The task of non-local quantum computation requires implementation of a unitary on $n$ qubits between two parties with only one round of communication, ideally with minimal pre-shared entanglement. We introduce a new protocol that makes use of the fact that port-based teleportation costs much less entanglement when done only on a small number of qubits at a time. Whereas previous protocols have entanglement cost independent of the unitary or scaling with its complexity, the cost of the new protocol scales with the non-locality of the unitary. Specifically, it takes the form $\sim n^{4V}$ with $V$ the maximum volume of a past light cone in a circuit implementing the unitary. Thus we can implement unitary circuits with $V \sim O(1)$ using polynomial entanglement, and those with $V \sim \text{polylog}(n)$ using quasi-polynomial entanglement. For a general unitary circuit with $d$ layers of $k$-qubit gates $V$ is at most $k^d$, but if geometric locality is imposed it is at most polynomial in $d$. We give an explicit class of unitaries for which our protocol’s entanglement cost scales better than any known protocol. We also show that several extensions can be made without significantly affecting the entanglement cost – arbitrary local pre- and post-processing; global Clifford pre- and post-processing; and the addition of a polynomial number of auxiliary systems.

1 Introduction

Non-local quantum computation (NLQC) is a quantum task with both practical applications and relevance to fundamental physics [1–12]. Practically, it is a fundamental primitive for position-based quantum cryptography [3, 13]. In fundamental physics, it appears to have deep connection with the holographic principle [14, 15].

The NLQC task involves two individuals that are given a quantum state, and must apply to it a given quantum computation with only one round of communication. Critically, it can be shown that for some unitaries the two individuals can only accomplish this if they share a certain amount of entanglement ahead of time [14]. Knowing exactly how much entanglement is necessary is the crux of determining whether a large class of position-based cryptography schemes is viable.

## Contents

1 Introduction

2 Background

   2.1 Non-local quantum computation

   2.2 Teleportation primitives

   2.3 Best known protocol for general unitary

3 The protocol and its cost

   3.1 The protocol

   3.2 Entanglement cost

   3.3 Regime of efficiency

   3.4 Distinction from other protocols

4 Enhancements

   4.1 Local pre/post-processing

   4.2 Clifford sandwich

   4.3 Auxiliary systems

5 Conclusion

Acknowledgement

A Protocol error bounds

References
Currently, linear lower bounds [14, 16] and exponential upper bounds [4] are known for the number of shared Bell pairs needed as a function of the number of qubits the computation acts on. However, if the structure of the computation is taken into account the upper bounds may be tightened. For example, there are protocols that need only entanglement exponential in the T-depth or T-count of the unitary [17], and others that can efficiently perform a certain class of unitaries related to classical complexity classes [18] and [19]. Furthermore, arguments from high energy physics are suggestive that the entanglement cost upper bound should be polynomial in the circuit depth for any unitary [20].

In this work we introduce a new protocol capable of efficiently performing NLQC for a new class of unitaries. Our protocol is a generalization of the one introduced in Ref. [4], which relies on a form of quantum teleportation known as port teleportation [21]. Unlike standard quantum teleportation, in which a teleported system is encrypted by the presence of an unknown Pauli operator, in port-based teleportation the teleported system is encrypted in that it appears in one of many systems or “ports”, the identity of which is unknown to the receiver. Unitaries can be easily implemented on a port-teleported system by transversally applying the unitary in question to all possible ports, whereas after standard teleportation the receiver would need to first undo an unknown Pauli encryption. However, easier implementation of unitaries comes at the cost of requiring entanglement exponential in the number of qubits being teleported, which is the origin of the exponential cost of the protocol in Ref. [4]. By contrast, our protocol makes use of the circuit structure of a unitary, allowing us to port-teleport only a small batch of qubits at a time.

At a high level, our protocol consists of Alice and Bob iterating through the gates of the circuit, teleporting back and forth the batch of qubits on which each gate acts. Alice always normal-teleports to Bob, while Bob always port-teleports to Alice. In this way Bob always knows the identity of the correct ports, and thus can port-teleport the right batch of systems to Alice. Meanwhile Alice always knows the identity of the Pauli encryptions, and thus can remove them to perform computations. However, because Alice does not know the identity of the correct port, she must normal-teleport all ports back to Bob, resulting in her obtaining Pauli keys that depend on the port, and thus she does not know which key to use when receiving the system at a later step. We deal with this issue via the re-indexing technique of [22], i.e. by having Bob port-teleport the system through a shared resource labeled by the correct port. Thus when Bob port-teleports a new batch of qubits to Alice, they must have set up a resource state for each combination of port values of all the port-based teleportations in the causal past of these qubits. The number of port teleportation resource states required to do this is proportional to an exponential of the number of such teleportations, which is the number of gates in the past light cone of the current gate. Furthermore, the size of the port teleportation resource state scales exponentially with k, the number of qubits each gate in the circuit acts on. This results in a total entanglement cost scaling like $n^{4V}$, with $V$ the volume of the largest past light cone in the circuit – that is, the total number of qubits acted on by gates in the causal past of a given gate, where the same qubit can be counted multiple times.

In the worst case, the past light cone volume scales as $k^d$ with $k$ the number of qubits each gate in the circuit acts on, and $d$ the depth of the circuit. Since the base of the exponent scales with $n$, functions implementable with only polynomial entanglement must have $O(1)$ layers of $O(1)$-sized gates. However, the number of efficiently implementable unitaries is much larger if we mildly relax the notion of “efficient” to include quasi-polynomial entanglement – that is, entanglement that scales as an exponential of a polylogarithmic function. This class grows only mildly faster than polynomials, and still much slower than exponential functions $^1$. One class of unitaries that our protocol efficiently performs (i.e. using a quasi-polynomial number of Bell pairs) is constant-depth circuits of polylogarithmic sized gates.

In section 2, we formally introduce the problem of NLQC and the primitives of normal and port-based teleportation, and review the protocol of [4] that ours generalizes. We present the protocol in section 3 and analyze its performance, calculating and analyzing the entanglement cost and comparing with existing protocols. In section 4, we give several enhancements to the protocol that increase the class of unitaries it can perform efficiently: (i) arbitrary local pre- and post-processing, whereby Alice and Bob are free to act on their initial states before and after the protocol; (ii) arbitrary global Clifford pre- and post-processing; and (iii) use of a polynomial number of auxiliary registers.

2 Background

2.1 Non-local quantum computation

A non-local quantum computation (NLQC) task involves two parties, Alice and Bob. At the start, Alice holds a quantum systems $A$ and $R_A$ while Bob holds $B$ and $R_B$. The systems $AB$ collectively contain $n$ qubits, and for simplicity we assume each party has $n/2$

$^1$For example, $n^m$ is larger than $\exp(\log(n)^2)$ until $n = e^m$. 


qubits. They are also potentially entangled with a reference state \( R \) that neither of them hold. These start out in a state \( |\psi\rangle_{A'B'} \otimes |\phi\rangle_{RA RB} \). The state \( |\psi\rangle_{A'B'} \) is unknown to Alice and Bob, but they are free to choose the “resource” state \( |\phi\rangle_{RA RB} \). Alice and Bob are told of a unitary \( U_{AB} \) acting on the system \( AB \), which they are to perform in the following restricted manner. First, Alice performs a quantum channel of her choice \( N_{ARA' \to A'M_A} \) on the systems she holds to produce an output system \( A' \) that she keeps and a message system \( M_A \) that she sends to Bob. Similarly Bob performs \( N_{BRB' \to B'M_B} \) to obtain \( B' \) and \( M_B \). Critically, the message systems do not interact during the exchange, which is why the computation is “non-local”. Alice then performs a channel \( N_{A'M_B \to A} \) and Bob the channel \( N_{B'M_A \to B} \). They succeed in the task if the final state of \( AB \) is \( U_{AB} |\psi\rangle_{A'B'} \).

For brevity, we henceforth omit the reference state \( R \) and refer to \( AB \) as a pure state; however our results still apply in the more general setting.

2.2 Teleportation primitives

We make heavy use of two types of quantum teleportation: normal teleportation [23] and port-based teleportation [21].

**Primitive 1. Normal teleportation**

1. **Setup:** Alice holds an \( n_A \)-qubit system \( A \) which, together with some reference system \( R \) is in a state \( |\psi\rangle_{AR} \). Alice and Bob each hold one of a maximally entangled pair of \( 2^{n_A} \) dimensional systems \( A'B' \).

2. Alice performs some joint measurement on \( A \) and \( A' \), receiving the identity of an \( n_A \)-qubit Pauli operator \( P \) drawn uniformly from all such operators.

3. Bob’s half of the maximally entangled state, together with the reference system, is then in the state \( P |\psi\rangle_{B'R} \), where \( P \) acts on the \( B' \) subsystem.

**Primitive 2. Port-based teleportation**

1. **Setup:** Alice holds an \( n_A \)-qubit system \( A \) which, together with some reference system \( R \) is in a state \( |\psi\rangle_{AR} \). Alice and Bob each hold one half of \( N \) maximally entangled pairs of \( 2^{n_A} \) dimensional systems \( \{A'_j B'_j\} \).

2. Alice performs some joint measurement on \( A \) and \( \{A'_j\} \), receiving a random number \( x^* \in [N]^2 \).

3. Bob’s half of the \( x^* \)th entangled system, together with the reference system, is then close to the state \( |\psi\rangle_{B'x^*, R} \), with error decreasing with \( N \).

Specifically, if \( E : B(A) \to B(B'x^*) \) is the CPTP map describing the error channel, then from [4] we have

\[
||E - I_{C\otimes n_A}||_\infty \leq \frac{2^{2n_A}}{\sqrt{N}}.
\]  

We say that the system \( A \) has been port-teleported.

2.3 Best known protocol for general unitary

The best known NLQC protocol for a generic unitary is due to Beigi and Koenig in Ref. [4], and proceeds as follows.

**Protocol 3. Beigi-Koenig**

1. Alice normal-teleports \( A \) to Bob, receiving Pauli correction \( P \).

2. Bob port-teleports the \( n \)-qubit system \( AB \) to Alice, receiving port key \( x^* \).

3. Alice then applies \( P^T \) to the \( A \) part of all the ports on her side. She then applies \( U \) to every port.

4. **Communication Round:** Alice sends the \( B \) side of every port to Bob, and Bob sends \( x^* \) to Alice. Both sides then throw away all systems not coming from the \( x^* \) port, completing the protocol.

From eq. (1) we see that this protocol requires \( N = 16^{4n_A} \) in order to obtain some constant error \( \epsilon \).

3 The protocol and its cost

3.1 The protocol

Because of the important role that circuit decompositions of a unitary plays in our protocol, we carefully define some formal terminology for use throughout.

**Definition 4.** Let a circuit decomposition of \( U \) be \( \{U^j\}_{i \in [d], j \in [n]} \), meaning \( U = U^d \cdots U^1 \), with each \( U^i \) being a product of \( n_i \) gates \( U^i = U^i_1 \cdots U^i_{n_i} \) each with disjoint support on \( k_{i,j} \) qubits. Denote the support of \( U^j \) as \( S^j_i = \text{supp}(U^j_i) \), the collection of which we refer to as the circuit structure \( \{S^j_i\}_{i \in [d], j \in [n]} \).

We will see that the circuit structure completely specifies the entanglement cost of our protocol. Specifically, it depends on causal properties of the circuit structure that we characterize as follows.

For low-depth circuits, a given gate acts on qubits whose state only depends on a small number of previous

\(^3\)By support we mean the set of qubits that the operator acts on.
gates (as well as the initial state), sometimes called the past light cone. We call the subsystems corresponding to these gates in the past light cone the ancestors of the subsystem in question, defined formally as follows, and depicted in fig. 1.

Definition 5. For a circuit structure \( \{ S_j^i \} \), we denote the parents \( \text{par}(i, j) \) of a subsystem \( S_j^i \) at circuit layer \( i \) and with subsystem label \( j \), to be the set of all subsystems from the previous layer \( S_{j^i-1}^i \) with nonzero overlap, i.e., \( S_j^i \cap S_{j^i-1}^i \neq \emptyset \). The ancestors \( \text{anc}(i, j) \) of \( S_j^i \) is then the set of all parents, parents’ parents, and so on; formally, it is defined recursively as

\[
\text{anc}(i, j) = \text{par}(i, j) \cup \text{anc}(\text{par}(i, j))
\]

Finally, we refer to the union of a subsystem with its ancestors as its family, \( \text{fam}(i, j) = \text{anc}(i, j) \cup \{ (i, j) \} \).

Now we have the notation needed to formally state the general protocol. In this protocol, steps 2-5 are looped over many times – once per gate in the circuit structure. Some parts of these steps are only relevant on iterations corresponding to gates beyond the first layer of the circuit, and are reliant on later steps that occurred in previous iterations. To aid the reader in such cases, we separately express the simpler form of those steps in the first layer.

Protocol 6.

Setup: \( N \) is fixed to be a constant that controls the accuracy of the protocol. We also have a fixed circuit structure \( \{ U_j^i \} \) corresponding to a circuit decomposition \( \{ U_j^i \} \) of the unitary to be implemented, \( U \). For each \( (i, j) \), Alice and Bob allocate a set of \( 2^{N|\text{fam}(i,j)|} \) maximally entangled pairs of \( 2^{k_{i,j}} \)-dimensional systems, labelled by \( (i, j, x_{\text{fam}(i,j)}, m) \). Here the notation \( x_{\text{fam}(i,j)} \) denotes a set of labels \( x_{j^i}^i \in [N] \) for each \( (i', j') \in \text{fam}(i, j) \), and we use similar notation throughout the protocol. The label \( m \in \{ A, B \} \) specifies whether the system is used for port-based teleportation from Bob to Alice (\( B \)) or for normal teleportation from Alice to Bob (\( A \)). We refer to Alice’s share of an entangled pair \( (i, j, x_{\text{fam}(i,j)}, m) \) as \( A(i, j, x_{\text{fam}(i,j)}, m) \), and similarly Bob’s share as \( B(i, j, x_{\text{fam}(i,j)}, m) \). A further \( n/2 \) qubits are allocated for an initial teleportation from Alice to Bob. The protocol then proceeds as follows.

1. Alice normal-teleports her \( n/2 \) qubits to Bob, resulting in him holding state \( P |\psi⟩ \) with \( P \) a Pauli known by Alice. It remains to implement \( UP^i \).

2. First layer: Bob port-teleports \( S_j^1 \) to Alice through the \( N \) systems labelled \( B(1, j, x_j^1, B) \), from which he gets a key \( x_j^1 \in [N] \).

Subsequent layers: Bob port-teleports \( S_j^i \) to Alice through the \( N \) systems labelled \( B(i, j, x_j^i, A) \), from which he gets a key \( x_j^i \in [N] \). This is depicted in fig. 2.

3. First layer: To each of the \( N \) systems labelled \( A(1, j, x_j^1, B), \) Alice applies \( U_j^1 P_j^1 |\psi⟩^5 \).

Subsequent layers: To each of the \( N|\text{fam}(i,j)| \) systems labelled \( A(i, j, x_{\text{fam}(i,j)}, B) \), Alice applies \( U_j^i \prod \{ P_{i',j'}^{i'}(x_{\text{fam}(i',j')}) \} |\psi⟩^6 \), that is, she looks up the normal-teleportation key corresponding to the values of the variables in \( x_{\text{fam}(i',j')} \) to decrypt each port.

4. Alice normal-teleports each system back to Bob using the entangled pair labelled \( A(i, j, x_{\text{fam}(i,j)}, A) \), receiving a separate key for each port. She labels these keys according to the corresponding port label, \( x_{\text{fam}(i,j)} \). She then has a lookup function \( P_{i,j}(x_{\text{fam}(i,j)}) \) that gives her the appropriate Pauli to be used in subsequent instances of step 3.

5. Bob discards all the systems \( B(i, j, x_{\text{fam}(i,j)}, A) \) not labelled \( x_{\text{fam}(i,j)} \). Repeat from step 2 for all \( j \) from 1 to \( n \), and then for all \( i \) from 1 to \( d \).

6. Communication Round: Bob sends Alice’s \( n/2 \) qubits back to her, and Alice and Bob send all keys to one another.

7. Both players fully decrypt their systems to approximately obtain the state \( U |\psi⟩ \).

\(^4\)This is \( N \) ports since only \( x_j^i \) varies; the label for each ancestor is fixed by the keys of previous port-based teleportations.

\(^5\)For a Pauli string \( P^i \), \( P^i |\psi⟩ \) means the string obtained by keeping only the part of the string supported on \( S_j^i \).

\(^6\)Note that the notation \( P_{i',j'}^{i'}(x_{\text{fam}(i',j')}) \) is defined in step 4; it is not used until the second layer.
In appendix A we show that the diamond norm between the channel $\mathcal{N}$ implemented by this protocol and the desired unitary channel $\mathcal{U}$ is bounded as

$$\|\mathcal{N} - \mathcal{U}\|_\diamond \leq \epsilon,$$

so long as we choose

$$N \geq \left(\frac{4}{\epsilon} \sum_{i,j} 2^{2k_{i,j}}\right)^2.$$

(3)

### 3.2 Entanglement cost

Let us determine the entanglement cost of this protocol, ignoring the $\frac{2}{7}$ term from the initial normal teleportation from Alice to Bob, which is subleading in all regimes of interest. We need $2N$ maximally entangled pairs of $k_{i,j}$-qubit systems for each combination of $i$ and $j$. Thus, our total entanglement cost as measured in Bell pairs is

$$E = 2 \sum_{i,j} k_{i,j} N^{|\text{fam}(i,j)|}.$$

(4)

We emphasize that this depends only on the circuit structure $\{S^j_i\}$ and not any other properties of the unitary.

For simplicity we henceforth assume that $k$ is constant. We also define the maximal past light cone volume as $V := k \max_{i,j} |\text{fam}(i,j)|$. Using $V$ as an upper bound for $|\text{fam}(i,j)|$ and substituting the expression for $N$ in eq. (3) gives

$$E \leq 2nd \left(\frac{4n d^{-1} 2^k}{\epsilon k^2}\right)^{\frac{2V}{k}}.$$

(5)

This is essentially dominated by the scaling

$$E \lesssim O\left(n^{4V}\right),$$

(6)

where we treat $\epsilon$ as a constant and ignore sub-leading dependencies in each variable. Here we have also made use of $V \geq d$ and used $n 2^k \leq n 2^k$ which is always true for large $n$ regardless of how $k$ might scale with $n$. These inequalities only mildly weaken the bound in eq. (6).

Firstly, if the circuit has generic all-to-all interactions with $d$ layers of $k$-local gates, then $V = \sum_{i=1}^d k^i \sim k^d$, and so $E$ is bounded by

$$E \sim O\left(n^{4k^d}\right).$$

(7)

In the case that the circuit has a geometrically local structure in $D$-dimensional Euclidean space, then $V = \alpha kd^{D+1}$ for some constant $\alpha$, and so

$$E \sim O\left(n^{4\alpha kd^{D+1}}\right).$$

(8)

### 3.3 Regime of efficiency

From the expression eqs. (7) and (8), we can make the following conclusions. A unitary $U$ can be computed non-locally with polynomial entanglement if it can be implemented by a circuit with $k \sim O(1)$ and $d \sim O(1)$. Furthermore, it can be computed with quasi-polynomial entanglement if any of the following hold:

1. $k \sim \text{polylog } n, \ d \sim O(1),$
2. $k \sim O(1), \ d \sim \log \log n,$ or
3. $k \sim \text{polylog } n, \ d \sim \text{polylog } n,$ and the circuit has geometrically local structure in $D$ spatial dimensions.

Without geometric locality but with $k \sim \text{polylog } n$ and $d \sim \log \log n$, the entanglement scales as $\exp \exp \log \log n$, which can be thought of as “quasi-quasi-polynomial”, and is still much slower than exponential growth.

Consider the classes described by cases 1 and 3 above. To the authors’ knowledge, there has been essentially no work studying circuits with such “medium” sized gates, and thus new methods are needed to characterize these classes of unitaries. They are both strictly contained in those unitaries implementable by quasi-polynomial depth circuits of $O(1)$-local gates. This follows by appealing to Ref. [24], which shows that a $k$-qubit gate can be decomposed into $4^k$ layers of $2$-qubit gates.

One can also use non-rigorous counting arguments of the sort found in Ref. [25] to characterize the size of such a class. These arguments characterize the “number of unitaries” in a set as the ratio of the volume of the set according to some metric to the volume of a ball of radius $\epsilon$. Including combinatorial factors, one can show that the log-number of distinct circuits$^7$ with $d$ layers of $k$-qubit gates on $n$ total qubits scales roughly as

$$\log |\text{circ}(n, k, d)| \sim nd \left[\log(n) + 4^k\right].$$

(9)

This indicates that, for example, the asymptotic scaling of the log number of unitaries implementable in class 1 above is comparable to that of the unitaries implementable by quasi-polynomial-depth circuits of $2$-qubit gates.

### 3.4 Distinction from other protocols

We will now show that the class of unitaries that our protocol can efficiently implement contains unitaries not

$^7$Note that the number of distinct circuits is larger than the number of distinct unitaries implemented by such a circuit; however for $d$ less than exponential in $n$ these numbers are believed to be similar [25].
achievable by other protocols. As we have already seen, the protocol of Ref. [4] requires entanglement exponential in the number of qubits regardless of the unitary. Thus our protocol outperforms this one for circuits with sufficiently small light cones.

The other protocol for general unitaries that outperforms the one from Ref. [4] in some regimes is that of Ref. [17]. There they provide two protocols whose entanglement cost is determined by Clifford + T circuit decompositions. One protocol scales as $n2^{k_T}$ where $k_T$ is the number of $T$ gates in the circuit. The other scales as $(68n)^{d_T}$ where $d_T$ is the number of circuit layers containing a $T$ gate, i.e. the $T$-depth. We will show that our protocol can efficiently implement a unitary with $k_T$ and $d_T$ polynomial in $n$, a regime where the aforementioned protocols perform poorly.

The simplest example of such a unitary is one that factorizes into unitaries acting on $O(\log n)$ qubits, with each of the smaller unitaries having near-maximal $T$-depth. This is exponential in the number of qubits acted on [24], so $k_T \sim d_T \sim \text{poly}(n)$. If we ran our protocol on the total unitary, treating each smaller unitary as a $k \sim \log n$-qubit gate, then the depth will be 1 and our protocol costs $\sim n^{\log n}$, a quasi-polynomial.
Note however that in this example our protocol does nothing but perform the protocol of Ref. [4] many times in parallel. To obtain a less trivial example, add a second layer of log $n$ sized gates which act across the supports of the original small unitaries. Choosing the gates of the second layer to have $O(1)$ T-count, we can be assured that the total unitary remains in the inefficient regime of the protocols in [17]. For this new unitary our protocol still requires only a quasi-polynomial amount of entanglement.

4 Enhancements

There are several complementary actions Alice and Bob can take in order to re-express the unitary they perform in a less costly manner. Firstly, they can apply local operations on their systems before and after the protocol. Secondly, they can apply arbitrary Cliffords at the beginning and end of the circuit. Finally, they can add auxiliary systems. We show how each of these is done, and give examples where the latter is useful.

4.1 Local pre/post-processing

Let Alice and Bob re-express $U$ as $(W'_A \otimes W'_B)U_{AB}(W_A \otimes W_B)$ for some $n/2$-qubit unitaries $W_A, W_B, W'_A,$ and $W'_B$ and $n$-qubit unitary $U_{AB}$. They act with $W_A$ and $W_B$ on the systems they respectively hold at the beginning of the protocol, and with $W'_A$ and $W'_B$ at the end of it. By running the protocol on $U_{AB}$ they then obtain the same result as though they had run it on $U$ without pre/post-processing. Crucially, the entanglement cost will depend on the circuit structure of $U_{AB}$, which may be more conducive to our protocol than that of $U$.

4.2 Clifford sandwich

Suppose that $U$ has a circuit decomposition $C_f U' C_i$ with $C_i, C_f$ being $n$-qubit Cliffords and $U'$ an $n$-qubit unitary that has a circuit decomposition with structure $\{S_i^{f}\}$. Then we can construct an NLQC protocol that accomplishes $U$ with the same cost as our original protocol takes to accomplish any unitary via a circuit structure $\{S_i^{f}\}$. To do so we run the protocol as though to implement $U'$ via this circuit structure, but modified as follows.

Between steps 2 and 3, i.e. right after Alice has teleported her $\frac{n}{2}$ qubits to Bob, Bob applies the Clifford $C_i$ to his combined system. This means he now holds the state $QC_i |\psi\rangle$ where $Q = C_i PC_i^\dagger$. Note that $Q$ is a Pauli, and that Alice knows its identity since she knows both $C_i$ and $P$. If Alice and Bob then run the remainder of the original protocol but replacing $P$ with $Q$, they will have implemented $U' C_i$.

To additionally implement $C_f$, the following modification is added right before step 6, the communication round. At this point Bob holds the state

$$P(x^*)U'_C |\psi\rangle_{AB},$$

where $P$ is a Pauli valued function of $x^*$, all indices of the port teleportations Bob has performed throughout the protocol. Alice posses knowledge of $P$ but not $x^*$, and vice versa for Bob. Nonetheless, Bob can apply $C_f$ to the state, and the communication round can commence as in the original protocol. They then both possess knowledge of $P(x^*)$, and can jointly apply $C_f P(x^*)C_f^\dagger$, since this is a Pauli and thus factorizes between the $A$ and $B$ systems. This completes the protocol.

Local pre/post-processing can straightforwardly be performed before and after the Clifford gates.

4.3 Auxiliary systems

Alice and Bob can make use of Auxiliary systems by generalizing the pre/post-processing step to make use of isometries rather than unitaries. More precisely, suppose $U$ can be written as

$$U = (W_{A\rightarrow\tilde{A}} \otimes W_{B\rightarrow\tilde{B}})U_{\tilde{A}\tilde{B}}(V_{A\rightarrow\tilde{A}} \otimes V_{B\rightarrow\tilde{B}})$$

(11)

where $V_{A\rightarrow\tilde{A}}$ and $V_{B\rightarrow\tilde{B}}$ are isometries, $W_{A\rightarrow\tilde{A}}$ and $W_{B\rightarrow\tilde{B}}$ are channels, and $U_{\tilde{A}\tilde{B}}$ is a unitary. Then the isometries and channels can be absorbed into local pre- and post-processing, and the NLQC protocol performed on $\tilde{U}$. The entanglement cost will depend only on the circuit structure needed to implement $U_{\tilde{A}\tilde{B}}$. Provided the number of auxiliary systems added is polynomial in $n$, and $d$ and $k$ are unchanged, the regime of efficiency will remain the same.

When would using auxiliary systems be useful? We will consider two examples: locality-preserving unitaries, and the embedding of the protocol in Ref. [19].

It is well known that locality-preserving unitaries do not always admit a circuit decomposition that reflects their causal structure [26]. For example, the unitary that shifts all $n$ qubits in a closed 1-d chain by one site in the same direction requires a circuit whose depth grows proportionally to the number of qubits. However, using the techniques of Ref. [26], $n$ auxiliary qubits can be introduced in the manner of eq. (11) to implement this unitary with a circuit of depth 2 and gate size 2, which our protocol can do efficiently. More generally these techniques can be used to decompose any locality-preserving unitary.

As a second example, we will consider the protocol introduced in [19] for the task of $f$--routing, a subclass
of NLQC in which Alice receives a qubit and a classical string $x$, Bob receives a classical string $y$, and their task is to return the qubit to Alice or Bob depending on the value of a Boolean function $f(x,y)$, subject to the same constraints as general NLQC. Their protocol can be written in the form of eq. (11) having $O(1)$ depth and $O(1)$-sized gates, and thus can be embedded into our protocol while still performed efficiently. In their protocol, auxiliary systems are introduced when Alice’s input qubit is encoded into a secret sharing scheme. Each of these is routed to Alice or Bob depending on the value of another Boolean function that depends only on an $O(1)$ subset of the classical bits in $x$ and $y$, and so can be implemented as an $O(1)$-sized gate. These gates can be parallelized by making as many copies of $x$ and $y$ in the pre-processing stage as needed for the cases when the routing of several different shares depends on the same bits. In particular, only a polynomial number of additional copies are needed because the construction of Ref. [19] requires that the number of gates be polynomial in $n$.

Future work is needed to better understand the classes of efficiently computable unitaries described in section 3.3, and how they relate to more familiar complexity classes of unitaries. In particular, it remains to be found which, if any, polynomial-depth circuits of two-qubit gates are outside the regime of efficiency of our protocol when accounting for the extensions of section 4. Finally, it may be possible to find a better method to deal with the issue of the port dependence of Pauli keys, as this is the greatest bottleneck of our protocol.

### Acknowledgement

We thank Alex May for suggesting the approach of exploiting a unitary’s decomposition into a circuit of medium-sized gates to make more efficient use of port teleportation. We also thank Nick Hunter-Jones, Adam Brown and Adam Bouland for useful discussions. SC is supported by a graduate fellowship award from Knight-Hennessy Scholars at Stanford University.

### A Protocol error bounds

Let $\mathcal{N}$ be the channel applied to an input state of the protocol in 3 for a unitary $U$ decomposed into $\{U_i\}$ with circuit structure $\{S_i\}$, with gate size $|S_i|=k_{i,j}$. Let $U:=U \cdot U^\dagger$. We would like to determine an upper bound on $||\mathcal{N} - U||_\diamond$.

First we need to write down the explicit form of $\mathcal{N}$. To do so define the following quantities

- $\mathcal{E}_j$ is the error channel defined by port-teleporting $S_i^j$ using $N$ maximally entangled $k_{i,j}$ qubit states, and keeping the correct port.
- $\mathcal{E}_i \defeq \mathcal{E}_1 \cdots \mathcal{E}_n$
- $\mathcal{U}_i \defeq U^i \cdot U^{\dagger}$ where $U^i = U_1 \cdots U_n$. Thus $\mathcal{U} = \mathcal{U}_d \cdots \mathcal{U}_i$.
- $\mathcal{P}_i \defeq P^i \cdot P^{\dagger}$ where $P^i = \prod_{(i',j') \in \text{par}(i,j)} P_{i',j'}(x_{\text{par}(i',j')}^{*}) |S_i^j \rangle \langle S_i^j|$ for $i \geq 1$ and $P^0 = P$.
- $\mathcal{E}_i' = \mathcal{P}_{i-1} \mathcal{E}_i \mathcal{P}_{i-1}$

Then we can write $\mathcal{N}$ as

$\mathcal{N} = \mathcal{U}_d \mathcal{E}_d \cdots \mathcal{U}_1 \mathcal{E}_1'$.

We will need to make use of the following properties of the diamond norm (see section 3.3 of Watrous’ book where it is referred to as the "completely bounded trace norm").
Let $\Phi_0, \Phi_1, \Psi_0, \Psi_1$ be CPTP maps from $\mathcal{B}(A)$ to $\mathcal{B}(A)$ for some quantum system $A$. Then
\begin{align}
||\Psi_1 \Psi_0 - \Phi_1 \Phi_0||_\diamond & \leq ||\Psi_0 - \Phi_0||_\diamond + ||\Psi_1 - \Phi_1||_\diamond \tag{12} \\
||\Phi_0||_\diamond & = 1 \tag{13}
\end{align}

If $\Phi_0$ and $\Phi_1$ are instead general linear maps then we have
\begin{align}
||\Phi_0 \otimes \Phi_1||_\diamond & = ||\Phi_0||_\diamond ||\Phi_1||_\diamond \tag{14}
\end{align}

We can use equation 12 to get
\begin{align}
||N - U||_\diamond & \leq \sum_{i=1}^d ||U_i \mathcal{E}_i' - U_i||_\diamond \\
& \leq \sum_{i=1}^d ||\mathcal{E}_i' - \mathcal{I}_{C^{2^n}}||_\diamond \\
& \leq \sum_{i=1}^d ||P_{i-1}^\dagger \mathcal{E}_i P_{i-1} - P_{i-1}^\dagger P_{i-1}||_\diamond \\
& \leq \sum_{i=1}^d ||P_{i-1}^\dagger \mathcal{E}_i - P_{i-1}^\dagger||_\diamond \\
& \leq \sum_{i=1}^d ||\mathcal{E}_i - \mathcal{I}_{C^{2^n}}||_\diamond \\
& \leq d||\mathcal{E}_i - \mathcal{I}_{C^{2^n}}||_\diamond
\end{align}

where in the last line we used that the argument of the sum does not depend on $i$. Writing $\mathcal{E}_i := \mathcal{E}_i^1 \cdots \mathcal{E}_i^n$, and again using equation 12 we get
\begin{align}
||N - U||_\diamond & \leq \sum_{i,j} ||\mathcal{E}_j^i - \mathcal{I}_{C^{2^n}}||_\diamond.
\end{align}

Finally, use the fact that $\mathcal{E}_j^i = \mathcal{E}_j^i |S_j^i \otimes \mathcal{I}_{C^{2^n-k_{i,j}}} \text{ and equations 14, and 13 to get}$
\begin{align}
||N - U||_\diamond & \leq \sum_{i,j} ||\mathcal{E}_j^i |S_j^i - \mathcal{I}_{C^{2^n-k_{i,j}}}||_\diamond.
\end{align}

From [4] we have that
\begin{align}
||\mathcal{E}_j^i |S_j^i - \mathcal{I}_{C^{2^n}}||_\diamond & \leq \frac{2^{2k}}{\sqrt{N}}.
\end{align}

Thus the bound we desire is
\begin{align}
||N - U||_\diamond & \leq 4 \sum_{i,j} \frac{2^{2k_{i,j}}}{\sqrt{N}}.
\end{align}

If we want the norm to be less than $\epsilon$, then we can choose
\begin{align}
\mathcal{N} = \frac{16}{\epsilon^2} \left( \sum_{i,j} 2^{2k_{i,j}} \right)^2.
\end{align}

References

[1] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. Physical Review A, 84(1):012326, 2011.

[2] Robert A. Malaney. Location-dependent communications using quantum entanglement. Physical Review A, 81(4), Apr 2010. ISSN 1094-1622. DOI: 10.1103/physreva.81.042319. URL http://dx.doi.org/10.1103/PhysRevA.81.042319.

[3] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. SIAM Journal on Computing, 43(1):150–178, Jan 2014. ISSN 1095-7111. DOI: 10.1137/130913687. URL http://dx.doi.org/10.1137/130913687.

[4] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. New Journal of Physics, 13(9):093036, Sep 2011. ISSN 1367-2630. DOI: 10.1088/1367-2630/13/9/093036. URL http://dx.doi.org/10.1088/1367-2630/13/9/093036.

[5] Adrian Kent. Quantum tagging for tags containing secret classical data. Physical Review A, 84(2), Aug 2011. ISSN 1094-1622. DOI: 10.1103/physreva.84.022335. URL http://dx.doi.org/10.1103/PhysRevA.84.022335.

[6] Gilles Brassard. Quantum information: The co-nundrum of secure positioning. Nature, 479(7373):307–308, November 2011. DOI: 10.1038/479307a.

[7] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. Physical Review A, 91(4), Apr 2015. ISSN 1094-1622. DOI: 10.1103/physreva.91.042337. URL http://dx.doi.org/10.1103/PhysRevA.91.042337.

[8] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. Physical Review A, 92(5), Nov 2015. ISSN 1094-1622. DOI: 10.1103/physreva.92.052304. URL http://dx.doi.org/10.1103/PhysRevA.92.052304.

[9] Marius Junge, Aleksander M Kubicki, Carlos Palazuelos, and David Pérez-García. Geometry of banach spaces: a new route towards position based cryptography. 2021. URL https://arxiv.org/abs/2103.16357.

[10] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating classical impossibility of position verification. 2021. URL https://arxiv.org/abs/2109.07517.

[11] Rene Allerstorfer, Harry Buhrman, Florian Spel-
man, and Philip Verduyn Lunel. New protocols and ideas for practical quantum position verification. 2021. URL https://arxiv.org/abs/2106.12911.

[12] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. Physical Review A, 83(1), Jan 2011. ISSN 1094-1622. DOI: 10.1103/physreva.83.012322. URL http://dx.doi.org/10.1103/PhysRevA.83.012322.

[13] Adrian P Kent, William J Munro, Timothy P Spiller, and Raymond G Beausoleil. Tagging systems, July 11 2006. US Patent 7,075,438.

[14] Alex May. Quantum tasks in holography. 2019. URL https://arxiv.org/abs/1902.06845.

[15] Alex May, Geoff Penington, and Jonathan Sorce. Holographic scattering requires a connected entanglement wedge. Journal of High Energy Physics, 2020(8), Aug 2020. DOI: 10.1007/jhep08(2020)132. URL http://dx.doi.org/10.1007/JHEP08(2020)132.

[16] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. New Journal of Physics, 15(10):103002, Oct 2013. DOI: 10.1088/1367-2630/15/10/103002. URL https://doi.org/10.1088%2F1367-2630%2F15%2F10%2F103002.

[17] Florian Speelman. Instantaneous non-local computation of low t-depth quantum circuits. In Anne Broadbent, editor, 11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016), volume 61 of Leibniz International Proceedings in Informatics (LIPIcs), pages 9:1–9:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, September 2016. DOI: 10.4230/LIPIcs.TQC.2016.9.

[18] Andreas Bluhm, Matthias Christandl, and Florian Speelman. Position-based cryptography: Single-qubit protocol secure against multi-qubit attacks, 2021. URL https://arxiv.org/abs/2104.06301.

[19] S. Cree and A. May. Code-routing: a new attack on position-verification. 2022. URL https://arxiv.org/abs/2202.07812.

[20] A. May. Complexity and entanglement in non-local computation and holography. 2022. URL https://arxiv.org/abs/2204.00908.

[21] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. Phys. Rev. Lett., 101:240501, Dec 2008. DOI: 10.1103/PhysRevLett.101.240501. URL https://link.aps.org/doi/10.1103/PhysRevLett.101.240501.