Experimental Blind Quantum Computing for a Classical Client

He-Liang Huang,[1,2,3] Qi Zhao,[4] Xiongfeng Ma,[4,*] Chang Liu,[1,2] Zu-En Su,[1,2] Xi-Lin Wang,[1,2] Li Li,[1,2,†] Nai-Le Liu,[1,2,‡] Barry C. Sanders,[1,2,5,6] Chao-Yang Lu,[1,2,§] and Jian-Wei Pan[1,2]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2]*CAS-Alibaba Quantum Computing Laboratory, CAS Centre for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[3]*Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou Information Science and Technology Institute, Zhengzhou, Henan 450000, China*

[4]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

[5]*Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*

[6]*Program in Quantum Information Science, Canadian Institute for Advanced Research, Toronto, Ontario M5G 1M1, Canada*

(Received 13 February 2017; published 2 August 2017)

To date, blind quantum computing demonstrations require clients to have weak quantum devices. Here we implement a proof-of-principle experiment for completely classical clients. Via classically interacting with two quantum servers that share entanglement, the client accomplishes the task of having the number 15 factorized by servers who are denied information about the computation itself. This concealment is accompanied by a verification protocol that tests servers' honesty and correctness. Our demonstration shows the feasibility of completely classical clients and thus is a key milestone towards secure cloud quantum computing.

DOI: 10.1103/PhysRevLett.119.050503

Whereas quantum computers could exponentially outperform classical computers for certain computational tasks, inaccessibility due to implementation complexity would hinder widespread adoption of quantum computing. Thus, quantum computation is increasingly being performed "in the cloud," such as IBM's 5-qubit quantum cloud service [1]. In this approach, quantum computing is outsourced from a client with classical hardware to a server who possesses expensive quantum hardware. Considering the types of applications to which quantum computing is likely to be applied, imformation security is important as clients may wish to keep the computation perfectly secret from untrusted servers implementing the quantum computation.

A solution to this issue is offered by blind quantum computing (BQC) [2], which is a quantum cryptographic protocol that enables a classical client with limited quantum technology to delegate a computation to the quantum server(s) without leaking any information about her computation to the server(s). Thus far various BQC protocols have been proposed [2–15], and some proof-of-principle experiments have been performed with photonic qubits [16–20]. However, all these experimental demonstrations only support quasiclassical clients. That is, the clients require the ability to prepare or measure single-qubit states, but wide use of quantum computing on the cloud would be much more attractive if clients did not require the ability to perform quantum tasks. Although using only classical communication between a classical client and a single quantum server may be infeasible for secure BQC [21], classical communication between a classical client and multiquantum servers can work [14].

Besides security, verifiability is another important concern for BQC, i.e., the ability of a client to test whether or not the servers perform the task correctly and honestly. As the complexity of quantum many-body systems scales up, verifiability becomes a major experimental challenge, not only in BQC, but also in quantum chemistry [22], quantum simulation [23], boson sampling [24], and other quantum algorithms. Thus, a verification protocol for BQC is significant not only as a cryptographic protocol but also for exploring the relation between quantum physics and computer science.

Here we demonstrate a proof-of-principle implementation of BQC for completely classical clients. In our experiment, we realize Shor's algorithm [25] for factorizing $N = 15$ via the framework of verifiable BQC based on the Reichardt, Unger, and Vazirani protocol [14]. The scheme employs quantum gate teleportation for computation and combines the rigidity of Clauser-Horne-Shimony-Holt (CHSH) tests [14] and stabilizer tests for verification, thereby providing a method for a client to control quantum servers classically.

Suppose we are given two quantum servers, Alice and Bob, that share Einstein-Podolsky-Rosen (EPR) states but cannot communicate with each other (enforced, e.g., through spacelike separation of the devices). The client Charlie, holding a completely classical device, wants to delegate quantum computing to the remote servers without leaking any information about the computation to servers. He can decompose the circuit into two parts, computation A and computation B, and send these two tasks to Alice and Bob, respectively. Alice and Bob operate on their respective halves of the shared EPR states according to Charlie's commands and return to Charlie the measurement results. As Alice and Bob cannot communicate with each other, they cannot learn the results from each other, so this delegated computation is "blind," meaning that each server learns nothing more about the computation than its length [14].

For the task of factorizing N using Shor's algorithm, if we pick a random number a that is coprime to N, Shor's algorithm can yield the minimum integer r that satisfies $a^r \bmod N = 1$. From this period r, the prime factors of N are given by the greatest common divisor (GCD) of $a^{r/2} \pm 1$ and N, which is solved classically. The quantum circuit for $N = 15$ and $a = 11$ is shown in Fig. 1(a) [26]. In fact, The inverse QFT is unnecessary for any order-2^l circuit [27]. Moreover, two qubits $|0\rangle_2$ and $|1\rangle_4$ evolve trivially during the computation and thus can be omitted. This fact allows us to simplify the circuit to Fig. 1(b) by omitting obsolete qubits and operations marked by dotted lines in the circuit in Fig. 1(a).

To delegate the circuit in Fig. 1(b) to two remote quantum servers, Charlie decomposes it into two parts [see Fig. 1(c)] and sends the tasks to Alice and Bob, respectively. Each observable of Alice (Bob) has eigenvalues ± 1 such that each outcome $a_i(b_i)$ reported to Charlie takes values of ± 1, where i denotes the ith qubit of Alice (Bob). By design, computation A performs the first controlled-NOT (CNOT) gate of the circuit and prepares the third input state $|0\rangle$ for Bob. If Alice implements computation A honestly, Bob's share of EPR states collapses into $|\Psi\rangle|\beta\rangle$, where $|\Psi\rangle$ is one of the four Bell states, and $|\beta\rangle \in \{|0\rangle, |1\rangle\}$, according to Alice's results. In particular, when Alice reports $a_1 = a_2 = a_3 = 1$, Bob's state collapses into the desired resource state $|\phi\rangle = |\Phi^+\rangle|0\rangle$, where $|\Phi^\pm\rangle = (1/\sqrt{2})(|00\rangle \pm |11\rangle)$, which is equivalent to the state after the first CNOT gate in the circuit in Fig. 1(b). Then Bob implements computation B to achieve the second CNOT gate and measures his second qubit in the Pauli X basis to output the result of Shor's algorithm. Bob's remaining two qubits contribute nothing to the outcome and are both measured in the Pauli Z basis as they can be employed in the validation procedure described below.

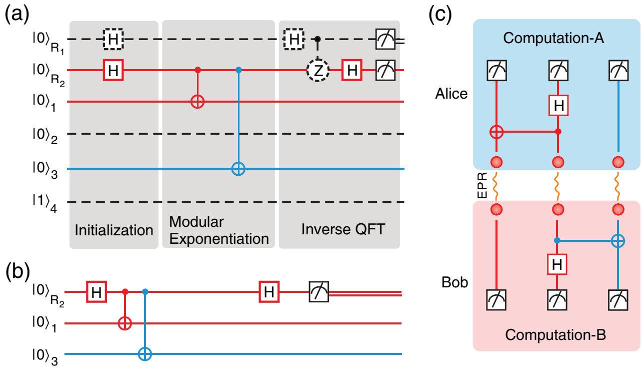

FIG. 1. Quantum circuit for factorizing $N = 15$ using Shor's algorithm. (a) Quantum circuit for $N = 15$ and $a = 11$ [26]. The modular exponential function is implemented by two CNOT gates, and the quantum Fourier transformation (QFT) is implemented by Hadamard rotations and two-qubit conditional-phase gates. (b) The simplified version of the circuit in (a), omitting the qubits and operations marked by dotted lines in (a). (c) The scheme of cloud quantum computing for factorizing $N = 15$. Each measurement is in the Z basis.

When performing such a computation on untrusted quantum servers, clients also wish to test the honesty of servers: did they implement the computation as promised? To realize this test, Charlie randomly switches tasks being implemented by Alice and Bob between the desired computation and "dummy" protocols. The dummy protocols are constructed such that Alice and Bob are unable to distinguish whether they are implementing the proper computation or the dummy, but such that Charlie is able to detect if the dummy tasks are being implemented dishonestly. Via repeated application of this randomized procedure, Charlie then determines whether Alice and Bob are being honest. Specifically, Charlie can randomly command the servers [see Fig. 2(a)] to implement the four subprotocols below:

1. Computation. As shown in Fig. 1(c), the computation is realized as the joint evolution of two isolated quantum servers. In our experiment, computation A and computation B can be compiled into the setup in Fig. 2(b), where the logical qubits $|0\rangle$ and $|1\rangle$ are encoded by horizontal (H) and vertical (V) polarizations of single photons, respectively. Instead of implementing the standard CNOT gate between the first and second qubits in computation A, Charlie can ask Alice to use a polarizing beam splitter to postselect events where there is exactly one photon exiting each output [the first two EPR states are transformed into $1/\sqrt{2}(|0\rangle_1^A|0\rangle_2^A|0\rangle_1^B|0\rangle_2^B + |1\rangle_1^A|1\rangle_2^A|1\rangle_1^B|1\rangle_2^B)$ after postselection, where A (B) represents Alice (Bob)], and measure these two photons in the Pauli X basis.

If Alice's reported results yield $a_1 a_2 = a_3 = 1$, then Bob's share of the EPR states collapses onto the desired state $|\phi\rangle$. The CNOT gate in computation B can be realized by combining three polarization-dependent beam splitters (PDBS)—an overlapping PDBS ($T_H = 1$ and $T_V = 1/3$), and two supplementary PDBSs ($T_V = 1$ and $T_H = 1/3$) at each exit port of the overlapping PDBS, along with two Hadamard gates (HWP) on the target photon before and after the PDBS [28]. The different treatment of the CNOT gates arises because Bob is required to complete the computation and convey the final outcomes, so he is instructed to implement the complete Bell measurement. However, Alice only needs to prepare resource states for Bob. As long as Alice can prepare the desired states, we deem her to be honest.

2. CHSH test. Charlie sends random bits $A \in \{0, 1\}$ and $B \in \{0, 1\}$ to Alice and Bob, respectively, which determines their measurement bases, and they respond with bits $M \in \{0, 1\}$ and $N \in \{0, 1\}$ corresponding to their binary measurement outcomes [see Fig. 2(c)]. In this test, Alice

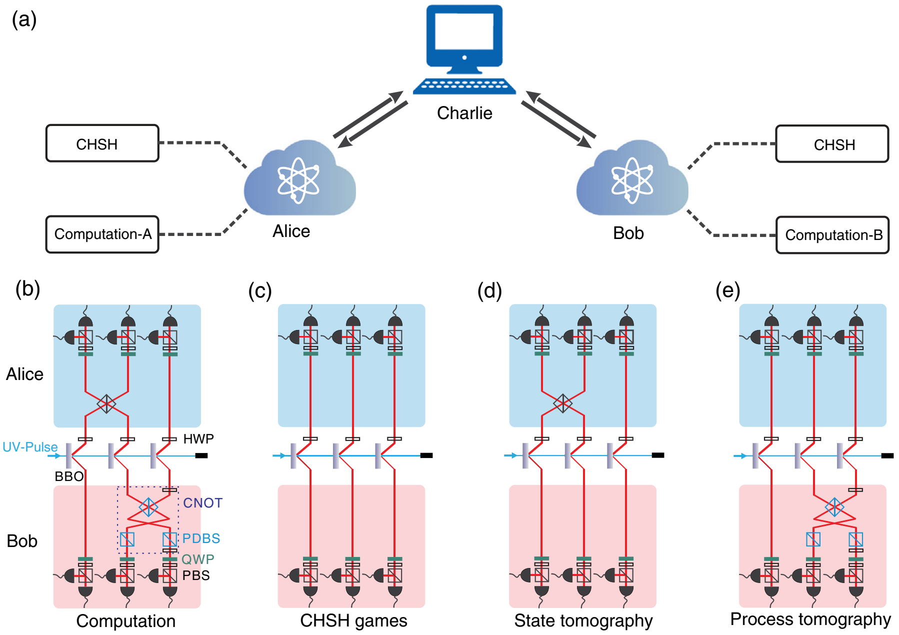

FIG. 2. Experimental setup. (a) Outline of the scheme. Charlie classically interacts with quantum servers Alice and Bob who share entanglement. Each of the quantum servers is randomly commanded to implement one of the two types of operations, CHSH and computation $A(B)$. (b) Computation setup. Ultraviolet laser pulses with a central wavelength of 394 nm, pulse duration of 150 fs, and repetition rate of 80 MHz pass through three β-barium borate (BBO) crystals to produce three polarization-entangled pairs $(1/\sqrt{2})(|H\rangle|V\rangle + |V\rangle|H\rangle)$. A half-wave plate (HWP) is placed at an arm of the entangled pairs to produce EPR states $(1/\sqrt{2})(|H\rangle|H\rangle + |V\rangle|V\rangle)$. To achieve good spatial and temporal overlap, all photons are spectrally filtered with 3-nm bandwidth filters. The final measurement results are then read out by single-photon detectors with dual-channel structure, which partially eliminates higher-order events. (c) CHSH test setup. (d) State tomography setup. (e) Process tomography setup.

and Bob "win" if $AB = M \oplus N$, and they can win with probability $\omega^* = \cos^2(\pi/8) \approx 0.854$ if Bob measures in the Pauli Z basis for $B = 0$ or Pauli X basis for $B = 1$, and if Alice measures $[Z + (-1)^A X]/\sqrt{2}$. According to Alice's and Bob's measurement outcomes a and b, i.e., ± 1, Charlie sets M and N to 0 or 1. In contrast, classical servers can win with probability at most 3/4. In our protocol, Charlie can also change the strategy to simultaneously swap the measurement bases of Alice and Bob; that is, Alice measures Z or X, and Bob measures $[Z + (-1)^B X]/\sqrt{2}$. According to the rigidity of the CHSH test [14], if the servers win with probability close to ω^*, the implement strategy is close to the ideal strategy. To ensure servers' honesty, Charlie runs n rounds of CHSH tests with both servers, and rejects if the servers fail to win at least $(\omega^* - \varepsilon)n$ rounds, where $\varepsilon = [1/(2\sqrt{2})]\sqrt{\log n/n}$ is the error threshold [29,30].

3. State tomography. Charlie asks Alice to implement computation A while running the CHSH test with Bob [see Fig. 2(d)]. If Alice honestly implements the command, Bob's state collapses to $|\Phi^{\pm}\rangle \otimes |\beta\rangle$. Bob is required to measure in the bases $X_1X_2Z_3$ or $Z_1Z_2Z_3$, where the first two bases X_1X_2 and Z_1Z_2 are the stabilizers for the Bell states, and Z_3 is the stabilizer of $|\beta\rangle$. In these cases, Bob's measurement outcomes are deterministic, depending on Alice's results. Thus, Charlie can test whether Alice is honest according Bob's measurement outcomes. If Bob reports the wrong stabilizer syndrome in even a single round, Charlie can reject. If Alice plays honestly, Charlie accepts with high probability.

4. Process tomography. Charlie asks Bob to implement computation B while running the CHSH test with Alice [see Fig. 2(e)]. If Bob honestly implements the command, Alice's state collapses to $|\beta\rangle|\Psi\rangle$. Alice is required to measure in the bases $Z_1X_2X_3$ or $Z_1Z_2Z_3$, where the last two bases, X_2X_3 and Z_2Z_3, are the Bell-state stabilizers, and the first basis Z_1 is the stabilizer of $|\beta\rangle$. Therefore, if Alice reports the wrong stabilizer syndrome in even a single round, Charlie can reject. If Bob plays honestly, Charlie accepts with high probability.

Charlie runs protocol 1 with a small probability η, and another three alternative protocols with probability $(1-\eta)/3$ so that servers are not aware of which protocol their measurements belong to. For instance, from Alice's perspective, she is entirely unaware whether Bob is implementing the CHSH test or computation B. From the CHSH test and stabilizer test, Charlie can determine whether the servers are being honest or not. The relationship among η, computational efficiency, and security parameters are analyzed in Supplemental Material [30].

To demonstrate the scheme, we employ polarization-entangled photons $|\Phi^+\rangle$ generated by spontaneous parametric down-conversion using a HWP-sandwiched β-barium borate (BBO) crystal [34]. For protocol 1, experimental

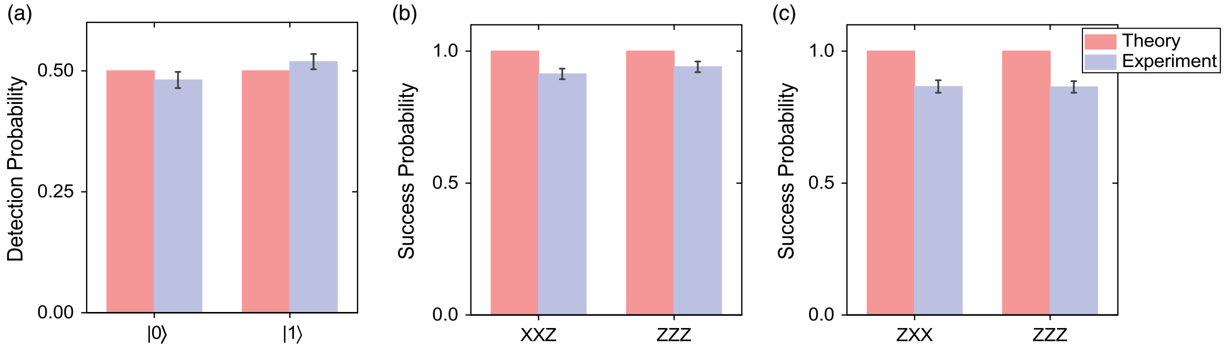

FIG. 3. Experimental results for honest Alice and Bob. (a) Output of quantum computing for factorizing $N = 15$, which is determined by the results of the second photon Bob observed in the subprotocol computation. Theoretical predictions and measured expectation values are shown as red and blue bars, respectively. (b) The probability that Alice passes the tests of state tomography when Bob measures in the $X_1X_2Z_3$ and $Z_1Z_2Z_3$ bases. (c) The probability that Bob passes the tests of process tomography when Alice measures in the $Z_1X_2X_3$ and $Z_1Z_2Z_3$ bases.

results are shown in Fig. 3(a). If Alice and Bob play honestly, then, with probability ~51.9%, the output is $|0\rangle$, corresponding to a failure. The remaining ~48.1% probability yields $|1\rangle$. Combining these with the known state of the redundant qubit $|0\rangle_{R_1}$ using classical processing yields the period $r = 2$. Thus, $\mathrm{GCD}(11^{2/2} \pm 1, 15) = 3$, 5, yielding a successful factorization. To quantify the performance of the CNOT operations realized by the PDBS, we measure process fidelity [35] for the CNOT gate as $0.87(2) \leq F_{\mathrm{process}} \leq 0.93(2)$ (see Supplemental Material [30] for details).

In our experiment, we run $n = 6000$ rounds of CHSH tests; then the error threshold is calculated as $\varepsilon = [1/(2\sqrt{2})]\sqrt{\log n/n} = 0.014$. Two honest quantum servers win with the probability ~0.846(6), from which ε is calculated as $\varepsilon = 0.007(6)$—below the error threshold. Thus, Charlie accepts the protocol (see Supplemental Material [30] for more detailed security analysis). On the other hand, if the quantum servers play dishonestly, for example, making the angle of the HWP in Bob's measurement setup always 5° higher than the target angle, they win with probability ~0.814(5) and thus $\varepsilon = 0.047(5)$, which is above the threshold, and Charlie rejects.

Protocol 3 is designed to monitor whether Alice honestly executes computation A. If Alice plays honestly, Bob's measurement outcomes are deterministic, depending on Alice's results. Figure 3(b) shows the theoretical and experimental results. The probability that Alice passes the tests is 0.92(2) and 0.94(2) when Bob measures in the $X_1X_2Z_3$ and $Z_1Z_2Z_3$ bases (see Supplemental Material [30] for details), respectively. To illustrate that the method can detect whether Alice is cheating, we consider two typical potential means of cheating: (1) If Alice deliberately reports the opposite outcomes of the first qubit, and the reported results yield $a_1a_2 = 1(-1)$, then Bob's share of the EPR state collapses into $|\Phi^-\rangle|0\rangle$ ($|\Phi^+\rangle|0\rangle$) instead of into $|\Phi^+\rangle|0\rangle$ ($|\Phi^-\rangle|0\rangle$) so the probability of passing the tests [see Fig. 4(a)] drops to 0.06(2) when Bob measures in the $X_1X_2Z_3$ basis and remains at 0.91(2) in the $Z_1Z_2Z_3$ basis; (2) if Alice's third measurement basis is X_3 instead of Z_3, the probability of passing the tests for $X_1X_2Z_3$ and $Z_1Z_2Z_3$ measurements is 0.47(4) and 0.49(4) [Fig. 4(b)], respectively. Obviously, Charlie can easily identify that Alice is dishonest based on Bob's reported results.

Protocol 4 monitors whether Bob honestly executes computation B. If Bob plays honestly, Alice's measurement outcomes are deterministic, depending on Bob's results. Figure 3(c) shows the theoretical and experimental results. The probability that Bob passes the tests is 0.87(2) and 0.86(2) when Alice measures in the $Z_1X_2X_3$ and $Z_1Z_2Z_3$ bases (see Supplemental Material [30] for details), respectively. To demonstrate that the method detects whether Bob is cheating, we consider two possible circumstances: (1) If Bob measures the last two qubits in the Z_2Z_3 basis instead of the X_2Z_3 basis, the probability of passing the tests [Fig. 4(c)] drops to 0.52(4) when Alice measures in the $Z_1X_2X_3$ basis and remains at 0.89(3) in the $Z_1Z_2Z_3$ basis. (2) If Bob's first measurement basis is Z_1 instead of X_1, the probability of passing $Z_1X_2X_3$ and $Z_1Z_2Z_3$ tests is 0.41(4) and 0.47(3) [Fig. 4(d)], respectively. Thus, Bob's cheating can easily be caught.

This scheme is device independent, in that it mitigates the need for clients to place trust in any preexisting device. The scheme is theoretically efficient, in the sense that its number of rounds scales with circuit size n, $O(n^c)$, where c is a constant [11,14]. Subsequent results indicate that the number of rounds can be reduced if we require only one-sided device independence [15].

In summary, we experimentally demonstrate secure computation on quantum cloud servers using a photonic setup where three EPR states are shared between two quantum servers. In our implementation, the correctness of results can be tested through verification protocols, based on the rigidity of the CHSH test and stabilizer tests. Our experiment introduces the features of multiple servers, device independence, and, especially, a completely classical client, leading to a heuristic exploration for future secure distributed quantum networks in the cloud. This type of encryption is crucial to enable scalable models for secure, outsourced quantum

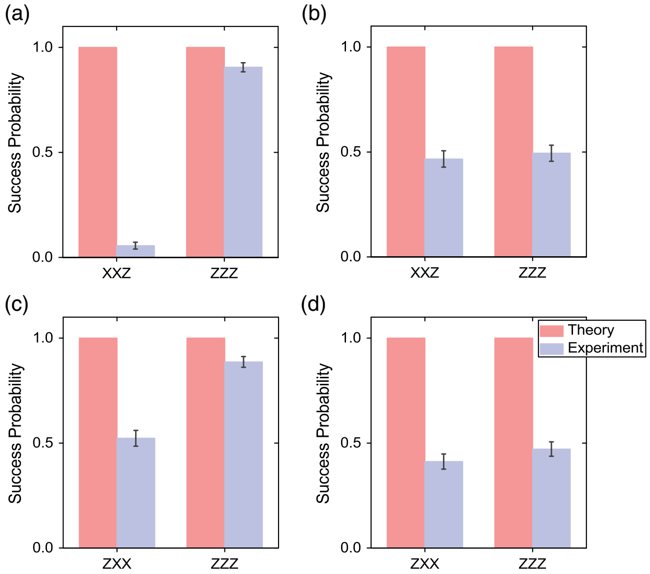

FIG. 4. Experimental result for dishonest Alice and Bob. (a) Probability that Alice passes the tests of state tomography when Bob measures in $X_1X_2Z_3$ and $Z_1Z_2Z_3$ bases, if Alice deliberately reports the opposite results for the first qubit. (b) Probability that Alice passes the tests of state tomography when Bob measures in $X_1X_2Z_3$ and $Z_1Z_2Z_3$ bases, if Alice's third measurement basis is X_3 instead of Z_3. (c) Probability that Bob passes the tests of process tomography when Alice measures in $Z_1X_2X_3$ and $Z_1Z_2Z_3$ bases, if Bob measures the last two qubits in Z_2Z_3 instead of the X_2Z_3 basis. (d) Probability that Bob passes the tests of process tomography when Alice measures in $Z_1X_2X_3$ and $Z_1Z_2Z_3$ bases, if Bob's first measurement basis is Z_1 instead of X_1.

computation to emerge, paving the way for the commercialization and widespread adoption of quantum computer technology.

We thank P. Rohde, M. McKague, X. Wu, Y.-H. Luo, C.-Y. Lai, K.-M. Chung, and X. Yuan for helpful discussions. This work was supported by the National Natural Science Foundation of China, the Chinese Academy of Sciences, and the National Fundamental Research Program. B. C. S. acknowledges financial support from AITF, NSERC, and China's 1000 Talent Plan.

[*] xiongfengma@gmail.com
[†] eidos@ustc.edu.cn
[‡] nlliu@ustc.edu
[§] cylu@ustc.edu.cn

[1] IBM, http://www.research.ibm.com/quantum/.

[2] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 2009), pp. 517–526.

[3] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217.

[4] D. Aharonov, M. Ben-Or, and E. Eban, arXiv:0810.5375.

[5] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).

[6] T. Morimae and K. Fujii, Phys. Rev. A **87**, 050301 (2013).

[7] T. Morimae, Phys. Rev. A **89**, 060302 (2014).

[8] M. Hayashi and T. Morimae, Phys. Rev. Lett. **115**, 220502 (2015).

[9] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).

[10] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, arXiv:1502.02563.

[11] A. Gheorghiu, E. Kashefi, and P. Wallden, New J. Phys. **17**, 083040 (2015).

[12] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, Phys. Rev. Lett. **111**, 230502 (2013).

[13] C. A. Pérez-Delgado and J. F. Fitzsimons, Phys. Rev. Lett. **114**, 220502 (2015).

[14] B. W. Reichardt, F. Unger, and U. Vazirani, Nature (London) **496**, 456 (2013).

[15] A. Gheorghiu, P. Wallden, and E. Kashefi, New J. Phys. **19**, 023043 (2017).

[16] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).

[17] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Nat. Phys. **9**, 727 (2013).

[18] K. Fisher, A. Broadbent, L. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. Resch, Nat. Commun. **5**, 3074 (2014).

[19] C. Greganti, M.-C. Roehsner, S. Barz, T. Morimae, and P. Walther, New J. Phys. **18**, 013020 (2016).

[20] K. Marshall, C. S. Jacobsen, C. Schäfermeier, T. Gehring, C. Weedbrook, and U. L. Andersen, Nat. Commun. **7**, 13795 (2016).

[21] S. Aaronson, A. Cojocaru, A. Gheorghiu, and E. Kashefi, arXiv:1704.08482.

[22] Z. Gan and R. J. Harrison, in *Proceedings of the ACM/IEEE SC 2005 Conference* (IEEE, New York, 2005), p. 22.

[23] C. Senko, J. Smith, P. Richerme, A. Lee, W. Campbell, and C. Monroe, Science **345**, 430 (2014).

[24] S. Aaronson and A. Arkhipov, Quantum Inf. Comput. **14**, 1383 (2014).

[25] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).

[26] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **99**, 250504 (2007).

[27] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, Phys. Rev. Lett. **99**, 250505 (2007).

[28] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter, Phys. Rev. Lett. **95**, 210505 (2005).

[29] B. W. Reichardt, F. Unger, and U. Vazirani, arXiv:1209.0448.

[30] See Supplemental Material http://link.aps.org/supplemental/10.1103/PhysRevLett.119.050503 for more information about the security analysis, and the details for CNOT gates, CHSH games, state tomography, and process tomography, which includes Refs. [31–33].

[31] M. McKague, New J. Phys. **18**, 045013 (2016).

[32] A. W. Coladangelo, Quantum Inf. Comput. **17**, 0831 (2017).

[33] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, Phys. Rev. A **93**, 062121 (2016).

[34] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, and J.-W. Pan, Phys. Rev. Lett. **117**, 210502 (2016).

[35] H. F. Hofmann, Phys. Rev. Lett. **94**, 160504 (2005).