Instantaneous Non-Local Computation of Low T-Depth Quantum Circuits

Florian Speelman[*]

Centrum Wiskunde & Informatica, Amsterdam, the Netherlands
f.speelman@cwi.nl

Abstract

Instantaneous non-local quantum computation requires multiple parties to jointly perform a quantum operation, using pre-shared entanglement and a single round of simultaneous communication. We study this task for its close connection to position-based quantum cryptography, but it also has natural applications in the context of foundations of quantum physics and in distributed computing. The best known general construction for instantaneous non-local quantum computation requires a pre-shared state which is exponentially large in the number of qubits involved in the operation, while efficient constructions are known for very specific cases only.

We partially close this gap by presenting new schemes for efficient instantaneous non-local computation of several classes of quantum circuits, using the Clifford+T gate set. Our main result is a protocol which uses entanglement exponential in the T-depth of a quantum circuit, able to perform non-local computation of quantum circuits with a (poly-)logarithmic number of layers of T gates with quasi-polynomial entanglement. Our proofs combine ideas from blind and delegated quantum computation with the garden-hose model, a combinatorial model of communication complexity which was recently introduced as a tool for studying certain schemes for quantum position verification. As an application of our results, we also present an efficient attack on a recently-proposed scheme for position verification by Chakraborty and Leverrier.

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases Quantum Cryptography, Quantum Communication

Digital Object Identifier 10.4230/LIPIcs.TQC.2016.9

1 Introduction

We study the task of instantaneous non-local quantum computation, and present new protocols to efficiently perform this task for specific classes of quantum circuits. Our main motivation comes from position-based quantum cryptography, where previous attacks on schemes for position-based quantum cryptography have taken either of two forms:

First results on quantum position-based cryptography involved attacks on specific proposals for schemes, such as the attacks by Lau and Lo [31], those by Kent, Munro and Spiller [28], and the attack on Beigi and König's scheme using mutually-unbiased-bases [37]. A certain family of efficient attacks on a concrete class of single-qubit schemes [13] was formalized by the garden-hose model. Described as 'fast protocols for bipartite unitary operators', Yu, Griffiths and Cohen [40, 39] give protocols that, although not directly inspired by position-based quantum cryptography, can be translated to our setting.

On the other hand Buhrman et al. [12] constructed a general attack which treats the quantum functionality of the protocol to be attacked as a black box. For a protocol which uses

[*] The author is supported by the EU projects SIQS and QALGO.

a message of n qubits, the entanglement consumption of this attack is around $2^{\log(\frac{1}{\varepsilon})2^{4n}}$ EPR pairs, doubly exponential in n. Here ε represents the probability that the attack does not succeed. The construction of Buhrman et al. was based on a protocol for 'instantaneous non-local measurement' by Vaidman [38, 16]. Beigi and König [5] later constructed a more efficient general attack, using port-based teleportation – a new teleportation method introduced by Ishizaka and Hiroshima [25, 26]. The improved attack uses $O(n\frac{2^{8n}}{\varepsilon^2})$ EPR pairs, still an exponential dependence on n.

These protocols were able to solve the following task. Given a constant $\varepsilon \geq 0$ and an n-qubit quantum operation[1] U, where n is a natural number. Two players, Alice and Bob, receive an arbitrary input state ρ_{AB} of n qubits, with the players receiving $n/2$ qubits each. After a single round of simultaneous quantum[2] communication, the players must output a state ε-close to $U\rho_{AB}U^\dagger$. Alice outputs the first $n/2$ qubits of the state and Bob outputs the other $n/2$ qubits. We define $\mathrm{INQC}_\varepsilon(U)$ as the smallest number of EPR pairs that the players have to share at the start of a protocol which performs this task. $\mathrm{INQC}(U)$ is used as a shorthand for $\mathrm{INQC}_0(U)$, a protocol which works with no error. We present a more precise definition of INQC is presented in Appendix A.

In this work we partially bridge the gap between efficient specific constructions for instantaneous non-local computation and expensive general ones, by constructing a protocol for non-local computation of a unitary transformation U such that the entanglement use of the protocol depends on the quantum circuit which describes U.

In particular, writing quantum circuits over the Clifford+T gate set, we create a protocol using entanglement exponential in the *T-count*. We also present a protocol that uses an amount of entanglement which scales as the number of qubits n raised to the power of the *T-depth* of the circuit. Even though this is a quickly-growing dependence, for circuits of constant T-depth this amounts to a polynomial dependence on n, unlike any earlier construction. For circuits of polylogarithmic T-depth we obtain an amount of entanglement which is quasi-polynomial in n, i.e. a dependence of the form $2^{(\log n)^c}$ for some constant c. Note that the depth and size of the quantum circuit can be much higher than its T-depth: we allow an arbitrary number of gates from the Clifford group in addition to the limited number of T gates. Our results imply new efficient attacks on any scheme for position-verification where the action of the honest party can be written as a low T-depth quantum circuit.

Linking blind quantum computation and instantaneous non-local quantum computation was first considered by Broadbent[3] [8], who considered a setting where the parties have access to non-local boxes – correlations even stronger than those allowed by quantum mechanics. The techniques we use are also based on delegated and blind quantum computation [15, 4, 18, 19, 7] and results on computation via teleportation [24], but we combine them with new ideas from the *garden-hose model* [13, 29] – a recently-introduced combinatorial model for communication complexity with close links to a specific class of schemes for position verification.

We prove two main theorems, each improving on the entanglement consumption of the best-known previous constructions for non-local instantaneous quantum computation

[1] Our constructions only consider unitaries given by quantum circuits, but the task naturally extends to more general quantum operations. The motivation for Vaidman's original scheme [38], which formed the basis of Buhrman et al.'s construction, was to instantaneously perform a non-local measurement. Our constructions can also be applied to that case, by writing the measurement as a unitary operation followed by a measurement in the computational basis.

[2] Since restriction to classical communication is not necessarily dictated by the application in position-based quantum cryptography, we allow quantum communication. All presented protocols work equally well when all messages are classical instead.

[3] These results were first available as privately-circulated notes in December 2011, and were made available online in December 2015.

for specific circuits[4]. Additionally, we use our proof method to construct a new attack on a scheme for position verification which was recently proposed by Chakraborty and Leverrier [14].

▶ **Theorem 3.** *Any n-qubit Clifford+T quantum circuit C which has at most k T gates has a protocol for instantaneous non-local computation using $O(n2^k)$ EPR pairs.*

▶ **Theorem 5.** *Any n-qubit quantum circuit C using the Clifford+T gate set which has* T*-depth d, has a protocol for instantaneous non-local computation using $O(\,(68n)^d\,)$ EPR pairs.*

The main technical tool we use in the proof of our depth-dependent construction is the following lemma, which is able to remove a conditionally-applied gate from the Clifford group without any communication – at an entanglement cost which scales with the garden-hose complexity of the function which describes the condition.

▶ **Lemma 4.** *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a function known to all parties, and let $GH(f)$ be the garden-hose complexity of the function f. Assume Alice has a single qubit with state $\mathrm{P}^{f(x,y)}|\psi\rangle$, for binary strings $x, y \in \{0,1\}^n$, where Alice knows the string x and Bob knows y. The following two statements hold:*

1. *There exists an instantaneous protocol without any communication which uses $2GH(f)$ pre-shared EPR pairs after which a chosen qubit of Alice is in the state $\mathrm{X}^{g(\hat{x},\hat{y})}\mathrm{Y}^{h(\hat{x},\hat{y})}|\psi\rangle$. Here $\hat{x}$ depends only on x and the $2GH(f)$ bits that describe the measurement outcomes of Alice, and $\hat{y}$ depends on y and the measurement outcomes of Bob.*
2. *The garden-hose complexities of the functions g and h are at most linear in the garden-hose complexity of the function f. More precisely, $GH(g) \leq 4GH(f) + 1$ and $GH(h) \leq 11GH(f) + 2$.*

Chakraborty and Leverrier [14] recently proposed a protocol for quantum position verification on the interleaved multiplication of unitaries. They show that all known attacks, applied to this protocol, require entanglement exponential in the number of terms t in the product. As an application of Lemma 4, we present an attack on their proposed protocol which has entanglement cost polynomial in t and the number of qubits n. The new attack requires an amount of entanglement which scales as $(\frac{t}{\varepsilon})^{O(1)}$ per qubit, and for each qubit succeeds with probability at least $1 - \varepsilon$.

2 Preliminaries

2.1 The Pauli matrices and the Clifford group

The single-qubit *Pauli matrices* are $\mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\mathrm{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and the identity $\mathrm{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. A *Pauli operator* on an n-qubit state is the tensor product of n one-qubit Pauli matrices, the group of n qubit Pauli operators[5] is $\mathcal{P} = \{\sigma_1 \otimes \cdots \otimes \sigma_n \mid$

[4] From now on, whenever we write 'quantum circuit', we will always mean a quantum circuit that only uses the Clifford group generators, together with T gates.

[5] The given definition includes a global phase, which is not important when viewing the elements as quantum gates.

$\forall j : \sigma_j \in \{I, X, Y, Z\}\} \times \{\pm 1, \pm i\}$. These are some of the simplest quantum operations and appear, for example, as corrections for standard quantum teleportation.

The *Clifford group* can be defined as those operations that take elements of the Pauli group to other elements of the Pauli group under conjugation – the *normalizer* of the Pauli group. We consider the Clifford group on n qubits, for some natural number n.

$$\mathcal{C} = \{U \in \mathcal{U}(2^n) \mid \forall \sigma : \sigma \in \mathcal{P} \implies U\sigma U^\dagger \in \mathcal{P}\} \tag{1}$$

Notable elements of the Clifford group are the single-qubit gates given by the Hadamard matrix $\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ and the phase gate $\mathrm{P} = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$, and the two-qubit CNOT gate given by $\mathrm{CNOT} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$.

The set $\{\mathrm{H}, \mathrm{P}, \mathrm{CNOT}\}$ generates the Clifford group up to a global phase when applied to arbitrary qubits, see e.g. [23]. For all these gates, we will use subscripts to indicate the qubits or wires to which they are applied; e.g. H_j is a Hadamard gate applied to the j-th wire, and $\mathrm{CNOT}_{j,k}$ is a CNOT that has wire j as control and k as target.

Even though there exist interesting quantum circuits that use only gates from the Clifford group, it is not a universal set of gates. Indeed, the Gottesman–Knill states that such a circuit can be efficiently simulated by a classical computer, something which is not known to be true for general quantum circuits [22, 1]. By extending $\mathcal{C}$ with *any* gate, we do obtain a gate-set which is universal for quantum computation [32].

The gate we will use to extend the Clifford gates to a universal set is the T gate, sometimes called $\pi/8$-gate or R, defined by $\mathrm{T} = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}$. We will write all circuits using gates from the set $\{\mathrm{X}, \mathrm{Z}, \mathrm{H}, \mathrm{P}, \mathrm{CNOT}, \mathrm{T}\}$. Technically X, P, and Z are redundant here, since they can be formed by the others as $\mathrm{P} = \mathrm{T}^2$, $\mathrm{Z} = \mathrm{P}^2$ and $\mathrm{X} = \mathrm{ZHZ}$, but we include them for convenience.

In our protocols for instantaneous non-local computation, we will alternate teleportation steps with gate operations, and therefore the interaction between the Pauli matrices and the other gates are especially important. We will make much use of the following identities, which can all be easily checked[6].

$$\begin{array}{lll} \mathrm{XZ} = \mathrm{ZX} & \mathrm{HX} = \mathrm{ZH} & \mathrm{CNOT}_{1,2}(\mathrm{X} \otimes \mathrm{I}) = (\mathrm{X} \otimes \mathrm{X})\mathrm{CNOT}_{1,2} \\ \mathrm{PZ} = \mathrm{ZP} & \mathrm{HZ} = \mathrm{XH} & \mathrm{CNOT}_{1,2}(\mathrm{I} \otimes \mathrm{X}) = (\mathrm{I} \otimes \mathrm{X})\mathrm{CNOT}_{1,2} \\ \mathrm{PX} = \mathrm{XZP} & \mathrm{TX} = \mathrm{PXT} & \mathrm{CNOT}_{1,2}(\mathrm{Z} \otimes \mathrm{I}) = (\mathrm{Z} \otimes \mathrm{I})\mathrm{CNOT}_{1,2} \\ & & \mathrm{CNOT}_{1,2}(\mathrm{I} \otimes \mathrm{Z}) = (\mathrm{Z} \otimes \mathrm{Z})\mathrm{CNOT}_{1,2} \end{array} \tag{2}$$

2.2 Key transformations from Clifford circuits

For a 0/1 vector v of length n and for any single-qubit operation U, we write $U^v = \bigotimes_{j=1}^n U^{v_j}$, i.e., U^v is the application of U on all qubits $j \in [n]$ for which $v_j = 1$. When Alice teleports a state $|\psi\rangle$ of n qubits to Bob, the uncorrected state at Bob's side can be written as $\mathrm{X}^{a_x}\mathrm{Z}^{a_z}|\psi\rangle$. Here we let a_x and a_z be the vectors representing the outcomes of the Bell measurements of Alice. In analogy with the the literature on assisted and blind quantum computation, we will call the teleportation measurement outcomes a_x and a_z the *key* needed to decode $|\psi\rangle$.

[6] Here equality is up to a global phase – which we will ignore from now on for simplicity.

The specific entries of these keys will often depend on several different measurement outcomes, given by earlier steps in the protocol, and we will therefore occasionally describe them as *polynomials* over $\mathbb{F}_2$. Viewing the keys as polynomials is especially helpful in the description of the more-complicated protocol of Section 5.

For any gate from the Clifford group $U \in \mathcal{C}$, if we apply U on the encoded state, we can describe the resulting state as $U|\psi\rangle$ with a new key. That is, $UX^{a_x}Z^{a_z}|\psi\rangle = X^{\hat{a}_x}Z^{\hat{a}_z}U|\psi\rangle$ for some new 0/1 keys $\hat{a}_x, \hat{a}_z$. The transformations of the keys will have a particularly simple form. (See for example [11] for a characterization of these transformations and a different application of Clifford circuit computation.)

For example, we can write the identities of Equation 2 in terms of key transformations. The transformations that occur when a bigger Pauli operator is applied, can then be easily found by writing the Pauli operator in terms of its generators $\{\mathrm{H}, \mathrm{P}, \mathrm{CNOT}\}$, and applying these rules one-by-one. We will write $(x_1, x_2 \mid z_1, z_2)$ as a shorthand for, respectively, the X key on the first and second qubit, and the Z key on the first and second qubit – this is a convenient notation[7] for the pair of vectors a_x and a_z that represent these keys. All addition of these keys will be over $\mathbb{F}_2$, i.e., the + represents the binary exclusive or.

$$\begin{aligned}
\mathrm{P}(x \mid z) &\to (x \mid x+z)\mathrm{P} \\
\mathrm{H}(x \mid z) &\to (z \mid x)\mathrm{H} \\
\mathrm{CNOT}_{1,2}(x_1, x_2 \mid z_1, z_2) &\to (x_1, x_1 + x_2 \mid z_1 + z_2, z_2)\mathrm{CNOT}_{1,2}
\end{aligned}$$

2.3 Clifford+T quantum circuits, T-count and T-depth

In several different areas of quantum information, gates from the Clifford group are 'well-behaved' or 'easy', while the other non-Clifford gates are hard – an observation which was also made, with several examples, in the recent [10].

The *T-count* of a quantum circuit is defined as the number of T gates in the entire quantum circuit. The *T-depth* is the number of layers of T gates, when viewing the circuit as alternating between Clifford gates and a layer of simultaneous T gates. See for example Figure 5.

Given a quantum operation, it is not always obvious what is the best circuit in terms of T-count or T-depth. Recent work gave algorithms for finding circuits that are optimized in terms of T-depth [3, 21, 35, 2] and optimal constructions for arbitrary single-qubit unitaries have also been found [30, 34, 36]. These constructions sometimes increase the number of qubits involved by adding ancillas – the use of which can greatly decrease the T-depth of the resulting circuit.

2.4 The garden-hose model

The garden-hose model is a combinatorial model of communication complexity, first introduced by Buhrman, Fehr, Schaffner and Speelman [13]. The recent work by Klauck and Podder [29] further investigated the notion, proving several follow-up results. Here we repeat the basic definitions of the garden-hose model and its link to attacks on schemes for position-based quantum cryptography.

Alice has an input $x \in \{0,1\}^n$, Bob has an input $y \in \{0,1\}^n$, and the players want to compute a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ in the following way. Between the two

[7] This mapping is called the symplectic notation when used in the stabilizer formalism, although we won't need to introduce the associated symplectic inner product for our construction.

players are s pipes, and, in a manner depending on their respective inputs, the players link up these pipes one-to-one with hoses. Alice also has a water tap, which she can connect to one of these pipes. When $f(x,y)=0$, the water should exit on Alice's side, and when $f(x,y)=1$ we want the water to exit at Bob's side. The garden-hose complexity of a function f, written $GH(f)$, then is the least number s of pre-shared pipes the players need to compute the function in this manner.

There is a natural translation from strategies of the garden-hose game to a quantum protocol that routes a qubit to either Alice or Bob depending on their local inputs, up to teleportation corrections. Consider the following quantum task, again dependent on a function f like in the previous paragraph. Alice now receives a quantum state $|\psi\rangle$ and a classical input x, Bob receives input y, and the players are allowed one round of simultaneous communication. If $f(x,y)=0$, Alice must output $|\psi\rangle$ after this round of communication, and otherwise Bob must output $|\psi\rangle$. We would like to analyze how much pre-shared entanglement the players need to perform this task.

From the garden-hose protocol for f, the players can come up with a strategy for this quantum task that needs at most $GH(f)$ EPR pairs pre-shared. Every pipe corresponds to an EPR pair. If a player's garden-hose strategy dictates a hose between some pipe j and another pipe k, then that player performs a Bell measurement of EPR-halves labeled j and k. Alice's connection of the water tap to a pipe corresponds to a Bell measurement between her input state $|\psi\rangle$ and the local half of an EPR pair. After their measurements, the correct player will hold the state $|\psi\rangle$, up to Pauli corrections incurred by the teleportations. The corrections can be performed after a step of simultaneous communication containing the outcomes of all measurements.

We will describe some of the logic in terms of the garden-hose model, as an abstraction away from the qubits involved. When we refer to a quantum implementation of a garden-hose strategy, we always mean the back-and-forth teleportation as described above.

The following lemma will prove to be useful. Let the number of *spilling pipes* of a garden-hose protocol for a player be the number of possible places the water could possibly exit. That is, the number of spilling pipes for Alice for a specific x, is the number of different places the water could exit on her side over all Bob's inputs y. The number of spilling pipes for Alice is then the maximum number of spilling pipes over all x. To be able to chain different parts of a garden-hose protocol together, it can be very convenient to only have a single spilling pipe for each player.

▶ **Lemma 1** (Lemma 11 of [29]). *A garden-hose protocol P for any function f with multiple spilling pipes can be converted to another garden-hose protocol P' for f that has only one spilling pipe on Alice's side and one spilling pipe on Bob's side. The size of P' is at most 3 times the size of P plus 1.*

Klauck and Podder also showed that computing the binary XOR of several protocols is possible with only a linear overhead in total garden-hose complexity [29, Theorem 18]. We give an explicit construction for this statement in AppendixC – the result already follows from the similar construction of [29, Lemma 12], except that we obtain a constant which is slightly better than unfolding their (more general) proof.

▶ **Lemma 2.** *Let $(f_1, f_2, \ldots, f_k)$ be functions, where each function f_i has garden-hose complexity $GH(f_i)$. Let $c \in \{0,1\}$ be an arbitrary bit. Then,*

$$GH\left(c \oplus \bigoplus_{i=1}^{k} f_i\right) \leq 4\sum_{i=1}^{k} GH(f_i) + 1\,.$$

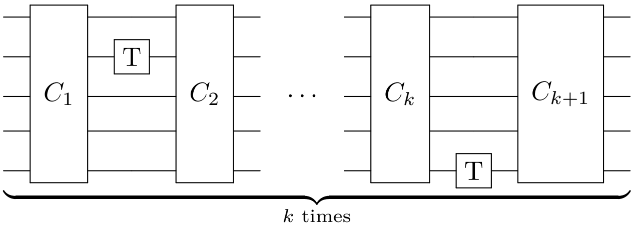


Figure 1 A circuit with T-count k. The C_i gates represent subcircuits consisting only of operation from the Clifford group $\mathcal{C}$.

3 Low T-count quantum circuits

▶ **Theorem 3.** *Let C be an n-qubit quantum circuit with gates from the Clifford+T gate set, and let C contain k T-gates in total. Then $\mathrm{INQC}(C) \leq O(n2^k)$, i.e., there exists a protocol for two-party instantaneous non-local computation of C which uses a pre-shared entangled state of $O(n2^k)$ EPR pairs.*

Proof. Let Alice's input state be some arbitrary quantum state $|\psi_0\rangle$. We will write the quantum state at step $t \in \{0, \ldots, k\}$, as intermediate result of executing the circuit C for t steps, as $|\psi_t\rangle$. Let C_t be the subcircuit, consisting only of Clifford gates, between the $(t-1)$th and tth T gates. At step t, the circuit alternates between the Clifford subcircuit C_t and a T-gate on some wire w_t which we write as T_{w_t}, that is, we define $T_{w_t} = \mathrm{I}^{\otimes w_t - 1} \otimes \mathrm{T} \otimes \mathrm{I}^{\otimes n - w_t - 1}$.

Because of the nature of the setting, all steps are done instantaneously unless noted otherwise, without waiting for a message of the other party. For example, if the description mentions that one party teleports a qubit, we can instantly describe the qubit as 'being on the other side', but the other party will act on the uncorrected qubit, since the communication will only happen afterwards and simultaneously.

We first give a high-level description of the protocol. Bob teleports his part of the state to Alice, who holds the entire state – up to teleportation corrections. Alice will now apply the first set of Clifford gates, followed by a single T gate. The teleportation corrections (all known to Bob) determine whether the T gate that Alice performs creates an unwanted extra P gate on the state. The extra P gate is created whenever an X correction is present, because of the relation TX = PXT. Therefore, even though Alice holds the state, only Bob knows whether the state has an extra unwanted P gate or not.

To remove the unwanted gate, Alice teleports all n qubits back to Bob, who corrects the phase gate (if present). The players then perform a garden-hose-like trick to keep the form of the key simple, at the cost of doubling the total size at each step.

Now we will give the precise description of the players' actions:

Step 0. Bob performs a Bell measurement to teleport all his $n/2$ qubits to Alice, where we write the needed X-corrections as $b^0_{x,i}$ and Z-corrections $b^0_{z,i}$, for $i = n/2 + 1, \ldots, n$. Now, since the qubits Alice already started with don't need a correction, we have $b^0_{x,i} = b^0_{z,i} = 0$ for $i = 1, \ldots, n/2$. Then we write b^0_x and b^0_z for the $0/1$ vector containing the X corrections and Z correction respectively. The complete state is $\mathrm{X}^{b^0_x}\mathrm{Z}^{b^0_z}|\psi_0\rangle$, where all qubits are at Alice's side while Bob knows the key.

Step 1.a. Alice executes C_1 on the (uncorrected) qubits, so that the state now equals

$$C_1 \mathrm{X}^{b^0_x}\mathrm{Z}^{b^0_z}|\psi_0\rangle = \mathrm{X}^{\hat{b}^1_x}\mathrm{Z}^{\hat{b}^1_z}C_1|\psi_0\rangle \, ,$$

where $(\hat{b}^1_x, \hat{b}^1_z) = f_1(b^0_x, b^0_z)$, with $f_1 : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$ is a formula that consists of relabeling and addition over $\mathbb{F}_2$, and that is known to all parties. Bob knows all the entries of the vectors $\hat{b}^1_x$ and $\hat{b}^1_z$ that contain the new teleportation corrections.

Step 1.b. Alice executes the T gate on the correct wire $w_1 \in \{1, \dots, n\}$ of the uncorrected qubits. Define $\mathbf{b}^1 = \hat{b}^1_{x,w_1}$, the w_1 entry of the vector $\hat{b}^1_x$. The state in Alice's possession is now

$$\mathrm{T}_{w_1}\mathrm{X}^{\hat{b}^1_x}\mathrm{Z}^{\hat{b}^1_z}C_1|\psi_0\rangle = \mathrm{P}^{\mathbf{b}^1}_{w_1}\mathrm{X}^{\hat{b}^1_x}\mathrm{Z}^{\hat{b}^1_z}\mathrm{T}_{w_1}C_1|\psi_0\rangle = \mathrm{P}^{\mathbf{b}^1}_{w_1}\mathrm{X}^{\hat{b}^1_x}\mathrm{Z}^{\hat{b}^1_z}|\psi_1\rangle\,.$$

That is, besides the presence of the Pauli gates, depending on the teleportation measurements, the w_1 qubit possibly has an extra phase gate that needs to be corrected before the protocol can continue.

Step 1.c. Alice teleports all qubits to Bob, with teleportation outcomes $a^1_x, a^1_z \in \mathbb{F}_2^n$. We will define the $\mathbf{a}^1$ as the w_1 entry of a^1_x. Bob then has the state

$$\mathrm{X}^{a^1_x}\mathrm{Z}^{a^1_z}\mathrm{P}^{\mathbf{b}^1}_{w_1}\mathrm{X}^{\hat{b}^1_x}\mathrm{Z}^{\hat{b}^1_z}|\psi_1\rangle = \mathrm{P}^{\mathbf{b}^1}_{w_1}\mathrm{X}^{\hat{b}^1_x}\mathrm{Z}^{\hat{b}^1_z}\mathrm{Z}^{\mathbf{a}^1\mathbf{b}^1}\mathrm{X}^{a^1_x}\mathrm{Z}^{a^1_z}|\psi_1\rangle\,.$$

Knowing the relevant variables from his measurement outcomes in the previous steps, Bob performs the operation $\mathrm{X}^{\hat{b}^1_x}\mathrm{Z}^{\hat{b}^1_z}(\mathrm{P}^{\mathbf{b}^1}_{w_1})^\dagger$ to transform the state to $\mathrm{Z}^{\mathbf{a}^1\mathbf{b}^1}\mathrm{X}^{a^1_x}\mathrm{Z}^{a^1_z}|\psi_1\rangle$.

Step 1.d. For this step the players share two sets of n EPR pairs, one set labeled "$\mathbf{b}^1 = 0$", the other set labeled "$\mathbf{b}^1 = 1$". Bob teleports the state to Alice using the set corresponding to the value of $\mathbf{b}^1$, with teleportation outcomes b^2_x and b^2_z.

Step 1.e. The set of qubits corresponding to the correct value of $\mathbf{b}^1$ are in the state

$$\mathrm{X}^{b^2_x}\mathrm{Z}^{b^2_x}\mathrm{Z}^{\mathbf{a}^1\mathbf{b}^1}\mathrm{X}^{a^1_x}\mathrm{Z}^{a^1_z}|\psi_1\rangle\,.$$

On the set labeled "$\mathbf{b}^1 = 0$", Alice applies $\mathrm{X}^{a^1_x}\mathrm{Z}^{a^1_z}$, and on the set labeled "$\mathbf{b}^1 = 1$" Alice applies $\mathrm{X}^{a^1_x}\mathrm{Z}^{a^1_z}\mathrm{Z}^{\mathbf{a}^1}_{w_1}$, so that the state (at the correct set of qubits) equals $\mathrm{X}^{b^2_x}\mathrm{Z}^{b^2_z}|\psi_1\rangle$. We are now in almost the same situation as before the first step: Alice is in possession of a state for which Bob completely knows the needed teleportation corrections – with the difference that Alice does not know which of the two sets that is.

Steps 2. . . k. The players repeat the protocol from Step 1, but Alice performs all steps in parallel for *all* sets of states. The needed resources then double with each step: two sets for step 2, four for step 3, etc.

Step k+1, final step. When having executed this protocol for the entire circuit, Alice only teleports Bob's qubits back to him, i.e. the qubits corresponding to the last $n/2$ wires, instead of the entire state, so that in the correct groups, Alice and Bob are in possession of the state $|\psi_k\rangle$ up to simple teleportation corrections. Then, in their step of simultaneous communication, the players exchange all teleportation measurement outcomes. After receiving these measurement outcomes, the players discard the qubits that did not contain the state, and perform the Pauli corrections on the correct qubits.

The needed EPR pairs for this protocol consist of $n/2$ for Step 0. Then every set uses at most $3n$ pairs: n for the teleportation of Alice to Bob, and $2n$ for the teleportation back. The t-th step of the circuit starts with 2^{t-1} sets of parallel executions, therefore the total entanglement is upper bounded by $n/2 + \sum_{t=1}^{k} 2^{t-1}3n \leq 3n2^k$. ◀

4 Conditional application of phase gate using garden-hose protocols

The following lemma connects the difficulty of removing an unwanted phase gate that is applied conditional on a function f, to the garden-hose complexity of f. This lemma is the

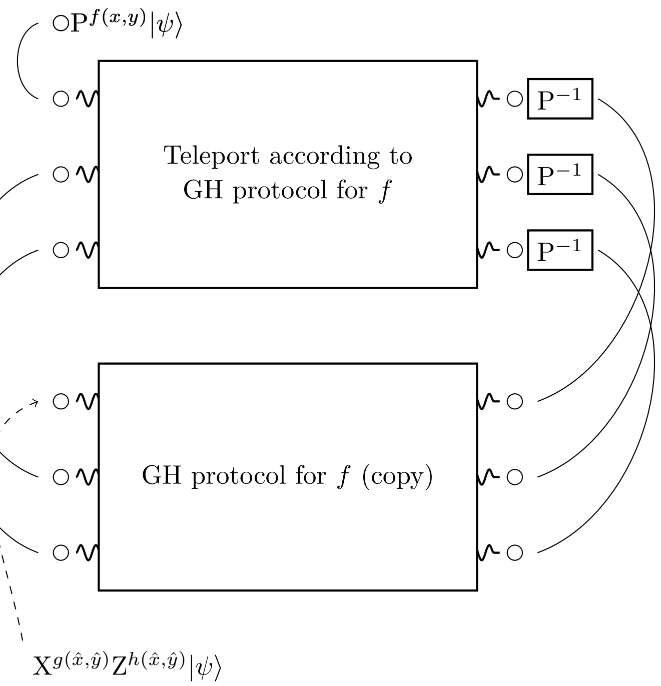

$\circ P^{f(x,y)}|\psi\rangle$
Teleport according to GH protocol for f
P^{-1}
P^{-1}
P^{-1}
GH protocol for f (copy)
$X^{g(\hat{x},\hat{y})}Z^{h(\hat{x},\hat{y})}|\psi\rangle$

Figure 2 Schematic overview of the quantum protocol to undo the conditionally-present phase gate on $|\psi\rangle$. The solid connections correspond to Bell measurements.

main technical tool which we use to non-locally compute quantum circuits with a dependence on the T-depth.

▶ **Lemma 4.** *Assume Alice has a single qubit with state $\mathrm{P}^{f(x,y)}|\psi\rangle$, for binary strings $x, y \in \{0,1\}^n$, where Alice knows the string x and Bob knows y. Let $GH(f)$ be the garden-hose complexity of the function f. The following two statements hold:*

1. *There exists an instantaneous protocol without any communication which uses $2GH(f)$ pre-shared EPR pairs after which a known qubit of Alice is in the state $\mathrm{X}^{g(\hat{x},\hat{y})}\mathrm{Y}^{h(\hat{x},\hat{y})}|\psi\rangle$. Here $\hat{x}$ depends only on x and the $2GH(f)$ bits that describe the measurement outcomes of Alice, and $\hat{y}$ depends on y and the measurement outcomes of Bob.*
2. *The garden-hose complexities of the functions g and h are at most linear in the complexity of the function f. More precisely, $GH(g) \leq 4GH(f) + 1$ and $GH(h) \leq 11GH(f) + 2$.*

Proof. To prove the first statement we will construct a quantum protocol that uses $2GH(f)$ EPR pairs, which is able to remove the conditional phase gate. The quantum protocol uses the garden-hose protocol for f as a black box.

For the second part of the statement of the lemma, we construct garden-hose protocols which are able to compute the teleportation corrections that were incurred by executing our quantum protocol. By explicitly exhibiting these protocols, we give an upper bound to the garden-hose complexity of the X correction g and the Z correction h.

The quantum protocol is shown as Figure 2. Alice and Bob execute the garden-hose protocol with the state $\mathrm{P}^{f(x,y)}|\psi\rangle$, i.e. they teleport the state back and forth, with the EPR pairs chosen depending on x and y. Afterwards, if $f(x,y) = 0$, the qubit will be at one of the unmeasured EPR halves on Alice's side, and if $f(x,y) = 1$ the qubit will be on Bob's side. The state of the qubit will be $\mathrm{X}^{g'(x',y')}\,\mathrm{Z}^{h'(x',y')}\,\mathrm{P}^{f(x,y)}|\psi\rangle = \mathrm{P}^{f(x,y)}\mathrm{X}^{g'(x',y')}\,\mathrm{Z}^{h'(x',y')\oplus f(x,y)g'(x',y')}\,|\psi\rangle$, for some functions g' and h'.

On each qubit on Bob's side, corresponding with an 'open pipe' in the garden-hose model, Bob applies P^{-1}, so that the state of the qubit is now equal to $\mathrm{X}^{g'(x',y')}\,\mathrm{Z}^{h'(x',y')\oplus f(x,y)g'(x',y')}$ $|\psi\rangle$. The exact location of our qubit depends on the protocol, and is unknown to both players. Here x' and y' are the measurement outcomes of Alice and Bob in this first half of the protocol.

To return the qubit to a known position without an extra communication step, we employ a trick that uses the reversibility of the garden-hose model. Alice and Bob repeat the exact same garden-hose strategy, except they leave the start open, and connect the open ends between the original and the copy. Alice performs a Bell measurement between the first open qubit in the original, and the first open qubit in the copy, etc. Bob does the same, after he applied the P gates. Afterwards, the qubit will be present in the start location, 'water tap' in garden-hose terminology, of the copied game, since it has followed the exact same path backwards. The final state of the qubit now is $\mathrm{X}^{g(\hat{x},\hat{y})}\,\mathrm{Z}^{h(\hat{x},\hat{y})}\,|\psi\rangle$, for some functions g and h and $\hat{x}$ and $\hat{y}$ the measurement outcomes of Alice and Bob respectively. The total entanglement consumption is $2GH(f)$.

Every measurement corresponds to a connection of two pipes in the garden-hose model, therefore each player performs at most $GH(f)$ teleportation measurements, of which the outcomes can be described by $2GH(f)$ bits.

Label the EPR pairs with numbers from $\{1, 2, \ldots, 2GH(f)\}$, and use the label 0 for the register holding the starting qubit $|\psi\rangle$. Let $\mathcal{A}$ be a list of disjoint pairs of the indices of the EPR pairs that Alice uses for teleportation in this protocol, and let $a_x, a_z \in \{0,1\}^{|\mathcal{A}|}$ be the bit strings that respectively hold the X and Z outcomes of the corresponding Bell measurements. Similarly, let $\mathcal{B}$ be a list of the indices of the EPR pairs that Bob uses, and let $b_x, b_z \in \{0,1\}^{|\mathcal{B}|}$ be the bit strings that hold the measured X and Z corrections.

To show the second part of the statement, we will construct a garden-hose protocol which tracks the newly-incurred Pauli corrections from teleporting the qubit back-and-forth, by following the qubit through the path defined by $\mathcal{A}$ and $\mathcal{B}$.

We will first construct the protocol for the final X-correction, a function we denoted by g. The protocol is also schematically shown as Figure 3. Note that to compute the X correction the conditional presence of the phase gate is not important: independent of whether $f(x,y)$ equals 1 or 0, we only need to track the X teleportation corrections that the qubit incurred by being teleported back-and-forth by Alice and Bob. An efficient garden-hose protocol for g is given by the following.

Use two pipes for each EPR pair in the protocol, $2GH(f)$ pairs of 2 pipes each. Label the top pipe of some pair i by I_i, and the bottom pipe by X_i. We will iterate over all elements of $\mathcal{A}$, i.e. all performed Bell measurements by Alice. Consider some element of $\mathcal{A}$, say the k-th pair $\mathcal{A}_k$ which consists of $\{i, j\}$. If the corresponding correction $b_{x,k}$ equals 0, we connect the pipe labeled I_i with the pipe labeled I_j and the pipe labeled X_i with the pipe labeled X_j. Otherwise, if $b_{x,k}$ equals 1, we connect them crosswise, so we connect I_i with X_j and X_i with I_j. Finally, the place where the qubit ends up after the protocol is unique (and is the only unmeasured qubit out of all $2GH(f)$ EPR pairs). For the set of open pipes corresponding to that EPR pair, say number i^*, we use one extra pipe to which we connect X_{i^*}, so that the water ends up at Bob's side for the 1-output. This garden-hose protocol computes the X correction on the qubit, and uses $4GH(f) + 1$ pipes in total, therefore $GH(g) \leq 4GH(f) + 1$.

For the Z-correction we can build a garden-hose protocol using the same idea, but there is one complication we have to take care of. At the start of the protocol, there might be an unwanted phase gate present on the state. If some teleportation is performed before this phase gate is corrected, say by Alice with outcomes a_x, a_z, then the effective correction can be

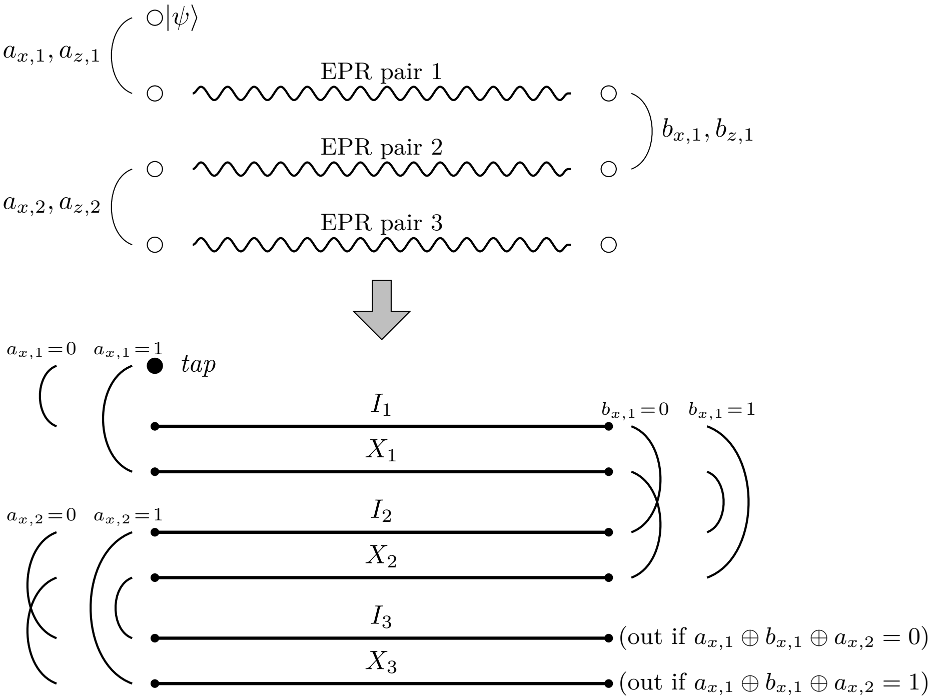
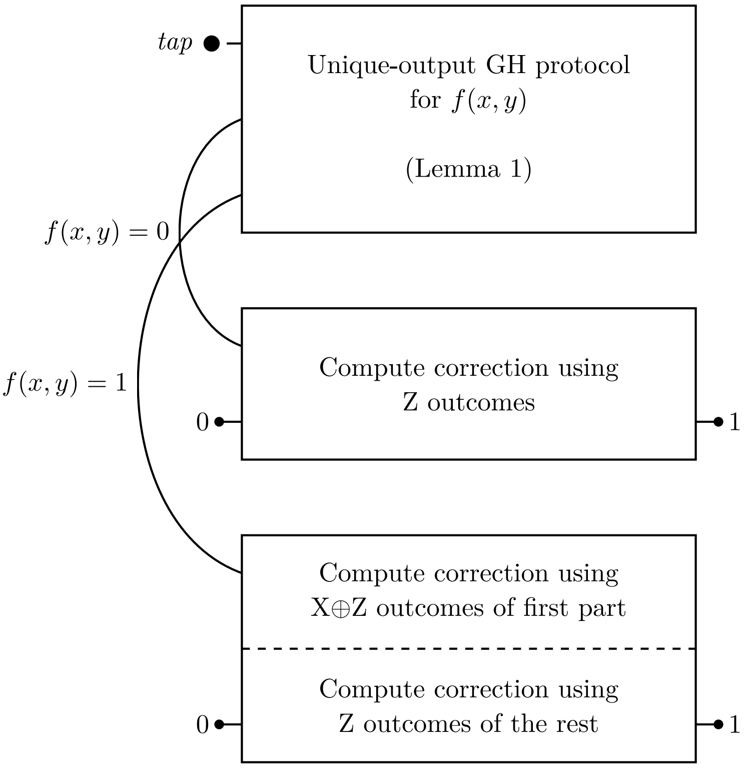


Figure 3 Example garden-hose protocol to compute the Pauli X incurred by Alice and Bob teleporting a qubit back-and-forth. When a teleportation requires a Pauli X correction, the corresponding pipes are connected crosswise, and otherwise they are connected in parallel.

written as $\mathrm{X}^{a_x}\mathrm{Z}^{a_z}\mathrm{P} = \mathrm{P}\mathrm{X}^{a_x}\mathrm{Z}^{a_x \oplus a_z}$. That is, for the part of the protocol that the unwanted phase gate is present, a Bell measurement gives a Z-correction whenever the *exclusive or* of the X- and Z-outcomes is 1, instead of just when the Z-outcome is 1. We will therefore use the garden-hose protocol that computes whether $f(x, y) = 1$, that is, compute whether the phase gate is present, and then execute a slightly different garden-hose protocol for each case.

See Figure 4 for an overview of the different parts of this garden-hose protocol for the Z-correction h. Using Lemma 1 we can transform the garden-hose protocol for f into a garden-hose protocol for f with unique 0 and 1 outputs at Alice's side, of size $3GH(f)$.[8] For the 0 output, that is if there was no unwanted phase gate present, we can track the Z corrections in exactly the same way as we did for the X corrections, for a subprotocol of size $4GH(f) + 1$. For the 1 output there was in fact a phase gate present, for the teleportations that happened in the protocol before the P^{-1} corrections. For that part of the protocol, we execute the correction-tracking protocol using the XOR of the X- and Z-measurement outcomes. For all teleportations after the phase correction, we again track the correction using just the Z-outcomes, since there is no phase gate present anymore. This part of the garden-hose protocol also uses $4GH(f) + 1$ pipes, for a total of $11GH(f) + 2$. ◀

[8] If the unique 0 output has to be at Alice's side, and the unique 1 output at Bob's side, the construction uses $3GH(f) + 1$ pipes. It is an easy exercise to show that the construction of Lemma 1 needs one pipe less if Alice wants to have both the designated 0 output and the 1 output.



tap
Unique-output GH protocol for $f(x,y)$
(Lemma 1)
$f(x,y)=0$
$f(x,y)=1$
Compute correction using Z outcomes
0
1
Compute correction using X⊕Z outcomes of first part
Compute correction using Z outcomes of the rest
0
1

Figure 4 Sketch of garden-hose protocol for the Z correction. The bottom two boxes use the construction which was used for the X-correction; in the top case using the Z-outcomes for all measurements, in the bottom case using the parity of the X- and Z-outcomes for those teleportations that happened before the unwanted phase gate was removed.

5 Low T-depth quantum circuits

▶ **Theorem 5.** *Let C be an n-qubit quantum circuit with gates out of the Clifford+T gate set, where C has T-depth d. Then there exists a protocol for two-party instantaneous non-local computation of C, where each party receives $n/2$ qubits, which uses a pre-shared entangled state of $O(\,(68n)^d\,)$ EPR pairs. That is,* $\mathrm{INQC}(C) \leq O(\,(68n)^d\,)$.

Proof. As in the proof of Theorem 3, we write the input state $|\psi\rangle$, and write the correct quantum state after step t of the circuit as $|\psi_t\rangle$. At a step t, the circuit alternates between a *layer* of T gates[9] and a subcircuit consisting of only Clifford gates, C_t.

The high-level idea of this protocol is as follows. During steps 1 to t, Alice will hold the entire uncorrected state and performs a layer of the circuit: she performs a layer of T gates and then a Clifford subcircuit. The Pauli corrections at each step are a function of earlier teleportation outcomes of both Alice and Bob. These functions determine for each qubit whether that qubit now has obtained an unwanted extra P gate when Alice performs the layer of T gates. The players then, for each qubit, correct this extra gate using Lemma 4 – removing the unwanted phase gate from the qubit in a way that both players still know its location.

[9] We will assume that for each layer of T gates *all* wires have a T gate. This is only done to avoid introducing extra notation needed when instead the gates are only applied to a subset – the protocol easily generalizes to the more common general situation.

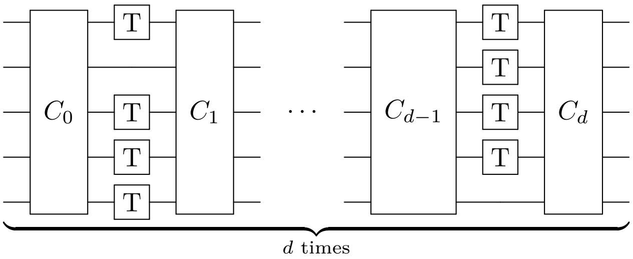


Figure 5 An example circuit with T-depth d. The C_i gates represent subcircuits consisting only of operations from the Clifford group $\mathcal{C}$. A layer does not necessarily have a T gate on all wires.

At each step we express the corrections as functions of earlier measurements and consider their garden-hose complexity, which is important when using Lemma 4. The Clifford subcircuit takes the correction functions to the XOR of several earlier functions. We can bound the growth in garden-hose complexity by taking XORs using Lemma 2. Taken together, the garden-hose complexity grows with a factor of at most a constant times n each step.

We will use $f^t_{x,i}$ to denote the function that describes the presence of an X correction on qubit i, at step t of the protocol. Similarly, $f^t_{z,i}$ is the function that describes the Z correction on qubit i at step t. Both will always be functions of outcomes of earlier teleportation measurements of Alice and Bob. For any t, let m_t be the maximum garden-hose complexity over all the key functions at step t.

Step 0. Bob teleports his qubits, the qubits labeled $n/2$ up to n, to Alice, obtaining the measurement outcomes $b^0_{x,1}, \dots, b^0_{x,n/2}$ and $b^0_{z,1}, \dots, b^0_{z,n/2}$. On these uncorrected qubits, Alice executes the Clifford subcircuit C_0.
Then, since Bob also knows how C_0 transforms the keys, the functions describing the Pauli corrections can all either be described by a single bit of information which is locally computable by Bob, or are constant and therefore known by both players. Let $f^0_{x,i}$ and $f^0_{z,i}$ be the resulting key function for any qubit i. The garden-hose complexity of all these key functions is constant: $GH(f^0_{x,i}) \leq 3$ and $GH(f^0_{z,i}) \leq 3$, and therefore also for the maximum garden-hose complexity we have $m_0 \leq 3$.

Step $t = 1, \dots, d$. At the start of the step, the X and Z corrections on any wire i are given by $f^{t-1}_{x,i}$ and $f^{t-1}_{z,i}$ respectively.
Alice applies the T gates on all wires. Any wire i now has an unwanted P if and only if $f^t_{x,i}$ equals 1.
Alice and Bob apply the construction of Lemma 4, which removes this unwanted phase gate. Let g^t_i be the function describing the extra X correction incurred by this protocol, so that the new X correction can be written as $f^t_{x,i} \oplus g^t_i$. Let h^t_i be the function describing the Z correction, so that the total Z correction is $f^t_{z,i} \oplus h^t_i$. The entanglement cost of this protocol is given by $2GH(f^t_{x,i})$ and the garden-hose complexities of the new functions are at most $GH(g^t_i) \leq 4GH(f^t_{x,i}) + 1$ and $GH(h^t_i) \leq 11GH(f^t_{x,i}) + 2$.
Alice now executes the Clifford subcircuit C_t. The circuit C_t determines how the current Pauli corrections, i.e. the key functions, transform. For a specification of the possible transformations, see Section 2.2. These new keys are formed by taking the exclusive OR of some subset of keys that were present in the previous step[10].

[10] This is slightly more general than necessary, since not all possible key transformations of this form are actually possible – only those transformations generated by the possibilities in Section 2.2 can occur.

Consider the worst case key for our construction: a key which is given by the XOR of all keys that were present when the Clifford subcircuit was executed. Applying Lemma 2, the worst-case key function of the form $\bigoplus_{i=1}^{n} f_{x,i}^{t-1} \oplus g_i^t \oplus f_{z,i}^{t-1} \oplus h_i^t$ has garden-hose complexity at most

$$\begin{aligned} m_t &\leq 4\left(\sum_{i=1}^{n} GH(f_{x,i}^{t-1}) + GH(g_i^t) + GH(f_{z,i}^{t-1}) + GH(h_i^t)\right) + 1 \\ &\leq 4\left(\sum_{i=1}^{n} GH(f_{x,i}^{t-1}) + 4GH(f_{x,i}^{t-1}) + 1 + GH(f_{z,i}^{t-1}) + 11GH(f_{x,i}^{t-1}) + 2\right) + 1 \\ &\leq 4\left(\sum_{i=1}^{n} m_{t-1} + 4m_{t-1} + 1 + m_{t-1} + 11m_{t-1} + 2\right) + 1 \\ &= 68nm_{t-1} + 12n + 1\,. \end{aligned} \tag{3}$$

Step $d+1$, final step. Alice teleports the last $n/2$ qubits back to Bob. Alice and Bob exchange all results of teleportation measurements and locally perform the needed corrections, using both players' measurement outcomes.

At every step t, the protocol uses at most $2nm_{t-1}$ EPR pairs for the protocol which corrects the phase gate. Using that $m_0 \leq 3$, we can write the upper bound of Equation 3 as the closed form $m_t \leq c_1(68n)^t + c_2$, with $c_1 = \frac{216n-2}{68n-1} \approx \frac{54}{17}$ and $c_2 = 3 - \frac{216n-2}{68n-1} \approx -\frac{3}{17}$. The total entanglement use therefore is bounded by $\sum_{t=1}^{d} 2nm_{t-1} \leq O(\,(68n)^d\,)$. ◀

6 The Interleaved Product protocol

Chakraborty and Leverrier [14] recently proposed a scheme for quantum position verification based on the interleaved multiplication of unitaries, the *Interleaved Product protocol*, denoted by $G_{\text{IP}}(n, t, \eta_{\text{err}}, \eta_{\text{loss}})$. The parameter n concerns the number of qubits that are involved in the protocol in parallel, while t scales with the amount of classical information that the protocol uses. Their paper analyzed several different attacks on this scheme, which all required exponential entanglement in the parameter t. In this section, as an application of the proof strategy of Theorem 5, we present an attack on the Interleaved Product protocol which requires entanglement polynomial in t.

The original protocol is described in terms of the actions of hypothetical honest parties and also involves checking of timings at spatial locations. For simplicity, we instead only describe a two-player game, for players Alice and Bob, such that a high probability of winning this game suffices to break the scheme. Let x be a string $x \in_R \{0,1\}^n$, and let U be a random (single-qubit) unitary operation, i.e. a random element of $U(2)$. Alice receives t unitaries $(u_i)_{i=1}^t$, and Bob receives t unitaries $(v_i)_{i=1}^t$ such that $U = \prod_{i=1}^t u_i v_i$. Alice receives the state $U^{\otimes n}|x\rangle$. The players are allowed one round of simultaneous communication. To break the protocol $G_{\text{IP}}(n, t, \eta_{\text{err}}, \eta_{\text{loss}})$, after the round of simultaneous communication the players need to output an identical string $y \in \{\emptyset, 0, 1\}^n$ such that the number of bits where y is different from x is at most $\eta_{\text{err}} n$ and the number of empty results $\emptyset$ is at most $\eta_{\text{loss}} n$. We will consider attacks on the strongest version of the protocol, where we take $\eta_{\text{loss}} = 0$.

▶ **Theorem 6.** *There exists an attack on $G_{\text{IP}}(n, t, \eta_{\text{err}}, \eta_{\text{loss}} = 0)$ that requires $p(t/\eta_{\text{err}})$ EPR pairs per qubit of the protocol, for some polynomial p, and succeeds with high probability.*

The detailed attack is included as Appendix D.

7 Discussion

We combined ideas from the garden-hose model with techniques from quantum cryptography to find a class of quantum circuits for which instantaneous non-local computation is efficient. These constructions can be used as attacks on protocols for quantum position-verification, and could also be translated back into the settings related to physics (most notable the relation between the constraints of relativity theory and quantum measurements) and distributed computing.

The resource usage of instantaneous non-local quantum computation quantifies the non-locality present in a bi- or multi-partite quantum operation, and there is still room for new upper and lower bounds. Any such bounds will result in new insights, both in terms of position-based quantum cryptography, but also in the other mentioned settings.

Some possible approaches for continuing this line of research are as follows:

- Computing the Pauli corrections happens without error in our current construction. Perhaps introducing randomness and a small probability of error – or the usage of entanglement as given in the *quantum garden-hose model* of [13, Section 2.5] – could make this scheme more efficient.
- Future research might be able to extend this type of construction to a wider gate set or model of computation. One could think for example of a Clifford+cyclotomic gate set [20], match-gate computation [27], or measurement-based quantum computation [6, 9].
- We presented an attack on the Interleaved Product protocol which required entanglement polynomial in t. Since the exponent of this polynomial was quite large, the scheme could still be secure under realistic assumptions. Since the parameter t concerns the *classical* information that the verifiers send, requiring attackers to manipulate an amount of entanglement which scales linearly with the classical information would already make a scheme unpractical to break in practice – let alone a quadratic or cubic dependence.
- The combination of the garden-hose model with the tool set of blind quantum computation is potentially powerful in other settings. For example, following up on Broadbent and Jeffery who published constructions for quantum homomorphic encryption for circuits of low T-gate complexity [10], Dulek, Speelman, and Schaffner [17] developed a scheme for quantum homomorphic encryption, based on this combination as presented in (a preprint of) this work.

Acknowledgments. The author is supported by the EU projects SIQS and QALGO, and thanks Anne Broadbent, Harry Buhrman, Yfke Dulek and Christian Schaffner for useful discussions.

A Definition of INQC

An *instantaneous non-local quantum protocol that uses k qubits of entanglement* is a protocol of the following form.

Alice and Bob start with a fixed, chosen $2k$-qubit state $\eta_{A_e B_e} \in \mathbb{C}^{2^k} \otimes \mathbb{C}^{2^k}$, the entanglement. (Our protocols all use the special case where this state is a tensor product of k EPR pairs.) The players receive an input state $\rho \in \mathcal{S}(A_{in} \otimes B_{in})$, where $\mathcal{S}(A)$ is used for the set of density matrices on some Hilbert space A. Let A_m, A_s, B_m, A_s denote arbitrary-sized quantum registers. Alice applies some quantum operation, i.e. completely positive trace-preserving map, $\mathcal{A}_\infty : \mathcal{S}(A_{in} \otimes A_e) \to \mathcal{S}(A_m \otimes A_s)$ and Bob applies the quantum operation $\mathcal{B}_\infty : \mathcal{S}(B_{in} \otimes B_e) \to \mathcal{S}(B_m \otimes B_s)$. Alice sends the register A_s to Bob, while simultaneously Bob sends B_s to Alice.

Afterwards Alice applies the quantum operation $\mathcal{A}_{\in} : \mathcal{S}(A_m \otimes B_s) \to \mathcal{S}(A_{out})$ on her memory and the state she received from Bob, and outputs the result. Likewise Bob applies the operation $\mathcal{B}_{\in} : \mathcal{S}(B_m \otimes A_s) \to \mathcal{S}(B_{out})$ on the part of the quantum state he kept and outputs the result of this operation.

▶ **Definition 7.** Let $\Phi : \mathcal{S}(A_{in} \otimes B_{in}) \to \mathcal{S}(A_{out} \otimes B_{out})$ be a bipartite quantum operation, i.e. a completely positive trace-preserving map, for some input registers A_{in}, B_{in} and output registers A_{out}, B_{out}.

We say that $\mathrm{INQC}_{\varepsilon}(\Phi)$ is the smallest number k such that there exists an instantaneous non-local quantum protocol that uses k qubits of entanglement, with induced channel $\Psi : \mathcal{S}(A_{in} \otimes B_{in}) \to \mathcal{S}(A_{out} \otimes B_{out})$, so that $\|\Phi - \Psi\|_{\diamond} \leq \varepsilon$.

For any unitary U, we write $\mathrm{INQC}_{\varepsilon}(U)$ as a shorthand for $\mathrm{INQC}_{\varepsilon}(\Phi_U)$, where Φ_U is the induced quantum operation defined by $\rho_{AB} \to U\rho_{AB}U^{\dagger}$. In this chapter, we assume for simplicity that Alice's and Bob's input and output registers all consist of n qubits.

These definitions are mostly compatible with those given in [5], but differ in two ways – both are unimportant for our results in this chapter, but might be relevant for follow-up results, especially when proving lower bounds. Firstly, we made the choice for generality to allow the players to communicate using qubits, instead of just classical messages. As long as the number of communicated qubits is not too large, quantum communication could potentially be replaced by classical communication using teleportation, at the cost of extra entanglement – the counted resource. Secondly, we make the choice to explicitly separate the shared entangled state from the local memory in notation – Beigi and König split the state in a measured and unmeasured part, but do not introduce notation for (free) extra local memory in addition to the shared entangled state.

Whether these choices are reasonable or not will also depend on the exact application. Since we mostly think about applications to position-based quantum cryptography, giving the players, i.e. 'attackers', as much power as possible seems the most natural.

B The Clifford hierarchy

The Clifford hierarchy, also called the Gottesman–Chuang hierarchy, generalizes the definition of the Clifford group of Equation 1 in the following way [24]. Define $\mathcal{C}_1 = \mathcal{P}$, the first level of the hierarchy, as the Pauli group. Recursively define the k-th level as

$$\mathcal{C}_k = \{U \in U(2^n) \mid \forall \sigma \in \mathcal{P} : U\sigma U^{\dagger} \in \mathcal{C}_{k-1}\}\,.$$

Then $\mathcal{C}_2$ is the Clifford group and the next levels consist of increasingly more quantum operations – although for $k \geq 3$ the set $\mathcal{C}_k$ is no longer a group [41].

The method behind the protocol of Theorem 3 immediately translates to the related setting of the Clifford hierarchy. Since the dependence on n is exponential, Proposition 8 will only be a qualitative improvement over Beigi and König's port-based teleportation construction when both n and the level k are small.

The results of Chakraborty and Leverrier [14] contain a complete proof of Proposition 8, proven independently and made available earlier than (the preprint of) the current paper. We still include a proof of the statement as an illustrative application of the proof technique of Section 3.

▶ **Proposition 8.** *Let U be an n-qubit operation in the k-th level of the Clifford hierarchy, where Alice receives $n/2$ qubits and Bob receives $n/2$ qubits, then* $\mathrm{INQC}(U) \leq O(n4^{nk})$.

Proof Sketch. First Bob teleports his qubits to Alice, with n outcomes for X and Z. Alice applies U to the uncorrected state, so that now the state equals $U\mathrm{X}^{b_x}\mathrm{Z}^{b_z}|\psi\rangle = V_{b_x,b_z}U|\psi\rangle$, where V_{b_x,b_z} is an operator in the $(k-1)$-th level of the Clifford hierarchy. Exactly which operator depends on Bob's measurement outcomes b_x, b_z.

Alice teleports the entire state to Bob, with outcomes a_x, a_z, and Bob applies the inverse $V^\dagger_{b_x,b_z}$, so that the state is

$$V^\dagger_{b_x,b_z}\mathrm{X}^{a_x}\mathrm{Z}^{a_z}V_{b_x,b_z}U|\psi\rangle = W_{a_x,a_z,b_x,b_z}U|\psi\rangle\,,$$

with W_{a_x,a_z,b_x,b_z} in the $(k-2)$-th level of the Clifford hierarchy. For every possible value of b_x, b_z, the players share a set of n EPR pairs. Bob teleports the state using the set labeled with his measurement outcome b_x, b_z, obtaining teleportation corrections $\hat{b}_x, \hat{b}_z$.

For every set the players repeat this protocol recursively, in the following way. For any set, Alice repeats the protocol as if it were the set used by Bob. At the correct set, Alice effectively knows the values b_x, b_z from the label, and a_x, a_z she knows as own measurement outcomes. The state present is $\mathrm{X}^{\hat{b}_x}\mathrm{Z}^{\hat{b}_z}W_{a_x,a_z,b_x,b_z}U|\psi\rangle$. When Alice applies $W^\dagger_{a_x,a_z,b_x,b_z}$, the state is given by $F_{a_x,a_z,b_x,b_z,\hat{b}_x,\hat{b}_z}U|\psi\rangle$, with F in the $(k-3)$-th level of the Clifford hierarchy. Of this state, effectively only $\hat{b}_x, \hat{b}_z$ is unknown to Alice. Alice teleports this state to Bob using the EPR pairs labeled with a_x, a_z, and the recursive step is complete.

The players continue these steps until the first level of the hierarchy is reached – formed by Pauli operators – after which they can exchange the outcomes of their measurements to undo these and obtain $U|\psi\rangle$.

After t steps, Every teleportation step after the first uses a set of n EPR pairs, picked out of 4^n possibilities corresponding to the Pauli correction of the n qubits teleported in the previous step.

Summing over all rounds gives a total entanglement use of $n\sum_{t=1}^{k} 4^{nt} = O(n4^{nk})$. ◀

C Proof of Lemma 2: Garden-hose protocols for XOR of functions

To prove: Let $(f_1, f_2, \ldots, f_k)$ be functions, where each function f_i has garden-hose complexity $GH(f_i)$. Let $c \in \{0,1\}$ be an arbitrary bit that is 0 or 1. Then,

$$GH\left(c \oplus \bigoplus_{i=1}^{k} f_i\right) \leq 4\sum_{i=1}^{k} GH(f_i) + 1\,.$$

Proof Sketch. This statement was proven by Klauck and Podder [29, Theorem 18] in a more general form, using the following two steps: First, any garden-hose protocol can be turned into a single-output garden-hose protocol, repeated in this paper as Lemma 1, such that the new complexity is at most three times the old complexity. Then, these single-output garden-hose protocols can be used as nodes in a permutation branching program. Our current case is simply an instantiation of that proof for the particular case of the exclusive OR, together with the observation that we can combine both steps into one for this particular case.

For all functions f_i we build a gadget with two input pipes and two output pipes, such that if the water flows in at input pipe labeled $b \in \{0,1\}$, it flows out at the pipe labeled $f_i \oplus b$. See Figure 6 for an overview. We use four copies of the garden-hose protocol for f_i.

The open 0 output pipes of the protocol for f_i in copy 0-IN$_i$ are connected to the open 0 output pipes in copy 0-OUT$_i$. The designated source pipe of the original protocol for f_i in

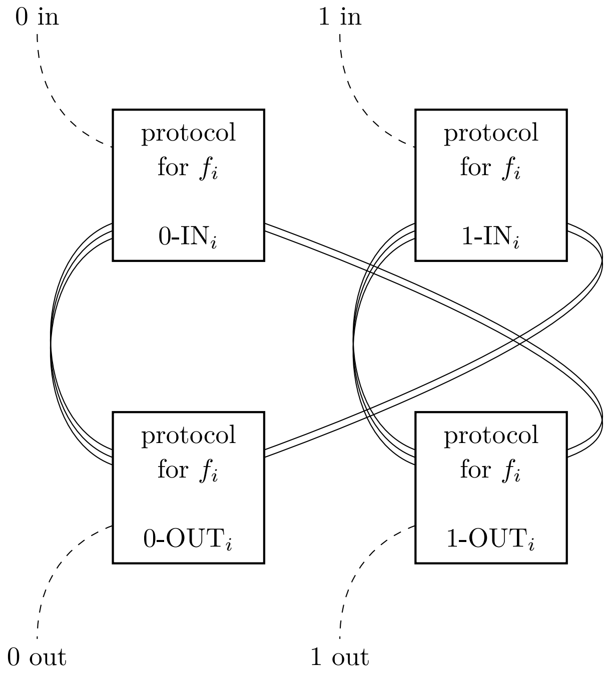

0 in
1 in
protocol for f_i 0-IN$_i$
protocol for f_i 1-IN$_i$
protocol for f_i 0-OUT$_i$
protocol for f_i 1-OUT$_i$
0 out
1 out

Figure 6 XOR gadget for any function f_i, total complexity $4GH(f_i)$.

copy 0-OUT$_i$ is then guaranteed to be the output.[11] We similarly connect the 1 outputs of 0-IN$_i$ to the 1 outputs of 1-OUT$_i$. This construction, i.e. before adding the 1-IN copy, is exactly the method used to create a single-output protocol. We connect the open 0 pipes of 1-IN$_i$ to the open 0 pipes of 1-OUT$_i$ and the open 1 pipes of the open 1 pipes of 1-IN$_i$ to the open 1 pipes of 0-OUT$_i$.

The gadget then works as claimed by direct inspection. Since all four copies are wired exactly the same, the path of the water through the 'OUT' copy is the reverse of the path it followed through the 'IN' copy, and therefore the water will exit correctly – at the pipe which was the source of the original protocol. ◀

D Proof of Theorem 6: attack on the Interleaved Product scheme

It was shown in [13] that polynomial garden-hose complexity is equivalent to log-space computation – up to a local preprocessing of the inputs. Instead of directly presenting garden-hose protocols, for the current construction it will be easier to argue about space-bounded algorithms and then using this equivalence as a black-box translation.

▶ **Theorem 9** (Theorem 2.12 of [13]). *If $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is log-space computable, then $GH(f)$ is polynomial in n.*

Our attack will involve the computation of the unitary $U = \prod_{i=1}^{t} u_i v_i$ in the garden-hose protocol. This is a simple function, but so far we have only defined the garden-hose model for functions with a binary output. Therefore we define an extension of the garden-hose

[11] This same trick is used in the proof of Lemma 1 in [29, Lemma 11] and in our proof of Lemma 4.

model to functions with a larger output range, where instead of letting the water exit at Alice's or Bob's side, we aim to let the water exit at correctly *labeled pipe*. A short proof of the following proposition is given after the proof of the main theorem.

▶ **Proposition 10.** *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k$ be a function, such that f is log-space computable and k is at most $O(\log k)$. Then there exists a garden-hose protocol which uses a polynomial number of pipes, and such that for any input x, y the water exists at Alice's side, at a pipe labeled by the output of $f(x,y)$.*

We will also need a decomposition of arbitrary unitary operations into the Clifford+T gate set. The Solovay–Kitaev theorem is a classic result which shows that any single-qubit quantum gate can be approximated up to precision ε using $O(\log^c(1/\varepsilon))$ gates from a finite gate set, where c is approximately equal to 2. See for example [33] for an exposition of the proof. Our constructions use a very particular gate set and we are only concerned with the number of T gates instead of the total number of gates. A recent result by Selinger strengthens the Solovay–Kitaev theorem for this specific case [36][12].

▶ **Theorem 11** (Selinger 2015). *Any single-qubit unitary can be approximated, up to any given error threshold $\epsilon > 0$, by a product of Clifford+T operators with T-count $11 + 12\log(1/\epsilon)$.*

With these auxiliary results in place, we can present our attack on the Interleaved Product protocol.

Proof of Theorem 6. We will describe the actions taken for any single qubit $U|b\rangle$, with $b \in \{0,1\}$, such that the probability of error is at most ε. The protocol will be attacked by performing these actions on each qubit, n times in parallel. Our construction can be divided in the following four steps. For operators A, B, let $\|A\|$ denote the operator norm, and we use $\|A - B\|$ as an associated distance measure.

1. Construct a (polynomial-sized) garden-hose protocol, with a number of pipes s, where the qubit is routed to a pipe labeled with a unitary $\tilde{U}$ which is ε_1-close to the total product U.
2. Decompose the unitaries of all labels in terms of the Clifford+T gate set, using Theorem 11. In particular, we have a Clifford+T circuit C with T-count $k = O(\log \varepsilon_2)$ such that C is ε_2-close to $\tilde{U}$, and therefore C is at most ε-close to U, where $\varepsilon = \varepsilon_1 + \varepsilon_2$.
3. After executing the garden-hose protocol as a series of teleportations, the state at pipe $\tilde{U}$ can be approximated by $X^{f_x} Z^{f_z} C|\psi\rangle$, with f_x and f_z functions of the connections Alice and Bob made in step 1 and their measurement outcomes. By the construction of Figure 3, described in the proof of Lemma 4, the garden-hose complexities $GH(f_x)$ and $GH(f_z)$ are at most linear in s.

   We can now alternate between applying a single gate of the circuit $C^\dagger$ and using Lemma 4, k times in total, to obtain a state which only has Pauli corrections left.
4. After Alice measures this final state, she can broadcast the outcome to Bob. Alice and Bob also broadcast their inputs and measurement outcomes, which together determine whether to flip the outcome of Alice's final measurement.

As the first step, we present a log-space computation solving the following problem (equivalent to the input of the protocol, with simplified notation): The input is given by t two-by-two unitary matrices, $u_1, \ldots, u_t$, and we output a matrix $\tilde{U}$ such that $\|\tilde{U} - u_t \ldots u_2 u_1\| \le$

[12] When the single-qubit unitary is a z-rotation, an even stronger version of the theorem is available [34].

ε_1, where $\tilde{U}$ is encoded using $O(\log t + \log 1/\varepsilon_1)$ bits. We can then use a simple extension of Theorem 9 to transform this computation to a garden-hose protocol.

Store the current intermediate outcome of the product in the memory of our computation, using $2\ell + 2$ bits for each entry of the two-by-two matrix, $\ell + 1$ for the real and imaginary part each. Let M_r denote the memory of our log-space computation after r steps, obtained by computing the product $u_r M_{r-1}$ with rounding. Since the rounded matrix entry has a difference of at most $2^{-\ell}$ with the unrounded entry, we can write the precision loss at each step as $M_r = u_r M_{r-1} + \Delta_r$, where Δ_r is some matrix with all entries absolute value at most $2^{-\ell}$. Note that $\|\Delta_r\| \leq 2^{-\ell+1}$.

The total error incurred by the repeated rounding can now be upper bounded by

$$\begin{aligned}\|M_t - u_t \dots u_2 u_1\| &\leq \|u_t M_{t-1} + \Delta_t - u_t \dots u_2 u_1\| \\ &\leq \|\Delta_t\| + \|u_t(M_{t-1} - u_{t-1} \dots u_2 u_1)\| \\ &\leq 2^{-\ell+1} + \|M_{t-1} - u_{t-1} \dots u_2 u_1\| \\ &\leq t 2^{-\ell+1}\end{aligned}$$

Here we use that $\|AB\| \leq \|A\|\|B\|$ together with the unitarity of all u_i. The final step is by iteratively applying the earlier steps t times. If we choose $\ell = \log t + \log 1/\varepsilon_1 + 1$ and note that the final output $\tilde{U}$ is given by M_t, we obtain the bound.

By application of Proposition 10 we can convert this log-space computation to a garden-hose protocol, using s pipes, where s is polynomial in ε_1 and t. We then teleport the qubit back-and-forth using Bell measurements given by this garden-hose protocol.

As second step, we approximate the unitaries that label each output pipe of the garden-hose protocol of the previous step. In particular, consider the pipe labeled $\tilde{U}$, and say we approximate $\tilde{U}$ using a Clifford+T circuit C. By Theorem 11, we can write C using $k = 11 + 12\log(1/\varepsilon_2)$ T gates, such that $\|\tilde{U} - C\| \leq \varepsilon_2$. Therefore, defining $\varepsilon = \varepsilon_1 + \varepsilon_2$, we have $\|U - C\| \leq \varepsilon$.

We will perform the next steps for all unmeasured qubits (corresponding to open pipes in the garden-hose model) in parallel. After the simultaneous round of communication, Alice and Bob are then able to pick the correct qubit and ignore the others.

Consider the state of the qubit after the teleportations chosen by the garden-hose protocol. For some functions f_x, f_z, with inputs Alice's and Bob's measurement outcomes, the qubit has state $\mathrm{X}^{f_x}\mathrm{Z}^{f_z}U|b\rangle$. From now on, we will assume this state is exactly equal to $\mathrm{X}^{f_x}\mathrm{Z}^{f_z}C|b\rangle$ – since U is ε-close to C in the operator norm, this assumption adds error probability at most 2ε to the final measurement outcome[13].

Write the inverse of this circuit as alternation between gates from the Clifford group and T gates, $C^\dagger = C_k \mathrm{T} C_{k-1} \mathrm{T} \dots C_1 \mathrm{T} C_0$. We will remove C from the qubit by applying these gates, one by one, by repeated application of Lemma 4. As convenient shorthand, define the state of the qubit after applying the first r layers of $C^\dagger$, i.e. up to and including C_r, of $C^\dagger$ as

$$|\psi_r\rangle = \mathrm{T}^\dagger C_{r+1}^\dagger \mathrm{T}^\dagger C_{r+2} \dots \mathrm{T}^\dagger C_k^\dagger |b\rangle\,.$$

In particular, we have $C_r \mathrm{T}|\psi_{r-1}\rangle = |\psi_r\rangle$.

By exactly the same construction used in the proof of Lemma 4, shown in Figure 3, we observe that the garden-hose complexities of the functions f_x and f_z is at most $2s + 1$. That is, the protocol uses 2 pipes for all of the s EPR pairs, and connects them in parallel if the

[13] See for instance [33, Box 4.1] for a computation of this added error.

corresponding X- or Z-correction is 0, or crosswise if the corresponding X- or Z-correction is 1.

We will use divide f_x^r and f_z^r as the functions describing the X and Z corrections at the end of the step r. Define $m_r = \max\{GH(f_x^i), GH(f_z^i)\}$ to be the maximum garden-hose complexity out the of functions describing the X and Z corrections after step r. After Alice executes the Clifford gate C_0, the new key functions f_x^0 and f_z^0 can be written as (the NOT of) an XOR of subsets of the previous keys, e.g., one of the keys could be $f_x \oplus f_z$. By Lemma 2, we then have that our starting complexities $GH(f_x^0)$ and $GH(f_z^0)$ are at most linear in s.

Now, for any layer $r = 1, 2, \ldots, k$: Our qubit starts in the state $\mathrm{X}^{f_x^{r-1}}\mathrm{Z}^{f_z^{r-1}}|\psi_{r-1}\rangle$, for some functions f_x^{r-1}, f_z^{r-1} that each have garden-hose complexity at most m_{r-1}. After Alice performs a T gate, the qubit is in the state

$$\mathrm{T}\mathrm{X}^{f_x^{r-1}}\mathrm{Z}^{f_z^{r-1}}|\psi_{r-1}\rangle = \mathrm{P}^{f_x^{r-1}}\mathrm{X}^{f_x^{r-1}}\mathrm{Z}^{f_z^{r-1}}\mathrm{T}|\psi_{r-1}\rangle\,.$$

Now, we apply Lemma 4, costing $2GH(f_x^{r-1})$ EPR pairs, so that Alice has the state

$$\mathrm{X}^{f_x^{r-1}\oplus g_r}\mathrm{Z}^{f_z^{r-1}\oplus h_r}\mathrm{T}|\psi_{r-1}\rangle\,,$$

for some functions g_r and h_r that depend on the measurement results by Alice and Bob. We have that $GH(g_r) \leq 4GH(f_x^{r-1}) + 1$ and $GH(g_r) \leq 11GH(f_x^{r-1}) + 2$.

Now Alice applies the Clifford group gate C_r, so that the state becomes

$$C_r\mathrm{X}^{f_x^{r-1}\oplus g_r}\mathrm{Z}^{f_z^{r-1}\oplus h_r}\mathrm{T}|\psi_{r-1}\rangle = \mathrm{X}^{f_x^r}\mathrm{Z}^{f_z^r}|\psi_r\rangle\,.$$

The functions f_x^r and f_z^r can be expressed as XOR of the functions f_x^{r-1}, f_y^{r-1}, g_r, h_r. These functions have garden-hose complexity respectively at most m_{r-1}, m_{r-1}, $4m_{r-1} + 1$ and $11m_{r-1}+2$. By application of Lemma 2, the exclusive OR of these functions therefore at most has garden-hose complexity $m_r \leq 4(m_{r-1}+m_{r-1}+4m_{r-1}+1+11m_{r-1}+2)+1 = 68m_{r-1}+13$.

Finally, after application of the gates in $\mathcal{C}^\dagger$, Alice has a qubit in a state which is ε-close to $\mathrm{X}^{f_x^r}\mathrm{Z}^{f_z^r}|b\rangle$. Measurement in the computational basis will produce outcome $b \oplus f_x^r$ with high probability. Besides this final measurement, Alice and Bob both broadcast all teleportation measurement outcomes in their step of simultaneous communication. From these outcomes they can each locally compute f_x^r and so derive the bit b from the outcome, which equals $b \oplus f_x^r$, breaking the protocol.

Our total entanglement usage is s for the first step, and then for each of the at most s output pipes, Alice performs the rest of the protocol. For the part of the protocol that undoes the unitary U, we use at most $2\sum_{r=0}^{k-1} m_r$ EPR pairs (for each of the at most s output pipes of the first part). We have $m_0 \leq O(s)$ and $m_r \leq m_0 \cdot 2^{O(k)}$. Since s is polynomial in t and ε_1 and $k = O(\log \varepsilon_2)$, the total protocol uses entanglement polynomial in t and ε. ◀

Our attack replaces the exponential dependence on t of the attacks presented in [14] by a polynomial dependence. For the case of $\eta_{\text{err}} = 0$, we would need an error per qubit of around $\frac{\varepsilon}{n}$ to achieve total error at most ε. In that case, the entanglement required still grows as a polynomial, now with a super-linear dependence of both parameters n and t.

Only the first step of our attack, i.e. the garden-hose protocol which computes a unitary from the inputs of the players, is specific to the interleaved product protocol. This attack can therefore be seen as a blueprint for attacks on a larger class of protocols: any protocol of this same form, where the unitary operation chosen depends on a log-space computable function with classical inputs, can be attacked with entanglement which scales as a polynomial in the size of the classical inputs.

Proof of Proposition 10. We can split up the computation $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k$ into k functions that each compute a bit, $f_1, \ldots, f_k$. Since f is a log-space computation, each of these functions is also a log-space computation and therefore has a polynomial-size garden-hose protocol by Theorem 9. Using Lemma 1, we can with linear overhead transform each of these protocol into a unique-output protocol, so that the water flows out at a unique pipe when the function is 0 and another unique pipe when the function is 1. Let p be a polynomial so that the single-output garden-hose protocol of each function f_i uses pipes at most $p(n)$.

First use the protocol for f_1, with output pipes labeled 0 and 1. Now each of these output pipes we feed into their own copy of f_2. The 0 output of the first copy we label 00 and its 1 output 10. Similarly, we label the 0 output of the second copy 01 and the 1 output we label 11. By recursively continuing this construction, we build a garden-hose protocol for the function f which uses s pipes, where s is at most

$$s \leq \sum_{i=1}^{k} 2^{i-1} p(n) \leq 2^k p(n)\,.$$

Since we have taken $k = O(\log n)$, this construction uses a number of pipes polynomial in n. ◀

References

1 Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, 2004.

2 Matthew Amy, Dmitri Maslov, and Michele Mosca. Polynomial-time T-depth optimization of Clifford+T circuits via matroid partitioning. *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, 33(10):1476–1489, Oct 2014. `doi:10.1109/TCAD.2014.2341953`.

3 Matthew Amy, Dmitri Maslov, Michele Mosca, and Martin Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *Trans. Comp.-Aided Des. Integ. Cir. Sys.*, 32(6):818–830, June 2013. `doi:10.1109/TCAD.2013.2244643`.

4 Pablo Arrighi and Louis Salvail. Blind quantum computation. *International Journal of Quantum Information*, 4(05):883–898, 2006.

5 Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

6 HJ Briegel, DE Browne, W Dür, R Raussendorf, and M Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, 2009.

7 Anne Broadbent. Delegating private quantum computations. *Canadian Journal of Physics*, 93(9):941–946, 2015. `doi:10.1139/cjp-2015-0030`.

8 Anne Broadbent. Popescu–Rohrlich correlations imply efficient instantaneous nonlocal quantum computation. *arXiv preprint arXiv:1512.04930*, 2015.

9 Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

10 Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology – CRYPTO 2015*, volume 9216 of *Lecture Notes in Computer Science*, pages 609–629. Springer Berlin Heidelberg, 2015. `doi:10.1007/978-3-662-48000-7_30`.

11 H. Buhrman, R. Cleve, M. Laurent, N. Linden, A. Schrijver, and F. Unger. New limits on fault-tolerant quantum computation. In *Foundations of Computer Science, 2006. FOCS'06. 47th Annual IEEE Symposium on*, pages 411–419, Oct 2006. doi:10.1109/FOCS.2006.50.

12 Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 429–446. Springer Berlin / Heidelberg, 2011.

13 Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, ITCS'13, pages 145–158, New York, NY, USA, 2013. ACM. doi:10.1145/2422436.2422455.

14 Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Phys. Rev. A*, 92:052304, Nov 2015. doi:10.1103/PhysRevA.92.052304.

15 Andrew M Childs. Secure assisted quantum computation. *Quantum Information & Computation*, 5(6):456–466, 2005.

16 S R Clark, A J Connor, D Jaksch, and S Popescu. Entanglement consumption of instantaneous nonlocal quantum measurements. *New Journal of Physics*, 12(8):083034, 2010. URL: http://stacks.iop.org/1367-2630/12/i=8/a=083034.

17 Yfke Dulek, Christian Schaffner, and Florian Speelman. Quantum homomorphic encryption for polynomial-sized circuits. *arXiv preprint arXiv:1603.09717*, 2016.

18 Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In *CRYPTO*, pages 685–706, September 2010. arXiv:1009.2096, doi:10.1007/978-3-642-14623-7_37.

19 KAG Fisher, A Broadbent, LK Shalm, Z Yan, J Lavoie, R Prevedel, T Jennewein, and KJ Resch. Quantum computing on encrypted data. *Nature communications*, 5, 2014.

20 Simon Forest, David Gosset, Vadym Kliuchnikov, and David McKinnon. Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets. *Journal of Mathematical Physics*, 56(8):–, 2015. doi:10.1063/1.4927100.

21 Brett Giles and Peter Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Physical Review A*, 87(3):032332, 2013.

22 Daniel Gottesman. The Heisenberg representation of quantum computers. In *Group theoretical methods in physics. Proceedings, 22nd International Colloquium, Group22, ICGTMP'98, Hobart, Australia, July 13-17, 1998*, 1998. arXiv:quant-ph/9807006.

23 Daniel Gottesman. Theory of fault-tolerant quantum computation. *Phys. Rev. A*, 57:127–137, Jan 1998. doi:10.1103/PhysRevA.57.127.

24 Daniel Gottesman and Isaac L. Chuang. Quantum Teleportation is a Universal Computational Primitive. *Nature*, 402:390–393, August 1999. arXiv:9908010, doi:10.1038/46503.

25 Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett.*, 101(24):240501, Dec 2008. doi:10.1103/PhysRevLett.101.240501.

26 Satoshi Ishizaka and Tohya Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Phys. Rev. A*, 79(4):042306, Apr 2009. doi:10.1103/PhysRevA.79.042306.

27 Richard Jozsa, Barbara Kraus, Akimasa Miyake, and John Watrous. Matchgate and space-bounded quantum computations are equivalent. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, page rspa20090433. The Royal Society, 2009.

28 Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84:012326, Jul 2011. doi:10.1103/PhysRevA.84.012326.

29 Hartmut Klauck and Supartha Podder. New bounds for the garden-hose model. In Venkatesh Raman and S. P. Suresh, editors, *34th International Conference on Foundation of Software Technology and Theoretical Computer Science (FSTTCS 2014)*, volume 29 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 481–492, Dagstuhl, Germany, 2014. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.FSTTCS.2014.481.

30 Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. Fast and efficient exact synthesis of single-qubit unitaries generated by Clifford and T gates. *Quantum Info. Comput.*, 13(7-8):607–630, July 2013.

31 Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Phys. Rev. A*, 83(1):012322, Jan 2011. doi:10.1103/PhysRevA.83.012322.

32 Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane. The invariants of the Clifford groups. *Designs, Codes and Cryptography*, 24(1):99–122, 2001. doi:10.1023/A:1011233615437.

33 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge university press, 2000.

34 Neil J Ross and Peter Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. *arXiv preprint arXiv:1403.2975*, 2014.

35 Peter Selinger. Quantum circuits of T-depth one. *Physical Review A*, 87(4):042302, 2013.

36 Peter Selinger. Efficient Clifford+T approximation of single-qubit operators. *Quantum Information & Computation*, 15(1-2):159–180, January 2015.

37 Florian Speelman. Position-based quantum cryptography and the garden-hose game. Master's thesis, University of Amsterdam, 2011.

38 Lev Vaidman. Instantaneous measurement of nonlocal variables. *Phys. Rev. Lett.*, 90(1):010402, Jan 2003. doi:10.1103/PhysRevLett.90.010402.

39 Li Yu. Fast controlled unitary protocols using group or quasigroup structures. *arXiv preprint arXiv:1112.0307*, 2011.

40 Li Yu, Robert B Griffiths, and Scott M Cohen. Fast protocols for local implementation of bipartite nonlocal unitaries. *Physical Review A*, 85(1):012304, 2012.

41 Bei Zeng, Xie Chen, and Isaac L Chuang. Semi-Clifford operations, structure of C_k hierarchy, and gate complexity for fault-tolerant quantum computation. *Physical Review A*, 77(4):042313, 2008.