Indistinguishability obfuscation for quantum circuits of low T-count

Anne Broadbent and Raza Ali Kazmi

University of Ottawa,
Department of Mathematics and Statistics
{abroadbe,rkazmi}@uottawa.ca

Abstract. An *indistiguishability 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 computationally indistinguishable. Here, we study schemes for indistinguishability obfuscation for *quantum* circuits ($qi\mathcal{O}$), which consists in a procedure that takes as input a quantum circuit and outputs a quantum state, together with a quantum circuit, which together can be used to evaluate the original quantum circuit on any quantum input; the security guarantee being that for two quantum circuits of the same size that have the same input-output behaviour, the outputs of the obfuscator are computationally indistinguishable. Our main result provides a construction for $qi\mathcal{O}$, where the size of the output of the obfuscator is exponential in the number of non-Clifford (T gates), which means that the construction is efficient as long as the number of T gates is logarithmic in the circuit size.

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 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 [10] to be unachievable in general. Motivated by this impossibility result, the same work proposed a weaker notion called *indistinguishability obfuscation* ($i\mathcal{O}$).

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 [26]. Indistinguishability obfuscation is a very powerful cryptographic tool which is known to enable, among others: digital signatures, public key encryption [34], multiparty key agreement, broadcast encryption [13], fully homomorphic encryption [17] and witness-indistinguishable proofs [12]. Notable in the context of these applications is the *punctured programming technique* [34] 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 [23], with security relying on the presumed hardness of multilinear maps [19,24,31]. Unfortunately, there have been many quantum attacks on multilinear maps [5,18,20]. Recently, a new $i\mathcal{O}$ scheme was proposed under different assumptions [9]. Whether or not this scheme is resistant against quantum attacks remains to be determined.

Indistinguishability obfuscation has been studied for *quantum* circuits in [3, 4]. In a nutshell (see Section 1.3 for more details), [4] shows a type of obfuscation for quantum circuits, but without a security reduction. On the other hand, the focus of [3] 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. We now overview our results and techniques.

First, we define indistinguishability obfuscation for quantum circuits ($qi\mathcal{O}$) (Section 3). Importantly, 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, with the property that $C_q'(|\phi\rangle, |\psi\rangle) = C_q(|\psi\rangle)$ for all inputs $|\psi\rangle$. 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 [28]. 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 [27]; 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.

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 [35]). 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 [28]: 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 bits. 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 (note that our construction does not require a full $i\mathcal{O}$ but rather relies on a weaker $i\mathcal{O}$ that can obfuscate a certain family of functions.) 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 2.10) 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, 16].

Obfuscating Beyond Cliffords. Next, in our main result (Section 5), we generalize the gate-teleportation scheme for Clifford circuits, and show a $qi\mathcal{O}$ 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+T gate-set[2], and we note that the T relates to the X, 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 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 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+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

---

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

[2] The term T-*count* thus refers to the *number* of T-gates in a given circuit.

number of T gates increases. We show that if we limit the number of 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 [25, 32].

We note that, for many other quantum cryptographic primitives, it is the case that the 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* [15, 22], and instantaneous quantum computation [37]. Because of these applications, and since the T is also typically also the bottleneck for fault-tolerant quantum computing, techniques exist to reduce the T-count in quantum circuits [7, 8, 21].

1.2 Applications

As mentioned above, indistinguishability obfuscation is known to enable a host of applications in the classical world. In contrast, relatively little is known about the applications of quantum indistinguishability obfuscation. We note that [3] shows that the existence of a computational quantum indistinguishability obfuscation implies a witness encryption scheme for all languages in QMA. 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.

1.3 More on Related Work

Quantum Obfuscation. Quantum obfuscation was first studied in [4], where a notion called (G, Γ)-*indistinguishability obfuscation* was proposed, where G is a set of gates and Γ is a set of relations satisfied by the elements of G. In this notion, any two circuits over the set of gates G are perfectly indistinguishable if they differ by some sequence of applications of the relations in Γ. Since perfect indistinguishability obfuscation is known to be impossible under the assumption that $\mathsf{P} \neq \mathsf{NP}$ [26], 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, Γ)-*indistinguishability obfuscation* is incomparable with computational indistinguishability obfuscation [10, 23], which is the topic of our work.

Quantum obfuscation is studied in [3], 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 [3] 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. For the case

of indistinguishability obfuscation, it is shown that efficient statistical indistinguishability obfuscation is impossible unless PSPACE is contained in QSZK[3] (for the case of circuits that include measurements), or unless coQMA[4] is contained in QSZK (for the case of unitary circuits). Notable here is that [3] define indistinguishable obfuscation even for circuits that are *close* in functionality (and not necessarily identical). It is unclear if their results hold for the more conventional notion (which we adopt here) that obfuscations are indistinguishable only in the case that the original circuits are perfectly equivalent. We note that [3] does not provide any concrete instantiation of obfuscation.

As described above, a major difference in our definition for $qi\mathcal{O}$ is that we require indistinguishability only in the case that the original circuits are functionally *identical*. This framework is necessary to establish our results. To see this, note that the basic instantiation of an indistinguishability obfuscator that outputs the canonical form is no longer valid in the more stringent definition of [3][5]. Since our work builds upon canonical forms, it is unclear if we could proceed according to the definition in [3]. Also, we rely on quantum-secure classical indistinguishability obfuscation, which currently is studied and believed to hold according to the traditional notion of indistinguishability obfuscation for *identical* functionalities[6]. Another difference is that [3] 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[7] and follows the lines of the classical definitions. As far as we know, other definitional differences between our work and [3] are purely a choice of presentation (see also Note 1).

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, thus obtaining the result of the quantum computation.

This primitive was formally defined in [15] (see also [14, 22]), where it was shown how to do homomorphic quantum computation for quantum circuits of low T-depth, by assuming quantum-secure classical fully homomorphic encryp-

---

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

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

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

[6] In other words, we require at a minimum that the classical $i\mathcal{O}$ scheme that uses post-quantum assumptions only be secure according to our quantum definition; this is only possible by making the quantum definition match as closely as possible the classical definition.

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

tion. We note that even the simplest scheme in [15] (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 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.

1.4 Open Questions

The main open question is efficient quantum indistinguishabiliy obfuscation for quantum circuits with super-logarithmic number of T-gates.

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. Finally, 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 T gates.

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. For $n \in \mathbb{N}$, the set of all $n \times n$ unitary matrices is $\{U \in \mathbf{M}_n(\mathbb{C}) \mid UU^\dagger = \mathbf{I}\}$, where $U^\dagger$ is the complex conjugate transpose of the matrix for U, and where we denote the set of all $n \times n$ matrices over complex numbers by $\mathbf{M}_n(\mathbb{C})$.

A function `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 $n > n_0$, `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[8] 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 computes functions whose range is $\{0,1\}^m$ are often called multi-output Boolean circuits [29], but in this paper we simply called them Boolean circuits [36].

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 nth 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 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.

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

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

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

---

[8] 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 nth circuit in the family.

Let Φ and Ψ be two admissible operators of type (n, m)[9]. The *diamond norm* between two quantum operators is

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

2.4 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 $|\beta_s\rangle$.

Quantum Gates. We will work with the following set of unitary gates

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

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

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) [6].

---

[9] 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.

The set of gates $\{X, Z, P, CNOT, H\}$ 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.)

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

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

2.5 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 T-*count* is the total number of 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 [30]. It is a well-known fact that Clifford gates are not universal, but adding any non-Clifford gate, such as T, gives a universal set of gates [30][10]. *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 [30].

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.

2.6 Classical and Quantum Indistinguishability

Here, we define indistinguishability for classical random variables, against a quantum distinguisher (Definition 2), and also indistinguishability for quantum states (Definition 3).

Definition 1. *(Statistical Distance) Let X and Y be two random variables over some countable set Ω. The statistical distance between X and Y is*

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

---

[10] In this work, we assume circuits are given in the Clifford $+$ T gateset

Definition 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* 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* negl *such that:*

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

Definition 3. *(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 ρ_n and σ_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* negl *such that for all sufficiently large n:*

$$||\rho_n - \sigma_n||_{tr} \leq \texttt{negl}(n).$$

3. *$\mathcal{R}$ and $\mathcal{S}$ are computationally indistinguishable if there exists a negligible function* 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:*

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

2.7   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 indistinguishability obfuscation $(i\mathcal{O})$ as defined in [26], but where we make a few minor modifications.[11]

---

[11] 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.

Definition 4. (**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 $p(|C|)$:*

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

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.*

2.8   Quantum Teleportation

Here we provide a high-level description of quantum teleportation; for a more rigorous treatment see [11]. Suppose Alice has a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$[12] 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 $Z^a X^b$ to the state he possesses and obtains the state $|\psi\rangle$.

2.9   Gate Teleportation

One of the main applications of quantum teleportation is in fault-tolerant quantum computation [28]. To construct unitary quantum circuits, we need to have access to some universal set of quantum gates[13]. Suppose we want to evaluate a

---

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

[13] $\{\mathsf{H}, \mathsf{T}, \mathsf{CNOT}\}$ is a universal set of quantum gates [30].

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 1. 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.

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 2.10).

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

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)).

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

2.10 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[14]

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

For each Clifford gate g, the update function f_g is defined below. Note how g relates to the X and 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 definitions for equivalent quantum circuits and Quantum Indistinguishability Obfuscation $(qi\mathcal{O})$. At the end of the section, we also make an observation about the existence of inefficient quantum indistinguishability obfuscation.

3.1 Equivalent Quantum Circuits

Definition 5. (Equivalent Quantum Circuits): *Let C_{q_0} and C_{q_1} be two n-qubit quantum circuits. We say C_{q_0} and C_{q_1} are* equivalent *if for every n-qubit state $|\psi\rangle$*

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

(recall that equivalence is defined up to global phase).

3.2 Indistinguishability Obfuscation for Quantum Circuits

Definition 6. (Quantum Indistinguishability Obfuscation $qi\mathcal{O}$) *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* quantum indistinguishability obfuscator $(qi\mathcal{O})$ *if the following conditions hold:*

---

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

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

$$(|\phi\rangle, C_q') \leftarrow qi\mathcal{O}(C_q) \quad and \quad ||C_q'(|\phi\rangle, \cdot) - C_q(\cdot)||_\diamond \leq \texttt{negl}(n).$$

   Where $|\phi\rangle$ *is an* ℓ*-qubit state, the circuits* C_q *and* C_q' *are of type* (n, n) *and* (m, n) *respectively* $(m = \ell + n)$.[15]

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 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 2. A subtlety that is specific to the quantum case is that Definition 6 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.

Note 1. As described in Section 1.3, our definition differs from [3] as it requires security only in the case of equivalent quantum circuits. We also note that in this work we focus on unitary circuits only.[16] Another difference is that the notion of indistinguishability (computational or statistical) in [3] 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 [3] focuses on impossibility, their results are strongest in their model.

   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 [3], 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".

Inefficient Quantum Indistinguishability Obfuscators Exist. Finally, we show a simple extension of a result in [10], which shows that if we relax the requirement that the obfuscator be efficient, then information-theoretic indistinguishability obfuscation exists.

Claim. Inefficient indistinguishability obfuscators exist for all circuits.

---

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

[16] 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 2.5).

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. 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 is invariant for any two equivalent n-qubit circuits[17]. 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 $\big(|\phi\rangle, C'_q\big)$.

Lemma 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 6) 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 $||C'_q(|\phi\rangle, \cdot) - C_q(\cdot)||_\diamond = 0 \leq$ `negl`(n) for any negligible function `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

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

- $\ell \leq p(|C_q|)$

- $n \leq p(|C_q|)$

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

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

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

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 $|\phi_1\rangle = |\phi_2\rangle$. 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. □

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[18]. 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.

---

[18] Circuits that compute update functions for Clifford circuits, see Section 2.10.

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 3.

   4. Set $C' \leftarrow i\mathcal{O}(C)$, where $i\mathcal{O}(C)$ is a perfectly secure indistinguishability obfuscation defined in Section 4.2.

   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 $(|\phi\rangle, C_q')$.

Theorem 1. *Algorithm 3 is a perfect quantum indistinguishability obfuscation for all Clifford Circuits.*

Proof. We have to show that Algorithm 3 satisfies Definition 6.

1. `Functionality:` Let C_q be an n-qubit Clifford Circuit and $(|\phi\rangle, C_q')$ 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 $|C_q'| = |i\mathcal{O}(C)| + |\text{Bell measurement}|$, 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 $|\text{Bell measurement}| \leq q(|C|)|$. The size of $|i\mathcal{O}(C)|$ is at most $r(|C|)$ for some polynomial $r(\cdot)$ (Lemma 3). Further, the size of $|C|$ is at most $s(|C_q|)$ for some polynomial $|C_q|$ (Lemma 3). By setting $p(|C|) = 2|C_q| + q(|C|) + r(s(|C|))$, we have

   − $\ell \leq p(|C|)$

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

3. **Perfect Indistinguishability:** Let C_{q_1} and C_{q_2} be two n-qubit equivalent Clifford circuits of the same size. Let $\big(|\phi_1\rangle, C'_{q_1}\big)$ and $\big(|\phi_2\rangle, C'_{q_2}\big)$ 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 2), 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 3). Therefore, C'_{q_1} and C'_{q_2} are perfectly indistinguishable. $\qquad \square$

Lemma 2. *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 $\mathbf{s} = a_1 b_1 \ldots a_n b_n \in \{0,1\}^{2n}$ 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.[19] $\qquad \square$

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.

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 2.10).
4. Output the classical circuit $\hat{C}$.

The main idea here is to compute the canonical form for the Clifford circuit, and then compute the update function for the canonical form.

Lemma 3. *Algorithm 4 is a perfect classical indistinguishability obfuscator for the Clifford update functions.*

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

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 2 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 2.10):

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

   $(a, b) \xrightarrow{\mathsf{H}} (b, a)$ (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. $\qquad\square$

---

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

Remark 3. 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 2). 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 1 or Section 2.10). 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 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 T-gate on an encrypted system using the quantum one-time pad. The following equation relates the T-gate to the X- and 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 P^b is the identity; otherwise we have a P-gate correction. This is undesirable as P does not commute with 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 X and 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* [28]. 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 [33]. 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 [25, 32]. 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 $\{\mathsf{H}, \mathsf{T}\}$[20]

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

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

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

where $\alpha_i \in \left\{0, 1, \frac{1+i}{2}, \frac{1-i}{2}\right\}$. Since $\{\mathsf{I}, \mathsf{X}, \mathsf{Z}, \mathsf{X}\mathsf{Z}\}$, 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

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

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 β_i grows at most as a polynomial in the number of T-gates. Therefore it follows

---

[20] The set $\{\mathsf{H}, \mathsf{T}\}$ is universal for 1-qubit unitaries [30].

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 2). Some subtleties, however are addressed below: the equivalence of the update functions (Lemma 4) and the circuit synthesis (Lemma 5).

Lemma 4. *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.*

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 $a, b \in \{0, 1\}$,

$$C_{q_1} \mathsf{X}^b \mathsf{Z}^a (|\psi\rangle) = C_{q_2} \mathsf{X}^b \mathsf{Z}^a (|\psi\rangle)$$

$$\Leftrightarrow (\beta_1 \mathsf{I} + \beta_2 \mathsf{X} + \beta_3 \mathsf{Z} + \beta_4 \mathsf{XZ}) C_{q_1} (|\psi\rangle) = (\gamma_1 \mathsf{I} + \gamma_2 \mathsf{X} + \gamma_3 \mathsf{Z} + \gamma_4 \mathsf{XZ}) C_{q_2} (|\psi\rangle)$$

$$\Leftrightarrow (\beta_1 \mathsf{I} + \beta_2 \mathsf{X} + \beta_3 \mathsf{Z} + \beta_4 \mathsf{XZ}) C_{q_1} (|\psi\rangle) = (\gamma_1 \mathsf{I} + \gamma_2 \mathsf{X} + \gamma_3 \mathsf{Z} + \gamma_4 \mathsf{XZ}) C_{q_1} (|\psi\rangle)$$

$$\Leftrightarrow ((\beta_1 - \gamma_1) \mathsf{I} + (\beta_2 - \gamma_2) \mathsf{X} + (\beta_3 - \gamma_3) \mathsf{Z} + (\beta_4 - \gamma_4) \mathsf{XZ}) C_{q_1} (|\psi\rangle) = \mathbf{0}.$$

$$\Rightarrow (\beta_1 - \gamma_1) \mathsf{I} + (\beta_2 - \gamma_2) \mathsf{X} + (\beta_3 - \gamma_3) \mathsf{Z} + (\beta_4 - \gamma_4) \mathsf{XZ} = \mathbf{0}.$$

$$\Rightarrow \beta_1 = \gamma_1, \ \beta_2 = \gamma_2, \ \beta_3 = \gamma_3, \ \beta_4 = \gamma_4.$$

Therefore, $F_{C_{q_1}}$ and $F_{C_{q_2}}$ are equivalent functions. $\qquad\square$

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 3.

Lemma 5. *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 2×2 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 [33]. $\qquad\square$

22

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

---

– Input: A n-qubit quantum Circuit C_q with 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 8).

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

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

   Compute a quantum circuit that applies $U_{F_{C_q}}$, using the circuit synthesis method of [33].

   (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 $C_q(|\psi\rangle)$.

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 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 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 2). For ease of presentation, the proof relies on three auxiliary lemmas that are presented in the following section: Lemma 6 (which shows that equivalent circuits have equivalent update functions), Lemma 7 (which bounds the number of terms of the update function), and Lemma 8 (which shows that update functions can be computed by a polynomial-size circuits).

Theorem 2. *(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 T-count $\in O(\log |C_q|)$.

Proof. We have to show that Algorithm 5 satisfies Definition 6. 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 1. Since the Clifford circuit synthesis has perfect correctness [33], we have $||C'_q(|\phi\rangle, \cdot) - C_q(\cdot)||_\diamond = 0 \leq \mathtt{negl}(n)$ for any negligible function $\mathtt{negl}(n)$.

2. **Polynomial Slowdown:** Note 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 7, Lemma 8, Lemma 9 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 [33]. 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 $(|\phi_1\rangle, C'_{q_1})$ and $(|\phi_2\rangle, C'_{q_2})$ 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 6). 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.[21] Therefore, Algorithm 5 is a perfectly/statistically/ computationally indistinguishable quantum obfuscator for the quantum circuits. $\square$

5.3 Equivalent Update Functions

Here, we provide a generalization of Lemma 2, applicable to the case of general circuits.

Lemma 6. *Let C_{q_1} and C_{q_2} be two equivalent n-qubit circuits. Then their corresponding update functions are also equivalent.*

---

[21] Note that circuits that compute update functions (for equivalent quantum circuits) may have different sizes. However, that can be managed as discussed in Remark 3.

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

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

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

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

Then Equation (24) can only hold if

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

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 T-gates can be defined as the following map.

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

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 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 T-count in $O(\log(|C_q|))$, the number of terms in F_{C_q} has at most $O(|C_q|)$ terms.

Lemma 7. *If C_q is an n-qubit quantum circuit with 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 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 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 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 T-gate (acting on some ℓ-th wire).

$$C_q(\mathsf{X}^{a_1} \mathsf{Z}^{b_1} \otimes \cdots \otimes \mathsf{X}^{a_n} \mathsf{Z}^{b_n})$$

$$= (\mathsf{X}^{\otimes_{i=1}^{\ell-1} b'_i} \mathsf{Z}^{\otimes_{i=1}^{\ell-1} a'_i}) \otimes \left(\sum_{j=1}^{4} \beta_j \mathsf{X}^{b'_j} \mathsf{Z}^{a'_j} \right) \otimes (\mathsf{X}^{\otimes_{i=\ell+1}^{n} b'_i} \mathsf{Z}^{\otimes_{i=\ell+1}^{n} a'_i}) C_q \tag{30}$$

$$= \sum_{i=1}^{4} \beta_i \mathsf{X}^{b'_{i_1}} \mathsf{Z}^{a'_{i_1}} \otimes \cdots \otimes \mathsf{X}^{b'_{i_n}} \mathsf{Z}^{a'_{i_n}}.$$

26

Therefore $k \leq 4$. It is important to realize that 4 is the maximum number of terms a circuit with T can have. No Clifford gate including CNOT can increase the number of terms beyond 4. This is because only a 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 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 $U_{F_{C_q}} = \sum_{i=1}^{4^2} \beta_i \mathsf{X}^{b_{i_1}} \mathsf{Z}^{a_{i_1}} \otimes \cdots \otimes \mathsf{X}^{b_{i_n}} \mathsf{Z}^{a_{i_n}}$, therefore $k \leq 16$. Note that it makes no difference whether 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 T will contribute 4 terms and the second 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 CNOTs are acting on the i-th to j-th wire, then we may have to expand all terms in the unitary to apply CNOTs. This again can contribute at most 16 terms.

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

Lemma 8. *If C_q be an n-qubit quantum circuit with 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 T-count $\in O(\log |C_q|)$. Recall from Section 2.10 that the corresponding update functions for the Clifford $+$ 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_{X}, C_{Z}, C_{H}, C_{P}, C_{CNOT} and C_{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_{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_{T} expands its 2-bit input into a 4ℓ-bit strings (where $\ell = \max\{\left|\frac{1+i}{2}\right|, \left|\frac{1-i}{2}\right|\}$[22]. 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

---

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

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 T-gates, then each C_T subcircuit will map a 2-bit string to a 4ℓ-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 $|C| \leq p(n)$. □

Acknowledgements

A   Size of Coefficients in Update Functions

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

Lemma 9. *Let C_q be an n-qubit quantum circuit with $O(\log|C_q|)$ 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 $\beta_i \in O(p(|C_q|))$ 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 β_i. So the coefficients can be affected by T gates. Therefore, to estimate the size of the coefficients we can ignore other gates. Each β_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 T, a coefficient will multiply and add at most polynomial time in the circuit size and there are $O(\log(|C_q|))$ such gates, therefore there exists a polynomial $p(\cdot)$ such that $|\beta_i| \in O(p(|C_q|))$, for every $i \in [4^k]$. □

References

1. S. Aaronson. Quantum copy-protection and quantum money. In *CCC 2009*, pages 229–242, 2009. DOI: 10.1109/CCC.2009.42.
2. S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70(5):052328, 2004. DOI: 10.1103/PhysRevA.70.052328.
3. G. Alagic and B. Fefferman. On quantum obfuscation, 2016. Available at https://arxiv.org/abs/1602.01771.
4. G. Alagic, S. Jeffery, and S. Jordan. Circuit obfucation using braids. In *TQC 2014*, pages 141–160, 2014. DOI: 10.4230/LIPIcs.TQC.2014.141.
5. M. Albrecht, S. Bai, and L. Ducas. A subfield lattice attack on overstretched NTRU assumptions. In *CRYPTO 2016*, volume 1, pages 153–178, 2016. DOI: 10.1007/978-3-662-53018-4_6.
6. A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *FOCS 2000*, pages 547–553, 2000. DOI: 10.1109/SFCS.2000.892142.
7. M. Amy, D. Maslov, and M. Mosca. Polynomial-time T-depth optimization of Clifford+T circuits via matroid partitioning. *IEEE Trans. Comput. Aided Des. Intgr. Circuit Syst.*, 33(10):1476–1489, 2014. DOI: 10.1109/TCAD.2014.2341953.
8. M. Amy, D. Maslov, M. Mosca, and M. Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *IEEE Trans. Comput. Aided Des. Intgr. Circuit Syst.*, 32(6):818–830, 2013. DOI: 10.1109/TCAD.2013.2244643.
9. 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 *CRYPTO 2019*, volume 3, pages 284–332, 2019. DOI: 10.1007/978-3-030-26954-8_10.
10. B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. *J. ACM*, 59(2):6, 2012. DOI: 10.1145/2160158.2160159.
11. 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. *Phys. Rev. Lett.*, 70(13):1895, 1993. DOI: 10.1103/PhysRevLett.70.1895.
12. N. Bitansky and O. Paneth. ZAPs and non-interactive witness indistinguishability from indistinguishability obfuscation. In *TCC 2015*, volume II, pages 401–427, 2015. DOI: 10.1007/978-3-662-46497-7_16.

13. D. Boneh and M. Zhandry. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. In *CRYPTO 2014*, volume I, pages 480–499, 2014. `DOI: 10.1007/978-3-662-44371-2_27`.
14. Z. Brakerski. Quantum FHE (almost) as secure as classical. In *CRYPTO 2018*, volume 3, pages 67–95, 2018. `DOI: 10.1007/978-3-319-96878-0_3`.
15. A. Broadbent and S. Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In *CRYPTO 2015*, volume 2, pages 609–629, 2015. `DOI: 10.1007/978-3-662-48000-7_30`.
16. A. Broadbent and S. Lord. Uncloneable quantum encryption via oracles, 2019. Available at `https://arxiv.org/abs/1903.00130`.
17. R. Canetti, H. Lin, S. Tessaro, and V. Vaikuntanathan. Obfuscation of probabilistic circuits and applications. In *TCC 2015*, volume II, pages 468–497, 2015. `DOI: 10.1007/978-3-662-46497-7_19`.
18. Y. Chen, C. Gentry, and S. Halevi. Cryptanalyses of candidate branching program obfuscators. In *EUROCRYPT 2017*, volume 3, pages 278–307, 2017. `DOI: 10.1007/978-3-319-56617-7_10`.
19. J.-S. Coron, T. Lepoint, and M. Tibouchi. Practical multilinear maps over the integers. In *CRYPTO 2013*, volume 1, pages 476–493, 2013. `DOI: 10.1007/978-3-642-40041-4_26`.
20. R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. In *EUROCRYPT 2016*, volume 2, pages 559–585, 2016. `DOI: 10.1007/978-3-662-49896-5_20`.
21. O. Di Matteo and M. Mosca. Parallelizing quantum circuit synthesis. *Quantum Sci. Technol.*, 1(1):015003, 2016. `DOI: 10.1088/2058-9565/1/1/015003`.
22. Y. Dulek, C. Schaffner, and F. Speelman. Quantum homomorphic encryption for polynomial-sized circuits. In *CRYPTO 2016*, pages 3–32, 2016. `DOI: 10.1007/978-3-662-53015-3_1`.
23. S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *FOCS 2013*, pages 40–49, 2013. `DOI: 10.1109/FOCS.2013.13`.
24. C. Gentry, S. Gorbunov, and S. Halevi. Graph-induced multilinear maps from lattices. In *TCC 2015*, volume 2, pages 498–527, 2015. `DOI: 10.1007/978-3-662-46497-7_20`.
25. 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`.
26. S. Goldwasser and G. N. Rothblum. On best-possible obfuscation. *J. Cryptology*, 27(3):480–505, 2014. `DOI: 10.1007/s00145-013-9151-z`.
27. D. Gottesman. The Heisenberg representation of quantum computers. In *GROUP 22*, pages 32–43, 1998. `arXiv: quant-ph/9807006`.
28. D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nat.*, 402:390–393, 1999. `DOI: 10.1038/46503`.
29. S. Guo, T. Malkin, I. C. Oliveira, and A. Rosen. The power of negations in cryptography. In *TCC 2015*, volume 1, pages 36–65, 2015. `DOI: 10.1007/978-3-662-46494-6_3`.
30. P. Kaye, R. Laflamme, and M. Mosca. *An introduction to quantum computing*. Oxford, 2007.
31. A. Langlois, D. Stehlé, and R. Steinfeld. GGHLite: More efficient multilinear maps from ideal lattices. In *EUROCRYPT 2014*, pages 239–256, 2014. `DOI: 10.1007/978-3-642-55220-5_14`.

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

33. P. Niemann, R. Wille, and R. Drechsler. Efficient synthesis of quantum circuits implementing Clifford group operations. In *ASP-DAC 2014*, pages 483–488, 2014. DOI: 10.1109/ASPDAC.2014.6742938.

34. A. Sahai and B. Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *STOC 2014*, pages 475–484, 2014. DOI: 10.1145/2591796.2591825.

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

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

37. F. Speelman. Instantaneous non-local computation of low T-depth quantum circuits. In *TQC 2016*, pages 9:1–9:24, 2016. DOI: 10.4230/LIPIcs.TQC.2016.9.