

Remote Blind State Preparation with Weak Coherent Pulses in the Field


Yang-Fan Jiang,^{1,2} Kejin Wei,^{1,2} Liang Huang,^{1,2} Ke Xu,³ Qi-Chao Sun,^{1,2} Yu-Zhe Zhang,^{1,2} Weijun Zhang,⁴ Hao Li,⁴ Lixing You,⁴ Zhen Wang,⁴ Hoi-Kwong Lo,^{3,*} Feihu Xu,^{1,2,†} Qiang Zhang[Ⓞ],^{1,2,‡} and Jian-Wei Pan^{1,2,§}

¹Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Shanghai 201315, China

²Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

³Centre for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada

⁴State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai, 200050, China

 (Received 13 March 2019; published 3 September 2019)

Quantum computing has seen tremendous progress in past years. Due to implementation complexity and cost, the future path of quantum computation is strongly believed to delegate computational tasks to powerful quantum servers on the cloud. Universal blind quantum computing (UBQC) provides the protocol for the secure delegation of arbitrary quantum computations, and it has received significant attention. However, a great challenge in UBQC is how to transmit a quantum state over a long distance securely and reliably. Here, we solve this challenge by proposing a resource-efficient remote blind qubit preparation (RBQP) protocol, with weak coherent pulses for the client to produce, using a compact and low-cost laser. We experimentally verify a key step of RBQP—quantum nondemolition measurement—in the field test over 100 km of fiber. Our experiment uses a quantum teleportation setup in the telecom wavelength and generates 1000 secure qubits with an average fidelity of $(86.9 \pm 1.5)\%$, which exceeds the quantum no-cloning fidelity of equatorial qubit states. The results prove the feasibility of UBQC over long distances, and thus serves as a key milestone towards secure cloud quantum computing.

DOI: [10.1103/PhysRevLett.123.100503](https://doi.org/10.1103/PhysRevLett.123.100503)

As physicist Richard Feynman realized three decades ago [1], quantum computation holds the promise of exponential speedup over classical computers in solving certain computational tasks. Quantum computation has been an area of wide interest and growth in the past couple of years [2,3]. Because of implementation complexity, it is speculated that future quantum computers will be accessed via the cloud service for common users. Indeed, the recent effort on quantum cloud service [4] demonstrates the path towards this speculation. Blind quantum computing (BQC) [5–7] is an effective method for a common user (namely, the client), who has limited or no quantum computational power, to delegate the computation to an untrusted quantum organization (namely, the server) without leaking any information about the user’s input and computational task.

Various BQC protocols have been proposed in theory [8–13]. In addition, several experiments have been reported to demonstrate the feasibility of BQCs with photonic qubits [14–19]. See Ref. [20] for a review. Notably, the universal BQC [7] [see Fig. 1(a)], built upon the model of measurement-based quantum computation [21], does not require any quantum computational power or quantum memory for the client. The security or blindness of the UBQC protocol is information theoretic; i.e., the server cannot

learn anything about the client’s computation except its size. The only nonclassical requirement for the client is that she can prepare qubits with a single-photon source perfectly. Nonetheless, practical single-photon sources are not yet readily available, despite a lot of effort [22].

To resolve the state-preparation issue, the recent remote blind qubit preparation (RBQP) protocol, which was proposed in [23], enables the preparation of blind qubits with weak coherent pulses that are generated from a compact and low-cost laser diode instead of a perfect single-photon source. In this protocol, the client prepares a sequence of WCPs with random polarization $\theta_i \in_R \{k\pi/4: 0 \leq k \leq 7\}$ and sends them to the server through a quantum channel. The server performs quantum nondemolition measurements on each of the received WCPs and declares the results to the client. The client checks the reported number of vacuum events: if the number is smaller than a preset threshold, she asks the server to perform the interlaced 1D cluster computation subroutine [23] on the nonvacuum pulses. The RBQP protocol is completed with a polarization angle θ that is only known by the client and a single qubit in the state $|+\theta\rangle$ held by the server. Running the RBQP protocol S times will result in a computational size of S single qubits. For a channel with transmittance η , this requires a total number of N WCPs [23],

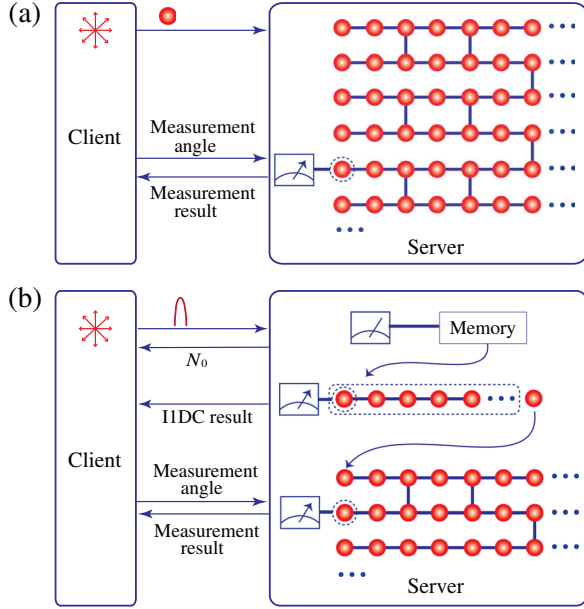


FIG. 1. (a) Universal blind quantum computing (UBQC) with single photons [7]. Client prepares S single qubits randomly prerotated in polarization states $|+\theta_i\rangle_{i=1}^S = (1/\sqrt{2})(|0\rangle + e^{i\theta_i}|1\rangle)$ and sends them to server, who builds up brickwork state to realize measurement-based quantum computing. Client transmits measurement angle $\sigma_i = (\phi_i + \theta_i + r_i\pi \bmod 2\pi)$ to server through a classical channel with $r_i \in \{0, 1\}$. Server reports each measurement outcome to client, who performs bit flips if $r_i = 1$. (b) UBQC with weak coherent pulses (WCPs) [23]. Client prepares a sequence of N phase-randomized WCPs with random polarization $|+\theta_i\rangle_{i=1}^S$ and sends them to server. Server performs quantum nondemolition (QND) measurement on each WCP, stores the nonvacuum pulses, and reports the number of vacuum events N_0 to client. Client checks N_0 and decides whether to continue. If protocol continues, server performs interlaced 1D cluster computation (I1DC) subroutine on stored photons and tells client the results server ends up with a perfect random qubit in state $|+\theta\rangle$, for which only the client knows θ . The rest of the computational steps are the same as in Fig. 1(a).

$$N \geq \frac{18 \log(S/\epsilon)}{\eta^4}, \quad (1)$$

where ϵ denotes the failure probability. Nonetheless, the RBQP is inefficient for small η ; i.e., N scales as $O(1/\eta^4)$. It is thus demanding to design an efficient protocol for the future quantum network where the client can access the server over a long distance.

We propose a refined RBQP protocol by employing the decoy-state method, which was originally invented in the field of quantum key distribution [24,25]. Our protocol can greatly reduce the required number of WCPs from $O(1/\eta^4)$ to $O(1/\eta)$. Furthermore, instead of generating one single qubit in each run, our protocol allows a client to generate S qubits simultaneously in a single instance. In our protocol, the client randomly modulates the intensity of each WCP according to the intensity choice μ (signal), ν (decoy), and

zero (vacuum). The client runs the same as the initial RBQP but with different postprocessing. With the reported QND results for each intensity, the client performs the decoy-state analysis to estimate the lower bound of the number of single-photon events [24,25]. If the bound is larger than her preset threshold, the client asks the server to discard all the decoy pulses and randomly divides the remaining M_μ signal pulses into S groups, with each group containing $m = M_\mu/S$ signal pulses. The server performs the I1DC subroutine [23] on each group and returns the measurement results to the client. The protocol completes with S single qubits held by the server, of which the polarization angles are only known to the client. By doing so, in the limit that the probability of sending a signal state is approximately one, the lower bound of N in our protocol is

$$N \geq \frac{2.1S \log(S/\epsilon)}{\eta}. \quad (2)$$

Compared with Eq. (1), N scales as $O(1/\eta)$, which is far less than that of the original protocol. We remark that any failure to detect a photon is subjected to the loss, which does not affect the security. We have also derived the analysis after considering the finite-data effect, and we show the details of these results in the Supplemental Material [26].

A key challenge to implement RBQP is the realization of the QND measurement. QND is a crucial technology in quantum information, and it has been investigated widely in matter-based platforms [27,28]. However, these matter-based realizations require challenging techniques such as strong light-matter interactions and optical wavelength conversion, which are not mature for real-life applications. Here, we solve the challenge by designing an experimentally feasible scheme based on linear optics and a teleportation-based method [29–33]. We move the QND to the field test over 100 km of fiber by using two independent photon sources. The scheme of our experiment is shown in Fig. 2(a). We construct a quantum link in the field in the city of Shanghai, in which the client sends the polarization-encoding (POL) WCPs with decoy states to a server who performs QND measurements. The field distance between the client and the server is about 199 m.

Figure 2(b) shows the details of our experimental realization. The client possesses a gain-switched distributed feedback laser (DFB) to generate laser pulses at a repetition frequency of 250 MHz. Each pulse is carved into a 37 ps pulse duration after passing through the first intensity modulator (IM). To generate the two decoy states, the intensities of the pulses are randomly modulated by the second IM. Key bits are encoded into polarization states of the WCPs by a loop-interferometer-based polarization-encoding scheme that consists of a polarization beam displacer (PBD) and a phase modulator (PM). After

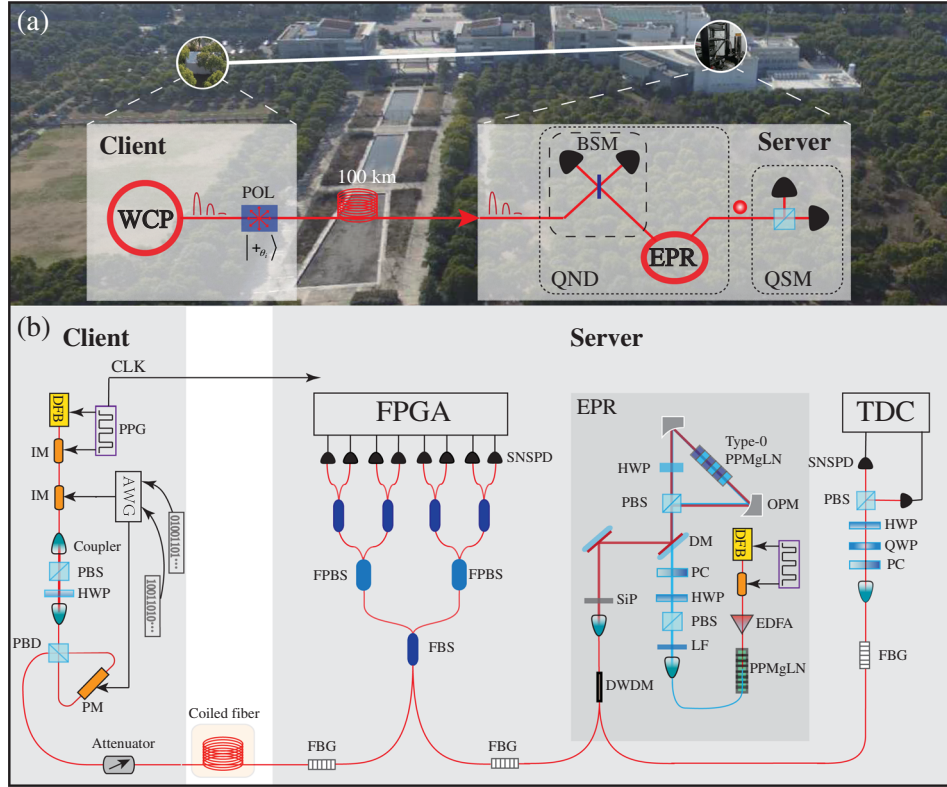


FIG. 2. (a) Bird's eye view of experiment between client and server over a field distance of 199 m. Client sends WCPs in polarization states of $|+\theta_i\rangle$, with signal and decoy intensities, to server who implements QND measurement based on quantum-teleportation and quantum-state-tomography measurements (QSMs). (b) Experimental setup. Client's setup: client generates laser pulses using a distributed feedback laser and an intensity modulator, which are driven by a pulse pattern generator (PPG). The other IM is used to generate signal and decoy intensities randomly. States of $|+\theta_i\rangle$ are encoded into the pulse by utilizing a loop-interferometer-based polarization modulation, which consists of a polarization beam displacer and phase modulation. All encodings are controlled by an arbitrary waveform generator (AWG) with independent random numbers. Pulses are attenuated by an attenuator and sent to server through a standard coiled fiber. Server's setup: laser pulses from 1558 nm gain-switched DFB are amplified by an erbium doped fiber amplifier (EDFA) and upconverted to 779 nm pulses in an inline periodically poled MgO doped lithium niobate (PPMgLN) crystal. The produced 779 nm pulses are focused into the second PPMgLN in the Sagnac loop to generate polarization-entangled photon pairs. Signal and idler photons are singled out by inline DWDMs: one used to implement the Bell state measurement (BSM) and the other used to perform QSM. The implementation of QSM includes a polarizing beam splitter (PBS), two SNSPDs, and a time-to-digital converter (TDC). CLK denotes synchronization signal, FBG denotes fiber Bragg grating, HWP denotes half-wave plate, LF denotes low-pass filter, PC denotes phase compensator, OPM denotes off-axis parabolic mirror, DM denotes dichroic mirror, and SiP denotes silicon pellet.

attenuation, the client sends the weak coherent pulses to the server through a standard telecom coiled fiber.

The server prepares Einstein-Podolsky-Rosen (EPR) pairs of signal (s) and idler (i) photons in the quantum state of

$$|\Phi^+\rangle_{si} = \frac{1}{\sqrt{2}}(|H\rangle_s|H\rangle_i + |V\rangle_s|V\rangle_i),$$

via a spontaneous parametric downconversion process. The signal and idler photons are singled out by an inline dense wavelength division multiplexing filter (DWDM). The signal photons are used to take a Bell state measurement with the received photons from the client. These photons are detected by high-quality superconducting nanowire

single-photon detectors (SNSPDs), where the detection events are registered by a field programmable gate array (FPGA). Note that, after the fiber polarization beam splitters (FPBSs), we use four fiber beam splitters (FBSs) and eight SNSPDs to mimic the photon-number-resolving detectors [34]. This allows us to probabilistically detect two or more inbound photons from the WCP. The idler photons undergo a quantum-state-tomography measurement for the quantification of the quality of the prepared qubits.

To implement the protocol, there are several technical challenges. First, a high-speed and high-fidelity polarization modulation is required to prepare eight polarization states θ_i . We use a loop-interferometer-based scheme to realize the polarization modulation at a rate of 250 MHz

with an average fidelity of $(99.42 \pm 0.09)\%$ [35]. Second, it requires a high-visibility interference between two independent sources, i.e., the EPR pairs and the WCPs that experience a long-distance transmission. To do so, we synchronize the two independent sources with a 12.5 GHz microwave clock and exploit two FBG filters with a bandwidth of 3.3 GHz to suppress the spectral distinguishability. Third, we optimize the average photon number from the WCP to obtain an optimal interference visibility. Finally, we detect the photons with a combination of four FBSs to decrease the multiphoton effect and eight high-efficiency and low-dark-count SNSPDs to maximize the interference visibility. See the Supplemental Material for further details [26]. These efforts allow us to achieve a high QND measurement fidelity of about 95%, which is much higher than those reported in previous works, e.g., 75% in [33].

We characterize the QND test by performing quantum-state-tomography measurements on the teleported quantum states. We run our protocol over the distance of 100 km of fiber, and we measure the density matrices of eight teleported states at the server. These results are shown in Fig. 3. The average fidelity is characterized as $(86.9 \pm 1.5)\%$, which exceeds the maximum value of $2/3$ achievable in classical teleportation, and the quantum phase-covariant

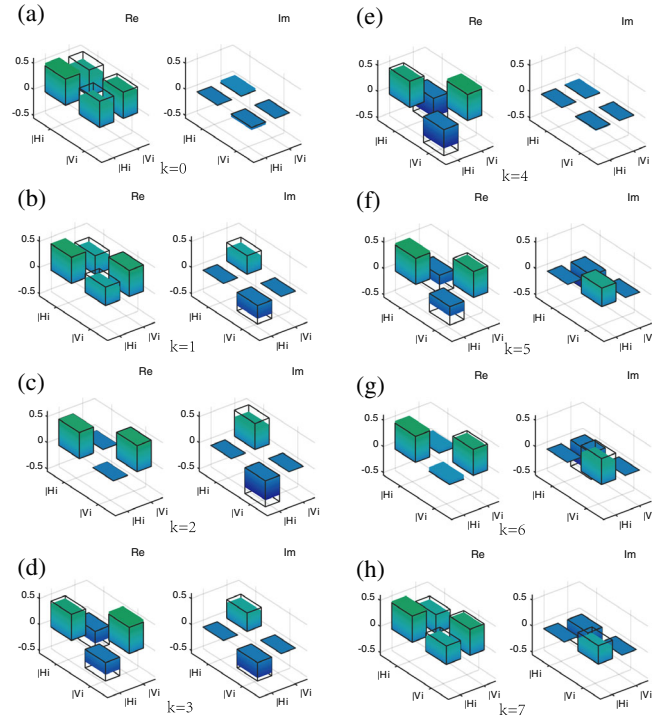


FIG. 3. (a)–(h) Real and imaginary parts of reconstructed density matrices for eight polarization states $|+\theta_i\rangle = (1/\sqrt{2})(|0\rangle + e^{i\theta_i}|1\rangle)$ with $\theta_i \in \{k\pi/4: 0 \leq k \leq 7\}$ after QND measurement over 100 km of fiber. Black frames denote ideal density matrices. Average fidelity is characterized as $(86.9 \pm 1.5)\%$. Error bars represent one standard deviation.

no-cloning bound of 85.4% [36,37]. This result indicates the high fidelity of our QND measurement.

We run the whole system with fibers at distances of 0, 26, 50, 76, and 100 km. Experimental parameters, including the intensities and probability distributions of the signal and decoy pulses, are optimized numerically (see Supplemental Material [26]). In each run, we generate $S = 1000$ qubits, which could be made blind via the IIDC. The experimental results are shown in Fig. 4(a). We can see that the required N of our protocol is much lower than that of the original protocol [23]. In particular, at the distance of 100 km, it is up to 20 orders of magnitude lower than that of the original protocol. At 0 km, the loss primarily comes from the inefficient QND measurement. Such a huge effective loss due to an inefficient QND measurement causes the original RBQP protocol to require at least $N \sim 10^{26}$ pulses. In contrast, our decoy-state-based protocol requires only

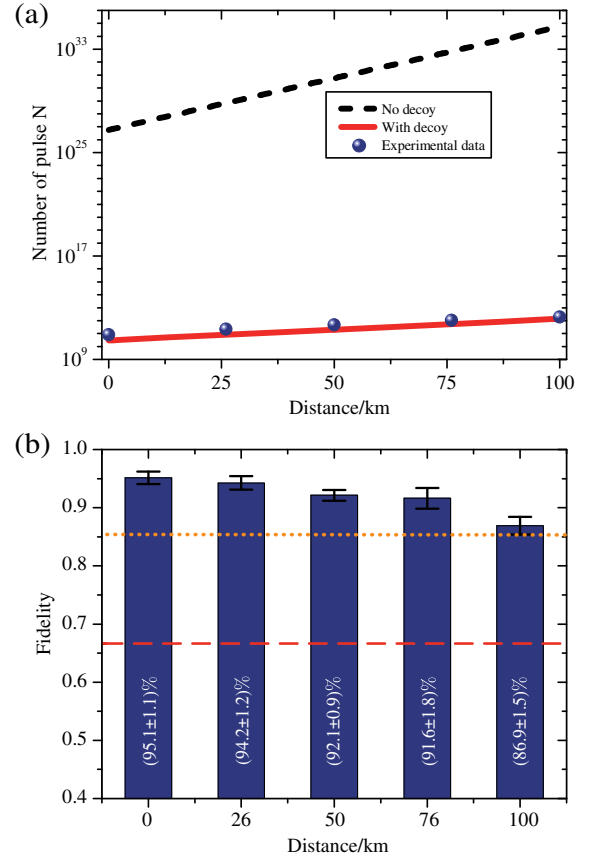


FIG. 4. (a) Required number N of WCPs for preparing 1000 secure qubits. Dashed black and solid red curves are numerical simulations of N for RBQC with and without decoy states [26]. Blue dots are our experimental results. (b) Average fidelities of polarization states after QND measurement. Fidelities are measured using quantum-state tomography. Error bars represent one standard deviation. All fidelities exceed both the classical fidelity limit of $2/3$ (represented by the dashed red line) and the quantum phase-covariant no-cloning bound of 85.4% (represented by the dotted orange line).

$N \sim 10^{10}$ pulses. This number of pulses can be generated in less than 1 min using our implementation system. Even at the 100 km distance, our experiment only needs about 2 h to generate $S = 1000$ blind qubits. The average fidelities of the eight polarization states $|+\theta_i\rangle$ for different distances are shown in Fig. 4(b).

In the RBQP, as shown in Fig. 1(b), the signal WCPs should be stored in a quantum memory after the QND measurement, and the IIDC is applied afterwards. We simulate this procedure by storing the density matrices of the signal states and performing the IIDC subroutine on a personal computer [26]. Our simulation results show that, at the fiber length of 0 km, the average fidelity of 1000 blind qubits is $(81.9 \pm 2.0)\%$. This fidelity can be improved if the client uses an error correction code for encoding. A full implementation demands a high-performance quantum memory. In our setup, to generate 1000 blind qubits at 100 km would require a storage time of ~ 2 h and near unity process fidelity, which is still beyond current quantum memory technology. Nevertheless, the long storage time, large bandwidth, and high-fidelity quantum memories have been achieved recently [38–41]. These subjects are important for future studies.

In summary, we have proposed a decoy-state RBQP protocol and reduced the required number of WCPs N from $O(1/\eta^4)$ to $O(1/\eta)$ to generate S blind qubits. We have demonstrated a key step of our protocol by implementing the QND with two independent photon sources in the field, up to 100 km of fiber. The fidelity of the generated qubits is above 86%. Our RBQP protocol with WCPs and the photonic experiment lead a heuristic exploration for UBQC over long-distance quantum networks, and they will be a crucial step for the commercialization and widespread adoption of secure quantum computation in the cloud.

The authors would like to thank Bing Bai, Tong Xiang, Xiaohui Bao, and Yong Yu for helpful discussions. This work was supported by the National Key R&D Program of China (2018YFB0504300), the National Natural Science Foundation of China, the Chinese Academy of Science, the Anhui Initiative in Quantum Information Technologies, and the Shanghai Sailing Program. H.-K. L. was supported by the NSERC, the U.S. Office of Naval Research, the CFI, the ORF, and Huawei Canada.

Y.-F. J. and K. W. contributed equally to this work.

*hklo@ece.utoronto.ca

†feihuxu@ustc.edu.cn

‡qiangzh@ustc.edu.cn

§pan@ustc.edu.cn

[1] R. P. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982).

[2] A. W. Harrow and A. Montanaro, *Nature (London)* **549**, 203 (2017).

[3] M. Mohseni, P. Read, H. Neven, S. Boixo, V. Denchev, R. Babbush, A. Fowler, V. Smelyanskiy, and J. Martinis, *Nature (London)* **543**, 171 (2017).

[4] The following are quantum cloud service examples: for IBM, see <https://www.research.ibm.com/ibm-q/>; for CAS-Alibaba, see <http://quantumcomputer.ac.cn/>; and for Rigetti, see <https://www.rigetti.com/>.

[5] A. M. Childs, *Quantum Inf. Comput.* **5**, 456 (2005).

[6] P. Arrighi and L. Salvail, *Int. J. Quantum. Inform.* **04**, 883 (2006).

[7] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE, 2009)*, p. 517.

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

[9] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, *Phys. Rev. Lett.* **111**, 230501 (2013).

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

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

[12] J. F. Fitzsimons and E. Kashefi, *Phys. Rev. A* **96**, 012303 (2017).

[13] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, *arXiv:1704.04487*.

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

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

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

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

[18] T. Gehring, C. Weedbrook, K. Marshall, C. S. Jacobsen, and C. Scha, *Nat. Commun.* **7**, 13795 (2016).

[19] H. L. Huang, Q. Zhao, X. Ma, C. Liu, Z. E. Su, X. L. Wang, L. Li, N. L. Liu, B. C. Sanders, C. Y. Lu, and J. W. Pan, *Phys. Rev. Lett.* **119**, 050503 (2017).

[20] J. F. Fitzsimons, *npj Quantum Inf.* **3**, 23 (2017).

[21] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).

[22] I. Aharonovich, D. Englund, and M. Toth, *Nat. Photonics* **10**, 631 (2016).

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

[24] H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).

[25] X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).

[26] See the Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.123.100503> for further details.

[27] C. Guerlin, J. Bernu, S. Deleglise, C. Sayrin, S. Gleyzes, S. Kuhr, M. Brune, J.-M. Raimond, and S. Haroche, *Nature (London)* **448**, 889 (2007).

[28] A. Reiserer, S. Ritter, and G. Rempe, *Science* **342**, 1349 (2013).

[29] B. C. Jacobs, T. B. Pittman, and J. D. Franson, *Phys. Rev. A* **66**, 052307 (2002).

- [30] X.-L. Wang, X.-D. Cai, Z.-E. Su, M.-C. Chen, D. Wu, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, *Nature (London)* **518**, 516 (2015).
- [31] T. Hiroki, D. Shellee, J. Martin, V. Varun, P. Richard, and W. N. Sae, *Optica* **2**, 832 (2015).
- [32] Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang *et al.*, *Nat. Photonics* **10**, 671 (2016).
- [33] R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, *Nat. Photonics* **10**, 676 (2016).
- [34] A. Divochiy, F. Marsili, D. Bitauld, A. Gaggero, R. Leoni, F. Mattioli, A. Korneev, V. Seleznev, N. Kaurova, O. Minaeva *et al.*, *Nat. Photonics* **2**, 302 (2008).
- [35] C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, *Opt. Lett.* **44**, 2398 (2019).
- [36] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, *Phys. Rev. A* **62**, 012302 (2000).
- [37] J. Du, T. Durt, P. Zou, H. Li, L. C. Kwek, C. H. Lai, C. H. Oh, and A. Ekert, *Phys. Rev. Lett.* **94**, 040505 (2005).
- [38] Z.-Q. Zhou, W.-B. Lin, M. Yang, C.-F. Li, and G.-C. Guo, *Phys. Rev. Lett.* **108**, 190505 (2012).
- [39] M. Zhong, M. P. Hedges, R. L. Ahlefeldt, J. G. Bartholomew, S. E. Beavan, S. M. Wittig, J. J. Longdell, and M. J. Sellars, *Nature (London)* **517**, 177 (2015).
- [40] S.-J. Yang, X.-J. Wang, X.-H. Bao, and J.-W. Pan, *Nat. Photonics* **10**, 381 (2016).
- [41] N. Jiang, Y.-F. Pu, W. Chang, C. Li, S. Zhang, and L.-M. Duan, *npj Quantum Inf.* **5**, 28 (2019).