
DOI

https://doi.org/10.1103/PhysRevLett.114.220502

Link to record in KAR

http://kar.kent.ac.uk/58146/

Document Version

Author's Accepted Manuscript

Copyright & reuse
Content in the Kent Academic Repository is made available for research purposes. Unless otherwise stated all content is protected by copyright and in the absence of an open licence (eg Creative Commons), permissions for further reuse of content should be sought from the publisher, author or other copyright holder.

Versions of research
The version in the Kent Academic Repository may differ from the final published version. Users are advised to check http://kar.kent.ac.uk for the status of the paper. Users should always cite the published version of record.

Enquiries
For any further enquiries regarding the licence status of this document, please contact: researchsupport@kent.ac.uk

If you believe this document infringes copyright then please contact the KAR admin team with the take-down information provided at http://kar.kent.ac.uk/contact.html
Iterated gate-teleportation and blind quantum computation

Carlos A. Pér ez-Delgado\textsuperscript{1} and Joseph F. Fitzsimons\textsuperscript{1,2,∗}

\textsuperscript{1}Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682
\textsuperscript{2}Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543

Blind quantum computation (BQC) allows a user to delegate a computation to an untrusted server while keeping the computation hidden. A number of recent works have sought to establish bounds on the communication requirements necessary to implement blind computation, and a bound based on the no-programming theorem of Nielsen and Chuang has emerged as a natural limiting factor. Here we show that this constraint only holds in limited scenarios, and show how to overcome it using a novel method of iterated gate-teleportations. This technique enables drastic reductions in the communication required for distributed quantum protocols, extending beyond the blind computation setting. Applied to BQC, this technique offers significant efficiency improvements, and in some scenarios offers an exponential reduction in communication requirements.

Blind quantum computation is a cryptographic task whereby a client seeks to hide a delegated computation from the server implementing the computation. A number of protocols for blind computation have been discovered \cite{1–11}, and a range of capabilities for the client have also been considered, from the ability to prepare or measure individual single qubit states \cite{1, 5, 6}, to the ability to perform universal computation on fixed size systems \cite{2}. Recently work has sought to unify this disparate family of protocols in terms of security definitions \cite{12} and in terms of resource accounting \cite{9, 11}.

Recently, Giovannetti et al. proposed a novel cheat-sensitive protocol for blind quantum computation \cite{11}. They also derived a lower bound on communication, and showed their protocol to be optimal with respect to it. Their bound—based on the no-programming theorem of Nielsen and Chuang \cite{13}—argues that $\Omega(S \log_2 G)$ qubits must be exchanged between client and server, where $S$ is the total number of gates performed, and $G$ is the cardinality of the gate set. It is tempting to conjecture that the no-programming bound applies to any approach to blind quantum computation \cite{16}. In this paper, however, we show that such an efficiency constraint can be overcome even if the client is only allowed to prepare arbitrary single qubit states. The protocols we construct are not only more efficient than previous blind computation protocols, but require less communication than is required to classically describe the delegated computation.

We introduce three protocols in this Letter. The purpose of the first protocol is to introduce our technique of iterated gate-teleportation. This is based on the usual gate teleportation \cite{14}, but differs from standard usages in that instead of directly correcting errors induced by teleportation byproducts, we make use of additional gate teleportation steps to correct the state of the system. This change, by itself, would not normally provide any drastic speedups. However, we show that there are certain universal gate-sets that allow for guaranteed correction in very few (constant) number of gate teleportations. This technique provides a general means of increasing the efficiency of delegated computation, independent of whether it is a stand-alone computation or forms part of some cryptographic protocol. We then leverage this new technique for efficiently delegating computation to improve the efficiency of BQC. In Prot. 2 we give a blind version of iterated gate-teleportation, and in Prot. 3, we build a complete universal BQC protocol that, using Prot. 2 as a building block, achieves a significant saving in the total communication cost, allowing our protocol to avoid the lower bound on communication of $S \log_2 G$ which results from a naive application of the no-programming theorem.

Consider the set $\mathcal{D}_{m,l}$ of all diagonal operators acting on $m$ qubits of the form $\exp(i \sum_{j=0}^{l-1} \theta_{ij} Z^{j} \otimes Z^{j} \otimes \ldots \otimes Z^{j})$, with $\theta_{ij} \in \{\frac{\pi}{2} | r \in \{0, 1, 2, 3, \ldots, 2^l - 1\}\}$. Our approach allows Alice to successfully teleport any given operator $D \in \mathcal{D}_{m,l}$ to Bob in at most $l$ steps, each involving the transmis- sion of $m$ qubits. This gives a total cost of $O(ml)$. Compare this to any setting where the no-programming theorem applies, which sets a minimum of $\Omega(l 2^m)$ qubits to be transmitted.

We will assume that Bob’s system contains two registers $R$ and $R'$. The multi-qubit gate teleportation circuit we use is depicted in Fig. 1. This procedure is formalised in Prot. 1. Note that at the end of Prot. 1, Bob is in possession of the desired output state, up to a series of Pauli-X corrections, which he can perform himself—in this non-blind version. Before discussing a blind version of Prot. 1 we show that this protocol, if followed by both Alice and Bob, does indeed yield the correct output \cite{17}.

We will begin by examining the effect of an iteration of the main loop (Steps 2a through 2d) on an arbitrary input state $|\psi\rangle$ in register $R$. Each iteration serves to implement a gate teleportation so that an input state $|\psi\rangle$ is transformed.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{figure1.png}
\caption{Gate teleportation procedure. The top set of wires corresponds to register $R$, while the bottom set correspond to $R'$.}
\end{figure}
Protocol 1: Iterated Gate-Teleportation

Alice’s input: Gate $D \in \mathcal{D}_m$ to be teleported.

Bob’s input: Initial state $|\psi\rangle$, in register $R$.

Output: The state $\mathcal{X}D|\psi\rangle$ in Bob’s register $R$, where $\mathcal{X}$ is a tensor product of the Pauli-X operator and the identity, known both to Bob and Alice.

Steps:
1. Set $D_1 = D$.
2. For $1 \leq \ell \leq l$
   
   (a) Alice prepares the state $D_\ell |+\rangle^{\otimes m}$, and sends it to Bob, who stores it in register $R'$.
   
   (b) Bob applies the teleportation procedure depicted in Fig. 1 obtaining measurement results $s^{(\ell)}_1, \ldots, s^{(\ell)}_m$. He sends the measurement results to Alice.
   
   (c) Bob swaps the contents of register $R$ and $R'$.
   
3. Set $\mathcal{X} = (\prod_{\ell=1}^l \mathcal{X}_\ell)$. Bob now has the desired state $\mathcal{X}D|\psi\rangle$ in register $R$.

$$|\psi_1\rangle = D_1 \mathcal{X}_1 |\psi\rangle,$$

where the product operator is used to denote that the left to right ordering is from highest to lowest value of $\ell$. Note that if an operator $D \in \mathcal{D}_m$ then $(\bigotimes_{k=1}^n \mathcal{X}_k)D (\bigotimes_{k=1}^n \mathcal{X}_k)D^\dagger \in \mathcal{D}_{m, l-1}$ for any choice of variables $a_k \in \{0, 1\}$. Thus, for any $\ell$, we have $D_\ell \in \mathcal{D}_{m, l-1}$. Since $\mathcal{D}_m$ corresponds to the set of tensor products of $Z$ and the identity, $D_\ell \mathcal{X}_\ell = \pm \mathcal{X}_\ell D_\ell$. Thus, up to a global phase, we have

$$|\psi_{\ell+1}\rangle = \mathcal{X}_\ell D_\ell \left( \prod_{l=1}^{\ell-1} D_l \mathcal{X}_l \right) |\psi_{\ell}\rangle,$$

which collapses telescopically, substituting in the definition of $D_l$, to yield

$$|\psi_{\ell}\rangle = \left( \prod_{l=1}^{\ell} \mathcal{X}_l \right) D_1 |\psi_1\rangle.$$

Setting $\mathcal{X} = (\prod_{\ell=1}^l \mathcal{X}_\ell)$ completes the proof. Note that, at this stage, Bob can correct his state by applying Pauli-X to his qubits as appropriate, without knowing the teleported gate, and without any further assistance or communication from Alice.

It is worth noting here that the set $\mathcal{D}_m$ was chosen precisely so that it exhibits the behaviour shown above. If one attempted to use the iterated gate-teleportation approach naively on an arbitrary gate set, one would have to repeat the teleportation process until the current gate teleportation succeeds. For a gate acting on $n$ qubits, this success probability is $2^{-n}$, giving an expected communication cost of $\Omega(2^n)$. Using the gate set $\mathcal{D}_m$, however, guarantees the correct gate to be teleported in at most $O(1)$ steps, independent of $n$. Setting $l = 3$ will include the $\pi/8$-gate in the set $\mathcal{D}_m$, making the set, along with Hadamard and CZ operators applied by Bob, universal for quantum computation, as well as making the iterated gate-teleportation succeed in $O(1)$ steps.

Next we present a blind version of Prot. 1. This procedure allows for the same functionality as the previous protocol, enabling Alice and Bob to perform gate teleportation of a gate encoded by Alice, while additionally ensuring that the gate remains unknown to Bob. The procedure for accomplishing this is presented in Prot. 2.

The proof of correctness of Prot. 2 is similar to that of Prot. 1. The only difference is that now each iteration adds a series of random Pauli-Z operators. With each iteration an input state $|\psi\rangle$ is transformed to $|\psi_{\ell+1}\rangle = Z_{\ell} |\psi_{\ell}\rangle$, where

$$|\psi_{\ell}\rangle = \left( \prod_{\ell=1}^{l-1} Z_{l-1} D_l \mathcal{X}_l \right) |\psi_1\rangle,$$

where, again, the product operator is used to denote that the left to right ordering is from highest to lowest value of $\ell$. As before, we use the property of $\mathcal{D}_m$, and the definition of $D_\ell$ to telescopically collapse the last equation to

$$|\psi_{\ell}\rangle = Z_{l} \left( \prod_{\ell=1}^{l} \mathcal{X}_\ell \right) D_1 |\psi_1\rangle.$$
information obtained by Bob after running $P$ depends only on $L(X)$ [18]. Accordingly, Prot. 2 is blind while leaking at most $(l, m)$. The only information transmitted from Alice to Bob are the set of quantum states $|\phi_i\rangle = Z_i Z_{i-1} D_i |0\rangle^\otimes m$. Note that only $|\phi_k\rangle$ is a function of $r_k^{(l)}$ for $1 \leq k \leq m$, and that as these values are unknown to Bob, this state is necessarily the maximally mixed state of $m$ qubits, and hence independent of the values of all other $r_k^{(l)}$ when $l \neq l$. Hence $|\phi_{l-1}\rangle$ is the only quantum state dependent on $r_k^{(l-1)}$ for $1 \leq k \leq m$, and must similarly be in a maximally mixed state. We can apply this argument recursively, implying that every state sent from Alice to Bob is in the maximally mixed state due to the unknown values of $\{r_k^{(l)} | 1 \leq k \leq m, 1 \leq l \leq l\}$, which serve as Alice’s key. As the joint state of all these messages are fixed to the maximally mixed state and hence independent of the computation, the only parameters leaked to Bob are $l$ and $m$.

We are now in a position to present a complete protocol for universal blind quantum computation. This is presented as a family of protocols which are parameterised by an integer $n$, corresponding to the size of the client’s system. During intermediate steps Alice will instruct Bob to perform $m$-qubit gates via gate-teleportation, using Prot. 2. The purpose of studying protocols with varying parameter $m$ is the following. When $m$ is small, we obtain a protocol with modest resource requirements on Alice while still outperforming previous protocols. On the other hand, when $m$ is proportional to the number of qubits used in the computation, $n$, the protocol achieves an exponential (in $n$) separation in total communication from the naive limit implied by the no-programming theorem.

The protocol proceeds in phases. During the $j$th teleportation phase, Alice will use gate teleportation to send the desired gates to Bob. Without loss of generality we assume that $m$ divides $n$ [19], such that $n = Pm$, for some integer $P$. Then for each contiguous set of $m$ qubits Alice will teleport an operator $D_{j,p}$, to Bob, for $1 \leq p \leq P$, who will then apply it to the qubits labelled $(p - 1)m + 1$ through $pm$ of his current state in memory. Thus, if at the beginning of the $j$th phase Bob’s register is in the state $|\psi_j\rangle$, by the end of the phase it will be in state $D_j |\psi_j\rangle$, where $D_j = \otimes_{p=1}^P D_{j,p}$.

As the set of gates which may be implemented by gate teleportation do not form a universal gate set, the scheme we present here leverages fixed gates implemented by Bob to bring about universality in a completely blind manner, as follows. Interspersed with the operations that Alice teleports, Bob will also apply the operation $CZ = \prod_{i=0}^{n-1} CZ(i, i+1)$, where $CZ(i, i+1)$ is the controlled-Z operator acting on qubits $i$ and $i+1$; as well as the operator $H^\otimes n$, where $H$ is the usual Hadamard operator. The order of phases of the protocol is as follows. The first step consists of controlled-Z operators, followed by a Hadamard step, then a teleportation phase, then another Hadamard phase, followed by a second teleportation phase. Then, the pattern repeats itself until $J$ teleportation phases have been achieved. To simplify the analysis, and without loss of generality, we assume $J$ is even. This set of operations forms a universal set of gates for quantum computation for any $m$, and any $x \geq 2$ (see for example [15]). See Fig. 2 for a schematic diagram and Prot. 3 for formal presentation of the protocol.

The correct operation of the protocol depends on the proper definition of the function $f_j$ used in Step 3c. This function is

**Protocol 3 General Iterated Teleportation Blind Quantum Computation**

1. Alice chooses a depth $J$ and a set of diagonal operations $D_j = \otimes_{p=1}^P D_{j,p}$, where $P = n/m$, and $n$ is the number of qubits used in the computation, such that her target computation is given by the measurement of $HD_j RD_{j-1} R H\ldots CZD_2 RD_1 |+\rangle^\otimes m$ in the computational basis.
2. Alice produces the state $Z_i D_i |+\rangle^\otimes m$, where $Z_i = \otimes_{k=1}^m Z^{(i)}_k$, where each $Z^{(1)}_k$ is chosen uniformly at random from the set $\{0, 1\}$, and transmits $J$ and this state to Bob, who stores the quantum state in register $R$.
3. For $2 \leq j \leq J$
   a. If $j \equiv 1 \pmod{2}$, then Bob applies $CZ$ to register $R$.
   b. Bob applies $H$ to register $R$.
   c. For $1 \leq p \leq P$
      i. Alice calculates the operators $f_j(p)(D_{j,p})$, where the function $f_j(p)$ is defined in the main text in Eq. 11.
      ii. Alice and Bob engage in Prot. 2 using $f_j(p)(D_{j,p})$ as Alice’s target gate, and Bob’s qubits $(p - 1)m$ through $pm$ as the target register.
      iii. Alice keeps a record of the operator $X_{j,p}$, the teleportation byproduct resulting from Prot. 2, and $Z_{j,p}$, her encryption key.
   d. Alice calculates the operators
      \[
      X_j = \bigotimes_p X_{j,p}, \quad Z_j = \bigotimes_p Z_{j,p},
      \]  
      and keeps a record of them.
4. Finally, Bob measures his resulting state in the $X$ basis, and sends the measurement outcomes $m_1\ldots m_n$ to Alice. Alice computes each output bit for the computation as $o_k = m_k \oplus r_k^{(1)}$, where $Z_j = \otimes_k Z^{(1)}_k$. 

**Fig. 2** Blind Quantum Computation with Teleportation Protocol. The dotted-line square shows the repeating pattern of operations.
meant to correct and remove the X errors and the Z obfuscation operators introduced in previous steps. Before giving a general definition of $f_j$, let’s first consider a simplified version of the protocol where $m = n$ and the phases of controlled-Z operators have been subsumed into the diagonal operator teleportation phases. Hence, the protocol simplifies into a series of teleportated gate phases followed by a layer of Hadamard gates. The output of the protocol is then given by

$$|\psi_o\rangle = \prod_{j=1}^{J} \left( Z_j X_j f_j(D_j) \Pi \right) |0\rangle^\otimes n,$$

where the product operator is used to denote that the left to right ordering is from highest to lowest value of $j$.

Because there is a layer of Hadamard gates in between every teleportation stage, the Z operator byproducts are turned into X operators, and vice versa, before the the next teleportation. Since Alice can only implement diagonal gates using $X$ and $Z$ gates only, the propagation of error teleportation stage, the product operator is used to denote that the left to right ordering is from highest to lowest value of $j$.

For even $j$ we take $X_j = z_j^{-1}x_j$ and $Z_j = z_j^{n-1}z_j^{n-1}$. Any scheme to which the no-programming theorem applies, such as that in [11], would require that at least $Jk(2^n-1)$ qubits be communicated, and hence the protocol presented here is exponentially more efficient than previous schemes.

However, setting $m$ equal to $n$ requires Alice to prepare large entangled states, which may be undesirable in realistic settings. Our main interest in considering such a setting is to highlight the inapplicability of lower bounds based on the no-programming theorem. On the other hand, setting $m$ to a small constant, gives a protocol that is at least as easily implementable as previous ones in terms of resources needed on Alice’s side, while still being universal for quantum computation, and offering a communication advantage. In the intermediate case where $m$ is of order $n^\alpha$ for $\alpha < 1$ the protocol obtained yields an exponential increase over previous schemes in terms of the rate at which gates can be encoded, while retaining the property that Alice’s device is insufficient to perform the desired computation alone.

The correctness of the general protocol follows from a similar argument to that of the special case previously considered. The output of the general protocol is given by

$$|\psi_o\rangle = \prod_{j=1}^{J} \left( Z_j X_j f_j(D_j) \Pi \right) |0\rangle^\otimes n,$$

where the product operator is used to denote that the left to right ordering is from highest to lowest value of $j$. Substituting Eq. 11 into Eq. 12, with some elementary algebra, gives

$$|\psi_o\rangle = Z_j X_j \prod_{j=1}^{J} (D_j \Pi) |0\rangle^\otimes n,$$

as required. Furthermore, it follows directly from the blindness of Prot. 2 that Prot. 3 is blind while leaking at most $(J, l, m, n)$.

Setting the parameter $m$ equal to $n$, the above protocol requires that Alice transmit exactly $Jx$ different $n$ qubit states to Bob, and hence requires only a total of $nJx$ qubits to be sent from Alice to Bob, and $nJx$ classical bits to be sent from Bob to Alice. However, this protocol implements $J$ unknown operations, each of which can be drawn arbitrarily from the set $\mathcal{D}_k$ which has cardinality $(2^k-1)$. Any scheme to which the no-programming theorem applies, such as that in [11], would require that at least $Jk(2^n-1)$ qubits or bits be communicated, and hence the protocol presented here is exponentially more efficient than previous schemes.
* Electronic address: joseph_fitzsimons@sutd.edu.sg


[16] A slightly weaker bound of $G/d_B$ can be shown for any protocol where the client is restricted to preparing or measuring qudits of dimension $d$ in one of $B$ bases, by counting the number of possible branches of the protocol.

[17] A minor modification of Prot. 1 involves Alice and Bob halting the protocol as soon as Bob measures all zeroes. In this case, no further corrections are necessary, and the protocol can conclude with the correct output state. In the case where $2^m < l$ this leads to an average-case communication cost which is independent of $l$.

[18] This definition of blindness is also compatible with the requirements for composable security in the abstract cryptography framework [12].

[19] This may always be done, since Alice can pad her input with unused ancilla qubits.