Quantum processing by remote quantum control

Xiaogang Qiang¹, Xiaoqi Zhou^{2,1}, Kanin Aungskunsiri¹, Hugo Cable¹, Jeremy L. O'Brien¹

¹Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory and Department of Electrical & Electronic Engineering, University of Bristol, BS8 1FD.UK.

²State Key Laboratory of Optoelectronic Materials and Technologies and School of Physics, Sun Yat-sen University, Guangzhou 510275, China.

E-mail: qiangxiaogang@gmail.com zhouxq8@mail.sysu.edu.cn jeremy.obrien@bristol.ac.uk

Abstract. Client-server models enable computations to be hosted remotely on quantum servers. We present a novel protocol for realizing this task, with practical advantages when using technology feasible in the near term. Client tasks are realized as linear combinations of operations implemented by the server, where the linear coefficients are hidden from the server. We report on an experimental demonstration of our protocol using linear optics, which realizes linear combination of two single-qubit operations by a remote single-qubit control. In addition, we explain when our protocol can remain efficient for larger computations, as well as some ways in which privacy can be maintained using our protocol.

1. Introduction

Quantum computing offers the possibility of achieving substantial algorithm speedups compared to classical computing [1–3], and can preserve the privacy of computations while doing so. Given the intrinsic difficulties in building a quantum computer, this privacy preservation will be crucial for any client-server model, which will likely provide a practical and efficient way to access quantum computing resources. In the scenario where a client delegates his computation to a quantum server, the data can readily be hidden from the server by using algorithms designed to work on encrypted data [4–8]. A protocol for "blind" quantum computing, based on the paradigm of measurement-based quantum computing [9, 10], was recently demonstrated using linear optics [11]. Here the client implements an algorithm by requesting that the server performs consecutive adaptive single-qubit measurements on a (large) blind cluster state—a multi-particle entangled state created from qubits transmitted by the client. Since the states of the transmitted qubits are chosen randomly by the client, the computations on the blind cluster state do not reveal any data or the algorithm to the server [11]. The randomness source that is used by the client should be carefully examined to avoid any correlations

with the server and must achieve high-speed operation (such as was recently reported in ref [12]). Full-scale demonstrations of this blind quantum computing protocol would also require that the server has the ability to create large cluster states, which is beyond the capabilities of current quantum technologies.

Here we propose a fundamentally new type of protocol for allowing clients to execute quantum processing on a remote server. In our approach, the client translates his task into a linear combination of quantum operations performed by server. Arbitrary unitary operations can be represented in a linear-combination form using the Cartan decomposition [1]. The linear coefficients are then encoded in a quantum state, and transmitted from client to server using quantum teleportation. As we will argue, the client can keep the linear coefficients hidden from the server. To enable the required linear combining of quantum operations in our protocol, we will utilise circuits based on a technique to add coherent control to arbitrary (unknown) quantum operations, demonstrated in Ref. [14]. This technique is based on gates which can exploit extensions of the logical Hilbert space used for computation. We will proceed as follows: we will first explain circuits for realising linear-combinations of a fixed family of quantum operations, before explaining in detail how they can be used to enable quantum computation in a client-server model. Then we will report a proof-of-principle experimental demonstration of our protocol in a linear-optic setup, which implements arbitrary linear combinations of two single-qubit quantum operations by a remote one-qubit control.

2. Linear combining of quantum operations

Suppose that we want to implement some unitary U_T which can be expressed in the form,

$$U_T = \sum_{j=0}^{n-1} \alpha_j V_j, \tag{1}$$

where the V_j are gates acting on a d-dimensional target (T) subspace, and the α_j are complex coefficients satisfying

$$\sum_{j=0}^{n-1} |\alpha_j|^2 = 1. (2)$$

When controlled- V_j gates are available, we can implement U_T probabilistically through the circuit illustrated in Fig. 1(A). Here the α_j are encoded in the initial state for the k-qubit control (C),

$$|\phi\rangle_C = \sum_{j=0}^{n-1} \alpha_j |j\rangle_C, \tag{3}$$

where $n=2^k$ and j labels the computational basis, and the circuit succeeds when all control qubits are measured to be 0 in the computational basis at the end.

However, this approach for implementing U_T cannot work when the V_j 's must be assumed to be black-box operations, due to a no-go theorem which states that adding

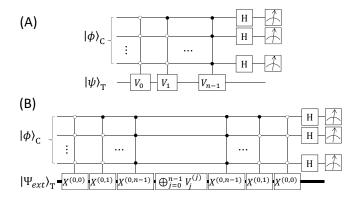


Figure 1. Implementing linear-combination operations: (A) Circuit for implementing linear-combination operations which assumes the availability of multiply-controlled V_j gates. There are k control qubits with initial state $|\phi\rangle_C = \sum_{j=0}^{n-1} \alpha_j |j\rangle_C$ and $n=2^k$. T is a d-dimensional target system. $U_T = \sum_{j=0}^{n-1} \alpha_j V_j$ acts on T when the measurement outcome is $|0\rangle\langle 0|_C^{\otimes k}$. (B) The LCC implements the same conditional operation as in (A) but without controlled V_j gates, with T extended to $(n \times d)$ -dimensions, using operations on subspaces of T.

control to unknown quantum operations is impossible in the (conventional) quantum circuit model [15, 16]: any protocol which attempts to add control to a black-box operation must be able to differentiate V_i and $\exp(i\theta)V_i$, but standard quantum circuits always generate identical measurement outcomes for these two cases. Nonetheless, control can be added in many systems, by exploiting the fact that physical operations often act non-trivially on some degrees of freedom or subspaces of quantum states, while acting trivially on others. The description of V_i for such cases should be modified to $V_i \oplus I$, and control can be added even when this extension is one dimensional [15]. It has been shown that control qubits can be simply added to a single-qubit unitary by moving part of the state of a target qubit into an expanded Hilbert space [17]. A more general scheme was proposed in reference [14] for adding control to an arbitrary quantum operation, with the implementation of its optical version based on the controlled-path (CP) gate [18] that controls the target photon's path conditioned on the control photon's polarization. The CP gate was first proposed for realizing quantum controlled gates in the context of weak optical cross-Kerr nonlinearities [19, 20]. Techniques based on expanding the computational Hilbert space have also been demonstrated for adding control for subroutines of quantum computation [21] and implementing the Fredkin gate [22]. Here we use the same techniques to implement a linear-combination circuit (LCC) which is illustrated in Fig. 1(B).

LCCs can exploit black box unitaries to implement a target quantum evolution using coherent control, using the control state as in Eq.(3), acting on a $(n \times d)$ -dimensional target subspace T. T decomposes into n d-dimensional subspaces, with the j^{th} subspace is spanned by basis elements $\{|jd\rangle_T, \cdots, |(j+1)d-1\rangle_T\}$. The LCC uses a series of subspace-swap operations, $X^{(0,j)}$ (which exchange corresponding basis elements for the 0^{th} and j^{th} subspaces) which are controlled by qubits in C, and performs

the sum operation $\bigoplus_{j=0}^{n-1} V_j^{(j)}$, where $V_j^{(j)}$ implements the same operation as V_j previously but on the j^{th} subspace of T. The initial state for T is taken to be

$$|\Psi_{ext}\rangle_T = \sum_{j=0}^{d-1} \beta_j |j\rangle_T + \sum_{j=d}^{nd-1} 0|j\rangle_T.$$
(4)

Following the step-by-step evolution given in Supplementary Material, it is straightforward to verify that, when the control qubits are all measured to be 0 in the computational basis, the target evolves according to:

$$|\Psi_{ext}\rangle_T \to \sum \alpha_j V_j^{(0)} |\Psi_{ext}\rangle_T.$$
 (5)

Note here $V_j^{(0)}$ implements V_j on the 0^{th} subspace of T as defined before. The success probability is readily found to be 1/n, which is independent of the size of the V_j .

Any arbitrary quantum unitary operation can in principle be decomposed into a linear sum of elementary operations. Using Cartan's KAK decomposition, we can explicitly rewrite any two-qubit unitary operation, $U_{SU(4)}$, as a linear combination of four tensor products of two single-qubit gates. Furthermore, Cartan's decomposition allows an n-qubit unitary operation $U_{SU(2^n)}$ to be recast as a linear combination of tensor products of n single-qubit gates [5]. Such a decomposition is, in general, not efficient, in the sense that there may be exponentially-many terms. And thus, the success probability of LCC for general $U_{SU(2^n)}$ can be exponentially small. for some non-trivial families of unitary operations the linear decomposition method can be efficient. For example, an n-qubit controlled-unitary gate CU can be decomposed as $\frac{I+\sigma_z}{2}\otimes I+\frac{I-\sigma_z}{2}\otimes U$ where U is an (n-1)-qubit operation [14]. Only one control qubit is required to implement this operation and high success probability can be obtained. Although the number of linear-combining terms is restricted, the size of each term can be large and reconfigurable, providing sufficient computing power and flexibility for various applications. It is worth noting that the proposed LCC can also be interpreted by using the notion of duality quantum computation [24–26], which was originally proposed to exploit the wave-particle duality and then developed to work within the framework of conventional quantum computing.

3. Implementing quantum processing by remote quantum state control

The LCC described above provides a way to implement quantum information processing using a client-server model, as illustrated in Fig. 2. We assume now the V_j 's are the computational resources provided by the server and the α_j 's are configured by the client to encode an algorithm. The α_j 's are encoded into the control state $|\phi\rangle_C$ and transmitted from the client to the server remotely. The transmission of states between the client and the server is performed by a (multi-)qubit teleportation protocol [27, 28] using generalised Bell measurements. The control state $|\phi\rangle_C$ has k qubits, and k EPR channels must be shared between the client and server to enable teleportation of this state. Similarly, $\lceil \log_2 d \rceil$ EPR channels are required to teleport the computational input

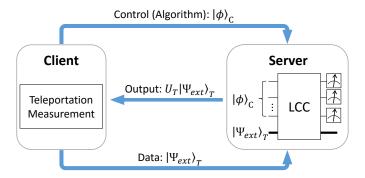


Figure 2. Protocol for remote quantum processing: For each of the client's requests, the server first repeatedly runs the LCC till it succeeds. The client then teleports a quantum control state $|\phi\rangle_C$ to the server using quantum teleportation EPR channels to complete his computation. The computational input $|\Psi_{ext}\rangle_T$ can be transmitted to the server (and the computational output $U_T |\Psi_{ext}\rangle_T$ back to the client) using additional quantum-teleportation channels or direct transmissions.

 $|\Psi_{ext}\rangle_T$ from client to server, and a further $\lceil \log_2 d \rceil$ EPR channels are required to teleport the computational output from server to client (d is defined as previously). To start the computation, the client requests the server to run the LCC, and the server repeatedly runs the LCC on the EPR channels (resetting them as required). When the LCC succeeds, the server informs the client and performs teleportation measurements on the LCC output and corresponding EPR channels. Finally, the client performs teleportation measurements on $|\phi\rangle_C$ and $|\Psi_{ext}\rangle_T$ (and the corresponding EPR channels). When all LCC and teleportation steps succeed, $U_T |\Psi_{ext}\rangle_T$ is returned to the client.

By keeping the control state $|\phi\rangle_C$ hidden from the server, this protocol can provide security for the client's computation. We first consider the simplest case where the client only sends a one-qubit control state to the server so that a linear combination of two quantum operations A and B can be implemented. The corresponding quantum circuit is shown in Fig. 3(A), where we assume that A and B are not black-box operations and also ignore the teleportation of the input state for the computation. The circuit starts from the initial state $\frac{1}{\sqrt{2}}|0\rangle_1(|0\rangle_2|0\rangle_3+|1\rangle_2|1\rangle_3)|\varphi\rangle_4$. In the case where the server follows the protocol, the server first runs the LCC until it succeeds—the qubit 3 (local control qubit) is then measured to be "0" in computational basis. The state of remaining qubits is $\frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 A|\varphi\rangle_4 + |0\rangle_1|1\rangle_2 B|\varphi\rangle_4$). The client then performs the quantum teleportation. When he measures the qubit 1 and qubit 2 to be "0" in computational basis, the state of remaining qubit becomes $(\alpha A + \beta B)|\phi\rangle_4$ immediately. During the whole process, the server does not have any chance to detect the control state (encoded in the qubit 1 by the client's local operation P), because he needs to measure the local control qubit (qubit 3) before the client performs the configuration of control.

Next we consider the case where the server does not perform the measurement on the local qubit before the teleportation as our protocol demands. In this case, the circuit will evolve as shown in Fig. 3(B). When the client measures the qubit 1 and qubit 2 to be "0", the state of remaining qubits will be $\alpha |0\rangle_3 A |\varphi\rangle_4 + \beta |1\rangle_3 B |\varphi\rangle_4$ (we denoted it

as $|\Psi\rangle$). Now the question is that whether the server can extract the information of the control state $|\phi\rangle_C = \alpha |0\rangle + \beta |1\rangle$ without being detectable to the client. To achieve this, the server needs to extract $|\phi\rangle_C$ and also output the correct result of the computation $(\alpha A + \beta B) |\varphi\rangle_4$ to the client. In other words, the server needs to find an operation U_s satisfying

$$(\alpha |0\rangle + \beta |1\rangle)(\alpha A + \beta B) |\varphi\rangle = U_s(\alpha |0\rangle A |\varphi\rangle + \beta |1\rangle B |\varphi\rangle). \tag{6}$$

Such an operation U_s does not exist for unknown parameters α and β , because it would allow copying of an unknown quantum state which violates the no-cloning theorem [29, 30]. However, it is possible for the server (or a third party) to generate a copy of the control state with imperfect fidelity, for example, by using a universal quantum cloning machine (UQCM) [31,32] even with a single copy of the control state. Such cloning attacks are difficult to prevent since they could be disguised as channel loss, and thus can lead to leaking of information about the client's computation.

For many applications such as Shor's factorization algorithm [1] and Grover's search algorithm [2], the client can get the result by just running the protocol a few times. Then the server (or a third party) might potentially obtain partial information about the control state by using UQCM. For applications that require many runs of the protocol, the client would need to send excess copies of the control state, and thus the server might potentially gain complete information about the control state, for example, by using quantum state tomography. To address this vulnerability we present a modified protocol below:

For a computation with the control state $\rho = |\phi\rangle_C \langle \phi|_C$, define a decoy state

$$\rho_m = \frac{1+\epsilon}{n} \mathbb{1} - \epsilon \rho \tag{7}$$

where n is the number of dimensions of ρ and $0 < \epsilon \le 1/(n-1)$. ρ_m can be generated by sending its eigenstates with probabilities given by corresponding eigenvalues. On each run of the protocol, the client sends the control state ρ with probability $\epsilon/(1+\epsilon)$ and the decoy state ρ_m with probability $1/(1+\epsilon)$. As the client knows exactly what state he sent each run, he can just discard the output states corresponding to the decoy states and keep the correct ones for further applications. From the perspective of the server, the state received will be

$$\frac{\epsilon}{1+\epsilon}\rho + \frac{1}{1+\epsilon}\rho_m = \frac{1}{n}\mathbb{1}.$$
 (8)

The state 1/n has the maximal entropy $(= \log n)$, implying that the server has no knowledge about the received states at all.

The client can verify the result directly for certain applications (e.g. Shor's factorization and Grover's search) but not others (e.g. some large quantum simulations). However, the client is still able to verify (or monitor) the computation process for applications whose results cannot be verified directly. We have shown that the

decomposed component V_i can be as simple as a tensor product of single-qubit gates and can therefore be verified with limited resources. Throughout the full computation process, the client can randomly send each basis state $|i\rangle$ $(i=0,1,\cdots,n-1)$ to the server, and since only the corresponding component V_i is applied, the output can be checked (via state tomography or measurements in multiple bases). This approach allows the client to diagnose whether the server is running the LCC correctly, and it can be combined with the strategy above for preventing the control state from being measured by the server (or a third party): the client chooses a proportion of the runs of the protocol for performing computation and the rest of the runs of the protocol for verification. Assuming the proportion of runs of the protocol for computation to be τ $(0 < \tau < 1)$, the client would send the control state ρ with probability $\tau \epsilon/(1 + \epsilon)$, the decoy state ρ_m with probability $\tau/(1 + \epsilon)$, and each basis state $|i\rangle$ with probability $(1 - \tau)/n$ on each run. The state the server receives is then

$$\tau \left(\frac{\epsilon}{1+\epsilon} \rho + \frac{1}{1+\epsilon} \rho_m \right) + \frac{1-\tau}{n} \sum_{i=0}^{n-1} |i\rangle \langle i| = \frac{1}{n} \mathbb{1}.$$
 (9)

Therefore, although the whole computation process takes longer, the server is given no information about whether the states it receives are for verification purposes or for performing an algorithm, and no information about the control state. If the server intercepts a fixed proportion of the control qubits in a way which randomizes the results, the probability that the server is not detected is suppressed exponentially as the number of runs of the protocol grows.

We have shown that the success probability of the LCC decreases exponentially with the number of control qubits. However, in the secure quantum processing protocol, the server only needs to inform the client when the LCC succeeds, ensuring that the LCC works with 100% success probability from the standpoint of the client. The success probability for teleporting the control state exponentially decreases with the number of teleported qubits, implying poor scaling with large control states. Therefore, our protocol is practical only for small control states, i.e. the number of linear terms n should be polynomial-sized with respect to the problem size. For a typical case of the modified protocol combining verification and computation where $\epsilon = 1/(n-1)$ and $\tau = 1/2$, the probability of the client sending the control state ρ for each run will be 1/2n, and thus the number of runs of the protocol required will be O(2n) times more than the original protocol, which brings only polynomially-increasing cost. The whole client-server computation scheme could (where required) include the quantum teleportation of the computation input and output. Teleporting the output has 100% success probability with necessary correction operations, while the success probability of teleporting the input depends on the dimension d of the target operation (specifically, equals to $1/d^2$) since the correction operations generally do not commute with the target operation. Taking these teleportation steps into account, the success probability of the whole scheme is 1/O(poly(nd)). The client here is required to have the capability to create small control states, which is trivial compared to the capabilities that the server must

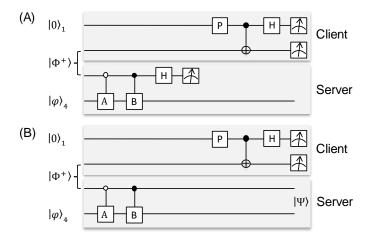


Figure 3. Security analysis for one-qubit control quantum processing. (A) $|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|0_{2}\rangle|0_{3}\rangle + |1_{2}\rangle|1_{3}\rangle)$ is the EPR state shared between the client and the server. A and B are two arbitrarily-large quantum operation of the same size. $|\varphi\rangle_{4}$ is the input state for the client's computation. We ignore the teleportation process of $|\varphi\rangle_{4}$ from the client to the server. P is a local single-qubit operation to configure the one-qubit control state $|\phi\rangle_{C}$. The server repeatedly runs the LCC until he measures the local control qubit (qubit 3) to be "0", and then he informs the client to start the configuration and teleportation of the control state. (B) In this case, the server tries to cheat by not performing the measurement on the local control qubit, and directs the client to start the teleportation process. $|\Psi\rangle$ represents the state of remaining qubits that the server obtains when the quantum teleportation succeeds. A step-by-step evolution is shown in Supplementary Material.

have. It is also noteworthy that the success probability could be further improved by using port-based teleportation (rather than conventional quantum teleportation) [33,34], which transmits a one-qubit state to one of K output ports using K EPR pairs and is asymptotically faithful and deterministic for large K.

4. Experimental demonstration

Here we report on a demonstration of our protocol using a linear-optic setup, which realises a circuit for generating linear combinations of two single-qubit gates with one-qubit quantum control, as shown in Fig. 4(A). Our experimental setup exploits both path and polarization degrees of freedom of photons. Since direct implementation of controlled- V_j 's is very challenging using current technology, we demonstrate a LCC using the method shown in Fig. 4(B). To understand how it works, suppose that server starts with a single photon in the state

$$\alpha |\psi\rangle_b |\mathrm{vac}\rangle_r + \beta |\mathrm{vac}\rangle_b |\psi\rangle_r,$$
 (10)

where $|\psi\rangle$ is an (arbitrary) polarization-encoded qubit, b and r label the blue and red spatial modes, and $|\text{vac}\rangle$ represents unoccupied modes (and will be dropped below). Two single-qubit gates A and B act only on photon in the blue or red path respectively,

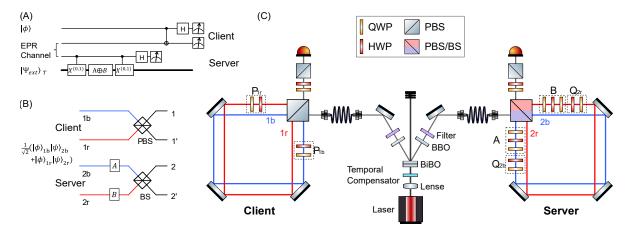


Figure 4. Experimental demonstration: (A) Circuit for implementing quantum processing by remote one-qubit quantum control. (B) Schematic for optical implementation of (A). Client and server share a pair of spatially-entangled photons: $(|\phi_{1b}\psi_{2b}\rangle + |\phi_{1r}\psi_{2r}\rangle)/\sqrt{2}$. When the photons exit at port 1 and 2, the output state of the photon on server's side will be $(\alpha A + \beta B)|\psi\rangle$, where α and β are controlled by client's one-qubit control state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. (C) In our setup, entangled photon pairs are generated by a SPDC source using paired type-I BiBO crystal in a sandwich configuration. P_{1b} and P_{1r} (Q_{2b} and Q_{2r}) configure $|\phi\rangle$ ($|\psi\rangle$). A and B can implement arbitrary single-qubit gates. Further details are given in Appendix.

yielding the state: $\alpha A |\psi\rangle_b + \beta B |\psi\rangle_r$. The blue and red modes are then mixed on a (non-polarising) beam splitter (BS) to remove path information. In the case where the photon exits at port 2, the output state of the photon which is obtained is $(\alpha A + \beta B) |\psi\rangle$, which corresponds to the action of linear combination $\alpha A + \beta B$ on $|\psi\rangle$.

In the remote quantum processing scenario, client and server start by sharing a pair of entangled photons in state

$$\left(\left| \phi \right\rangle_{1h} \left| \psi \right\rangle_{2h} + \left| \phi \right\rangle_{1r} \left| \psi \right\rangle_{2r} \right) / \sqrt{2}, \tag{11}$$

where $|\phi\rangle = \alpha |H\rangle + \beta |V\rangle$ (client photon) and $|\psi\rangle$ (server photon) encodes a qubit in the polarization basis. When the blue and red modes of client's photon are mixed on a polarising beam splitter (PBS), the client-server state becomes

$$|D\rangle_{1} (\alpha |\psi\rangle_{2b} + \beta |\psi\rangle_{2r}) + |D\rangle_{1'} (\alpha |\psi\rangle_{2r} + \beta |\psi\rangle_{2b}), \tag{12}$$

where $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, and contributions corresponding to anti-diagonal polarization at 1 and 1' have been dropped (corresponding to postselection on detection outcomes with diagonal-polarization only). In the case where client's photon exits at port 1, the state of the server's photon is given by Eq. (10), and the operation $\alpha A + \beta B$ is implemented as above. The experimental setup is shown in Fig. 4(C), and the details are shown in Appendix.

It is worth noting that an arbitrary single-qubit quantum operation $U_{\mathrm{SU}(2)}$ can be implemented as

$$U_{SU(2)} = \alpha_0 I + \alpha_1 \sigma_x + \alpha_2 \sigma_y + \alpha_3 \sigma_z \tag{13}$$

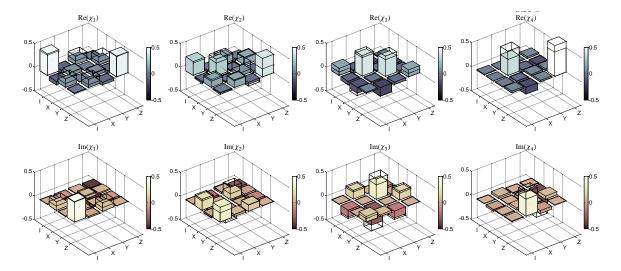


Figure 5. Experimental reconstructed χ matrices with corresponding theoretical predictions overlaid: Three unitary operations $U_1=0.9239A+0.3827B,\ U_2=0.7071A+0.7071B,\ U_3=-0.3827A+0.9239B$ and one non-unitary operation $U_4=0.7071X+0.7071iZ$ were tested. The corresponding process matrices χ_1,χ_2,χ_3 and χ_4 are shown with their theoretical values overlaid. We observed process fidelities $94.38\pm0.87\%,\ 94.79\pm0.85\%,\ 95.98\pm0.73\%$ and $88.56\pm1.58\%$ respectively. The errors are estimated by adding random noise to the raw data and performing many reconstructions. Further results are given in Supplementary Material.

where σ_x , σ_y and σ_z are Pauli matrices, and α_i are complex coefficients satisfying $\sum_{i=0}^{3} |\alpha_i|^2 = 1$ (see details in Supplementary Material). Therefore, linear combination of four gates would be required to implement an arbitrary single-qubit operation if the server were to provide only Pauli gates as the resource to the client. In our experimental setup, the two single-qubit gates provided by the server can be arbitrarily configured, which allows us to demonstrate the secure realization of a wide range of linear-combination operations. We tested a series of linear-combination operations where the two single-qubit gates are set to be

$$A = \begin{pmatrix} \frac{1-i}{\sqrt{2}} & 0\\ 0 & \frac{-1-i}{\sqrt{2}} \end{pmatrix}, B = \begin{pmatrix} 0 & \frac{1+i}{\sqrt{2}}\\ \frac{1-i}{\sqrt{2}} & 0 \end{pmatrix}.$$
 (14)

The linear combinations of A and B are always unitary when the client's one-qubit control state has real amplitudes. Our main results are shown in Fig. 5, and additional results are also given in Supplementary Material. Our protocol also allows the client to implement non-unitary operations (even though the server provides only unitary gates). For example, when the two gates A and B are set to be X (Pauli-X) and Z (Pauli-Z) gates respectively, the client can implement non-unitary operation $(X+iZ)/\sqrt{2}$ by teleporting one-qubit quantum control $|\phi\rangle_C = (|0\rangle + i\,|1\rangle)/\sqrt{2}$. To evaluate the performance of each the operations we tested, we performed quantum process tomography and reconstructed corresponding process (χ) matrices from the experimental data, using the maximum-likelihood-estimation technique. As shown in

Fig. 5, all of the reconstructed process matrices achieve high process fidelities compared to the corresponding ideal cases.

Our experiment serves as a proof-of-principle demonstration of the essential part of our protocol—a remote control state can be used to implement the linear-combining operation. As we mentioned above, the server (or a third party) could use a UQCM to extract partial information about the control state. Also, as post-selection was used in the experiments to choose cases where the teleportation of the control state and the LCC succeed simultaneously, the server can obtain extra copies of the control state by disguising his measurements as failures of the LCC, leading to potential information leak of the control state.

The proposed modified protocol aims to eliminate possible leak of the control state, but requires enhanced capability of the experimental setup. In particular, it costs much increased experimental time to generate the required mixed states and thus needs improved robustness and stability—which would be challenging for our current bulkoptical setup (but could potentially be achieved in a future experiment using integrated photonic waveguide techniques [35–37]). Possible issues for future demonstration of the modified protocol include experimental imperfections, loss in transmission channels and the photon source. Imperfections in the server's gates (such as A, B, Q_{2b} , Q_{2r} shown in Fig. 4(C)) do not affect the security of the protocol, rather just the outcome of the computation. Imperfections in the client's gates (such as P_{1b} , P_{1r} shown in Fig. 4(C)) can affect the creation of the mixed state 1/n (and also potentially mimic effects of a malicious third party or server) and thereby reduce the security offered by the modified protocol. However, loss in the transmission channels would not cause any added security issue for the modified protocol, since it would just act as a normalization factor for the mixed state 1/n. The SPDC photon source creates photon pairs probabilistically, which can be viewed as being equivalent to loss in the channels from a deterministic source, and the security is similarly unaffected by this. A completely quantitative security analysis is beyond the scope of this work and is for future research.

5. Conclusion

In summary, we have described and demonstrated a novel protocol, which can enable a client to implement complex quantum processing on a remote server without revealing the precise algorithm to the server. We leave as an interesting open question whether unconditional security can always be guaranteed using our protocol, which will require an information-theoretic analysis of diverse attacks on the security, as well as the effects of experimental imperfections, such as multi-pair contributions to the state generated by the SPDC source. Although our discussion has focused on protecting the privacy of the client's algorithm, it can be extended to protect the privacy of the client's data by exploiting existing encryption schemes [4]. Our protocol cannot always achieve efficient implementation of arbitrary quantum circuits (efficient universality), but it could be suitable for some practicable applications, for example, adding control

to a remote operation, with less resources and experimental difficulties. circuits used by our protocol are based on decompositions into linear combinations of elementary gates, and differ greatly from the circuits generated by the Solovay-Kitaev algorithm [38] for example. Compared with more conventional techniques to implement quantum computation, such linear-combination-based methods would lead to greater efficiency for some problems: Several works have shown that simulations of Hamiltonian dynamics based on linear combinations of unitary operations can achieve exponentiallyimproved precision-dependence compared to the conventional product-formula-based algorithms [39,40], and even nearly-optimal dependence on all parameters [41]. By using the linear-combination technique, the dependence on precision can be exponentially improved [42] compared to the Harrow-Hassidim-Lloyd algorithm [43] for the quantum linear systems problem. It can also reduce the query complexity and improve precision for simulations of open quantum systems [26] based on linear combinations of Kraus operators [3]. These applications generally require linear combinations of a great number of unitary operations. It is an interesting open question whether there exist some particular instances that can critically benefit using only a limited number of linear Considering the alternative interpretation of the LCCs in duality quantum computation, our protocol could be treated as an interesting and important application of duality quantum computation. Finally, the protocol we have demonstrated here can be implemented in a wide range of physical systems. For example, future photonic demonstrations of our protocol could exploit time-bin and orbital angular momentum degrees of freedom (which can offer high-dimensional quantum subspaces) to implement complex controlled operations.

Acknowledgements

The authors would like to express their appreciation to Navin Khaneja for valuable discussions. This work was supported by EPSRC, ERC, BBOI, QUCHIP(H2020-FETPROACT-3-2014), PICQUE(FP7-PEOPLE-2013-ITN), US Army Research Office(ARO) Grant W911NF-14-1-0133 and the Centre for Nanoscience and Quantum Information(NSQI). X.Z. acknowledges support from the National Key R & D Program (Grant No. 2016YFA0301700), the National Young 1000 Talents Plan and Natural Science Foundation of Guangdong (2016A030312012). J.L.OB. acknowledges a Royal Society Wolfson Merit Award and a Royal Academy of Engineering Chair in Emerging Technologies. The experimental data are available for download from the Research Data Repository of University of Bristol at https://data.bristol.ac.uk/data/dataset/35xkv6pvafi8d23orogggewm9u.

Appendix

Linear decomposition of a unitary operation. Here we show how to decompose a unitary quantum operation into the linear combination form. We first consider two-

qubit unitary operations. By using the KAK decomposition [1], an arbitrary two-qubit unitary operation $U_{SU(4)}$ can be decomposed as

$$U_{SU(4)} = (U_1 \otimes V_1)U_D(U_2 \otimes V_2), \tag{15}$$

where U_1 , V_1 , U_2 and V_2 are single-qubit quantum gates, and U_D is a non-factorable two-qubit gate responsible for the non-local characteristic of the gate U, which is given by

$$U_D = \exp(-i(k_1\sigma_x \otimes \sigma_x + k_2\sigma_y \otimes \sigma_y + k_3\sigma_z \otimes \sigma_z)), \tag{16}$$

where k_i are real numbers, and σ_x , σ_y and σ_z are Pauli matrices. Consider the facts that $\exp(iAx) = \cos(x)I + i\sin(x)A$ for an arbitrary real number x and a matrix A satisfying $A^2 = I$ [3] and $\sigma_a\sigma_b = -\sigma_b\sigma_a = i\sigma_c$ for $\{a,b,c\} \in \{\{x,y,z\}, \{y,z,x\}, \{z,x,y\}\}$, we can obtain

$$U_{SU(4)}$$

$$= (U_{1} \otimes V_{1}) \cdot (\alpha_{0}I \otimes I + \alpha_{1}\sigma_{x} \otimes \sigma_{x} + \alpha_{2}\sigma_{y} \otimes \sigma_{y} + \alpha_{3}\sigma_{z} \otimes \sigma_{z}) \cdot (U_{2} \otimes V_{2})$$

$$= \alpha_{0}U_{1}U_{2} \otimes V_{1}V_{2} + \alpha_{1}U_{1}\sigma_{x}U_{2} \otimes V_{1}\sigma_{x}V_{2} + \alpha_{2}U_{1}\sigma_{y}U_{2} \otimes V_{1}\sigma_{y}V_{2} + \alpha_{3}U_{1}\sigma_{z}U_{2} \otimes V_{1}\sigma_{z}V_{2}.$$

$$(17)$$

where α_i $(i=0,\cdots,3)$ are complex coefficients derived from k_i (i=1,2,3) in Eq. (16). The details are shown in Supplementary Material, together with the explicit results of decomposing universal three-qubit unitaries. More generally, an arbitrary n-qubit quantum operation $U \in SU(2^n)$ can be decomposed as a linear combination of the tensor products of n single qubit gates, by applying Cartan's KAK decomposition recursively [5]. The computational complexity of applying Cartan's decomposition on a unitary $U \in SU(d)$ is O(poly(d)) [45], and thus it is not efficient for a general exponential-sized unitary. It is an open problem to find efficient ways for applying Cartan's decomposition on specific families of unitary, for example, multiple controlled-unitary operations.

Experimental setup. The polarization-entangled photon pairs are generated by a spontaneous parametric down-conversion source using paired type-I BiBO crystal in sandwich configuration [46], where a diagonally polarized, 120 mW, continuous-wave laser beam with central wavelength of 404 nm is focused at the centre of paired BiBO crystals with their optical axes orthogonally aligned to each other. The generated photons pass through a PBS cube on the client's side and a PBS/BS (half-PBS, half-BS) cube on the server's side respectively, generating the spatially-entangled state

$$(|H_{1b}\rangle |H_{2b}\rangle + |V_{1r}\rangle |V_{2r}\rangle)/\sqrt{2}. \tag{18}$$

The client can prepare an arbitrary polarization-state $|\phi\rangle$ by configuring P_{1b} and P_{1r} —consisting of half- and quarter- waveplates and acting on spatial modes 1b and 1r respectively. The server configures the computational input state $|\psi\rangle$ for computation

by Q_{2b} and Q_{2r} which act on the spatial modes 2b and 2r respectively. Note here that we assume that the client informs the server of the computational input state $|\psi\rangle$ in advance. The two single-qubit gates A and B are configured by the server using two sets of wave plates, each consisting of quarter-, half- and quarter waveplates. When detecting two-photon coincidences between detectors at ports 1 and 2, the client implements the quantum computation $(\alpha A + \beta B) |\psi\rangle$ securely on the remote server.

Comparison with related work. Previous protocols in refs [4–8] provide security by hiding the computation data from the server while the algorithm itself is exposed to the server. Blind quantum computing [9–11] can hide all of the computation input, output and algorithm. Since our protocol focuses on hiding the computation algorithm, we present here a comparison with blind quantum computing as below:

Table 1. Comparing our protocol with blind quantum computing.

	Blind quantum computing	Our protocol
Privacy	input, output and algorithm	algorithm
Computation model	measurement-based model	quantum circuit model
Algorithm encoding	consecutive adaptive single-	amplitudes of a quantum state
	qubit measurements	
Requirements for client	perfect randomness source; cre-	creation of small-scale states
	ation of single-qubit states	
Requirements for server	generation of large cluster	implementation of basic com-
	states	putation components
Communications	transmission of quantum states;	EPR channels; Bell measure-
	classical measurement instruc-	ment results
	tions	
Universality	universal	limited number of linear combi-
		nation terms
Feasibility	difficult	near-term implementation

Reference

- [1] Shor P W 1997 SIAM J. Sci. Statist. Comput. 26 1484–1509
- [2] Grover L K 1997 Phys. Rev. Lett. **79** 325
- [3] Montanaro A 2016 NPJ Quantum Inf. 2 15023 URL http://dx.doi.org/10.1038/npjqi.2015.
- [4] Fisher K A G, Broadbent A, Shalm L K, Yan Z, Lavoie J, Prevedel R, Jennewein T and Resch K J 2014 Nat. Commun. 5 3074 URL http://dx.doi.org/10.1038/ncomms4074
- [5] Aharonov D, Ben-Or M and Eban E 2008 arXiv preprint arXiv:0810.5375
- [6] Childs A M 2005 Quantum Inf. and Comput. 5 456–466
- [7] Dupuis F, Nielsen J B and Salvail L 2012 Actively secure two-party evaluation of any quantum operation Advances in Cryptology-CRYPTO 2012 (Lecture Notes in Computer Science vol 7417) (Springer) pp 794-811
- [8] Broadbent A, Gutoski G and Stebila D 2013 Quantum one-time programs Advances in Cryptology— CRYPTO 2013 (Lecture Notes in Computer Science vol 8043) (Springer) pp 344–360
- [9] Arrighi P and Salvail L 2006 Int. J. Quantum Inf. 4 883–898
- [10] Broadbent A, Fitzsimons J and Kashefi E 2009 Universal blind quantum computation 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009) (IEEE) pp 517–526

- [11] Barz S, Kashefi E, Broadbent A, Fitzsimons J F, Zeilinger A and Walther P 2012 Science 335 303–308
- [12] Abellan C, Amaya W, Domenech D, Muñoz P, Capmany J, Longhi S, Mitchell M W and Pruneri V 2016 Optica 3 989–994
- [13] Kraus B and Cirac J I 2001 Phys. Rev. A 63 062309
- [14] Zhou X Q, Ralph T C, Kalasuwan P, Zhang M, Peruzzo A, Lanyon B P and O'Brien J L 2011 Nat. Commun. 2 413
- [15] Araújo M, Feix A, Costa F and Brukner Č 2014 New J. Phys. 16 093026
- [16] Thompson J, Gu M, Modi K and Vedral V 2013 arXiv preprint arXiv:1310.2927
- [17] Lanyon B P, Barbieri M, Almeida M P, Jennewein T, Ralph T C, Resch K J, Pryde G J, OBrien J L, Gilchrist A and White A G 2009 Nature Physics 5 134–140
- [18] Lin Q and Li J 2009 Physical Review A **79** 022301
- [19] Lin Q and He B 2009 Physical Review A 80 042310
- [20] Lin Q, He B, Bergou J A and Ren Y 2009 Physical Review A 80 042311
- [21] Zhou X Q, Kalasuwan P, Ralph T C and O'Brien J L 2013 Nat. Photon. 7 223–228
- [22] Patel R B, Ho J, Ferreyrol F, Ralph T C and Pryde G J 2016 Science advances 2 e1501531
- [23] Khaneja N and Glaser S J 2001 Chemical Physics 267 11–23
- [24] Gui-Lu L 2006 Communications in Theoretical Physics 45 825
- [25] Long G L 2007 Quantum Information Processing 6 49–54
- [26] Wei S J, Ruan D and Long G L 2016 Scientific Reports 6 30727
- [27] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Phys. Rev. Lett. 70 1895
- [28] Chen P X, Zhu S Y and Guo G C 2006 Phys. Rev. A 74 032324
- [29] Wootters W K and Zurek W H 1982 Nature 299 802–803
- [30] Dieks D 1982 Physics Letters A **92** 271–272
- [31] Bužek V and Hillery M 1996 Physical Review A 54 1844
- [32] Gisin N and Massar S 1997 Physical review letters 79 2153
- [33] Ishizaka S and Hiroshima T 2008 Phys. Rev. Lett. 101 240501
- [34] Ishizaka S and Hiroshima T 2009 Phys. Rev. A 79 042306
- [35] Politi A, Cryan M J, Rarity J G, Yu S and O'brien J L 2008 Science 320 646-649
- [36] Carolan J, Harrold C, Sparrow C, Martín-López E, Russell N J, Silverstone J W, Shadbolt P J, Matsuda N, Oguma M, Itoh M et al. 2015 Science 349 711–716
- [37] Wang J, Bonneau D, Villa M, Silverstone J W, Santagati R, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H et al. 2016 Optica 3 407–413
- [38] Dawson C M and Nielsen M A 2005 arXiv:quant-ph/0505030
- [39] Childs A M and Wiebe N 2012 Quantum Inf. Comput. 12 901-924 ISSN 1533-7146 URL http://dl.acm.org/citation.cfm?id=2481569.2481570
- [40] Kothari R 2014 Efficient algorithms in quantum query complexity Ph.D. thesis University of Waterloo
- [41] Berry D W, Childs A M and Kothari R 2015 Hamiltonian simulation with nearly optimal dependence on all parameters *Proceedings of the 56th IEEE Symposium on Foundations of Computer Science (FOCS 2015)* (IEEE) pp 792–809
- [42] Childs A M, Kothari R and Somma R D 2015 arXiv preprint arXiv:1511.02306
- [43] Harrow A W, Hassidim A and Lloyd S 2009 Physical review letters 103 150502
- [44] Nielsen M A and Chuang I L 2010 Quantum computation and quantum information (Cambridge University Press)
- [45] Khaneja N 2016 arXiv preprint arXiv:1607.02692
- [46] Rangarajan R, Goggin M and Kwiat P 2009 Opt. Express 17 18920–18933

Supplementary Material for: Quantum processing by remote quantum control

S1. Evolution for the proposed LCC

Here we show the step-by-step evolution of the LCC described in main text. The $(n \times d)$ -dimensional target subspace T decomposes into n d-dimensional subspaces, with the j^{th} subspace spanned by basis elements $|jd\rangle_T, \dots, |(j+1)d-1\rangle_T$. The 0^{th} subspace, spanned by the basis states $|0\rangle_T, |1\rangle_T, \dots, |d-1\rangle_T$ and encodes the computational input state, while all other subspaces have zero amplitudes. Therefore, the initial state for T is of the form

$$|\Psi_{ext}\rangle_T = \sum_{j=0}^{d-1} \beta_j |j\rangle_T + \sum_{j=d}^{nd-1} 0|j\rangle_T, \tag{S1}$$

where d represents the dimension for the target computation, k represents the number of control qubits, and $n = 2^k$ (as defined in main text).

We define $|\Psi_{ext}\rangle_T^s$ $(s=0,1,\cdots,n-1)$ as

$$|\Psi_{ext}\rangle_T^s = \sum_{j=0}^{sd-1} 0|j\rangle_T + \sum_{j=sd}^{(s+1)d-1} \beta_j|j\rangle_T + \sum_{j=(s+1)d}^{nd-1} 0|j\rangle_T$$
 (S2)

where only the basis of the s^{th} subspace have non-zero amplitudes. The initial state $|\Psi_{ext}\rangle_T$ can then be represented as $|\Psi_{ext}\rangle_T^0$. $X^{(0,j)}$ exchanges corresponding basis elements between 0^{th} and j^{th} subspaces, which equivalently swaps the two states $|\Psi_{ext}\rangle_T^0$ and $|\Psi_{ext}\rangle_T^j$. The sum operation $V_{sum} = \bigoplus_{j=0}^{n-1} V_j^{(j)}$ is an $n \times d$ dimension quantum operation, where $V_j^{(j)}$ implements the d-dimension quantum operation V_j on j^{th} subspace of T.

The k-qubit control $|\phi\rangle_C$ can be expanded as follows (note $n=2^k$),

$$|\phi\rangle_C = \sum_{j=0}^{n-1} \alpha_j |j\rangle = \alpha_0 |00\cdots 0\rangle + \alpha_1 |00\cdots 1\rangle + \cdots + \alpha_{n-1} |11\cdots 1\rangle.$$
 (S3)

The evolution of the LCC can be obtained as follows, with time going from left to right:

$$\begin{split} &|\phi\rangle_{C} |\Psi_{ext}\rangle_{T}^{0} \\ &= \alpha_{0} \overbrace{|00\cdots0\rangle}^{k} |\Psi_{ext}\rangle_{T}^{0} + \alpha_{1} \overbrace{|00\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{0} + \cdots + \alpha_{n-1} \overbrace{|11\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{0} \qquad (S4) \\ &\rightarrow \alpha_{0} \overbrace{|00\cdots0\rangle}^{k} |\Psi_{ext}\rangle_{T}^{0} + \alpha_{1} \overbrace{|00\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{1} + \cdots + \alpha_{n-1} \overbrace{|11\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{n-1} \qquad (S5) \\ &\rightarrow \alpha_{0} \overbrace{|00\cdots0\rangle}^{k} |\Psi_{ext}\rangle_{T}^{0} + \alpha_{1} \overbrace{|00\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{1} + \cdots + \alpha_{n-1} \overbrace{|11\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{n-1} \qquad (S6) \\ &= \alpha_{0} \overbrace{|00\cdots0\rangle}^{k} |\Psi_{ext}\rangle_{T}^{V_{0}^{(0)},0} + \alpha_{1} \overbrace{|00\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{V_{1}^{(1)},1} + \cdots + \alpha_{n-1} \overbrace{|11\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{V_{n-1}^{(n-1)},n-1} \qquad (S7) \\ &\rightarrow \alpha_{0} \overbrace{|00\cdots0\rangle}^{k} |\Psi_{ext}\rangle_{T}^{V_{0}^{(0)},0} + \alpha_{1} \overbrace{|00\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{V_{1}^{(0)},0} + \cdots + \alpha_{n-1} \overbrace{|11\cdots1\rangle}^{k} |\Psi_{ext}\rangle_{T}^{V_{n-1}^{(n)},0} \qquad (S8) \\ &\rightarrow \frac{1}{2^{k/2}} \overbrace{|00\cdots0\rangle}^{k} \left(\alpha_{0} |\Psi_{ext}\rangle_{T}^{V_{0}^{(0)},0} + \alpha_{1} |\Psi_{ext}\rangle_{T}^{V_{1}^{(0)},0} + \cdots + \alpha_{n-1} |\Psi_{ext}\rangle_{T}^{V_{n-1}^{(0)},0}\right) + \cdots + \frac{1}{2^{k/2}} \overbrace{|00\cdots1\rangle}^{k} \left(\alpha_{0} |\Psi_{ext}\rangle_{T}^{V_{0}^{(0)},0} - \alpha_{1} |\Psi_{ext}\rangle_{T}^{V_{1}^{(0)},0} + \cdots + \alpha_{n-1} |\Psi_{ext}\rangle_{T}^{V_{n-1}^{(0)},0}\right) + \cdots + \frac{1}{2^{k/2}} \overbrace{|11\cdots1\rangle}^{k} \left(\alpha_{0} |\Psi_{ext}\rangle_{T}^{V_{0}^{(0)},0} - \alpha_{1} |\Psi_{ext}\rangle_{T}^{V_{1}^{(0)},0} + \cdots + (-1)^{k} \alpha_{n-1} |\Psi_{ext}\rangle_{T}^{V_{n-1}^{(0)},0}\right) \qquad (S9) \end{aligned}$$

Note here that $|\Psi_{ext}\rangle_T^{V_j^{(k)},k}$ $(j,k=0,1,\cdots,n-1)$ means that the *d*-dimension operation V_j acts on the k^{th} subspace of T where T has the state of $|\Psi_{ext}\rangle_T^k$.

When the k control qubits are all measured to be 0 in the computational basis, the resulting state of T is obtained as

$$\alpha_{0}|\Psi_{ext}\rangle_{T}^{V_{0}^{(0)},0} + \alpha_{1}|\Psi_{ext}\rangle_{T}^{V_{1}^{(0)},0} + \dots + \alpha_{n-1}|\Psi_{ext}\rangle_{T}^{V_{n-1}^{(0)},0}$$

$$= \left(\sum_{j=0}^{n-1} \alpha_{j} V_{j}^{(0)}\right) \sum_{j=0}^{d-1} \beta_{j}|j\rangle_{T} + \sum_{j=d}^{nd-1} 0|j\rangle_{T}.$$
(S10)

This shows that the operation $U = \sum_{j=0}^{n-1} \alpha_j V_j$ is implemented on the state $|\psi\rangle = \sum_{j=0}^{d-1} \beta_j |j\rangle_T$ which lies in the 0^{th} subspace of T. The success probability of this LCC is $(\frac{1}{2^{k/2}})^2 = \frac{1}{n}$, decreasing polynomially with the length of the gate sequence for operations being combined.

S2. Linear decomposition of unitary quantum operation

Here we present more details of the linear decomposition of a unitary quantum operation. We start by showing the explicit linear decomposition of universal two-qubit quantum operation. It has been shown that an arbitrary two-qubit operation $U_{SU(4)} \in SU(4)$ can be decomposed as [1]:

$$U_{SU(4)} = (U_1 \otimes V_1)U_D(U_2 \otimes V_2), \tag{S11}$$

where U_1 , V_1 , U_2 and V_2 are single-qubit quantum gates, and U_D is a non-factorable two-qubit gate responsible for the non-local characteristic of the gate U, which is given by

$$U_D = \exp(-i(k_1\sigma_x \otimes \sigma_x + k_2\sigma_y \otimes \sigma_y + k_3\sigma_z \otimes \sigma_z)), \tag{S12}$$

where k_i are real numbers, and σ_x , σ_y and σ_z are Pauli matrices. Define a matrix M as

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & i & 1 & 0 \\ 0 & i & -1 & 0 \\ 1 & 0 & 0 & -i \end{pmatrix}, \tag{S13}$$

and then $U_1 \otimes V_1$ and $U_2 \otimes V_2$ can be obtained as

$$U_1 \otimes V_1 = MLM^{\dagger} \tag{S14}$$

$$U_2 \otimes V_2 = MRM^{\dagger} \tag{S15}$$

where L and R are two real orthogonal matrices that are obtained by performing the simultaneous singular value decomposition for $U'_R = \text{Real}(M^{\dagger}U_{SU(4)}M)$ (real part) and $U'_I = \text{Imag}(M^{\dagger}U_{SU(4)}M)$ (imaginary part), together with two non-negatively real diagonal matrices D_R and D_I . They satisfy that

$$D_R = L^{\dagger} U_R' R, \tag{S16}$$

$$D_I = L^{\dagger} U_I' R. \tag{S17}$$

 U_D and further k_i 's can be obtained through

$$U_D = M(D_R + iD_I)M^{\dagger}. \tag{S18}$$

A step-by-step procedure for obtaining the decomposition result in Eq. (S11) is given in ref [2].

Consider the facts that

$$\exp(iAx) = \cos(x)I + i\sin(x)A \tag{S19}$$

where x is an arbitrary real number and A is a matrix satisfying $A^2 = I$ [3] and

$$\sigma_x \sigma_y = -\sigma_y \sigma_x = i\sigma_z, \tag{S20}$$

$$\sigma_y \sigma_z = -\sigma_z \sigma_y = i\sigma_x, \tag{S21}$$

$$\sigma_z \sigma_x = -\sigma_x \sigma_z = i\sigma_y. \tag{S22}$$

 $U_{SU(4)}$ can be rewritten into the following form:

$$U_{SU(4)} = (U_1 \otimes V_1) \cdot (\alpha_0 I \otimes I + \alpha_1 \sigma_x \otimes \sigma_x + \alpha_2 \sigma_y \otimes \sigma_y + \alpha_3 \sigma_z \otimes \sigma_z) \cdot (U_2 \otimes V_2)$$

$$= \alpha_0 U_1 I U_2 \otimes V_1 I V_2 + \alpha_1 U_1 \sigma_x U_2 \otimes V_1 \sigma_x V_2 + \alpha_2 U_1 \sigma_y U_2 \otimes V_1 \sigma_y V_2 + \alpha_3 U_1 \sigma_z U_2 \otimes V_1 \sigma_z V_2.$$
(S23)

where α_0 , α_1 , α_2 and α_3 are complex coefficients defined as

$$\alpha_0 = (\cos(k_1)\cos(k_2)\cos(k_3) - i\sin(k_1)\sin(k_2)\sin(k_3)),$$

$$\alpha_1 = (\cos(k_1)\sin(k_2)\sin(k_3) - i\sin(k_1)\cos(k_2)\cos(k_3)),$$

$$\alpha_2 = (\sin(k_1)\cos(k_2)\sin(k_3) - i\cos(k_1)\sin(k_2)\cos(k_3)),$$

$$\alpha_3 = (\sin(k_1)\sin(k_2)\cos(k_3) - i\cos(k_1)\cos(k_2)\sin(k_3)).$$
(S24)

This shows that an arbitrary two-qubit operation can be decomposed into a linear combiantion of four terms, each of which is a tensor product of two single-qubit quantum gates. Similarly, an arbitrary three-qubit quantum operation $U_{SU(8)} \in SU(8)$ can be decomposed as [4]:

$$U_{SU(8)} = (A_4 \otimes B_4) N_2 (A_3 \otimes B_3) M(A_2 \otimes B_2) N_1 (A_1 \otimes B_1), \tag{S25}$$

where A_i is two-qubit gate, B_i is single-qubit gate, N_1 , N_2 and M are defined as

$$N_{k} = \exp(i(\alpha_{0}^{(k)}\sigma_{x} \otimes \sigma_{x} \otimes \sigma_{z} + \alpha_{1}^{(k)}\sigma_{y} \otimes \sigma_{y} \otimes \sigma_{z} + \alpha_{2}^{(k)}\sigma_{z} \otimes \sigma_{z} \otimes \sigma_{z}))$$
(S26)

$$M = \exp(i(\beta_{0}\sigma_{x} \otimes \sigma_{x} \otimes \sigma_{x} + \beta_{1}\sigma_{y} \otimes \sigma_{y} \otimes \sigma_{x} + \beta_{2}\sigma_{z} \otimes \sigma_{z} \otimes \sigma_{x} + \beta_{3}I \otimes I \otimes \sigma_{x})).$$
(S27)

Here $\alpha_i^{(k)}$ and β_j are real numbers. Applying similar algebra as that used in the case of two-qubit operations, we can obtain the linear-combination decomposition form of $U_{SU(8)}$ where each of term is a tensor-product of three single-qubit gates.

More generally, an arbitrary n-qubit quantum operation $U \in SU(2^n)$ can be decomposed as

$$U = K_1 A K_2, \tag{S28}$$

where $K_1, K_2 \in SU(2^{n-1}) \otimes SU(2^{n-1}) \otimes U(1)$ and $A \in \exp(h)$, with h being a Cartan subalgebra of the Riemannian symmetric space $SU(2^n)/SU(2^{n-1}) \otimes SU(2^{n-1}) \otimes U(1)$ [5]. A recursive formula can then be obtained by further decomposing K_1 and K_2 in terms of the elements of $SU(2^{n-2}) \otimes SU(2^{n-2}) \otimes U(1)$ and so on [5]. Finally, we can rewrite the given n-qubit operation into a linear combination of tensor products of n single-qubit gates. It is easy to find that such a linear-combination decomposition is not efficient—it generally requires exponentially many linear terms.

However, in some cases, the number of the linear terms for the decomposition of a given operation is much less. We have mentioned that in the main text an arbitrary controlled-unitary operation can be rewritten into the linear combination of four terms.

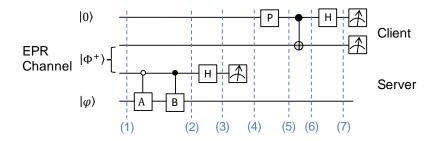


Figure S1. Linear-combining two known operations by remote one-qubit control. $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is the EPR state used for quantum teleportation. $|\varphi\rangle$ is a quantum regiseter state used for the input of quantum computation, and A and B are two corresponding quantum operations with the same size. P represents the single-qubit operation to configure the one-qubit control state: $\alpha |0\rangle + \beta |1\rangle$.

Here is another example: when the coefficients $\alpha_i^{(k)}$ (i = 0, 1, 2; k = 1, 2), β_1 , β_2 and β_3 in Eq. (S26) and (S27) are all zeros, the corresponding linear decomposition of $U_{SU(8)}$ will include only two terms as follows:

$$U_{SU(8)} = (A_4 A_3 \otimes B_4 B_3) \exp(i\beta_0 \sigma_x^{\otimes 3}) (A_2 A_1 \otimes B_2 B_1)$$

= $\cos(\beta_0) (A_4 A_3 A_2 A_1) \otimes (B_4 B_3 B_2 B_1) + i \sin(\beta_0) (A_4 A_3 \sigma_x^{\otimes 2} A_2 A_1) \otimes (B_4 B_3 \sigma_x B_2 B_1)$
(S29)

where A_i and B_i $(i=1,\cdots,4)$ are defined as in Eq. (S25) and $\sigma_x^{\otimes 3} = \sigma_x \otimes \sigma_x \otimes \sigma_x$.

S3. Security analysis of the proposed protocol

The security of our proposed protocol has been discussed in the main text. Here we present more details of the security analysis for one-qubit control quantum processing (see Figure 3 in the main text): we have chosen the case where the client only sends a one-qubit control state to the server to linearly combine two quantum operations A and B. We also assume that A and B are not black-box operations to the server, and thus the server can implement the linear-combination operation using the circuit shown in Fig.1(A) in main text. This assumption does not weaken our security arguments, since in our protocol the privacy is kept just through hiding the linear coefficients. We assume the server runs the LCC before the client teleports the control state. The corresponding circuit is shown in Fig. S1, with the step-by-step evolution states being labeled. The evolution of the circuit is then given as follows.

$$(1): \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 |0\rangle_3 |\varphi\rangle + |0\rangle_1 |1\rangle_2 |1\rangle_3 |\varphi\rangle)$$
(S30)

$$(2): \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 |0\rangle_3 A |\varphi\rangle + |0\rangle_1 |1\rangle_2 |1\rangle_3 B |\varphi\rangle)$$
(S31)

(3):
$$\frac{1}{2}(|0\rangle_{1}|0\rangle_{2}|0\rangle_{3}A|\varphi\rangle + |0\rangle_{1}|0\rangle_{2}|1\rangle_{3}A|\varphi\rangle + |0\rangle_{1}|1\rangle_{2}|0\rangle_{3}B - |0\rangle_{1}|0\rangle_{2}|1\rangle_{3}B|\varphi\rangle)$$
(S32)

$$(4): \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 A |\varphi\rangle + |0\rangle_1 |1\rangle_2 B |\varphi\rangle)$$
(S33)

$$(5): \frac{1}{\sqrt{2}} (\alpha |0\rangle_1 |0\rangle_2 A |\varphi\rangle + \beta |1\rangle_1 |0\rangle_2 A |\varphi\rangle + \alpha |0\rangle_1 |1\rangle_2 B |\varphi\rangle + \beta |1\rangle_1 |1\rangle_2 B |\varphi\rangle)$$
(S34)

(6):
$$\frac{1}{\sqrt{2}} (\alpha |0\rangle_1 |0\rangle_2 A |\varphi\rangle + \beta |1\rangle_1 |1\rangle_2 A |\varphi\rangle + \alpha |0\rangle_1 |1\rangle_2 B |\varphi\rangle + \beta |1\rangle_1 |0\rangle_2 B |\varphi\rangle)$$
(S35)

$$(7): \frac{1}{2}(\alpha |0\rangle_{1} |0\rangle_{2} A |\varphi\rangle + \alpha |1\rangle_{1} |0\rangle_{2} A |\varphi\rangle + \beta |0\rangle_{1} |1\rangle_{2} A |\varphi\rangle - \beta |1\rangle_{1} |1\rangle_{2} A |\varphi\rangle + \alpha |0\rangle_{1} |1\rangle_{2} B |\varphi\rangle + \alpha |1\rangle_{1} |1\rangle_{2} B |\varphi\rangle + \beta |0\rangle_{1} |0\rangle_{2} B |\varphi\rangle - \beta |1\rangle_{1} |0\rangle_{2} B |\varphi\rangle)$$
(S36)

Here, the subscripts "1", "2" and "3" represent the client's local qubit and the EPR qubits owned by the client and the server respectively, the same below. When the client measures the qubit 1 and qubit 2 to be "0" in the computational basis, the state of the quantum register ($|\varphi\rangle$) will be $(\alpha A + \beta B) |\varphi\rangle$. In this case, the server measures the control qubit before the client prepares it, and thus the linear coefficients are kept hidden from the server.

Next, we consider the case where the server lies to the client that he had measured the qubit 3 but actually he did not. The corresponding circuit is shown in Fig. S2, with step-by-step evolution state being labeled. The evolution of this circuit is then given as follows.

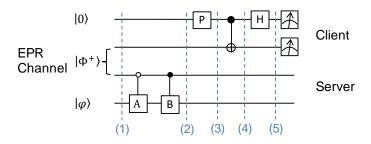


Figure S2. Server lies in the process of linear-combining two known operations by remote one-qubit control. $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is the EPR state used for quantum teleportation. $|\varphi\rangle$ is a quantum regiseter state used for the input of quantum computation, and A and B are two corresponding quantum operations with the same size. P represents the single-qubit operation to configure the one-qubit control state: $\alpha |0\rangle + \beta |1\rangle$.

$$(1): \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 |0\rangle_3 |\varphi\rangle + |0\rangle_1 |1\rangle_2 |1\rangle_3 |\varphi\rangle)$$
(S37)

$$(2): \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 |0\rangle_3 A |\varphi\rangle + |0\rangle_1 |1\rangle_2 |1\rangle_3 B |\varphi\rangle)$$
(S38)

$$(3): \frac{1}{\sqrt{2}} (\alpha |0\rangle_{1} |0\rangle_{2} |0\rangle_{3} A |\varphi\rangle + \beta |1\rangle_{1} |0\rangle_{2} |0\rangle_{3} A |\varphi\rangle + \alpha |0\rangle_{1} |1\rangle_{2} |1\rangle_{3} B |\varphi\rangle + \beta |1\rangle_{1} |1\rangle_{2} |1\rangle_{3} B |\varphi\rangle)$$

$$(S39)$$

$$(4): \frac{1}{\sqrt{2}} (\alpha |0\rangle_{1} |0\rangle_{2} |0\rangle_{3} A |\varphi\rangle + \beta |1\rangle_{1} |1\rangle_{2} |0\rangle_{3} A |\varphi\rangle + \alpha |0\rangle_{1} |1\rangle_{2} |1\rangle_{3} B |\varphi\rangle + \beta |1\rangle_{1} |0\rangle_{2} |1\rangle_{3} B |\varphi\rangle)$$

$$(S40)$$

$$(5): \frac{1}{2}(\alpha |0\rangle_{1} |0\rangle_{2} |0\rangle_{3} A |\varphi\rangle + \alpha |1\rangle_{1} |0\rangle_{2} |0\rangle_{3} A |\varphi\rangle + \beta |0\rangle_{1} |1\rangle_{2} |0\rangle_{3} A |\varphi\rangle - \beta |1\rangle_{1} |1\rangle_{2} |0\rangle_{3} A |\varphi\rangle + \alpha |0\rangle_{1} |1\rangle_{2} |1\rangle_{3} B |\varphi\rangle + \alpha |1\rangle_{1} |1\rangle_{2} |1\rangle_{3} B |\varphi\rangle + \beta |0\rangle_{1} |0\rangle_{2} |1\rangle_{3} B |\varphi\rangle - \beta |1\rangle_{1} |0\rangle_{2} |1\rangle_{3} B |\varphi\rangle)$$

$$(S41)$$

When the client measures the qubit 1 and qubit 2 to be "0" in the computational basis, the state of remaining qubits will be

$$|\Psi\rangle = \alpha |0\rangle_3 A |\varphi\rangle + \beta |1\rangle_3 B |\varphi\rangle.$$
 (S42)

Now we need to know if the server can extract the information of the control state without being found by the client. This requires that the server can extract the control state $|\phi\rangle_C = \alpha |0\rangle + \beta |1\rangle$ while the client obtains the correct result $(\alpha A + \beta B) |\varphi\rangle$. The server can only achieve this if there exists a quantum operation U_s that satisfies

$$(\alpha |0\rangle + \beta |1\rangle)(\alpha A + \beta B) |\varphi\rangle = U_s(\alpha |0\rangle A |\varphi\rangle + \beta |1\rangle B |\varphi\rangle).$$
 (S43)

Such an U_s does not exist for unknown α and β , since the no-cloning theorem forbids faithful copying of unknown quantum states.

We can see this more clearly from an explicit example. Suppose A = I, B = X and $|\varphi\rangle = |0\rangle$, then the state that the server expected is

$$|\Phi\rangle_{exp} = (\alpha |0\rangle + \beta |1\rangle)(\alpha A + \beta B) |\varphi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \beta\alpha \\ \beta^2 \end{pmatrix} \quad (S44)$$

The state $|\Psi\rangle$ will be

$$|\Psi\rangle = \alpha |0\rangle_3 I |0\rangle + \beta |1\rangle_3 X |0\rangle = \alpha |0\rangle_3 |0\rangle + \beta |1\rangle_3 |1\rangle = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{pmatrix}$$
 (S45)

Comparing Eqs. (S44) and (S45), there is no U_s that satisfies $|\Phi\rangle_{exp} = U_s |\Psi\rangle$ for general α and β .

S4. Linear decomposition of single-qubit gate

An arbitrary single-qubit quantum operation $U_{SU(2)} \in SU(2)$ can be written into the form [6,7]

$$U_{SU(2)} = \exp(-i(d_1\sigma_x + d_2\sigma_y + d_3\sigma_z))$$
 (S46)

where d_i (i = 1, 2, 3) is real number. We can rewrite $U_{SU(2)}$ in the linear-combination form as follows

$$U_{SU(2)} = (\cos(d_1)I - i\sin(d_1)\sigma_x)(\cos(d_2)I - i\sin(d_2)\sigma_y)(\cos(d_3)I - i\sin(d_3)\sigma_z)$$
(S47)
= $\alpha_0I + \alpha_1\sigma_x + \alpha_2\sigma_y + \alpha_3\sigma_z$

where α_0 , α_1 , α_2 and α_3 are given by

$$\alpha_0 = \cos(d_1)\cos(d_2)\cos(d_3) - \sin(d_1)\sin(d_2)\sin(d_3), \tag{S48}$$

$$\alpha_1 = -i(\cos(d_1)\sin(d_2)\sin(d_3) + \sin(d_1)\cos(d_2)\cos(d_3)), \tag{S49}$$

$$\alpha_2 = -i(\cos(d_1)\sin(d_2)\cos(d_3) - \sin(d_1)\cos(d_2)\sin(d_3)), \tag{S50}$$

$$\alpha_3 = -i(\cos(d_1)\cos(d_2)\sin(d_3) + \sin(d_1)\sin(d_2)\cos(d_3)). \tag{S51}$$

i.e., an arbitrary single-qubit unitary operation can be decomposed as a linear combination of four terms: the identity and three Pauli matrices.

S5. Further experimental results

When the two single-qubit gates A and B are set to be

$$A = \begin{pmatrix} \frac{1-i}{\sqrt{2}} & 0\\ 0 & \frac{-1-i}{\sqrt{2}} \end{pmatrix}, B = \begin{pmatrix} 0 & \frac{1+i}{\sqrt{2}}\\ \frac{1-i}{\sqrt{2}} & 0 \end{pmatrix}, \tag{S52}$$

the client can always implement unitary operation $U = \alpha A + \beta B$ by teleporting an arbitrary one-qubit control state $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ with α and β being real numbers. By just using a single half-waveplate in P, the polarization state of the photon on the client's side, i.e., $|\phi\rangle$, can be configured into any single-qubit state with real amplitudes. We set the angle of half-waveplate into 0°, 11.25°, 22.5°, 45°, 56.25°, 67.5°, 78.75°, and thus, eight different unitary operations denoted as $U_i(i=1,2,\cdots,8)$ are implemented by the client. We performed quantum process tomography for each operation and reconstructed their process matrices from experimental data using maximum-likelihood estimation technique. The reconstructed process matrices are shown in Fig. S3, with corresponding process fidelities. The errors are estimated by adding random noise to the raw date obtained experimentally assuming Poissonian statistics, and then performing the reconstructions many times.

We also tested other configurations of A and B: A = I (Identity), B = Z (Pauli-Z) and A = X (Pauli-X), B = Z. By transmitting different one-qubit control state $|\phi\rangle$, the client implements various quantum operations on the server's side as follows:

$$U_9 = \frac{1}{\sqrt{2}}I + \frac{i}{\sqrt{2}}Z, \ U_{10} = \frac{1}{\sqrt{2}}I - \frac{i}{\sqrt{2}}Z, \ U_{11} = \frac{1}{\sqrt{2}}X + \frac{1}{\sqrt{2}}Z, \ U_{12} = \frac{1}{\sqrt{2}}X + \frac{i}{\sqrt{2}}Z.$$
(S53)

The reconstructed process matrices for these operations are shown in Fig. S4, with corresponding process fidelities. The errors are estimated in the same way as mentioned above.

- [1] Kraus B and Cirac J I 2001 Phys. Rev. A 63 062309
- [2] Tucci R R 2005 arXiv preprint quant-ph/0507171
- [3] Nielsen M A and Chuang I L 2010 Quantum computation and quantum information (Cambridge University Press)
- [4] Vatan F and Williams C P 2004 arXiv preprint quant-ph/0401178
- [5] Khaneja N and Glaser S J 2001 Chemical Physics 267 11–23
- [6] Khaneja N and Glaser S 2000 arXiv preprint quant-ph/0010100
- [7] Chatzisavvas K C, Chadzitaskos G, Daskaloyannis C and Schirmer S 2009 Physical Review A 80 052329

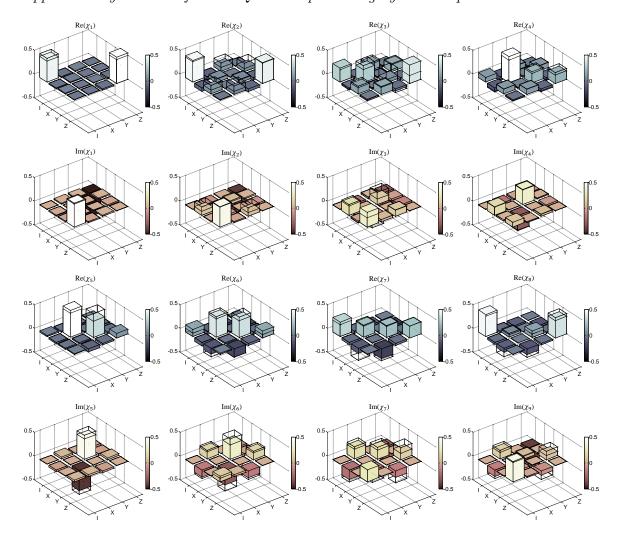


Figure S3. Experimental reconstructed χ matrices with ideal theoretical predictions overlaid: A single half-waveplate enables preparation of arbitrary one-qubit quantum control state $|\phi\rangle$ with real amplitudes. By setting half-waveplate angle to be 0°, 11.25°, 22.5°, 33.75°, 45°, 56.25°, 67.5° and 78.75°, $|\phi\rangle$ will be the state $|0\rangle$, 0.9239 $|0\rangle$ + 0.3827 $|1\rangle$, 0.7071 $|0\rangle$ + 0.7071 $|1\rangle$, 0.3827 $|0\rangle$ + 0.9239 $|1\rangle$, $|1\rangle$,

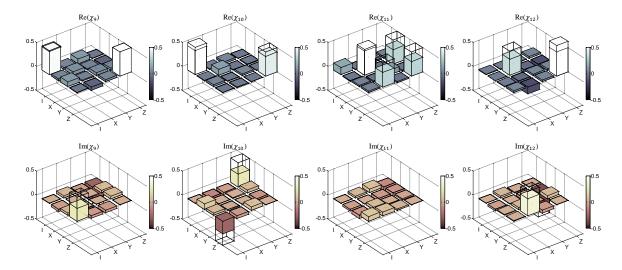


Figure S4. Experimental reconstructed χ matrices with ideal theoretical predictions overlaid: Four quantum operations $U_9 = \frac{1}{\sqrt{2}}I + \frac{i}{\sqrt{2}}Z$, $U_{10} = \frac{1}{\sqrt{2}}I - \frac{i}{\sqrt{2}}Z$, $U_{11} = \frac{1}{\sqrt{2}}X + \frac{1}{\sqrt{2}}Z$ and $U_{12} = \frac{1}{\sqrt{2}}X + \frac{i}{\sqrt{2}}Z$ are implemented. Here U_9 , U_{10} and U_{11} are unitary operations. U_{12} is a non-unitary operation, which can filter out $|L\rangle (= (|0\rangle - i|1\rangle)/\sqrt{2})$ and project all other basis state onto $|L\rangle$. The maximum-likelihood technique was used to reconstruct the χ matrices from the experimental data. The matrix χ_i $(i = 9, \dots, 12)$ corresponds to the operation U_i $(i = 9, \dots, 12)$. The obtained fidelities are $91.05\pm1.51\%$, $90.16\pm1.91\%$, $91.67\pm0.62\%$ and $88.56\pm1.58\%$ respectively.