Overcoming efficiency constraints on blind quantum computation

Carlos A. Pérez-Delgado and Joseph F. Fitzsimons

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

Blind quantum computation 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 hold in limited scenarios and show how to overcome it using a method based on iterated gate-teleportations. We present our results as a family of protocols, with varying degrees of computational-ability requirements on the client. Certain protocols in this family exponentially outperform previously known schemes in terms of total communication. The approach presented here can be adapted to other distributed computing protocols to reduce 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 exhibiting either information theoretic security [1–10], for which it can be proven that a cheating server cannot learn anything about the computation being performed based on purely information theoretic grounds, or cheat-sensitivity [11], whereby a cheating server can be detected even though the computation cannot be kept hidden from it. A range of capabilities for the client have also been considered, from the ability to prepare or measure individual single qubit states [11], to the ability to perform universal computation on fixed size systems [2]. Recently work has sought to unify this disparate family of protocols in terms of security definitions [12] and in terms of resource accounting [9,11].

Recently, Giovannetti, Maccone, Morimae and Rudolph proposed a novel cheat-sensitive protocol for blind quantum computation, for which the total communication required scales optimally for their specific setting [11]. However, their optimality argument applies only to the case where the client is restricted to preparing and performing projective measurements on single qubits in two bases. In this case, they argued—based on the no-programming theorem of Nielsen and Chuang [13]—that \( \Omega(J \log_G G) \) qubits must be exchanged between client and server, where \( J \) is the total number of gates performed, and \( G \) is the cardinality of the gate set. A slightly weaker bound than that provided by the no-programming theorem 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: the client’s actions amount to a series of \( s \) preparations and measurements, since any classical communication can also be viewed in this way. As the client has no memory, preparations correspond to the transmission of a qudit to the server, and measurements correspond to the transmission of a qudit from the server. As such, \( s \) qudits in total are exchanged. In order for the client’s actions to determine which of \( N_C \) possible computations is performed, it is necessary to have \( s \geq \log_{Bd} N_C \) by the pigeon-hole principle. Hence, in this setting, blind computation of a circuit of depth \( J \) consisting of gates independently chosen from a set of cardinality \( G \) requires an exchange of at least \( J \log_G G \) qubits. While for any fixed choice of \( d \) and \( B \) this approach yields a bound similar to the no-programming theorem, it is more widely applicable. As such, it is tempting to conjecture that the no-programming bound of \( \Omega(J \log_G G) \) on the number of bits/qubits exchanged applies to any approach to blind quantum computation. In this paper, however, we show that such an efficiency constraint can be overcome if the client is allowed to prepare arbitrary single or multi-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.

Before presenting the main protocol, we first present a precursor protocol which forms the main building block of our final protocol. Our approach is based on gate teleportation [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 avoids the need to provide a classical description of the correction operator, leading to a saving in the total communication cost of the protocol, in turn allowing our protocol to avoid the lower bound on communication of \( J \log_G G \) 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 \( \exp(i \sum_{j \in \{0,1\}^l} \theta_j Z^j) \otimes Z^1 \otimes Z^2 \otimes \cdots \otimes Z^m \), with \( \theta_j \in \{2\pi r / 2^l | r \in \{0,1,2,3,\ldots,2^l - 1\}\} \). Our approach al-

![FIG. 1: Gate teleportation procedure. The top set of wires corresponds to register \( R \), while the bottom set correspond to \( R' \).](image-url)
up to a global phase, we have
\[ D \text{ if an operator} \]

allows Alice to successfully teleport any given operator \( D \in \mathcal{D}_{m,l} \) to Bob in at most \( l \) steps, each involving the transmission 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 \( \Omega(l2^m) \) 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 \( |\psi'_l\rangle \).

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 \( |\psi_l\rangle \) is transformed to \( |\psi_{l+1}\rangle = D_lX_l|\psi_l\rangle \). Thus,
\[
|\psi_l\rangle = \prod_{l=1}^{l} D_l X_l |\psi_l\rangle,
\]
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 \( D \in \mathcal{D}_{m,l} \) then \( (\otimes_{k=1}^{m} X_{a_k})D(\otimes_{k=1}^{m} X_{a_k})D^\dagger \in \mathcal{D}_{m,l-1} \) for any choice of variables \( a_k \in \{0,1\} \). Thus, for any \( \ell \), we have \( D_l \in \mathcal{D}_{m,l-\ell+1} \). Since \( \mathcal{D}_{m,1} \) corresponds to the set of tensor products of \( Z \) and the identity, \( D_l X_l = \pm X_l D_l \). Thus, up to a global phase, we have
\[
|\psi_l\rangle = X_l D_l \prod_{l=1}^{l} D_l X_l |\psi_l\rangle,
\]
which collapses telescopically, substituting in the definition of \( D_l \), to yield
\[
|\psi_l\rangle = \prod_{l=1}^{l} X_l |\psi_l\rangle.
\]

Setting \( X = (\prod_{l=1}^{l} X_l) \) 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.

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 \( |\psi_l\rangle \) is transformed to \( |\psi_{l+1}\rangle = Z_l Z_{l-1} D_l X_l |\psi_l\rangle \). Thus,
\[
|\psi_l\rangle = \prod_{l=1}^{l} Z_l Z_{l-1} D_l X_l |\psi_l\rangle,
\]
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 \( \mathcal{D}_{m,1} \), and the definition of \( D_l \) to telescopically collapse the last equation to
\[
|\psi_l\rangle = Z_l \prod_{l=1}^{l} X_l |\psi_l\rangle.
\]
in the maximally mixed state due to the unknown values of 
maximally mixed state. We can apply this argument recur-
dependent on \( l \)
mixed state and hence independent of the computation, the 

\[ |r_k \rangle \text{ for } 1 \leq k \leq m, \text{ and that as these values are un-
known to Bob, this state is necessarily the maximally mixed state of } m \text{ qubits, and hence independent of the values of all }
\text{other } r_k^l \text{ when } l \neq k. \text{ Hence } |\phi_{-1} \rangle \text{ is the only quantum state }
dependent on \( r_k^{l-1} \) for \( 1 \leq k \leq m, \text{ and must similarly be in a }
maximally mixed state. We can apply this argument recur-
sively, implying that every state sent from Alice to Bob is 
in the maximally mixed state due to the unknown values of 
\( \{ r_k^l | 1 \leq k \leq m, 1 \leq l \leq \ell \} \), 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. Rather than present a 
single protocol, we introduce a family of protocols which are 
parameterised by an integer \( m \), 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 \( m = 1 \), we obtain a protocol with the most modest computational requirements 
on Alice—she need only be able to prepare and send single 
qubits in a finite set of states—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 telepor-
tation phase, Alice will use gate teleportation to send the desired 
gates to Bob. Without loss of generality we assume that \( m \) 
divides \( n \) [17], 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 fol-
loows. Interspersed with the operations that Alice teleports, 
Bob will also apply the operation \( CZ = \prod_{i=1}^{l} CZ(i,i+1) \), 
where \( CZ(i,i+1) \) is the controlled-Z operator acting on qubits 
\( i \) and \( i+1 \); as well as the operator \( H = H^\otimes n \), 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 telepor-
tation phase. Then, the pattern repeats itself until \( J \) telepor-
tation 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 computa-
tion for any \( m \), and any \( x \geq 2 \) (see for example [15]). See 
Fig. 2 for a schematic diagram and Prot. 3 for formal presen-
tation of the protocol.

The correct operation of the protocol depends on the proper 
definition of the function \( f_j \) used in Step 3. This function is 
meant to correct and remove the \( X \) errors and the \( Z \) obfus-
cation operators introduced in previous steps. Before giving a 
general definition of \( f_j \), lets first consider a simplified version 
of the protocol where \( m = n \) and the phases of controlled-Z 
operators have been submerged into the diagonal operator tele-
portation phases. Hence, the protocol simplifies into a series 
teleported gate phases followed by a layer of Hadamard gates. 
The output of the protocol is then given by

\[ |\psi_o \rangle = \prod_{j=1}^{J} (Z_j X_j f_j(D_j) |H\rangle) |0\rangle^\otimes n, \quad (7) \]

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 ev-
ery teleportation stage, the \( Z \) operator byproducts are turned 
into \( X \) operators, and \textit{vice versa}, before the the next telepor-
tation. Since Alice can only implement diagonal gates using 
Prot. 2, she can only correct the \( X \) byproducts of the previous 
stage. She can, however, conjugate her current gate with the 
previous \( Z \) operators, so as to commute that operator forward, 
so that it can be corrected in the following teleportation stage. 
In this case, \( f_j \) is given by:

\[ f_j(D) = HZ_{j-1}HDZ_{j-2}H X_{j-2}Z_{j-1}H, \quad (8) \]

where \( Z_j = X_j = I \) for all \( j < 1 \). It is straightforward to verify 
from the definition above that \( f_j \) maps \( D_{m,1} \) onto itself. Now, 
substituting into Eq. 7 we get

\[ |\psi_o \rangle = Z_j X_j \prod_{j=1}^{J} (D_j |H\rangle) |0\rangle^\otimes n. \quad (9) \]

From this state, Alice can get the correct output for computa-
tion by having Bob measure in the \( X \) basis, and sending her 
the output. After this, she uses her decryption key.

\[ \text{FIG. 2: Blind Quantum Computation with Teleportation Protocol.} \]
\[ \text{The dotted-line square shows the repeating pattern of operations.} \]
Protocol 3 General Iterated Teleportation Blind Quantum Computation

1. Alice chooses a depth $J$ and a set of diagonal operations $D_j = \bigotimes_{p=1}^{n/m} D_{j,p}, D_{j,p} \in \mathbb{D}_{m,k}$, 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 $\mathcal{H}D_j \mathcal{H}_j^{-1} \mathcal{H} \mathcal{C}Z \mathcal{D}_2 \mathcal{H}_j \mathcal{D}_1 \mathcal{H} \mathcal{C}Z \mathcal{D}_2 \mathcal{H}_j \mathcal{D}_1 \mathcal{H}$ in the computational basis.

2. Alice produces the state $Z_1|D_1|+\rangle^{\otimes n}$, where $Z_1 = \bigotimes_{k=1}^{n} Z_1^{(k)}$, where each $r_1^{(k)}$ 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 $j \equiv 1 \bmod 2$, then Bob applies $\overline{CZ}$ to register $R$.
   
   (b) Bob applies $\Pi$ to register $R$.
   
   (c) For $1 \leq p \leq P$
      
      i. Alice calculates the operator $f_{j,p}(D_{j,p})$, 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 $X_j$, the teleportation byproduct resulting from Prot. 2 and $Z_{j,p}$, her encryption key.
      
   (d) Alice calculates the operators
      
      \[ X_j = \bigotimes_{p=1}^{n/m} X_{j,p}, \quad Z_j = \bigotimes_{p=1}^{n/m} Z_{j,p} \]
      
      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 $a_k = m_k \otimes r_k^j$, where $Z_j = \bigotimes_k Z_{1,k}$.

The analysis of the full protocol is slightly more involved due to the (re-)introduction of the CZ gates, since these affect the propagation of $X$ byproducts. Fortunately, errors propagate only once, to the nearest neighbours before they can be corrected. To see this, note that in between every two CZ gate stages, there are two sequences of Hadamard operators followed by gate teleportations. Hence, any error that cannot be fixed in the gate-teleportation phase immediately preceding the CZ stage, can be corrected in the subsequent phase. In order to define the general correction function $f_{j,p}$, let $x_{j,k}$ and $y_{j,k}$ be such that

\[ X_j = \bigotimes_{k=1}^{n} X^{c_{j,k}}, \quad \text{and} \quad Z_j = \bigotimes_{k=1}^{n} Z^{c_{j,k}}. \]

For even $j$ we take $x_{j,k} = z_{j-1,k}$ and $y_{j,k} = z_{j-2,k} + x_{j-1,k} + \sum_{t \in \{-1,1\}} (z_{j-3,k+t} + x_{j-2,k+t})$, and for odd $j$ we take $x_{j,k} = z_{j-1,k} + \sum_{t \in \{-1,1\}} (z_{j-2,k+t} + x_{j-1,k+t})$ and $y_{j,k} = z_{j-2,k} + x_{j-1,k} + \sum_{t \in \{-1,1\}} (z_{j-3,k+t} + x_{j-2,k+t})$, and for odd $j$ we take $x_{j,k} = z_{j-1,k} + \sum_{t \in \{-1,1\}} (z_{j-2,k+t} + x_{j-1,k+t})$ and $y_{j,k} = z_{j-2,k} + x_{j-1,k} + \sum_{t \in \{-1,1\}} (z_{j-3,k+t} + x_{j-2,k+t})$.

Then, finally, for all $j$ and $p$ we define

\[ f_{j,p}(D) = \left( \bigotimes_{k=1}^{n} X^{c_{j,k}} \right) D \left( \bigotimes_{k=1}^{n} Z^{c_{j,k}} X^{c_{j,k}} \right), \]

where the tensor products are taken over values of $k$ ranging from $(p-1)m+1$ to $pm$.

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

\[ |\psi_o\rangle = \prod_{j=1}^{J} \left( Z_j X_j \bigotimes_{p=1}^{n/m} (f_{j,p}(D_{j,p})) \mathcal{H} \mathcal{C}Z \mathcal{D}_2 \mathcal{H}_j \mathcal{D}_1 \mathcal{H} \mathcal{C}Z \mathcal{D}_2 \mathcal{H}_j \mathcal{D}_1 \mathcal{H} \right) |0\rangle^{\otimes n}, \]

where the product operator is defined 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

\[ |\psi_o\rangle = Z_j X_j \bigotimes_{j=1}^{J} \left( D_{j,p} \mathcal{H} \mathcal{C}Z \mathcal{D}_2 \mathcal{H}_j \mathcal{D}_1 \mathcal{H} \mathcal{C}Z \mathcal{D}_2 \mathcal{H}_j \mathcal{D}_1 \mathcal{H} \right) |0\rangle^{\otimes n}, \]

as required.

The proof of blindness of the main protocol follows directly from the proof of blindness of Prot. 2.

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 $(2^k)^{(2^k-1)}$. 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.

Setting $m$ equal to $n$ requires Alice to prepare large entangled states, which may be undesirable in realistic settings. 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.

The approach of iterated teleportation introduced in this comment can be applied to other measurement-based blind computation protocols (such as [11], [5] and [9]) to achieve smaller advantages over the no-programming theorem bound. It can be used outside of the blind computation setting, to reduce communication requirements in other delegated computation scenarios via Prot. 1. The notion of blindness used here is compatible with requirements for composable security in the abstract cryptography framework [12], meaning that there is no compromise in security.

This material is based on research funded by the Singapore National Research Foundation under NRF Award NRF-NRFF2013-01. We thank Lorenzo Maccone, Tomoyuki Morimae and Terry Rudolph for helpful comments on the manuscript.
[1] A. Broadbent, J. Fitzsimons, and E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009) pp. 517–526 (2009).
[2] D. Aharonov, M. Ben-Or, and E. Eban, in Proceedings of Innovations in Computer Science 2010 (2010), p. 453.
[3] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science 335, 303 (2012).
[4] T. Morimae and K. Fujii, Nature Communications 3, 1036 (2012).
[5] J. F. Fitzsimons and E. Kashefi, arXiv preprint arXiv:1203.5217 (2012).
[6] T. Morimae, Phys. Rev. Lett 109 (2012).
[7] T. Morimae and K. Fujii, Physical Review A 87, 050301 (2013).
[8] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Nature Physics (2013).
[9] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, Phys. Rev. Lett. 111, 230502 (2013).
[10] T. Sueki, T. Koshiba, and T. Morimae, Physical Review A 87 (2013).
[11] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. 111, 230501 (2013).
[12] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, arXiv preprint arXiv:1301.3662 (2013).
[13] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. 79, 321 (1997).
[14] D. Gottesman and I. L. Chuang, Nature 402, 390 (1999).
[15] J. Fitzsimons, L. Xiao, S. C. Benjamin, and J. A. Jones, Phys. Rev. Lett. 99, 030501 (2007).
[16] 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 $l$.
[17] This may always be done, since Alice can pad her input with unused ancilla qubits.