing, techniques exist to reduce the number of $\mathsf{T}$ gates in quantum circuits [8,9,24] (see Section 1.2 for more on this topic).

### 1.1.2 Indistinguishability obfuscation for quantum circuits, with respect to a pseudo-distance

Next in Section 6, we define indistinguishability obfuscation for quantum circuits with respect to some pseudo-norm $\mathbf{D}$, which we call $qi\mathcal{O}_{\mathbf{D}}$. This definition specifies that on input a classical description of a quantum circuit $C_q$, the obfuscator outputs a *pair* $(|\phi\rangle, C'_q)$, where $|\phi\rangle$ is an auxiliary quantum state and $C'_q$ is a quantum circuit. For correctness, we require that $\mathbf{D}(C'_q(|\phi\rangle, \cdot), C_q(\cdot)) \leq \mathtt{negl}(n)$, whereas for security, we require that, on input two *approximately* equivalent quantum circuits (Definition 6.1), the outputs of $qi\mathcal{O}_{\mathbf{D}}$ are statistically indistinguishable. This definition is more in line with [4].

We show how to construct a statistically-secure quantum indistinguishability obfuscation with respect to the pseudo-distance $\mathbf{D}$ (see Algorithm 6) for quantum circuits that are very close to $k$th level of the Gottesman-Chuang hierarchy [32], for some fixed $k$ (see Section 2.9). The construction takes a cir-

cuit $U_q$ as an input with a promise that the distance $\mathbf{D}(U_q, C) \leq \epsilon < \frac{1}{2^{k+1/2}}$ for some $C \in \mathcal{C}_k$. It computes the conjugate circuit $U_q^\dagger$ and then runs Low's learning algorithm as a subroutine on inputs $U_q$ and $U_q^\dagger$ [37]. The algorithm outputs whatever Low's learning algorithm outputs. Note that Low's learning algorithm runs in time super-polynomial in $k$, therefore for our construction to remain efficient the parameter $k$ is some small fixed integer (say $k = 5$). Note that for $k > 2$, the set $\mathcal{C}_k$ includes all Clifford unitaries as well as some non-Clifford unitaries [37].

### 1.1.3 Comparison of the two Approaches

Our notions of $qi\mathcal{O}$ and $qi\mathcal{O}_{\mathbf{D}}$ are incomparable. To see this, on one hand, note that the basic instantiation of an indistinguishability obfuscator that outputs a canonical form is no longer secure in the definition of indistinguishability with respect to a pseudo-norm.[2] On the other hand, the construction for $qi\mathcal{O}_{\mathbf{D}}$ that we give in Algorithm 6 does not satisfy the definition of $qi\mathcal{O}$, because the functionality is not perfectly preserved, which is a requirement for $qi\mathcal{O}$. We recall that in the classical case, it is generally considered an *advantage* that $i\mathcal{O}$ is a relatively weak notion (since it is more easily attained) and that, despite this, a host of uses of $i\mathcal{O}$ are known. We thus take $qi\mathcal{O}$ as the more natural extension of classical indistinguishability obfuscation to the quantum case, but we note that issues related to the continuity of quantum mechanics and the inherent approximation in any universal quantum gateset justify the relevance for our approach to $qi\mathcal{O}_{\mathbf{D}}$.

We now compare the schemes that we achieve. The most general scheme that we give as a construct for $qi\mathcal{O}$ (Algorithm 5) allows to obfuscate any polynomial-size quantum circuit (with at most $O(\log)$ non-Clifford gates). While this is a restricted class, it is well-understood and we believe that this technique may be amenable to an extension that would result into a full $qi\mathcal{O}$.

In comparison, the scheme that we give for $qi\mathcal{O}_{\mathbf{D}}$, based on Low's learning algorithm [37] has some advantages over the teleportation-based constructions. Firstly, the circuits to be obfuscated don't need to be of equal size or perfectly equivalent and the outputs of the obfuscator remain statistically indistinguishable as long as the circuits are approximately equivalent (with respect to the pseudo-distance $\mathbf{D}$). Secondly, Algorithm 6 does not require any computational assumptions, whereas the teleportation-based constructions require a quantum-secure classical indistinguishability obfuscator. However, beyond the fact that $\mathcal{C}_k$ contains all Clifford circuits, it is not clear how powerful unitaries are in the $k$th level of the Gottesman-Chuang hierarchy (especially for a fixed small $k$). Even when $k \to \infty$, the hierarchy does not include all unitaries. In terms of extending this technique, Low's learning algorithm exploits the structure of the Gottesman-Chuang hierarchy and it not obvious how one can apply this technique to arbitrary quantum circuits.

[2] If two different circuits are close in functionality but not identical, then we have no guarantee that their canonical forms are close.

## 1.2 More on Related Work

**Quantum Obfuscation.** Quantum obfuscation was first studied in [5], where a notion called $(G, \Gamma)$-*indistinguishability obfuscation* was proposed, where $G$ is a set of gates and $\Gamma$ 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 $\Gamma$.

Since perfect indistinguishability obfuscation is known to be impossible under the assumption that $\mathsf{P} \neq \mathsf{NP}$ [30], one of the motivations of this work was to provide a weaker definition of perfectly indistinguishable obfuscation, along with possibility results. However, to the best of our knowledge, $(G, \Gamma)$-*indistinguishability obfuscation* is incomparable with computational indistinguishability obfuscation [12, 26], which is the main focus of our work.

Quantum obfuscation is studied in [4], where the various notions of quantum obfuscation are defined (including quantum black-box obfuscation, quantum indistinguishability obfuscation, and quantum best-possible obfuscation). A contribution of [4] is to extend the classical impossibility results to the quantum setting, including *e.g.* showing that each of the three variants of quantum indistinguishability obfuscation is equivalent to the analogous variant of quantum best-possible obfuscation, so long as the obfuscator is efficient. This work shows that the existence of a computational quantum indistinguishability obfuscation implies a witness encryption scheme for all languages in $\mathsf{QMA}$. Various impossibiliity results are also shown: that efficient statistical indistinguishability obfuscation is impossible unless $\mathsf{PSPACE}$ is contained in $\mathsf{QSZK}$[3] (for the case of circuits that include measurements), or unless $\mathsf{coQMA}$[4] is contained in $\mathsf{QSZK}$ (for the case of unitary circuits). Notable here is that [4] defines a notion of indistinguishability obfuscation where security must hold for circuits that are *close* in functionality (this is similar to our definition of $qi\mathcal{O}_{\mathbf{D}}$); it is however unclear if their impossibility results hold for a notion of quantum indistinguishability along the lines of our definition of $qi\mathcal{O}$. See Section 3.2 for further discussion of the links between this definition and ours. We note that [4] does not provide any concrete instantiation of obfuscation.

Recently it has been shown that virtual black-box obfuscation of classical circuits via quantum mechanical means is also impossible [3, 11].

**Quantum Homomorphic Encryption.** In *quantum homomorphic encryption*, a computationally-weak client is able to send a ciphertext to a quantum server, such that the quantum server can perform a quantum computation on the encrypted data, thus producing an encrypted output which the client can decrypt, and obtaining the result of the quantum computation.

This primitive was formally defined in [17] (see also [16, 25]), where it was

[3] $\mathsf{PSPACE}$ is the class of decision problems solvable by a Turing machine in polynomial space and $\mathsf{QSZK}$ is the class of decision problems that admit a quantum statistical zero-knowledge proof system.

[4] $\mathsf{coQMA}$ is the *complement* of $\mathsf{QMA}$, which is the class of decision problems that can be verified by a one-message quantum interactive proof.

shown how to achieve homomorphic quantum computation for quantum circuits of low $\mathsf{T}$-depth, by assuming quantum-secure classical fully homomorphic encryption. We note that even the simplest scheme in [17] (which allows the homomorphic evaluation of *any* Clifford circuit), requires computational assumptions in order for the server to update homomorphically the classical portion of the ciphertext, based on the choice of Clifford. In contrast, here we are able to give information-theoretic constructions for this class of circuits (essentially, because the choice of Clifford is chosen by the obfuscator, not by the evaluator). We thus emphasize that in $i\mathcal{O}$, we want to hide the *circuit*, whereas in homomorphic encryption, we want to hide the *plaintext* (and allow remote computations on the ciphertext). Since the evaluator in homomorphic encryption has control of the circuit, but not of the data, the evaluator knows which types of gates are applied, and the main obstacle is to perform a correction after a $\mathsf{T}$-gate, controlled on a classical value that is held only in an encrypted form by the evaluator. In contrast to this, in $i\mathcal{O}$, we want to hide the inner workings of the circuit. By using gate teleportation, we end up in a situation where the evaluator *knows* some classical values that have affected the quantum computation in some undesirable way, and then we want to hide the inner workings of *how* the evaluator should compensate for these undesirable effects. Thus, the techniques of quantum homomorphic encryption do not seem directly applicable, although we leave as an open question if they could be used in some indirect way, perhaps towards efficient $qi\mathcal{O}$ for a larger family of circuits.

### 1.3 Open Questions

The main open question is efficient quantum indistinguishability obfuscation for quantum circuits with super-logarithmic number of $\mathsf{T}$-gates. Another open question is about the applications of quantum indistinguishability obfuscation. While we expect that many of the uses of classical $i\mathcal{O}$ carry over to the quantum case, we leave as future work the formal study of these techniques.

**Outline.** The remainder of this paper is structured as follows. Section 2 overviews basic notions required in this work. In Section 3, we formally define indistinguishability obfuscation for quantum circuits. In Section 4, we provide the construction for Clifford circuits. In Section 5, we give our main result which shows quantum indistinguishability obfuscation for quantum circuits, which is efficient for circuits having at most a logarithmic number of $\mathsf{T}$ gates. Finally in Section 6, we consider the notion of quantum indistinguishability obfuscation with respect to a pseudo-distance, and show how to instantiate it for a family of circuits close to the Gottesman-Chuang hierarchy.

# 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. Given two bit strings $x$ and $y$ of equal length, we denote their bitwise XOR by $x \oplus y$. For a finite set $X$, the notation $x \xleftarrow{\$} X$ indicates that $x$ is selected uniformly at random from $X$. We denote the set of all $d \times d$ unitary matrices by $\mathcal{U}(d) = \{U \in \mathbb{C}^{d\times d} \mid UU^\dagger = \mathbf{I}\}$, where $U^\dagger$ denotes the conjugate transpose of $U$.

A function $\mathtt{negl} : \mathbb{N} \to \mathbb{R}^+ \cup \{0\}$ is *negligible* if for every positive polynomial $p(n)$, there exists a positive integer $n_0$ such that for all $n > n_0$, $\mathtt{negl}(n) < 1/p(n)$. 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.

## 2.2 Classical Circuits and Algorithms

A deterministic polynomial-time (or **PT**) algorithm $\mathcal{C}$ is defined by a polynomial-time uniform[5] family $\mathcal{C} = \{C_n \mid n \in \mathbb{N}\}$ of classical Boolean circuits over some gate set, with one circuit for each possible input size $n \in \mathbb{N}$. For a bitstring $x$, we define $\mathcal{C}(x) := \mathcal{C}_{|x|}(x)$. We say that a function family $f : \{0,1\}^n \to \{0,1\}^m$ is **PT**-computable if there exists a polynomial-time $\mathcal{C}$ such that $\mathcal{C}(x) = f(x)$ for all $x$; it is implicit that $m$ is a function of $n$ which is bounded by some polynomial, *e.g.*, the same one that bounds the running time of $\mathcal{C}$. Note that in the literature, circuits that compute functions whose range is $\{0,1\}^m$ are often called multi-output Boolean circuits [33], but in this paper we simply called them Boolean circuits [42].

A probabilistic polynomial-time algorithm (or **PPT**) is again a polynomial-time uniform family of classical Boolean circuits, one for each possible input size $n$. The $n$th circuit still accepts $n$ bits of input, but now also has an additional "coins" register of $p(n)$ input wires. Note that uniformity enforces that the function $p$ is bounded by some polynomial. For a **PPT** algorithm $\mathcal{C}$, $n$-bit input $x$ and $p(n)$-bit coin string $r$, we set $\mathcal{C}(x;r) := \mathcal{C}_n(x;r)$. In contrast with the PT case, the notation algorithm $\mathcal{C}(x)$ will now refer to the random variable algorithm $\mathcal{C}(x;r)$ where $r \xleftarrow{\$} \{0,1\}^{p(n)}$.

## 2.3 Classical Indistinguishability

Here, we define indistinguishability for classical random variables, against a quantum distinguisher (Definition 2.2).

[5] Recall that polynomial-time uniformity means that there exists a polynomial-time Turing machine which, on input $n$ in unary, prints a description of the $n$th circuit in the family.

**Definition 2.1.** (Statistical Distance) Let $X$ and $Y$ be two random variables over some countable set $\Omega$. The statistical distance between $X$ and $Y$ is

$$\Delta(X,Y) = \frac{1}{2}\left\{\sum_{\omega\in\Omega}|Pr[X(\omega)] - Pr[Y(\omega)]|\right\}.$$

**Definition 2.2.** (Indistinguishability) Let $\mathcal{X} = \{X_n\}_{n\in\mathbb{N}}$ and $\mathcal{Y} = \{Y_n\}_{n\in\mathbb{N}}$ be two distribution ensembles indexed by a parameter $n$. We say

1. $\mathcal{X}$ and $\mathcal{Y}$ are *perfectly indistinguishable* if for all $n$,

$$\Delta(X_n, Y_n) = 0.$$

2. $\mathcal{X}$ and $\mathcal{Y}$ are *statistically indistinguishable* if there exists a negligible function $\texttt{negl}$ such that for all sufficiently large $n$:

$$\Delta(X_n, Y_n) \leq \texttt{negl}(n).$$

3. $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ are *computationally indistinguishable* if for any polynomial-time quantum distinguisher $\mathcal{D}_q$, there exists a negligible function $\texttt{negl}$ such that:

$$\left|\Pr[\mathcal{D}_q(X_n) = 1] - \Pr[\mathcal{D}_q(Y_n) = 1]\right| \leq \texttt{negl}(n).$$

## 2.4 Classical Indistinguishability Obfuscation

Let $\mathcal{C}$ be a family of probabilistic polynomial-time circuits. For $n \in \mathbb{N}$, let $C_n$ be the circuits in $\mathcal{C}$ of input length $n$. We now provide a definition of classical indistinguishability obfuscation ($i\mathcal{O}$) as defined in [30], but where we make a few minor modifications.[6]

**Definition 2.3.** (**Indistinguishability Obfuscation**, $i\mathcal{O}$) A probabilistic polynomial-time algorithm is a *quantum-secure indistinguishability obfuscator* ($i\mathcal{O}$) for a class of circuits $\mathcal{C}$, if the following conditions hold:

1. `Preserving Functionality:` For any $C \in C_n$ :

$$i\mathcal{O}(x) = C(x), \text{ for all } x \in \{0,1\}^n$$

   The probability is taken over the $i\mathcal{O}$'s coins.

2. `Polynomial Slowdown:` There exists a polynomial $p(n)$ such that for all input lengths, for any $C \in C_n$, the obfuscator $i\mathcal{O}$ only enlarges $C$ by a factor of $p(|C|)$ :

$$|i\mathcal{O}(C)| \leq p(|C|).$$

[6] We make a few design choices that are more appropriate for our situation, where we show the *possibility* of $i\mathcal{O}$ against quantum adversaries: our adversary is a probabilistic polynomial-time quantum algorithm, we dispense with the mention of the random oracle, and note that our indistinguishability notions are defined to hold for all inputs.

3. `Indistinguishability:` An $i\mathcal{O}$ is said to be a computational/statistical/perfect indistinguishability obfuscation for the family $\mathcal{C}$, if for all large enough input lengths, for any circuit $C_1 \in C_n$ and for any $C_2 \in C_n$ that computes the same function as $C_1$ and such that $|C_1| = |C_2|$, the distributions $i\mathcal{O}(C_1))$ and $i\mathcal{O}(C_2)$ are (respectively) computationally/statistically/perfectly indistinguishable.

## 2.5 Basic Quantum Notions

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

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

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.

## 2.6 Norms and Pseudo-Distance

The trace distance between two quantum states $\rho, \sigma \in \mathcal{D}(\mathcal{H}_n)$ is given by:

$$||\rho - \sigma||_{tr} := \frac{1}{2}\,\mathrm{Tr}\left(\left|\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}\right|\right),$$

where $|\cdot|$ denotes the positive square root of the matrix $\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}$.

Let $\Phi$ and $\Psi$ be two admissible operators of type $(n,m)$[7]. The *diamond norm* between two quantum operators is

$$||\Phi - \Psi||_\diamond := \underset{\rho \in \mathcal{D}(\mathcal{H}_{2n})}{max} ||(\Phi \otimes I_n)\rho - (\Psi \otimes I_n)\rho||_{tr}$$

The Frobenius norm of a matrix $A \in \mathbb{C}^{n\times m}$ is defined as $||A||_F = \sqrt{\mathrm{Tr}(AA^\dagger)}$. Let $U_1, U_2 \in \mathcal{U}(d)$ be two $d \times d$ unitary matrices. The phase invariant distance between $U_1$ and $U_2$ is

$$\begin{aligned}\mathbf{D}(U_1,U_2) &= \frac{1}{\sqrt{2d^2}}||U_1 \otimes U_1^* - U_2 \otimes U_2^*||_F \\ &= \sqrt{1 - \left|\frac{\mathrm{Tr}(U_1U_2^\dagger)}{d}\right|^2},\end{aligned}$$

where $U_i^*$ denotes the matrix with only complex conjugated entries and no transposition and $|z|$ denotes the norm of the complex number $z$. Note that $\mathbf{D}$ is a pseudo-distance since $\mathbf{D}(U_1,U_2) = 0$ does not imply $U_1 = U_2$, but that

[7] An operator is admissible if its action on density matrices is linear, trace-preserving, and completely positive. A operator's type is $(n,m)$ if it maps $n$-qubit states to $m$-qubit states.

$U_1$ and $U_2$ are equivalent up to a phase so the difference is unobservable. It is easy to see that $\mathbf{D}$ satisfies the axioms of symmetry ($\mathbf{D}(U_1, U_2) = \mathbf{D}(U_2, U_1)$), the triangle inequality ($\mathbf{D}(U_1, U_2) \leq \mathbf{D}(U_1, U) + \mathbf{D}(U, U_2)$) and non-negativity ($\mathbf{D}(U_1, U_2) \geq 0$).

## 2.7 Bell Basis and Measurement

The four states $\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\}$ are called *Bell States* or *EPR pairs* and form an orthonormal basis of $\mathcal{H}_2$.

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

We define a generalized Bell state as a tensor product of $n$ Bell states

$$|\beta_s\rangle = |\beta_{a_i,b_i}\rangle^{\otimes_{i=1}^n},$$

where $s = a_1 b_1, \ldots, a_n b_n \in \{0,1\}^{2n}$. The set of generalized Bell States $\{|\beta_s\rangle \mid s \in \{0,1\}^{2n}\}$ forms an orthonormal basis of $\mathcal{H}_n$. Given a quantum state

$$|\psi\rangle = \sum_{s \in \{0,1\}^{2n}} \alpha_s |\beta_s\rangle,$$

a Bell measurement in the (generalized) Bell basis on the state $|\psi\rangle$ outputs the string $s$ with probability $|\alpha_s|^2$ and leaves the system in the state $|\beta_s\rangle$.

## 2.8 Quantum Gates

We will work with the following set of unitary gates

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

$$\mathsf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \mathsf{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \text{ and } \quad \mathsf{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$

For any single-qubit density operator $\rho \in \mathcal{D}(\mathcal{H}_1)$, we can encrypt it via the *quantum one-time pad* by sampling uniform bits $s$ and $t$, and producing $\mathsf{X}^s\mathsf{Z}^t\rho\mathsf{Z}^t\mathsf{X}^s$. To an observer that has no knowledge of $s$ and $t$, this system is information-theoretically indistinguishable from the state $\mathbb{1}_1/2$ (where $\mathbb{1}_1$ is the 2 by 2 identity matrix) [7].

## 2.9 Gottesman-Chuang Hierarchy

The $n$-qubit Pauli group $\mathcal{P}_n$ is a multiplicative group of order $4^{n+1}$, defined as:

$$\mathcal{P}_n = \{\alpha_1 P_1 \otimes \cdots \otimes \alpha_n P_n \mid \alpha_i \in \{\pm 1, \pm i\}, P_i \in \{\mathsf{I}, \mathsf{X}, \mathsf{Z}, \mathsf{Y}\}\}\,.$$

Let $C_1$ be the Pauli group $\mathcal{P}_n$. Then the level $\mathcal{C}_k$ of the *Gottesman-Chuang* hierarchy is defined recursively [32]:

$$\mathcal{C}_k = \{U \in \mathcal{U}(2^n) : U\mathcal{P}_n U^\dagger \subseteq \mathcal{C}_{k-1}\}.$$

Note that $\mathcal{C}_2$ is the Clifford group and for $k > 2$, $\mathcal{C}_k$ is no longer a group but contains unitaries that contains a universal gate set.

The set of gates $\{\mathsf{X}, \mathsf{Z}, \mathsf{P}, \mathsf{CNOT}, \mathsf{H}\}$ applied to arbitrary wires redundantly generates the *Clifford group*. We note the following relations between these gates (these relations hold up to *global phase*; in this work, we use the convention that equal signs for pure states and unitaries hold up to global phase.)

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

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

## 2.10 Quantum Circuits and Algorithms

A quantum circuit is an acyclic network of quantum gates connected by wires. The quantum gates represent quantum operations and wires represent the qubits on which gates act. In general, a quantum circuit can have $n$-input qubits and $m$-output qubits for any integer $n, m \geq 0$. The $\mathsf{T}$-*count* is the total number of $\mathsf{T}$-gates in a quantum circuit.

A quantum circuit that computes a 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 is said to be *universal* if for any integer $n \geq 1$, any $n$-qubit unitary operator can be approximated to arbitrary accuracy by a quantum circuit using only gates from that set [35]. It is a well-known fact that Clifford gates are not universal, but adding any non-Clifford gate, such as $\mathsf{T}$, gives a universal set of gates [35][8]. *Generalized quantum circuits* (which implement *superoperators*) are composed of the unitary gates, together with trace-out and measurement operations. It is well-known that a generalized quantum circuit can be implemented by adding auxiliary states to the original system, applying a unitary operation on the joint system, and then tracing out some subsystem [35].

A family of generalized quantum circuits $\mathcal{C} = \{C_{q_n} \mid n \in \mathbb{N}\}$, one for each input size $n \in \mathbb{N}$, is called *polynomial-time uniform* if there exists a deterministic Turing machine $M$ such that: (i) for each $n \in \mathbb{N}$, $M$ outputs a description of $C_{q_n} \in \mathcal{C}$ on input $1^n$; and (ii) for each $n \in \mathbb{N}$, $M$ runs in $poly(n)$. We define a *quantum polynomial-time algorithm* (or QPT) to be a polynomial-time uniform family of generalized quantum circuits.

[8] In this work, we assume circuits are given in the Clifford + $\mathsf{T}$ gateset

## 2.11 Quantum Indistinguishability

Here, we define indistinguishability for indistinguishability for quantum states (Definition 2.4).

**Definition 2.4.** (Indistinguishability of Quantum States) Let $\mathcal{R} = \{\rho_n\}_{n\in\mathbb{N}}$ and $\mathcal{S} = \{\sigma_n\}_{n\in\mathbb{N}}$ be two ensembles of quantum states such that $\rho_n$ and $\sigma_n$ are $n$-qubit states. We say

1. $\mathcal{R}$ and $\mathcal{S}$ are *perfectly indistinguishable* if for all $n$,
$$\rho_n = \sigma_n.$$
2. $\mathcal{R}$ and $\mathcal{S}$ are *statistically indistinguishable* if there exists a negligible function $\mathtt{negl}$ such that for all sufficiently large $n$:
$$||\rho_n - \sigma_n||_{tr} \leq \mathtt{negl}(n).$$
3. $\mathcal{R}$ and $\mathcal{S}$ are *computationally indistinguishable* if there exists a negligible function $\mathtt{negl}$ such that for every state $\rho_n \in \mathcal{R}$, $\sigma_n \in \mathcal{S}$ and for all polynomial-time quantum distinguisher $\mathcal{D}_q$, we have:
$$\left|\Pr[\mathcal{D}_q(\rho_n) = 1] - \Pr[\mathcal{D}_q(\sigma_n) = 1]\right| \leq \mathtt{negl}(n).$$

## 2.12 Quantum Teleportation

Here we provide a high-level description of quantum teleportation; for a more rigorous treatment see [13]. Suppose Alice has a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$[9] that she wants to send to Bob who is located far away from Alice. One way for Alice to send her qubit to Bob is via the quantum teleportation protocol. For teleportation to work, Alice prepares a 2-qubit Bell state

$$|\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle\right)_{AB},$$

and sends physically one of the qubit to Bob and keeps the other to herself (this is what subscript $AB$ means). We can now write the 3-qubit system as

$$|\psi\rangle \otimes |\beta_{00}\rangle_{AB} \tag{2}$$

Alice now performs a joint measurement on $|\psi\rangle$ and her part of the EPR pair in the Bell basis and obtains the output of the measurement (classical bits $a, b$). After this step, Bob's part of EPR pair has been transformed into the state

$$\mathsf{X}^b\mathsf{Z}^a|\psi\rangle.$$

Alice sends the two classical bits $(a, b)$ to Bob, who performs the correction unitary $Z^aX^b$ to the state he possesses and obtains the state $|\psi\rangle$.

[9] For simplicity we assume that $|\psi\rangle$ is single-qubit pure state.

### 2.13 Gate Teleportation

One of the main applications of quantum teleportation is in fault-tolerant quantum computation [32]. To construct unitary quantum circuits, we need to have access to some universal set of quantum gates[10]. Suppose we want to evaluate a single-qubit gate on some quantum state $|\psi\rangle$. If we directly apply $U$ on $|\psi\rangle$ and $U$ fails, then it may also destroy the state. Quantum teleportation gives a way of solving this problem. Instead of applying $U$ directly to $|\psi\rangle$, we can apply $U$ to the system $B$ in Equation (2) and then follow the gate teleportation protocol and obtain $U(|\psi\rangle)$. If $U$ fails, then the Bell state might be destroyed, but there is no harm done, since we can create another EPR pair and try again. The gate teleportation can easily be generalized to evaluate any $n$-qubit Clifford circuit (Algorithm 1).

**Remark 2.5.** In this section, we only discuss how to evaluate Clifford gates using gate teleportation. Note that we can evaluate any unitary circuit using gate teleportation but the correction unitary becomes more complicated (it is no longer a tensor product of Paulis). This is discussed in Section 5.

### 2.14 Update Functions for Quantum Gates

Let $C_q$ be an $n$-qubit circuit consisting of a sequence of Clifford gates $g_1, \ldots, g_{|C_q|}$. Then the update function for $C_q$ is a map from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$ and is constructed by composing the update functions for each gate in $C_q$[11]

$$\begin{aligned} F_{C_q} &= \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n} \\ F_{C_q} &= f_{g_{|C_q|}} \circ \cdots \circ f_{g_2} \circ f_{g_1} \end{aligned} \tag{6}$$

For each Clifford gate $g$, the update function $f_g$ is defined below. Note how $g$ relates to the $\mathsf{X}$ and $\mathsf{Z}$ gates.

$\mathsf{X}(\mathsf{X}^b\mathsf{Z}^a)\psi = (\mathsf{X}^b\mathsf{Z}^a)\mathsf{X}|\psi\rangle$ (update function) $f_{\mathsf{X}}(a,b) = (a,b)$

$\mathsf{Z}(\mathsf{X}^b\mathsf{Z}^a)\mathsf{Z} = (\mathsf{X}^b\mathsf{Z}^a)\mathsf{Z}|\psi\rangle$ (update function) $f_{\mathsf{Z}}(a,b) = (a,b)$

$\mathsf{H}(\mathsf{X}^b\mathsf{X}^a)\mathsf{Z} = (\mathsf{X}^b\mathsf{X}^a)\mathsf{H}|\psi\rangle$ (update function) $f_{\mathsf{H}}(a,b) = (b,a)$

$\mathsf{P}(\mathsf{X}^b\mathsf{X}^a)\mathsf{Z} = (\mathsf{X}^b\mathsf{X}^a)\mathsf{P}|\psi\rangle$ (update function) $f_{\mathsf{P}}(a,b) = (a, a \oplus b)$

$\mathsf{CNOT}(\mathsf{X}^{a_1}\mathsf{Z}^{b_1} \otimes \mathsf{X}^{a_2}\mathsf{Z}^{b_2})|\psi\rangle = (\mathsf{X}^{b_1}\mathsf{Z}^{a_1 \oplus a_2} \otimes \mathsf{X}^{b_1 \oplus b_2}\mathsf{Z}^{b_2})\mathsf{CNOT}(|\psi\rangle)$ (update function)

$f_{\mathsf{CNOT}}(a_1, b_1, a_2, b_2) = (a_1 \oplus a_2, b_1, a_2, b_1 \oplus b_2)$.

## 3 Definitions

In this section, we provide a definition of perfectly equivalent quantum circuits (see Section 3.1), and define our notion of quantum indistinguishability obfus-

[10] $\{\mathsf{H}, \mathsf{T}, \mathsf{CNOT}\}$ is a universal set of quantum gates [35].

[11] This composition implicitly assumes that when an update function is applied, it acts non-trivially on the appropropriate bits, as indicated by the original circuit, and as the identity elsewhere.

**Algorithm 1** Gate Teleportation Protocol.

**Input**: A $n$-qubit Clifford Circuit $C_q$ and $n$-qubit quantum state $|\psi\rangle$

1. Prepare a tensor product of $n$ Bell states: $|\beta^{2n}\rangle = |\beta_{00}\rangle \otimes \cdots \otimes |\beta_{00}\rangle$.
2. Write the joint system as $|\psi\rangle_C |\beta^{2n}\rangle_{AB}$.
3. Apply the circuit $C_q$ on the subsystem $B$.
4. Perform a measurement in the generalized Bell Basis (generalized Bell measurement) on the system $CA$ and obtain a binary string $a_1 b_1, \ldots, a_n b_n$. The remaining system after the measurement is

$$C_q \left(\mathsf{X}^{b_i} \mathsf{Z}^{a_i}\right)^{\otimes_{i=1}^n} |\psi\rangle. \tag{3}$$

5. Compute the correction bits using the update function $F_{C_q}$ (Section 2.14).

$$F_{C_q}(a_1 b_1, \ldots, a_n b_n) = a'_1 b'_1, \ldots, a'_n b'_n \in \{0,1\}^{2n}. \tag{4}$$

6. Compute the correction unitary $U_{F_{C_q}} = \left(\mathsf{Z}^{a'_i} \mathsf{X}^{b'_i}\right)^{\otimes_{i=1}^n}$
7. Apply $U_{F_{C_q}}$ to the system (Equation (3)).

$$\begin{aligned} U_{F_{C_q}} \cdot C_q \left(\mathsf{X}^{b_i} \mathsf{Z}^{a_i}\right)^{\otimes_{i=1}^n} |\psi\rangle &= \left(\mathsf{Z}^{a'_i} \mathsf{X}^{b'_i}\right)^{\otimes_{i=1}^n} C_q \left(\mathsf{X}^{b_i} \mathsf{Z}^{a_i}\right)^{\otimes_{i=1}^n} |\psi\rangle \\ &= \left(\mathsf{Z}^{a'_i} \mathsf{X}^{b'_i}\right)^{\otimes_{i=1}^n} \left(\mathsf{X}^{b'_i} \mathsf{Z}^{a'_i}\right)^{\otimes_{i=1}^n} C_q(|\psi\rangle) \\ &= C_q(|\psi\rangle). \end{aligned} \tag{5}$$

cation for equivalent circuits (Section 3.2). At the end of the section, we also make an observation about the existence of inefficient quantum indistinguishability obfuscation. Note that in Section 6, we present our alternative definition for quantum indistinguishability obfuscation, applicable to the case where the circuits are approximately equivalent.

## 3.1 Perfectly Equivalent Quantum Circuits

**Definition 3.1.** (*Perfectly 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 *perfectly equivalent* if

$$||C_{q_0} - C_{q_1}||_\diamond = 0.$$

## 3.2 Indistinguishability Obfuscation for Quantum Circuits

**Definition 3.2.** (*Quantum Indistinguishability Obfuscation for Perfectly Equivalent Quantum Circuits*): Let $\mathcal{C}_Q$ be a polynomial-time family of reversible quantum circuits. For $n \in \mathbb{N}$, let $C_q^n$ be the circuits in $\mathcal{C}_Q$ of input length $n$. A polynomial-time quantum algorithm for $\mathcal{C}_Q$ is a *Computational/Statistical/Perfect quantum indistinguishability obfuscator* ($qi\mathcal{O}$) if the following conditions hold:

1. `Functionality:` There exists a negligible function $\texttt{negl}(n)$ such that for every $C_q \in C_q^n$

$$(|\phi\rangle, C'_q) \leftarrow qi\mathcal{O}(C_q) \text{ and } ||C'_q(|\phi\rangle, \cdot) - C_q(\cdot)||_\diamond = 0.$$

   Where $|\phi\rangle$ is an $\ell$-qubit state, the circuits $C_q$ and $C'_q$ are of type $(n, n)$ and $(m, n)$ respectively $(m = \ell + n)$.[12]

2. `Polynomial Slowdown:` There exists a polynomial $p(n)$ such that for any $C_q \in C_q^n$,
   - $\ell \leq p(|C_q|)$
   - $m \leq p(|C_q|)$
   - $|C'_q| \leq p(|C_q|)$.

3. `Computational/Statistical/Perfect Indistinguishability:` For any two perfectly equivalent quantum circuits $C_{q_1}, C_{q_2} \in C_q^n$, of the same size, the two distributions $qi\mathcal{O}(C_{q_1})$ and $qi\mathcal{O}(C_{q_2})$ are (respectively) computationally/statistically/perfectly indistinguishable.

**Remark 3.3.** A subtlety that is specific to the quantum case is that Definition 3.2 only requires that $(|\phi\rangle, C'_q)$ enable a *single* evaluation of $C_q$. We could instead require a $k$-time functionality, which can be easily achieved by executing the single-evaluation scheme $k$ times in parallel. This justifies our focus here on the single-evaluation scheme.

[12] A circuit is of type $(i, j)$ if it maps $i$ qubits to $j$ qubits.

**Note 3.4.** As described in Section 1.2, our Definition 3.2 differs from [4] as it requires security only in the case of equivalent quantum circuits (see Definition 6.2 for a definition that addresses this). Compared to [4], we note that in this work we focus on unitary circuits only.[13] Another difference is that the notion of indistinguishability (computational or statistical) in [4] is more generous than ours, since it allows a finite number of inputs that violate the indistinguishability inequality. Since our work focuses on *possibility* of obfuscations, our choice leads to the strongest results; equally, since [4] focuses on impossibility, their results are strongest in their model. We also note that that [4] defines the efficiency of the obfuscator in terms of the number of qubits. We believe that our definition, which bounds the size of the output of the obfucation by a polynomial in the *size* of the input circuit, is more appropriate[14] and follows the lines of the classical definitions. As far as we are aware, further differences in our definition are purely a choice of style. For instance, we do not include an *interpreter* as in [4], but instead we let the obfuscator output a quantum circuit together with a quantum state; we chose this presentation since it provides a clear separation between the quantum circuit output by the $qi\mathcal{O}$ and the "quantum advice state".

### 3.2.1 Inefficient Quantum Indistinguishability Obfuscators Exist

Finally, we show a simple extension of a result in [12], which shows that if we relax the requirement that the obfuscator be efficient, then information-theoretic indistinguishability obfuscation exists.

**Claim 3.5.** Inefficient indistinguishability obfuscators exist for all circuits.

*Proof.* Let $qi\mathcal{O}(C)_q$ be the lexicographically first circuit of size $|C_q|$ that computes the same quantum map as $C_q$. □

# 4 Quantum Indistinguishability Obfuscation for Clifford Circuits

Here, we show how to construct $qi\mathcal{O}$ for Clifford circuits with respect to definition Definition 3.2. The first construction (Section 4.1) is based on a canonical form, and the second is based on gate teleportation (Section 4.2).

## 4.1 $qi\mathcal{O}$ for Clifford Circuits via a Canonical Form

Aaronson and Gottesman developped a polynomial-time algorithm that takes a Clifford circuit $C_q$ and outputs its canonical form (see [2], section VI), which

[13] This is without loss of generality, since a $qi\mathcal{O}$ for a generalized quantum circuit can be obtained from a $qi\mathcal{O}$ for a reversible version of the circuit, followed by a trace-out operation (see Section 2.10).

[14] It would be unreasonable to allow an obfuscator that outputs a circuit on $n$ qubits, but of depth super-polynomial in $n$.

is invariant for any two equivalent $n$-qubit circuits[15]. Moreover the size of the canonical form remains polynomial in the size of the input circuit. Based on this canonical form, we define a $qi\mathcal{O}$ in Algorithm 2.

**Algorithm 2** $qi\mathcal{O}$-Canonical

- Input: An $n$-qubit Clifford Circuit $C_q$.
  1. Using the Aaronson and Gottesman algorithm [2], compute the canonical form of $C_q$
  $$C'_q \xleftarrow{\text{canonical form}} C_q$$
  2. Let $|\phi\rangle$ be an empty register.
  3. Output $\left(|\phi\rangle, C'_q\right)$.

**Lemma 4.1.** Algorithm 2 is a Perfect Quantum Indistinguishability Obfuscation for all Clifford Circuits.

*Proof.* We have to show that Algorithm 2 satisfies the definition of a perfect quantum indistinguishability obfuscation (Definition 3.2) for all Clifford circuits.

1. `Functionality:` Since $|\phi\rangle$ is an empty register, it is a 0 qubit state ($\ell = 0$.) The circuit $C'_q$ is the canonical form of $C_q$, therefore, it is also of type $(n, n)$ and has the same functionality as $C_q$. We have $||C'_q(|\phi\rangle, \cdot) - C_q(\cdot)||_\diamond = 0 \leq \texttt{negl}(n)$ for any negligible function $\texttt{negl}(n)$.

2. `Polynomial Slowdown:` Note $C'_q$ is constructed using Aaronson and Gottesman algorithm [2]. Therefore, there exists a polynomial $q(\cdot)$ such that $|C'_q| \leq q(|C_q|)$. Let $p(n) = q(n) + n$ then we clearly have
   - $\ell \leq p(|C_q|)$
   - $n \leq p(|C_q|)$
   - $|C'_q| \leq p(|C_q|)$.

3. `Perfectly Indistinguishability:` Let $C_{q_1}, C_{q_2} \in C^n_q$, be any two equivalent Clifford circuits of the same size. Let

   $(|\phi_1\rangle, C'_{q_1}) \leftarrow qi\mathcal{O}\text{-Canonical}(C_{q_1})$ and $(|\phi_2\rangle, C'_{q_2}) \leftarrow qi\mathcal{O}\text{-Canonical}(C_{q_2})$.

   Since the canonical form of any two equivalent Clifford circuits are exactly the same, we have $C_{q'_1} = C_{q'_2}$. Moreover both $|\phi_1\rangle$ and $|\phi_2\rangle$ are empty registers we have $|\phi_1\rangle = |\phi_2\rangle$. Then we have $qi\mathcal{O}\text{-Canonical}(C_{q_1}) = qi\mathcal{O}\text{-Canonical}(C_{q_2})$. Therefore, Algorithm 2 is a perfect quantum indistinguishability obfuscation for all Clifford circuits. □

[15] Their algorithm outputs a canonical form (unique form) provided it runs on the standard initial tableau see pages 8-10 of [2].

## 4.2 $qi\mathcal{O}$ for Clifford Circuits via Gate Teleportation

In this section, we show how gate teleportation (see Algorithm 1) can be used to construct a quantum indistinguishability obfuscation for Clifford circuits. Our construction, given in Algorithm 3, relies on the existence of a quantum-secure $i\mathcal{O}$ for classical circuits; however, upon closer inspection, our construction relies on the assumption that a quantum-secure classical $i\mathcal{O}$ exists for a very specific class of classical circuits[16]. In fact, it is easy to construct a perfectly secure $i\mathcal{O}$ for this class of circuits: like Clifford circuits, the circuits that compute the update functions also have a canonical form. Then the $i\mathcal{O}$ takes as input a Clifford circuit and outputs a canonical form of a classical circuit that computes the update function for $C_q$. The $i\mathcal{O}$ is described formally in Algorithm 4.

**Algorithm 3** $qi\mathcal{O}$ via Gate Teleportation for Clifford

- Input: An $n$-qubit Clifford Circuit $C_q$.

1. Prepare a tensor product of $n$ Bell states: $|\beta^{2n}\rangle = |\beta_{00}\rangle \otimes \cdots \otimes |\beta_{00}\rangle$.
2. Apply the circuit $C_q$ on the right-most $n$ qubits to obtain a system $|\phi\rangle$:
$$|\phi\rangle = (\mathsf{I}_n \otimes C_q)|\beta^{2n}\rangle.$$
3. Compute a classical circuit $C$ that computes the update function $F_{C_q}$. The classical circuit $C$ can be computed in polynomial-time by Lemma 4.4.
4. Set $C' \leftarrow i\mathcal{O}(C)$, where $i\mathcal{O}(C)$ is a perfectly secure indistinguishability obfuscation defined in Section 4.2.1.
5. Description of the circuit $C'_q$ :
   (a) Perform a general Bell measurement on the leftmost $2n$-qubits on the system $|\phi\rangle \otimes |\psi\rangle$, where $|\phi\rangle$ is an auxiliary state and $|\psi\rangle$ is an input state. Obtain classical bits $(a_1, b_1 \ldots, a_n, b_n)$ and the state
   $$C_q(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})|\psi\rangle. \tag{7}$$
   (b) Compute the correction bits
   $$(a'_1, b'_1, \ldots, a'_n, b'_n) = C'(a_1, b_1 \ldots, a_n, b_n). \tag{8}$$
   (c) Using the above, the correction unitary is $U' = (\mathsf{X}^{\otimes_{i=1}^n b'_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a'_i})$.
   (d) Apply $U'$ to the system $C_q(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})|\psi\rangle$ to obtain the state $C_q(|\psi\rangle)$.
6. Output $\left(|\phi\rangle, C'_q\right)$.

[16] Circuits that compute update functions for Clifford circuits, see Section 2.14.

**Theorem 4.2.** Algorithm 3 is a perfect quantum indistinguishability obfuscation for all Clifford Circuits.

*Proof.* We have to show that Algorithm 3 satisfies Definition 3.2.

1. `Functionality:` Let $C_q$ be an $n$-qubit Clifford Circuit and $\left(|\phi\rangle, C'_q\right)$ be the output of the Algorithm 3 on input $C_q$. On input $(\mathsf{I}_n \otimes C_q)|\beta^{2n}\rangle$ and $|\psi\rangle$ the circuit $C'_q$ outputs the state $C_q(|\psi\rangle)$ (this follows from the principle of gate teleportation). Therefore $C'_q(|\phi\rangle, \cdot) = C_q(\psi)$, which implies that $||C'_q(|\phi\rangle, \cdot) - C_q(\cdot)||_\diamond = 0 \leq \mathtt{negl}(n)$ for any negligible function $\mathtt{negl}(n)$.

2. `Polynomial Slowdown:` Note $\ell = 2n$ (the number of qubits in $|\phi\rangle$) and $C'_q$ is a circuit of type $(3n, n)$. The size of the circuit $|C'_q| = |i\mathcal{O}(C)| +$ |Bell measurement|, where $C$ is the classical circuit that computes the update function corresponding to $C_q$. The size of a Bell measurement circuit for an $O(n)$-qubit state is $O(n)$. Therefore, there exists a polynomial $q(|C|)$ such that |Bell measurement| $\leq q(|C|)|$. The size of $|i\mathcal{O}(C)|$ is at most $r(|C|)$ for some polynomial $r(\cdot)$ (Lemma 4.4). Further, the size of $|C|$ is at most $s(|C_q|)$ for some polynomial $|C_q|$ (Lemma 4.4). By setting $p(|C|) = 2|C_q| + q(|C|) + r(s(|C|))$, we have

   - $\ell \leq p(|C|)$
   - $m = 3n \leq p(|C|)$
   - $|C'_q| = |i\mathcal{O}(C)| +$ |Bell measurement| $\leq p(|C|)$.

3. `Perfect Indistinguishability:` Let $C_{q_1}$ and $C_{q_2}$ be two $n$-qubit equivalent Clifford circuits of the same size. Let $\left(|\phi_1\rangle, C'_{q_1}\right)$ and $\left(|\phi_2\rangle, C'_{q_2}\right)$ be the outputs of Algorithm 3 on inputs $C_{q_1}$ and $C_{q_2}$ respectively. Since $C_{q_1}(|\tau\rangle) = C_{q_2}(|\tau\rangle)$ for every quantum state $|\tau\rangle$ we have,

$$|\phi_1\rangle = (I \otimes C_{q_1})|\beta^{2n}\rangle = (I \otimes C_{q_2})|\beta^{2n}\rangle = |\phi_2\rangle. \tag{9}$$

   The update functions for any two equivalent Clifford circuits are equivalent (Lemma 4.3), further the classical $i\mathcal{O}$ that obfuscates the update functions (circuits) is perfectly indistinguishable for any two equivalent Clifford circuits (not necessarily of the same size) (Lemma 4.4). Therefore, $C'_{q_1}$ and $C'_{q_2}$ are perfectly indistinguishable. □

**Lemma 4.3.** Let $C_{q_1}$ and $C_{q_2}$ be two equivalent $n$-qubit Clifford circuits. Then their corresponding update functions are also equivalent.

*Proof.* Let $F_{C_{q_1}}$ and $F_{C_{q_2}}$ be the update functions for two $n$-qubit Clifford circuits $C_{q_1}$ and $C_{q_2}$ respectively. Suppose $F_{C_{q_1}} \neq F_{C_{q_2}}$, then there must exist at least one binary string $\mathbf{s} = a_1 b_1 \dots a_n b_n \in \{0,1\}^{2n}$ such that

$$F_{C_{q_1}}(\mathbf{s}) \neq F_{C_{q_2}}(\mathbf{s}) \tag{10}$$

Since $C_{q_1}$ and $C_{q_2}$ are equivalent circuit we must have that for every quantum state $|\psi\rangle$:

$$C_{q_1}(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})|\psi\rangle = C_{q_2}(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})|\psi\rangle \tag{11}$$

Let $F_{C_{q_1}}(\mathbf{s}) = (a'_1 b'_1, \ldots a'_n b'_n)$ and $F_{C_{q_2}}(\mathbf{s}) = (d'_1 e'_1, \ldots, d'_n e'_n)$, then we can rewrite Equation (11) as

$$(\mathsf{X}^{\otimes_{i=1}^n b'_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a'_i})C_{q_1}(|\psi\rangle) = (\mathsf{X}^{\otimes_{i=1}^n e'_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n d'_i})C_{q_2}(|\psi\rangle). \tag{12}$$

We can replace $C_{q_2}(|\psi\rangle)$ with $C_{q_1}(|\psi\rangle)$ in Equation (12)

$$(\mathsf{X}^{\otimes_{i=1}^n b'_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a'_i})C_{q_1}(|\psi\rangle) = (\mathsf{X}^{\otimes_{i=1}^n e'_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n d'_i})C_{q_1}(|\psi\rangle). \tag{13}$$

Now if there exists a $j$ such that $a'_j \neq d'_j$ or $b'_j \neq e'_j$, then Equation (13) does not hold. This contradicts the assumption that $C_{q_1}$ and $C_{q_2}$ are equivalent Clifford circuits. Therefore $F_{C_{q_1}}$ and $F_{C_{q_2}}$ are equivalent functions.[17] □

#### 4.2.1 Indistinguishability Obfuscator for Clifford: Update Functions

Here, we describe a perfect indistinguishability obfuscator $i\mathcal{O}$ for the update functions corresponding to the Clifford circuits. The algorithm takes an $n$-qubit Clifford circuit $C_q$ and output a classical circuit $C$ that computes the update function $F_{C_q}$. The circuit $C$ is invariant for any two equivalent Clifford circuits. The main idea here is to compute the canonical form for the Clifford circuit, and then compute the update function for the canonical form.

**Algorithm 4** $i\mathcal{O}$ for Clifford: Update Functions.

1. Compute the canonical form $C_q$ using the algorithm presented in [2] (section VI). Denote the canonical form as $\widehat{C}_q$.
2. Let $g_1, g_2, \ldots, g_m$ be a topological ordering of the gates in $\widehat{C}_q$, where $m = |\widehat{C}_q|$.
3. Construct the classical circuit $\hat{C}$ that computes the update function $F_{\widehat{C}_q}$ as follows. For $i = 1$ to $m$, implement the update rule for each gate $g_i$ (Section 2.14).
4. Output the classical circuit $\hat{C}$.

**Lemma 4.4.** Algorithm 4 is a perfect classical indistinguishability obfuscator for the Clifford update functions.

*Proof.* We have to show that Algorithm 4 satisfies Definition 2.3.

[17] The Equation (12) is derived from the assumption that $C_{q_1}$ and $C_{q_2}$ are equivalent Clifford circuits.

1. `Functionality:` Let $C_q$ be an $n$-qubit Clifford circuit and $C$ be the circuit that computes $F_{C_q}$ (the update function for $C_q$). Let $\widehat{C}_q$ be the canonical form of $C_q$. Since $C_q$ and $C_q{}'$ are equivalent circuits, it follows from Lemma 4.3 that $F_{C_q}$ and $F'_{C_q}$ are equivalent functions, therefore any circuit that computes $F'_{C_q}$ also computes $F_{C_q}$. From the construction above (Algorithm 4) it follows that the circuit $\hat{C}$ computes $F'_{C_q}$ therefore $\hat{C}(x) = C(x)$ for all inputs $x$.

2. `Polynomial Slowdown:` For each gate $g_i$ in $\widehat{C}_q$, the classical circuit $\widehat{C}$ has to implement one of the following operations (Section 2.14):

   $(a, b) \xrightarrow{\mathsf{X},\mathsf{Z}} (a, b)$.

   $(a, b) \xrightarrow{\mathsf{H}} (b, a)$ (one swap).

   $(a, b) \xrightarrow{\mathsf{P}} (a, a \oplus b)$ (one $\oplus$ operation).

   $(a_1, b_1, a_2, b_2) \xrightarrow{\mathsf{CNOT}} (a_1 \oplus a_2, b_1, a_2, b_1 \oplus b_2)$ (two $\oplus$ operations).

   Therefore the size of $|\widehat{C}|$ can be at most be $O(|\widehat{C}_q|)$. The $\widehat{C}_q$ is a canonical form of $C_q$ and of at most $q(|C_q|)$ for some polynomial $q(\cdot)$ [2]. Therefore, there exists a polynomial $p(\cdot)$ such that $|\widehat{C}| \leq p(|C_q|)$.

3. `Perfectly Indistinguishability:` Let $C_{q_1}, C_{q_2}$ be two equivalent $n$-qubit Clifford circuits (not necessarily of the same size) and $\widehat{C_q}$ be their canonical form. Note that the output of Algorithm 4 only depends on the canonical form of the input Clifford circuit. Since, $C_{q_1}$ and $C_{q_2}$ have the same canonical form we have

   $$\hat{C} \leftarrow \textit{Algorithm 4}(\widehat{C_q}) = \textit{Algorithm 4}(C_{q_1}) = \textit{Algorithm 4}(C_{q_2}),$$

   Therefore, Algorithm 4 is a perfect indistinguishability obfuscation for the Clifford update functions. □

**Remark 4.5.** What is convenient about the $i\mathcal{O}$ of Algorithm 4 is that it works for any two equivalent Clifford circuits (regardless of their relative sizes) (see Lemma 4.3). However, we can use any perfectly secure $i\mathcal{O}$ in our construction with some care. Suppose $i\mathcal{O}$ is some perfectly secure indistinguishability obfuscator for classical circuits (for Clifford update functions) of the same size. Suppose we want to obfuscate an update circuit corresponding to some Clifford $C_q$. The classical circuit $C$ is constructed by going through each gate in $C_q$. Some gates are more costly than others (for *e.g.*, CNOT vs. Z, see proof of Theorem 4.2 or Section 2.14). Since we assume all Clifford circuits are of the same size, we can obtain an upper bound on all the classical circuits (for the update functions) by replacing each gate in $C_q$ with the most costly gate and then computing the classical circuit for the resulting quantum gate. Now suppose $m$ is the upper bound on the size of classical circuits, then for any circuit $C_q$, we first calculate the circuit $C$ that computes $F_{C_q}$ and then pad $C$ with $m - |C|$ identity gates. This will ensure that if $|C_{q_1}| = |C_{q_2}|$, then $|C_1| = |C_2|$.

# 5 Obfuscating Beyond Clifford Circuits

In this section, we extend the gate teleportation technique to show how we can construct $qi\mathcal{O}$ for *any* quantum circuit. Our construction is efficient as long as the circuit has $\mathsf{T}$-count at most logarithmic in the circuit size. For the sake of simplicity, we first construct a $qi\mathcal{O}$ for an arbitrary 1-qubit quantum circuit (Section 5.1), then extend the 1-qubit construction to any $n$-qubit quantum circuit (Section 5.2).

We first start with some general observations on quantum circuits which are relevant to this section. Consider the application of the $\mathsf{T}$-gate on an encrypted system using the quantum one-time pad. The following equation relates the $\mathsf{T}$-gate to the $\mathsf{X}$- and $\mathsf{Z}$-gates:

$$\mathsf{T}\mathsf{X}^b\mathsf{Z}^a = \mathsf{X}^b\mathsf{Z}^{a\oplus b}\mathsf{P}^b\mathsf{T}\,. \tag{14}$$

If $b = 0$, then $\mathsf{P}^b$ is the identity; otherwise we have a $\mathsf{P}$-gate correction. This is undesirable as $\mathsf{P}$ does not commute with $\mathsf{X}$, making the update of the encryption key $(a, b)$ complicated (since it is no longer a tensor product of Paulis). Note that we can write $\mathsf{P} = \left(\frac{1+i}{2}\right)\mathsf{I} + \left(\frac{1-i}{2}\right)\mathsf{Z}$, therefore Equation (14) can be rewritten as:

$$\mathsf{T}\mathsf{X}^b\mathsf{Z}^a = \mathsf{X}^b\mathsf{Z}^{a\oplus b}\left[\left(\frac{1+i}{2}\right)\mathsf{I} + \left(\frac{1-i}{2}\right)\mathsf{Z}\right]^b\mathsf{T} \tag{15}$$

Since $\left[\left(\frac{1+i}{2}\right)\mathsf{I} + \left(\frac{1-i}{2}\right)\mathsf{Z}\right]^b = \left(\frac{1+i}{2}\right)\mathsf{I} + \left(\frac{1-i}{2}\right)\mathsf{Z}^b$ for $b \in \{0,1\}$, we can rewrite Equation (15) as,

$$\begin{aligned}\mathsf{T}\mathsf{X}^b\mathsf{Z}^a &= \mathsf{X}^b\mathsf{Z}^{a\oplus b}\left[\left(\frac{1+i}{2}\right)\mathsf{I} + \left(\frac{1-i}{2}\right)\mathsf{Z}^b\right]\mathsf{T}\\ &= \left[\left(\frac{1+i}{2}\right)\mathsf{X}^b\mathsf{Z}^{a\oplus b} + \left(\frac{1-i}{2}\right)\mathsf{X}^b\mathsf{Z}^a\right]\mathsf{T}.\end{aligned} \tag{16}$$

It follows from Equation (16) that for any $a, b \in \{0,1\}$, we can represent $\mathsf{T}\mathsf{X}^b\mathsf{Z}^a$ as a linear combination of $\mathsf{X}$ and $\mathsf{Z}$.

$$\mathsf{T}\mathsf{X}^b\mathsf{Z}^a = (\alpha_1\mathsf{I} + \alpha_2\mathsf{X} + \alpha_3\mathsf{Z} + \alpha_4\mathsf{X}\mathsf{Z})\mathsf{T} \tag{17}$$

where $\alpha_j \in \left\{0, 1, \frac{1+i}{2}, \frac{1-i}{2}\right\}$, for $j \in [4]$.

We further note that for a general $n$-qubit quantum unitary $U$ and $n$-qubit Pauli $P$, there exists a Clifford $C$ such that $UP|\psi\rangle = CU|\psi\rangle$. This is due to the *Clifford hierarchy* [32]. We also mention that if an $n$-qubit Clifford operation is given in matrix form, an efficient procedure exists in order to produce a circuit that executes this Clifford [39]. This is a special case of the general problem of *synthesis* of quantum circuits, which aims to produce quantum circuits, based on an initial description of a unitary operation.

## 5.1 Single-Qubit Circuits

Here, we show an indistinguishability obfuscation for single-qubit circuits. As previously mentionned, we note that for the single-qubit case, an efficient indistinguishability obfuscation can also be built using the Matsumoto-Amano normal form [29, 38]. Here, we give an alternate construction based on gate teleportation. Let $C_q$ be a 1-qubit circuit we want to obfuscate and $|\psi\rangle$ be the quantum state on which we want to evaluate $C_q$. Note that we can write any 1-qubit circuit as a sequence of gates from the set $\{\mathsf{H}, \mathsf{T}\}$[18]

$$C_q = (g_{|C_q|}, \ldots, g_2, g_1),\ g_i \in \{\mathsf{H}, \mathsf{T}\}\,.$$

For the indistinguishability obfuscation of a single-qubit circuit, we use the gate teleportation protocol (Algorithm 1), which leaves us (after the teleportation) with a subsystem of the form $C_q\mathsf{X}^b\mathsf{Z}^a(|\psi\rangle)$

$$C_q\mathsf{X}^b\mathsf{Z}^a(|\psi\rangle) = (g_{|C_q|}, \ldots, g_2, g_1)\mathsf{X}^b\mathsf{Z}^a(|\psi\rangle), \tag{18}$$

and to evaluate the circuit on $|\psi\rangle$, we have to apply a correction unitary. Now suppose we apply the gate $g_1$. We can write the system in Equation (18) as

$$C_q\mathsf{X}^b\mathsf{Z}^a(|\psi\rangle) = (g_{|C_q|}, \ldots, g_2)(\alpha_0\mathsf{I} + \alpha_1\mathsf{X} + \alpha_2\mathsf{Z} + \alpha_3\mathsf{XZ})g_1(|\psi\rangle) \tag{19}$$

where $\alpha_i \in \left\{0, 1, \frac{1+i}{2}, \frac{1-i}{2}\right\}$. Since $\{\mathsf{I}, \mathsf{X}, \mathsf{Z}, \mathsf{XZ}\}$, forms a basis, after applying the remaining gates in the sequence $(g_{|C_q|}, \ldots, g_3, g_2)$, we can write Equation (19) as

$$C_q\mathsf{X}^b\mathsf{Z}^a(|\psi\rangle) = (\beta_1\mathsf{I} + \beta_2\mathsf{X} + \beta_3\mathsf{Z} + \beta_4\mathsf{XZ})(g_{|C_q|}, \ldots, g_2, g_1)(|\psi\rangle) \tag{20}$$

where each $\beta_i \in \mathbb{C}$ and is computed by multiplying and adding numbers from the set $\{0, 1, \frac{1+i}{2}, \frac{1-i}{2}\}$. We show in Appendix A that the size of the coefficients $\beta_i$ grows at most as a polynomial in the number of $\mathsf{T}$-gates. Therefore it follows from Equation (20) that the update function for any 1-qubit circuit $C_q$ can be defined as the following map,

$$F_{C_q} : \{0,1\}^2 \to \mathbb{C}^4,\ (a, b) \mapsto (\beta_1, \beta_2, \beta_3, \beta_4),$$

and is in one-to-one correspondence with the correction unitary $\beta_1\mathsf{I} + \beta_2\mathsf{X} + \beta_3\mathsf{Z} + \beta_4\mathsf{XZ}$. As indicated, our construction for 1-qubit circuits is nearly the same as the gate teleportation scheme for Clifford circuits (Algorithm 3). The proof that this is a $qi\mathcal{O}$ scheme is also very similar to the proof for the Clifford construction (Section 4.2); we thus omit the formal proof here (it can also be seen as a special case of the proof of Theorem 5.3). Some subtleties, however are addressed below: the equivalence of the update functions (Lemma 5.1) and the circuit synthesis (Lemma 5.2).

**Lemma 5.1.** Let $C_{q_1}$ and $C_{q_2}$ be two equivalent 1-qubit circuits. Then their corresponding update functions in the gate teleportation protocol are also equivalent.

[18] The set $\{\mathsf{H}, \mathsf{T}\}$ is universal for 1-qubit unitaries [35].

*Proof.* Suppose $F_{C_{q_1}}(a,b) = (\beta_1, \beta_2, \beta_3, \beta_4, )$ and $F_{C_{q_2}}(a,b) = (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ are the corresponding update functions for $a, b \in \{0,1\}$. Since $C_{q_1}$ and $C_{q_2}$ are equivalent circuits, for every quantum state $|\psi\rangle$ and any $a, b \in \{0,1\}$,

$$
\begin{aligned}
& C_{q_1}\mathsf{X}^b\mathsf{Z}^a(|\psi\rangle) = C_{q_2}\mathsf{X}^b\mathsf{Z}^a(|\psi\rangle) \\
\Leftrightarrow\ & (\beta_1\mathsf{I} + \beta_2\mathsf{X} + \beta_3\mathsf{Z} + \beta_4\mathsf{XZ})C_{q_1}(|\psi\rangle) = (\gamma_1\mathsf{I} + \gamma_2\mathsf{X} + \gamma_3\mathsf{Z} + \gamma_4\mathsf{XZ})C_{q_2}(|\psi\rangle) \\
\Leftrightarrow\ & (\beta_1\mathsf{I} + \beta_2\mathsf{X} + \beta_3\mathsf{Z} + \beta_4\mathsf{XZ})C_{q_1}(|\psi\rangle) = (\gamma_1\mathsf{I} + \gamma_2\mathsf{X} + \gamma_3\mathsf{Z} + \gamma_4\mathsf{XZ})C_{q_1}(|\psi\rangle) \\
\Leftrightarrow\ & ((\beta_1 - \gamma_1)\mathsf{I} + (\beta_2 - \gamma_2)\mathsf{X} + (\beta_3 - \gamma_3)\mathsf{Z} + (\beta_4 - \gamma_4)\mathsf{XZ})C_{q_1}(|\psi\rangle) = \mathbf{0}. \\
\Rightarrow\ & (\beta_1 - \gamma_1)\mathsf{I} + (\beta_2 - \gamma_2)\mathsf{X} + (\beta_3 - \gamma_3)\mathsf{Z} + (\beta_4 - \gamma_4)\mathsf{XZ} = \mathbf{0}. \\
\Rightarrow\ & \beta_1 = \gamma_1,\ \beta_2 = \gamma_2,\ \beta_3 = \gamma_3,\ \beta_4 = \gamma_4.
\end{aligned}
$$

Therefore, $F_{C_{q_1}}$ and $F_{C_{q_2}}$ are equivalent functions. □

We note that, on top of being equal, the circuits that compute the update functions $F_{C_{q_1}}$, $F_{C_{q_2}}$ can be assumed to be of the same size. This follows by an argument very similar to the one in Remark 4.5.

**Lemma 5.2.** Based on the classical $i\mathcal{O}$ that computes the coefficients in Equation (20), it is possible to build a quantum circuit that performs the correction efficiently.

*Proof.* Given a $2 \times 2$ unitary matrix that represents a Clifford operation as in Equation (20), it is simple to efficiently derive the Clifford circuit that implements the unitary. This is a special case of the general efficient synthesis for Clifford circuits as presented in [39]. □

## 5.2 $qi\mathcal{O}$ via Gate Teleportation for all Quantum Circuits

In this section, we construct a $qi\mathcal{O}$ for all quantum circuits. The construction is efficient whenever the number of $\mathsf{T}$-gates is at most logarithmic in the circuit size (see Algorithm 5). The reason for this limitation is that the update function blows up once the number of $\mathsf{T}$-gates is greater than logarithmic in the circuit size. The construction is very similar to the gate teleportation for Clifford circuits (Section 4.2) and assumes the existence of a quantum-secure $i\mathcal{O}$ for classical circuits.

We are now ready to present our main theorem (Theorem 5.3). For ease of presentation, the proof relies on three auxiliary lemmas that are presented in the following section: Lemma 5.4 (which shows that equivalent circuits have equivalent update functions), Lemma 5.5 (which bounds the number of terms of the update function), and Lemma 5.6 (which shows that update functions can be computed by a polynomial-size circuits).

**Theorem 5.3.** (Main Theorem) If $i\mathcal{O}$ is a perfect/statistical/computational quantum-secure indistinguishability obfuscation for classical circuits, then Algorithm 5 is a perfect/statistical/computational quantum indistinguishability obfuscator for any quantum circuit $C_q$ with $\mathsf{T}$-count $\in O(\log |C_q|)$.

**Algorithm 5** $qi\mathcal{O}$ via Gate Teleportation for Quantum Circuits

- Input: A $n$-qubit quantum Circuit $C_q$ with $\mathsf{T}$-count $\in O(\log(|C_q|))$.

  1. Prepare a tensor product of $n$ Bell states: $|\beta^{2n}\rangle = |\beta_{00}\rangle \otimes \cdots \otimes |\beta_{00}\rangle$.
  2. Apply the circuit $C_q$ on the right-most $n$ qubits to obtain a system $|\phi\rangle$:
  $$|\phi\rangle = (\mathsf{I}_n \otimes C_q)|\beta^{2n}\rangle.$$
  3. Set $\hat{C} \leftarrow i\mathcal{O}(C)$. Where $C$ is a circuit that computes the update function $F_{C_q}$ as in Section 5.4. Note the size of $C$ is at most a polynomial in $|C_q|$ (Lemma 5.6).
  4. Description of the circuit $C'_q$ :
     (a) Perform a general Bell measurement on the leftmost $2n$-qubits on the system $|\phi\rangle \otimes |\psi\rangle$, where $|\phi\rangle$ is an auxiliary state and $|\psi\rangle$ is an input state. Obtain classical bits $(a_1, b_1 \ldots, a_n, b_n)$ and the state
     $$C_q(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})|\psi\rangle.$$
     (b) Compute the correction using the obfuscated circuit
     $$((\beta_1, \mathbf{s}_1), \ldots, (\beta_n, \mathbf{s}_k)) = \hat{C}(a_1, b_1 \ldots, a_n, b_n).$$
     (c) Using the above, the correction unitary is
     $$U_{F_{C_q}} = \sum_{i=1}^{4^k} \beta_i \mathsf{X}^{b_{i_1}} \mathsf{Z}^{a_{i_1}} \otimes \cdots \otimes \mathsf{X}^{bi_n} \mathsf{Z}^{a_{i_n}}.$$
     Compute a quantum circuit that applies $U_{F_{C_q}}$, using the circuit synthesis method of [39].
     (d) Apply the quantum circuit for $U_{F_{C_q}}$ to the system $C_q(\mathsf{X}^{\otimes_{i=1}^n b_i} \cdot \mathsf{Z}^{\otimes_{i=1}^n a_i})|\psi\rangle$ to obtain the state $C_q(|\psi\rangle)$.

*Proof.* We have to show that Algorithm 5 satisfies Definition 3.2. Throughout the proof, we assume that the quantum circuits have a logarithmic T-count in the circuit size.

1. `Functionality:` The proof of functionality follows from the principle of gate teleportation and is very similar to the proof in Theorem 4.2. Since the Clifford circuit synthesis has perfect correctness [39], we have $||C'_q(|\phi\rangle, \cdot) - C_q(\cdot)||_\diamond = 0 \leq \texttt{negl}(n)$ for any negligible function $\texttt{negl}(n)$.

2. `Polynomial Slowdown:` Note that $|\phi\rangle$ is a $2n$-qubit state and $C'_q$ is of type $(m, n)$, where $m = 3n$, therefore both $|\phi\rangle$ and $m$ have size in $O(|C_q|)$. The size of $C'_q$ is equal to the size of $\hat{C}$ plus the size of the circuit that performs the general Bell measurement ($GBM$) and the size of the circuit that computes the circuit for $U_{F_{C_q}}$. Since the size of $|GBM|$ is in $O(n)$, the size of $|\hat{C}|$ is polynomial in $|C_q|$ (Lemma 5.5, Lemma 5.6, Lemma A.1 and the definition of $i\mathcal{O}$). Moreover, efficient Clifford synthesis implies that the size of the circuit for $U_{F_{C_q}}$ is polynomial [39]. Therefore, there exists a polynomial $p(\cdot)$ such that

   - $||\phi\rangle| \leq p(|C_q|)$
   - $m \leq p(|C_q|)$
   - $|C'_q| \leq p(|C_q|)$.

3. `Perfect/Statistical/Computational Indistinguishability:` Let $C_{q_1}$ and $C_{q_2}$ be two $n$-qubit circuits of the same size. Let $\left(|\phi_1\rangle, C'_{q_1}\right)$ and $\left(|\phi_2\rangle, C'_{q_2}\right)$ be the outputs of Algorithm 3 on inputs $C_{q_1}$ and $C_{q_2}$ respectively. Since $C_{q_1}(|\tau\rangle) = C_{q_2}(|\tau\rangle)$ for every quantum state $|\tau\rangle$ we have,

$$|\phi_1\rangle = (I \otimes C_{q_1})|\beta^{2n}\rangle = (I \otimes C_{q_2})|\beta^{2n}\rangle = |\phi_2\rangle, \tag{21}$$

   The update functions for any two equivalent quantum circuits are equivalent (Lemma 5.4). If the classical $i\mathcal{O}$ that obfuscates the circuits for the update functions is perfectly/statistically/computationally indistinguishable, then states $C'_{q_1}$ and $C'_{q_2}$ are perfectly/statistically/computationally indistinguishable.[19] Therefore, Algorithm 5 is a perfectly/statistically/computationally indistinguishable quantum obfuscator for the quantum circuits. □

## 5.3 Equivalent Update Functions

Here, we provide a generalization of Lemma 4.3, applicable to the case of general circuits.

**Lemma 5.4.** Let $C_{q_1}$ and $C_{q_2}$ be two equivalent $n$-qubit circuits. Then their corresponding update functions are also equivalent.

[19] Note that circuits that compute update functions (for equivalent quantum circuits) may have different sizes. However, that can be managed as discussed in Remark 4.5.

*Proof.* Suppose $C_{q_1}$ and $C_{q_2}$ are two equivalent $n$-qubit quantum circuits, then for any quantum state $|\psi\rangle$ and for any binary string $\mathbf{r} \in \{0,1\}^{2n}$.

$$C_{q_1}(\mathsf{X}^{a_i}\mathsf{Z}^{b_i})^{\otimes_{i=1}^n}|\psi\rangle = C_{q_2}(\mathsf{X}^{a_i}\mathsf{Z}^{b_i})^{\otimes_{i=1}^n}|\psi\rangle. \tag{22}$$

Then the corresponding update functions are (see Equation (26))

$$F_{C_{q_1}}(\mathbf{r}) = ((\beta_1, \mathbf{s}_1), \ldots, (\beta_n, \mathbf{s}_k))$$
$$F_{C_{q_1}}(\mathbf{r}) = ((\beta'_1, \mathbf{s}'_1), \ldots, (\beta'_\ell, \mathbf{s}'_\ell))$$

where $\mathbf{s}_i = a_{i_1}b_{i_1}, \ldots, a_{i_n}b_{i_n} \in \{0,1\}^{2n}$, and $\mathbf{s}'_j = a_{j_1}b_{j_1}, \ldots, a_{j_n}b_{j_n} \in \{0,1\}^{2n}$. Without loss of generality, we can assume that $\beta_i \neq 0, \beta'_j \neq 0$ for $i \in [k], j \in [\ell]$. Using the update functions, we can rewrite Equation (22) as

$$\left(\sum_{i=1}^{4^k} \beta_i \mathsf{X}^{b_{i_1}}\mathsf{Z}^{a_{i_1}} \otimes \cdots \otimes \mathsf{X}^{bi_n}\mathsf{Z}^{a_{i_n}}\right) C_{q_1}|\psi\rangle = \left(\sum_{j=1}^{4^\ell} \beta'_j \mathsf{X}^{b'_{j_1}}\mathsf{Z}^{a'_{j_1}} \otimes \cdots \otimes \mathsf{X}^{b'_{j_n}}\right) C_{q_2}|\psi\rangle. \tag{23}$$

Since $C_{q_1}$ and $C_{q_2}$ are equivalent, we can replace $C_{q_2}$ with $C_{q_1}$ in Equation (23)

$$\left(\sum_{i=1}^{4^k} \beta_i \mathsf{X}^{b_{i_1}}\mathsf{Z}^{a_{i_1}} \otimes \cdots \otimes \mathsf{X}^{bi_n}\mathsf{Z}^{a_{i_n}}\right) C_{q_1}|\psi\rangle = \left(\sum_{j=1}^{4^\ell} \beta'_j \mathsf{X}^{b'_{j_1}}\mathsf{Z}^{a'_{j_1}} \otimes \cdots \otimes \mathsf{X}^{b'_{j_n}}\right) C_{q_1}|\psi\rangle \tag{24}$$

Then Equation (24) can only hold if

$$\left(\sum_{i=1}^{4^k} \beta_i \mathsf{X}^{b_{i_1}}\mathsf{Z}^{a_{i_1}} \otimes \cdots \otimes \mathsf{X}^{bi_n}\mathsf{Z}^{a_{i_n}}\right) = \left(\sum_{j=1}^{4^\ell} \beta'_j \mathsf{X}^{b'_{j_1}}\mathsf{Z}^{a'_{j_1}} \otimes \cdots \otimes \mathsf{X}^{b'_{j_n}}\right) \tag{25}$$

Note the update functions $F_{C_{q_1}}$ and $F_{C_{q_2}}$ are in one-to-one mapping with the unitaries on the left- and right-hand side of Equation (25) respectively. Since, the unitaries are equivalent, the corresponding update functions are also equivalent. □

## 5.4 Complexity of Computing the Update Function

Let $C_q$ be an $n$-qubit circuit consisting of a sequence of gates $g_1 \ldots, g_{|C_q|}$. The update function $F_{C_q}$ is computed by composing update functions for each gate in $C_q$.

$$F_{C_q} = f_{g_{|C_q|}} \circ \cdots \circ f_{g_2} \circ f_{g_1}.$$

Therefore the update function for any $n$-qubit quantum circuit $C_q$ with $k$ $\mathsf{T}$-gates can be defined as the following map.

$$\begin{aligned} &F_{C_q} : \{0,1\}^{2n} \longrightarrow (\mathbb{C} \times \{0,1\}^{2n})^{min(k,n)}, \\ &(a_1, b_1, \ldots, a_n, b_n) \mapsto ((\beta_1, \mathbf{s}_1), \ldots, (\beta_{4^k}, \mathbf{s}_{4^k})). \end{aligned} \tag{26}$$

which corresponds to the following correction unitary

$$\sum_{i=1}^{4^k} \beta_i \mathsf{X}^{b_{i_1}} \mathsf{Z}^{a_{i_1}} \otimes \cdots \otimes \mathsf{X}^{bi_n} \mathsf{Z}^{a_{i_n}}. \tag{27}$$

where $\beta_i \in \mathbb{C}$ and $\mathbf{s}_i = a_{i_1} b_{i_1}, \ldots, a_{i_n} b_{i_n} \in \{0,1\}^{2n}$, $i \in [4^k]$. Therefore, in order to satisfy the efficiency requirement (polynomial-slowdown), we must have $k \in O(\log(|C_q|))$. Note that the range of the update function can increase exponentially in the number of $\mathsf{T}$-gates as long as $k \leq n$ (Equation (26)). This is because there are at most $2^{2n}$ binary strings of length $2n$, therefore for any $n$-qubit circuit, the correction unitary Equation (27) can be written as a summation of at most $2^{2n}$ terms. We will first prove that as long as the $\mathsf{T}$-count in $O(\log(|C_q|)$, the number of terms in $F_{C_q}$ has at most $O(|C_q|)$ terms.

**Lemma 5.5.** If $C_q$ is an $n$-qubit quantum circuit with $\mathsf{T}$-count in $O(\log(|C_q|)$, then the update function $F_{C_q}$ (Equation (26)) has at most $O(|C_q|)$ terms.

*Proof.* Let $C_q$ be an $n$-qubit circuit with $\mathsf{T}$-count in $O(\log(|C_q|)$. Suppose we want to evaluate $C_q$ on some $n$-qubit state $|\psi\rangle$, then after the step 4a of Algorithm 5, we will obtain a state

$$C_q(\mathsf{X}^{a_1}\mathsf{Z}^{b_1} \otimes \mathsf{X}^{a_2}\mathsf{Z}^{b_2} \otimes \cdots \otimes \mathsf{X}^{a_n}\mathsf{Z}^{b_n})|\psi\rangle. \tag{28}$$

In order to recover $C_q(|\psi\rangle)$ from the above expression, we multiply the correction unitary $U_{F_{C_q}}$ to the left hand side of expression Equation (28). To compute $U_{F_{C_q}}$ we first compute the update function $F_{C_q}$ on the input $a_1 b_1, \ldots, a_n b_n$

$$F_{C_q}(a_1 b_1, \ldots, a_n b_n) = ((\beta_1, \mathbf{s}_1), \ldots, (\beta_{4^k}, \mathbf{s}_{4^k}))$$

where $\beta_i \in \mathbb{C}$, $\mathbf{s}_i \in \{0,1\}^{2n}$, $k \in \mathbb{N}$

$$U_{F_{C_q}} = \sum_{i=1}^{4^k} \beta_i \mathsf{X}^{b_{i_1}} \mathsf{Z}^{a_{i_1}} \otimes \cdots \otimes \mathsf{X}^{bi_n} \mathsf{Z}^{a_{i_n}}.$$

We will show that if the $\mathsf{T}$-count is in $O(\log(|C_q|)$, then $k \in O(|C_q|)$ (number of terms). Recall that

$$\mathsf{T}\mathsf{X}^b\mathsf{Z}^a = (\alpha_1 \mathsf{I} + \alpha_2 \mathsf{X} + \alpha_3 \mathsf{Z} + \alpha_4 \mathsf{X}\mathsf{Z})\mathsf{T} \tag{29}$$

- **Case 0**: Suppose $C_q$ has no $\mathsf{T}$-gates, then $C_q$ is a Clifford and there is only one term in $F_{C_q}$. Therefore $k = 0$.
- **Case 1**: Suppose $C_q$ has one $\mathsf{T}$-gate (acting on some $\ell$-th wire).

$$\begin{aligned} &C_q(\mathsf{X}^{a_1}\mathsf{Z}^{b_1} \otimes \cdots \otimes \mathsf{X}^{a_n}\mathsf{Z}^{b_n}) \\ &= (\mathsf{X}^{\otimes_{i=1}^{\ell-1} b'_i}\mathsf{Z}^{\otimes_{i=1}^{\ell-1} a'_i}) \otimes \left(\sum_{j=1}^{4} \beta_j \mathsf{X}^{b'_j}\mathsf{Z}^{a'_j}\right) \otimes (\mathsf{X}^{\otimes_{i=\ell+1}^{n} b'_i}\mathsf{Z}^{\otimes_{i=\ell+1}^{n} a'_i}) C_q \\ &= \sum_{i=1}^{4} \beta_i \mathsf{X}^{b'_{i_1}} \mathsf{Z}^{a'_{i_1}} \otimes \cdots \otimes \mathsf{X}^{b'_{i_n}} \mathsf{Z}^{a'_{i_n}}. \end{aligned} \tag{30}$$

Therefore $k \leq 4$. It is important to realize that 4 is the maximum number of terms a circuit with $\mathsf{T}$ can have. No Clifford gate including $\mathsf{CNOT}$ can increase the number of terms beyond 4. This is because only a $\mathsf{T}$ gate can contribute a 4-term expression and then we expand all the terms in the correction unitary to maximum (Equation (30)). Now any Clifford acting on the correction unitary will act linearly on $U_{F_{C_q}}$ and only affect the bits $a'_i$ and $b'_i$ (Equation (30)).

- **Case 2**: Similarly, if $C_q$ has two $\mathsf{T}$ gates, then each will contribute at most one expression of the form $(\beta_1 \mathsf{I} + \beta_2 \mathsf{X} + \beta_3 \mathsf{Z} + \beta_4 \mathsf{XZ})$. This will give us a correction unitary $U_{F_{C_q}} = \sum_{i=1}^{4^2} \beta_i \mathsf{X}^{b_{i_1}} \mathsf{Z}^{a_{i_1}} \otimes \cdots \otimes \mathsf{X}^{bi_n} \mathsf{Z}^{a_{i_n}}$, therefore $k \leq 16$. Note that it makes no difference whether $\mathsf{T}$ gates are acting on the same wire or on different wires for the worst-case analysis. If they are on the same wire, then the first $\mathsf{T}$ will contribute 4 terms and the second $\mathsf{T}$ will expand each term into 4 more terms, resulting in 16 terms. If they are acting on different wires, say $i$ and $j$ and suppose $\mathsf{CNOT}$s are acting on the $i$-th to $j$-th wire, then we may have to expand all terms in the unitary to apply $\mathsf{CNOT}$s. This again can contribute at most 16 terms.

  **General Case**: Suppose $C_q$ has $O(\log(|C_q|)$ $\mathsf{T}$ gates, then each $\mathsf{T}$-gate will contribute at most a linear combination of 4 terms and in total at most $4^{O(\log(|C_q|)}$ terms. therefore $k \in O(|C_q|)$. □

**Lemma 5.6.** If $C_q$ be an $n$-qubit quantum circuit with $\mathsf{T}$-count $\in O(\log |C_q|)$, then there exists a classical circuit $C$ and a polynomial $p(\cdot)$ such that

- $C$ computes the update function $F_{C_q}$,
- $|C| \leq p(|C_q|)$.

*Proof.* Let $C_q$ be a $n$-qubit quantum circuit with $\mathsf{T}$-count $\in O(\log |C_q|)$. Recall from Section 2.14 that the corresponding update functions for the Clifford + $\mathsf{T}$ gate set are:

- $f_{\mathsf{X}}(a_1, b_1) = (a_1, b_1)$
- $f_{\mathsf{Z}}(a_1, b_1) = (a_1, b_1)$
- $f_{\mathsf{H}}(a_1, b_1) = (b_1, a_1)$
- $f_{\mathsf{P}}(a_1, b_1) = (a_1, a_1 \oplus b_1)$
- $f_{\mathsf{CNOT}}(a_1, b_1, a_2, b_2) = (a_1 \oplus a_2, b_1, a_2, b_1 \oplus b_2)$
- $f_{\mathsf{T}}(a, b) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$

Let $C_{\mathsf{X}}$, $C_{\mathsf{Z}}$, $C_{\mathsf{H}}$, $C_{\mathsf{P}}$, $C_{\mathsf{CNOT}}$ and $C_{\mathsf{T}}$ denote the classical circuits (called *subcircuits*) that compute $f_{\mathsf{X}}, f_{\mathsf{Z}}, f_{\mathsf{H}} f_{\mathsf{P}}, f_{\mathsf{CNOT}}$ and $f_{\mathsf{T}}$ respectively. Clearly, these subcircuits are of constant size. Recall that all subcircuits for Cliffords map $k$-bit strings to $k$-bit strings ($k \in \{0, 1\}$), but $C_{\mathsf{T}}$ expands its 2-bit input into a $4\ell$-bit

strings (where $\ell = \max\{\left|\frac{1+i}{2}\right|, \left|\frac{1-i}{2}\right|\}$[20]. Let $C$ be a circuit that computes $F_{C_q}$. Then $C$ can be expressed in terms of these gadgets. To construct $C$, we go gate-by-gate in $C_q$ and employ the corresponding subcircuit. If $C_q$ is a Clifford circuit, then $C$ only consists of Clifford subcircuit (as mentioned earlier they map $k$ bits to $k$ bits $k \in \{2, 4\}$ there are $O(|C_q|)$ gadgets in the circuit $C$). Otherwise if $C_q$ has $k$ $\mathsf{T}$-gates, then each $C_{\mathsf{T}}$ subcircuit will map a 2-bit string to a $4\ell$-bit string, potentially increasing the size of $C$ to $O((4\ell)^k)$, but since $k \in O(\log(|C_q|)$, we have $O((4\ell)^k) \in O(|C_q|)$. Therefore, there exists a polynomial $p(\cdot)$ such that $|C| \leq p(n)$. □

# 6 Quantum Indistinguishability Obfuscation with Respect to a Pseudo-Distance

In this section, we provide a definition for circuits that are approximately equivalent (with respect to a pseudo-distance) (Definition 6.1). In Section 6.2, we present a definition of quantum indistinguishability obfuscation with respect to a pseudo-distance, and in Section 6.3, we present a scheme that satisfies this definition, for circuits close to a fixed level of the Gottesman-Chuang hierarchy.

## 6.1 Approximately Equivalent Quantum Circuits

**Definition 6.1.** (Approximately Equivalent Quantum Circuits): Let $C_{q_0}$ and $C_{q_1}$ be two $n$-qubit quantum circuits and $\mathbf{D}$ be a pseudo-distance. We say $C_{q_0}$ and $C_{q_1}$ are *approximately equivalent* with respect to $\mathbf{D}$ if there exists a negligible function $\mathtt{negl}(n)$ such that

$$\mathbf{D}(C_{q_0}, C_{q_1}) \leq \mathtt{negl}(n).$$

## 6.2 Indistinguishability Obfuscation for Approximately Equivalent Quantum Circuits

In this section, we provide a definition of quantum indistinguishability obfuscation for approximately equivalent circuits, $qi\mathcal{O}_{\mathbf{D}}$. To be consistent with Definition 3.2, we require that the obfuscator, on input a quantum circuit $C_q$, outputs an auxiliary quantum state $|\phi\rangle$ and a quantum circuit $C'_q$, but note in the actual construction (Algorithm 6), the state $|\phi\rangle$ is an empty register. Here, we consider only the case of *statistical* security. Notable here is the indistinguishability property is required to hold not only for equivalent quantum circuits, but also for *approximately* equivalent quantum circuits. Also, contrary to Definition 3.2, we only require the indistinguishability for large values of $n$.

**Definition 6.2.** Let $\mathcal{C}_Q$ be a polynomial-time family of reversible quantum circuits and let $\mathbf{D}$ be a pseudo-distance. For $n \in \mathbb{N}$, let $C_q^n$ be the circuits in $\mathcal{C}_Q$ of input length $n$. A polynomial-time quantum algorithm for $\mathcal{C}_Q$ is a *statistically*

[20] The notation $|a + bi|$ denotes the number of bits to represent the complex number $a + bi$.

*secure quantum indistinguishability obfuscator* ($qi\mathcal{O}_{\mathbf{D}}$) for $\mathcal{C}_Q$ *with respect to* $\mathbf{D}$ if the following conditions hold:

1. `Functionality:` There exists a negligible function $\mathtt{negl}(n)$ such that for every $C_q \in C_q^n$

$$(|\phi\rangle, C_q') \leftarrow qi\mathcal{O}_{\mathbf{D}}(C_q) \text{ and } \mathbf{D}(C_q'(|\phi\rangle, \cdot), C_q(\cdot)) \leq \mathtt{negl}(n).$$

   Where $|\phi\rangle$ is an $\ell$-qubit state, the circuits $C_q$ and $C_q'$ are of type $(n, n)$ and $(m, n)$ respectively ($m = \ell + n$).[21]

2. `Polynomial Slowdown:` There exists a polynomial $p(n)$ such that for any $C_q \in C_q^n$,
   - $\ell \leq p(|C_q|)$
   - $m \leq p(|C_q|)$
   - $|C_q'| \leq p(|C_q|)$.

3. `Statistically Secure Indistinguishability:` For any two **approximately equivalent** quantum circuits $C_{q_0}, C_{q_1} \in C_q^n$, of the same size **and for large enough** $n$, the two distributions $qi\mathcal{O}_{\mathbf{D}}(C_{q_0})$ and $qi\mathcal{O}_{\mathbf{D}}(C_{q_1})$ are statistically indistinguishable.

## 6.3 $qi\mathcal{O}_{\mathbf{D}}$ for Circuits Close to the Gottesman-Chuang Hierarchy

Here, we present a quantum indistinguishability obfuscation (Definition 3.2) for a family of circuits that are approximately equivalent (Definition 6.1) with respect to the pseudo-distance $\mathbf{D}(U_1, U_2) = \frac{1}{\sqrt{2d^2}}||U_1 \otimes U_1^* - U_2 \otimes U_2^*||_F$ (see Section 2.6). There are two main ingredient in our construction, one is Low's learning algorithm [37] (described below) and the second is Lemma 6.3.

In [37] Low presents a learning algorithm that, given oracle access to a unitary $U$ and its conjugate $U^\dagger$ with the promise that the distance $\mathbf{D}(U, C) \leq \epsilon < \frac{1}{2^{k-1/2}}$ for some $C \in \mathcal{C}_k$ (Section 2.9), outputs a circuit $C_q$ for computing $C$ with probability at least $1 - \delta$ with

$$O\left(\frac{1}{\epsilon'^2}(2n)^{k-1}\log\left(\frac{(2n+1)^{k-1})}{\delta}\right)\right)$$

queries. Where $\epsilon' := \sqrt{2(1-(2^{k-1}\epsilon)^2} - 1 > 0$ and $\mathbf{D}(U_1, U_2) = \frac{1}{\sqrt{2d^2}}||U_1 \otimes U_1^* - U_2 \otimes U_2^*||_F$ is the pseudo-distance defined in Section 2.6.

Based on Low's work, we construct an quantum indistinguishability obfuscation $qi\mathcal{O}_{\mathbf{D}}$ with respect to this pseudo-distance $\mathbf{D}$ for circuits that are very close to $\mathcal{C}_k$. Note that the run-time of Low's algorithm is exponential in $k$. Moreover, the algorithm becomes infeasible if $\epsilon'$ is very small. Therefore, to ensure that

[21] A circuit is of type $(i, j)$ if it maps $i$ qubits to $j$ qubits.

our construction in Algorithm 6 runs in polynomial-time we set $k$ to be some fixed positive integer and $\epsilon \leq \texttt{negl}(n) < \frac{1}{2^{k-1/2}}$ for all $n$. Note if $\epsilon < \frac{1}{2^{k-1/2}}$, then $\epsilon' \geq \frac{\sqrt{7}}{2} - 1$.

**Lemma 6.3.** Let $U$ and $C$ be unitaries. If the distance $\mathbf{D}(U, C) < \frac{1}{2^{k-1/2}}$ for some $C \in \mathcal{C}_k$, then $C$ is unique up to phase.

*Proof.* See [37]. □

**Theorem 6.4.** Let $\mathcal{C}_Q = \{U_{q^{n,k}} \mid n \in \mathbb{N} \text{ and } k \text{ is fixed positive integer}\}$, be a polynomial-time family of reversible quantum circuits. Here, $U_{q^{n,k}}$ denotes the $n$-qubit circuits for which there exists a negligible function $\texttt{negl}(n)$ such that for any $U_q \in U_{q^{n,k}}$, there exists a $C_q \in \mathcal{C}_k$ that satisfies $\mathbf{D}(U_q, C_q) < \texttt{negl}(n) < \frac{1}{2^{k+1/2}}$. Then Algorithm 6 is a statistically-secure quantum indistinguishability obfuscation for $\mathcal{C}_Q$ with respect to $\mathbf{D}$.

**Algorithm 6** *qi*$\mathcal{O}$-Gottesman-Chuang

- Input: An $n$-qubit circuit $U_q \in U_{q^{n,k}}$, $k$ and $\delta = \texttt{negl}(n)$).
  1. From $U_q$ compute the circuit $U_q^\dagger$.
  2. Using Low's approximate learning algorithm on inputs $U_q$ and ${U_q}^\dagger$ compute the circuit $C_q$ [37].
  3. Output the circuit $C_q$.

*Proof.* We have to show that Algorithm 6 satisfies Definition 6.2.

1. `Functionality:` On input $U_q \in U_{q^{n,k}}$, let $C_q$ be the output of Algorithm 6. By assumption (Theorem 6.4) there exists a unitary $C \in \mathcal{C}_k$ such that $\mathbf{D}(U_q, C) < \texttt{negl}(n) < \frac{1}{2^{k+1/2}}$. From Lemma 6.3, $C$ is unique up to a global phase. Therefore with overwhelming probability, Low's approximate learning algorithm will output a circuit $C_q$ that computes $C$. We have $\mathbf{D}(U_q, C_q) = \mathbf{D}(U_q, C_q) < \texttt{negl}(n)$, therefore $U_q$ and $C_q$ are approximately equivalent.

2. `Polynomial Slowdown:` The total cost of Algorithm 6 is the cost of computing the circuit $U_q^\dagger$ from $U_q$ plus the cost of Low's learning algorithm. Clearly, we can compute $U_q^\dagger$ from $U_q^\dagger$ in polynomial-time. Using Low's algorithm (for parameters defined in Theorem 6.4 and setting $\delta = \texttt{negl}(n)$) we can learn $C_q$ with probability at least $1 - \texttt{negl}(n)$ in time at most

$$O\left(n^{k-1}\left[(k-1)\log((2n+1)) - \log(\texttt{negl}(n))\right]\right).$$

   Which is at most a polynomial in $n$ (since $k$ is a constant). Therefore, Algorithm 6 runs in polynomial-time.

3. `Statistically Indistinguishability:` Let $U_q, U'_q \in U_{q^{n,k}}$ be two circuits such that

$$\mathbf{D}(U_q, U'_q) < \mathtt{negl}(n).$$

By assumption (Theorem 6.4), there exist unitaries $C, C' \in \mathcal{C}_k$ such that $\mathbf{D}(U_q, C) < \mathtt{negl}(n) < \frac{1}{2^{k+1/2}}$ and $\mathbf{D}(U'_q, C') < \mathtt{negl}(n) < \frac{1}{2^{k+1/2}}$. Using the triangle inequality we can easily show that $C$ and $C'$ are equivalent circuit (up to a global phase) for large $n$.

$$\mathbf{D}(U_q, C') \leq \mathbf{D}(U_q, U'_q) + \mathbf{D}(U'_q, C') \leq \mathtt{negl}(n) + \frac{1}{2^{k+1/2}}$$
$$\implies \mathbf{D}(U_q, C') < \frac{1}{2^{k+1/2}} + \frac{1}{2^{k+1/2}} < \frac{1}{2^{k-1/2}}$$

According Lemma 6.3 $C'$ is unique (up to a global phase) such that $\mathbf{D}(U_q, C') < \frac{1}{2^{k-1/2}}$, But $C$ also satisfies $\mathbf{D}(U_q, C) < \frac{1}{2^{k-1/2}}$. It follows that $C$ and $C'$ are equivalent circuits (up to a global phase). Moreover, the outputs of Low's algorithm $C_q$ and $C'_q$ on any two equivalent unitaries (up to global phase) is statistically indistinguishable [37]. Therefore, for any $U_q, U'_q \in U_{q^{n,k}}$, the two distributions $qi\mathcal{O}_{\mathbf{D}}(U_q)$ and $qi\mathcal{O}_{\mathbf{D}}(U'_q)$ are statistically indistinguishable. □


## Acknowledgements

We thank an anonymous reviewer for pointing out the work of [37]; we would also like to thank Yfke Dulek for related discussions. This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-20-1-0375, Canada's NFRF and NSERC, an Ontario ERA, and the University of Ottawa's Research Chairs program.


## A Size of Coefficients in the Update Functions

Here, we prove a Lemma that is used in Section 5.1.

**Lemma A.1.** Let $C_q$ be an $n$-qubit $poly(n)$ size quantum circuit with $O(\log(n))$ number of gates and $F_{C_q}$ be the corresponding update function

$$F_{C_q} : \{0,1\}^{2n} \longrightarrow (\mathbb{C} \times \{0,1\}^{2n})^{min(k,n)},$$
$$(a_1, b_1, \ldots, a_n, b_n) \mapsto ((\beta_1, \mathbf{s}_1), \ldots, (\beta_{4^k}, \mathbf{s}_{4^k}))\,.$$

then there exists a polynomial $p(\cdot)$ such $\beta_i \in O(p(n))$ for all $i \in [4^k]$.

*Proof.* The following map is an isomorphism between $\mathbb{C}$ and $\mathbb{R}^2$

$$f : \mathbb{C} \leftarrow \mathbb{R}^2,\ (a + b_i) \mapsto (a, b) \tag{31}$$

Note that there is a one-to-one map between $F_{C_q}$ and the corresponding unitary $U_{F_{C_q}} = \sum_{i=1}^{4^k} \beta_i \mathsf{X}^{b_{i_1}} \mathsf{Z}^{a_{i_1}} \otimes \cdots \otimes \mathsf{X}^{bi_n} \mathsf{Z}^{a_{i_n}}$, $k \leq n$. Note that any Clifford gate can only affect the correction bits in unitaries of type $U_{F_{C_q}}$, but will have no effect on the coefficients $\beta_i$. So the coefficients can be affected by $\mathsf{T}$ gates. Therefore, to estimate the size of the coefficients we can ignore other gates. Each $\beta_i$ is constructed by adding and multiplying numbers from the set $\left\{0, 1, \frac{1+i}{2}, \frac{1-i}{2}\right\}$. We note the following relationships between $\frac{1+i}{2}, \frac{1-i}{2}$

$$\left(\frac{1+i}{2}\right) \pm \left(\frac{1-i}{2}\right) = \pm 1.$$

If $m = 2\ell + 1$ and $\ell \in \mathbb{N}$, then

$$\left(\frac{1 \pm i}{2}\right)^m = \left(\frac{a}{2}\right)^\ell, \; a \in \{\pm 1, \pm i\}.$$

Else if $m = 2\ell$ and $\ell \in \mathbb{N} \cup \{0\}$, then

$$\left(\frac{1 \pm i}{2}\right)^m = \left(\frac{a}{2}\right)^\ell \left(\frac{1 \pm i}{2}\right), \; a \in \{\pm 1, \pm i\}$$

Therefore, we can represent $\left(\frac{1 \pm i}{2}\right)^m$ in $O(m)$ bits and $\left(\frac{1+i}{2}\right)^m \left(\frac{1-i}{2}\right)^m$ in $O(m)$ bits. Of course $1^m = 1$ and adding 1 to itself is $m$. For each application of $\mathsf{T}$, a coefficient will multiply and add at most polynomial time in the circuit size and there are $O(\log(n))$ such gates, therefore there exists a polynomial $p(\cdot)$ such that $|\beta_i| \in O(p(n))$, for every $i \in [4^k]$. □

# References


[1] S. Aaronson. Quantum copy-protection and quantum money. In *24th Annual Conference on Computational Complexity—CCC 2009*, pages 229–242, 2009. DOI: 10.1109/CCC.2009.42.

[2] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, 2004. DOI: 10.1103/PhysRevA.70.052328.

[3] G. Alagic, Z. Brakerski, Y. Dulek, and C. Schaffner. Impossibility of quantum virtual black-box obfuscation of classical circuits, 2020. https://arxiv.org/abs/2005.06432.

[4] G. Alagic and B. Fefferman. On quantum obfuscation, 2016. Available at https://arxiv.org/abs/1602.01771.

[5] G. Alagic, S. Jeffery, and S. Jordan. Circuit obfucation using braids. In *9th Conference on the Theory of Quantum Computation, Communication and Cryptography—TQC 2014*, pages 141–160, 2014. DOI: 10.4230/LIPIcs.TQC.2014.141.

[6] M. Albrecht, S. Bai, and L. Ducas. A subfield lattice attack on overstretched NTRU assumptions. In *Advances in Cryptology—CRYPTO 2016*, volume 1, pages 153–178, 2016. DOI: 10.1007/978-3-662-53018-4_6.

[7] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *41st Annual Symposium on Foundations of Computer Science—FOCS 2000*, pages 547–553, 2000. DOI: 10.1109/SFCS.2000.892142.

[8] M. Amy, D. Maslov, and M. Mosca. Polynomial-time $T$-depth optimization of Clifford+$T$ circuits via matroid partitioning. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(10):1476–1489, 2014. DOI: 10.1109/TCAD.2014.2341953.

[9] M. Amy, D. Maslov, M. Mosca, and M. Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 32(6):818–830, 2013. DOI: 10.1109/TCAD.2013.2244643.

[10] P. Ananth, A. Jain, H. Lin, C. Matt, and A. Sahai. Indistinguishability obfuscation without multilinear maps: New paradigms via low degree weak pseudorandomness and security amplification. In *Advances in Cryptology—CRYPTO 2019*, volume 3, pages 284–332, 2019. DOI: 10.1007/978-3-030-26954-8_10.

[11] P. Ananth and R. L. La Placa. Secure software leasing, 2020. https://arxiv.org/abs/2005.05289.

[12] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. *Journal of the ACM*, 59(2):6, 2012. DOI: 10.1145/2160158.2160159.

[13] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895, 1993. DOI: 10.1103/PhysRevLett.70.1895.

[14] N. Bitansky and O. Paneth. ZAPs and non-interactive witness indistinguishability from indistinguishability obfuscation. In *12th Theory of Cryptography Conference—TCC 2015*, volume II, pages 401–427, 2015. DOI: 10.1007/978-3-662-46497-7_16.

[15] D. Boneh and M. Zhandry. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. In *Advances in Cryptology—CRYPTO 2014*, volume I, pages 480–499, 2014. DOI: 10.1007/978-3-662-44371-2_27.

[16] Z. Brakerski. Quantum FHE (almost) as secure as classical. In *Advances in Cryptology—CRYPTO 2018*, volume 3, pages 67–95, 2018. DOI: 10.1007/978-3-319-96878-0_3.

[17] A. Broadbent and S. Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In *Advances in Cryptology—CRYPTO 2015*, volume 2, pages 609–629, 2015. DOI: 10.1007/978-3-662-48000-7_30.

[18] A. Broadbent and R. A. Kazmi. Constructions for quantum indistinguishability obfuscation. 2020. Available online: https://eprint.iacr.org/2020/639.

[19] A. Broadbent and S. Lord. Uncloneable quantum encryption via oracles. In *Theory of Quantum Computation, Communication, and Cryptography—TQC 2020*, pages 4:1–4:22, 2020. DOI: 10.4230/LIPIcs.TQC.2020.4.

[20] R. Canetti, H. Lin, S. Tessaro, and V. Vaikuntanathan. Obfuscation of probabilistic circuits and applications. In *12th Theory of Cryptography Conference—TCC 2015*, volume II, pages 468–497, 2015. DOI: 10.1007/978-3-662-46497-7_19.

[21] Y. Chen, C. Gentry, and S. Halevi. Cryptanalyses of candidate branching program obfuscators. In *Advances in Cryptology—EUROCRYPT 2017*, volume 3, pages 278–307, 2017. DOI: 10.1007/978-3-319-56617-7_10.

[22] J.-S. Coron, T. Lepoint, and M. Tibouchi. Practical multilinear maps over the integers. In *Advances in Cryptology—CRYPTO 2013*, volume 1, pages 476–493, 2013. DOI: 10.1007/978-3-642-40041-4_26.

[23] R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Advances in Cryptology—EUROCRYPT 2016*, volume 2, pages 559–585, 2016. DOI: 10.1007/978-3-662-49896-5_20.

[24] O. Di Matteo and M. Mosca. Parallelizing quantum circuit synthesis. *Quantum Science and Technology*, 1(1):015003, 2016. DOI: 10.1088/2058-9565/1/1/015003.

[25] Y. Dulek, C. Schaffner, and F. Speelman. Quantum homomorphic encryption for polynomial-sized circuits. In *Advances in Cryptology—CRYPTO 2016*, pages 3–32, 2016. DOI: 10.1007/978-3-662-53015-3_1.

[26] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th Annual Symposium on Foundations of Computer Science—FOCS 2013*, pages 40–49, 2013. DOI: 10.1109/FOCS.2013.13.

[27] R. Gay, A. Jain, H. Lin, and A. Sahai. Indistinguishability obfuscation from simple-to-state hardness assumptions. 2021. Available at https://eprint.iacr.org/2020/764.pd.

[28] C. Gentry, S. Gorbunov, and S. Halevi. Graph-induced multilinear maps from lattices. In *12th Theory of Cryptography Conference—TCC 2015*, volume 2, pages 498–527, 2015. DOI: 10.1007/978-3-662-46497-7_20.

[29] B. Giles and P. Selinger. Remarks on Matsumoto and Amano's normal form for single-qubit Clifford+$T$ operators, 2019. Available at https://arxiv.org/abs/1312.6584.

[30] S. Goldwasser and G. N. Rothblum. On best-possible obfuscation. *Journal of Cryptology*, 27(3):480–505, 2014. DOI: 10.1007/s00145-013-9151-z.

[31] D. Gottesman. The Heisenberg representation of quantum computers. In *22nd International Colloquium on Group Theoretical Methods in Physics—GROUP 22*, pages 32–43, 1998. arXiv: quant-ph/9807006.

[32] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390–393, 1999. DOI: 10.1038/46503.

[33] S. Guo, T. Malkin, I. C. Oliveira, and A. Rosen. The power of negations in cryptography. In *12th Theory of Cryptography Conference—TCC 2015*, volume 1, pages 36–65, 2015. DOI: 10.1007/978-3-662-46494-6_3.

[34] A. Jain, H. Lin, and A. Sahai. Indistinguishability obfuscation from well-founded assumptions, 2020. Available at https://eprint.iacr.org/2020/1003.

[35] P. Kaye, R. Laflamme, and M. Mosca. *An introduction to quantum computing*. Oxford, 2007.

[36] A. Langlois, D. Stehlé, and R. Steinfeld. GGHLite: More efficient multilinear maps from ideal lattices. In *Advances in Cryptology—EUROCRYPT 2014*, pages 239–256, 2014. DOI: 10.1007/978-3-642-55220-5_14.

[37] R. A. Low. Learning and testing algorithms for the Clifford group. *Physical Review A*, 80(5):052314, 2009. DOI: https://doi.org/10.1103/PhysRevA.80.052314.

[38] K. Matsumoto and K. Amano. Representation of quantum circuits with Clifford and $\pi/8$ gates, 2008. Available at https://arxiv.org/abs/0806.3834.

[39] P. Niemann, R. Wille, and R. Drechsler. Efficient synthesis of quantum circuits implementing Clifford group operations. In *19th Asia and South Pacific Design Automation Conference—ASP-DAC 2014*, pages 483–488, 2014. DOI: 10.1109/ASPDAC.2014.6742938.

[40] A. Sahai and B. Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *46th Annual ACM Symposium on Theory of Computing—STOC 2014*, pages 475–484, 2014. DOI: 10.1145/2591796.2591825.

[41] P. Selinger. Generators and relations for $n$-qubit Clifford operators, 2013. Available at https://arxiv.org/abs/1310.6813.

[42] M. Sipser. *Introduction to the Theory of Computation*. Cengage Learning, 3rd edition, 2012.

[43] F. Speelman. Instantaneous non-local computation of low $T$-depth quantum circuits. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography—TQC 2016*, pages 9:1–9:24, 2016. DOI: 10.4230/LIPIcs.TQC.2016.9.