Photonic Implementation of Quantum Information Masking

Zheng-Hao Liu,[1,2] Xiao-Bin Liang (梁晓斌),[3,4] Kai Sun,[1,2] Qiang Li,[1,2] Yu Meng,[1,2] Mu Yang,[1,2] Bo Li,[3,4,*] Jing-Ling Chen,[5,†] Jin-Shi Xu,[1,2,‡] Chuan-Feng Li,[1,2,§] and Guang-Can Guo[1,2]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, People's Republic of China*

[2]*CAS Centre For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China*

[3]*School of Mathematics and Computer Science, Shangrao Normal University, Shangrao 334001, China*

[4]*Quantum Information Research Center, Shangrao Normal University, Shangrao 334001, China*

[5]*Theoretical Physics Division, Chern Institute of Mathematics, Nankai University, Tianjin 300071, People's Republic of China*

(Received 20 August 2020; accepted 1 April 2021; published 30 April 2021)

Masking of quantum information spreads it over nonlocal correlations and hides it from the subsystems. It is known that no operation can simultaneously mask all pure states [Phys. Rev. Lett. **120**, 230501 (2018)], so in what sense is quantum information masking useful? Here, we extend the definition of quantum information masking to general mixed states, and show that the resource of maskable quantum states is far more abundant than the no-go theorem seemingly suggests. Geometrically, the simultaneously maskable states lays on hyperdisks in the state hypersphere, and strictly contains the broadcastable states. We devise a photonic quantum information masking machine using time-correlated photons to experimentally investigate the properties of qubit masking, and demonstrate the transfer of quantum information into bipartite correlations and its faithful retrieval. The versatile masking machine has decent extensibility, and may be applicable to quantum secret sharing and fault-tolerant quantum communication. Our results provide some insights on the comprehension and potential application of quantum information masking.

DOI: 10.1103/PhysRevLett.126.170505

Introduction.—The distinctive nonclassicality of quantum mechanics establishes the pronounced discrepancy between quantum and classical information [1]. Especially, the celebrated quantum nonlocality [2] alludes to the possibility of spreading information over the nonlocal correlation and hiding it from observers who only have access to some subsystems, namely, quantum information masking (QIM) [3]. However, the postulates of unitarity and linearity [4] of quantum theory impose severe limitations on QIM. In the seminal work [3], unconditioned masking of all quantum states is deemed impossible. This assertion establishes a novel no-go theorem to paraphrase its conspicuous precedents like the interdicts against universal cloning [5], broadcasting [6,7], deleting [8,9], and hiding [10] of an unknown state.

Despite the handicap of universal implementation, QIM admits state dependent [11] and probabilistic realization [12,13], which is similar to other conditional quantum information tasks [14,15]. Extrapolations of masking into multipartite [16], multilevel [17], scenarios and channel states [18] have been proposed. QIM shows profound affiliation with quantum state discrimination [19], qubit commitment [20,21], secret sharing [22], and fundamental principles like information conservation [23]. Although significant progress has sprouted regarding QIM, its capability ultimately depends on the scale of a maskable set, which is not yet determined. Moreover, given its intrinsically nonlocal feature, QIM on flying quanta has exceptional prospects of application in quantum communication. However, to our best knowledge, QIM has not been demonstrated in photonic experiments.

The purpose of this Letter is twofold. We first provide a geometric description of QIM and prove the "disk conjecture" [3]—that the maskable qudit states corresponding to any masker belong to some hyperdisks in the state hypersphere. This shows the copiousness of the maskable states, and allows us to identify the inclusion of the broadcastable states within it. Next, we devise a photonic masking machine capable of masking any disk in the qubit Bloch sphere, and give the recipe for qudit state masking. Assisted by the versatility of the machine, we experimentally confirm the geometric property of the maximally maskable set [11,24], and discuss the practical aspects of photonic QIM. Our results provide a systematic method for experimental studies of QIM, shed some lights on its applications as a novel quantum information processing protocol, and the connection between quantum information and nonlocality.

Geometric characterization of QIM.—We start from the formal definition of QIM for general quantum states.

A qudit "masker" $\mathcal{U}$ is a linear isometry mapping a density matrix ρ_s^A to a two-qudit state ρ_s^{AB}:

$$\rho_s^A \to \rho_s^{AB} = \mathcal{U}\rho_s^A \otimes |0\rangle\langle 0|\mathcal{U}^\dagger, \qquad s \in \{1, 2, \ldots\}, \quad (1)$$

where $|0\rangle\langle 0|$ represents a blank state. We say that $\mathcal{U}$ "masks" the quantum information contained in a set Ω of density matrices $\{\rho_s^A \in \Omega\}$ if for all s, the marginal states of ρ_s^{AB} for the two parties are, respectively, identical [3].

To construct a geometric representation of a quantum state, we span a qudit state on the SU(d) basis $\{\Lambda_i\}_{i=1}^{d^2-1}$. Explicitly, $\rho = I_d/d + \sum_{i=1}^{d^2-1} x_i\Lambda_i/2$ with $\sum_{i=1}^{d^2-1} x_i^2 \le r_d^2$, where x_i represents the coefficients, and r_d is determined by the dimension d [25,26]. Consequently, every qudit state corresponds to a unique point in a hypersphere, which is analogous to the Bloch sphere for qubits. Based on this representation, we directly compare the coefficients of the local states after masking to bound the maskable sets, and use the impossibility of universal masking [3] to prove the following result:

Theorem 1.—The maskable set corresponds to any linear qudit isometry lays on some hyperdisk $\mathcal{D}$.

The above Theorem first appears in Ref. [3] as a conjecture, and its proof goes to Sec. IB of the Supplemental Material [27]. Because the Euclidean dimension of a hyperdisk is smaller than a hypersphere by only 1, Theorem 1 shows the possibility of masking a large class of quantum states and the potential of QIM in quantum information tasks. It also inspires us to identify the relationship between the sets of broadcastable and maskable quantum states. Specifically, because noncommuting mixed states cannot be broadcast [6], and commuting mixed states are simultaneously maskable (cf. Supplemental Material [27], Sec. IC), we have

Theorem 2.—Any qudit broadcastable set is a proper subset of some qudit maskable sets. Moreover, the qudit maskable set can have nonzero measure in d-dimensional Euclidean space.

The implication of our results can be clearly visualized in the qubit case using the Bloch sphere representation. For simplicity, we interchangeably denote a state $\rho = (I_2 + x\sigma_x + y\sigma_y + z\sigma_z)/2$ using its SU(2) expansion $\rho := (x, y, z)$. A qubit disk containing the reference state $\rho_0 = (x_0, y_0, z_0)$ can be expressed in a parametric form:

$$\mathcal{D}_\alpha^\theta(\rho_0) = \{\rho : x\sin\alpha\cos\theta + y\sin\alpha\sin\theta + z\cos\alpha = c\}, \quad (2)$$

with $c = x_0\sin\alpha\cos\theta + y_0\sin\alpha\sin\theta + z_0\cos\alpha$, $\alpha \in [0, \pi]$ and $\theta \in [0, 2\pi]$. In comparison, the geometric form of the broadcastable set is a line segment through the center of the Bloch sphere, so the dimensions of the disk and line segment conforms Theorem 2, and the resource in the maskable set is far more abundant than the broadcastable set. Notably, the qubit isometry $\mathcal{U}_\alpha^\theta$ capable of masking the disk $\mathcal{D}_\alpha^\theta(\rho_0)$ always exists (cf. Supplemental Material [27], Sec. IB), and can be devised and reliably implemented on the photonic architecture, as will be elucidated in the following section.

A photonic masking machine.—The polarization degree of freedom of the photons is a natural courier of qubit information. Specifically, the correspondences $|H\rangle \leftrightarrow |0\rangle, |V\rangle \leftrightarrow |1\rangle$ link the isomorphic Hilbert spaces of a photon's polarization state and a qubit state, with $|H\rangle$ and $|V\rangle$ denoting the horizontal and vertical polarization of the photon, respectively. We exploit the photon fusion gate [29] to construct a class of maskers $\mathcal{U}_0^0$, which is further promoted to arbitrary parameters $\mathcal{U}_\alpha^\theta$ using additional wave plates.

The quantum circuit of the masking machine is illustrated in Fig. 1(a). The photon fusion gate performs a two-photon interference on a polarizing beam splitter (PBS), and is conditioned on two-photon coincidence detection at two different output ports. This effectively casts an entangling projector $|HH\rangle\langle HH| - |VV\rangle\langle VV|$ onto the input photons [30]. Given an auxiliary photon initialized in the $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, the behavior of the fusion gate on the target photon is equivalent to the masking isometry $\mathcal{U}_0^0$ up to a renormalization (cf. Supplemental Material [27], Sec. IIA). More explicitly, applying the fusion gate on a qubit state $|\psi\rangle = \cos\delta|H\rangle + \sin\delta e^{i\phi}|V\rangle$ yields $|\psi\rangle \otimes |D\rangle \to \cos\delta|HH\rangle - \sin\delta e^{i\phi}|VV\rangle$. Because the phase factor ϕ does not appear in either of the marginal states, all the states with the same δ can be masked, and they fall on the disk $\mathcal{D}_0^0 = \{\rho : z = \cos\delta\}$.

Using this photonic masking machine, an agent (Alice) can conceal some quantum information into the bipartite correlation between her photons and the ones held by another agent (Bob). The experimental setup is illustrated in Fig. 1(b). An ultraviolet laser with a central wavelength

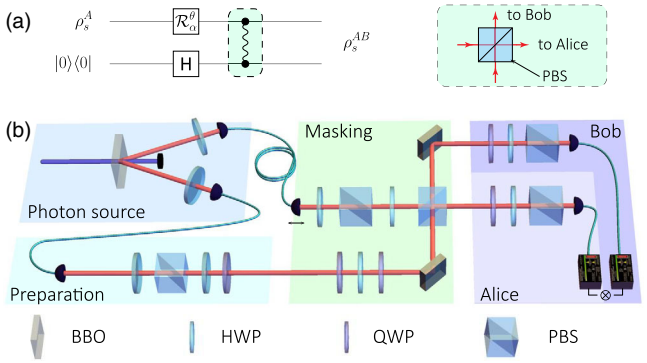

FIG. 1. Photonic qubit masking machine. (a) The quantum circuit of the masking machine. $\mathcal{R}_\alpha^\theta$ and H represent an arbitrary SU(2) rotation and the Hadamard gate, respectively. The tilde line in the rounded rectangle denotes the photon fusion gate, with the detailed implementation using the polarizing beam splitter illustrated in the right subpanel. (b) Experimental configuration. See the main text for details.

of 400 nm is used to pump a type-II phase-matched β-barium borate (BBO) crystal to generate photon pairs in product polarization states via the spontaneous parametric down-conversion process. The photon pairs are collected by two single-mode fibers (SMFs), with one of the photons sent to Alice for initial state preparation using a half-wave plate (HWP) and a quarter-wave plate (QWP), and the other photon directly fed into the masking machine, where its polarization is rotated to $|D\rangle$.

Subsequent to initial state preparation, Alice inputs her photon to the masking machine, which first undergoes a polarization rotation induced by a HWP sandwiched by two QWPs. This rotation maps the arbitrary disk to be masked to a latitudinal plane in the Bloch sphere [31]. The two photons are then interfered on a PBS, with their trajectory and arrival time carefully aligned to ensure the proper overlapping of the spatial and temporal wave functions. The output photon from one port is kept by Alice, and the other is sent to Bob. The polarization states of the photons are later analyzed by a PBS preceded by a QWP and a HWP. Finally, the photons are again collected by two SMFs and sent to single-photon avalanche detectors for coincidence counting.

To exemplify the aptitude of the masking machine, we experimentally realize $\mathcal{U}_{\vartheta}^{\pi/4}$ and mask the disk $\mathcal{D}_{\vartheta}^{\pi/4}(\rho_1)$, with $\vartheta = \arctan\sqrt{2}$. The disk passes through $\rho_1 = |H\rangle\langle H| = (0,0,1), \rho_2 = |D\rangle\langle D| = (1,0,0)$, and $\rho_3 = |L\rangle\langle L| = (0,1,0)$ with $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$. The form of $\mathcal{U}_{\vartheta}^{\pi/4}$ requires the orientation of the three cascaded wave plates in the masking machine set to 58.18°, 0°, and 64.66°. The masker is also applicable for the other states on the disk, and here we test the cases of the pure state $\rho_4 = (2/3, 2/3, -1/3)$ and the mixed state $\rho_5 = (1/2, 1/2, 0)$, with the latter prepared using the temporal-mixing technique [32].

The experimental initial states in a Bloch sphere (blue dots) are shown in Fig. 2(a). To retrieve the masked information, we numerically apply the inverse isometry $\mathcal{U}^{-1}$ on the reconstructed bipartite density matrix. The final state is also shown in Fig. 2(a) (orange dots) for comparison. The reconstruction achieved a mean fidelity of 99.87%, and the average total absolute spectra error is 3.72×10^{-2}. The effect of masking can be further reflected by the marginal states of Alice and Bob. See Fig. 2(b), they almost completely overlap, with the average trace distance $T(\rho_i, \rho_j) = \frac{1}{2}\|\rho_i - \rho_j\|_1$ [33] of Alice's and Bob's marginal states being 1.55×10^{-2} and 4.06×10^{-2}, respectively. On the other hand, joint measurements on two photons show that the average fidelity of the masking-resulted states with respect to the theoretical predictions is 97.70%. Two instances of reconstructed bipartite density matrices are shown in Figs. 2(c) and 2(d), in accord with their theoretical values. Overall, the quantum information has almost completely retreated from the local marginal states, and is faithfully kept in the bipartite correlation.

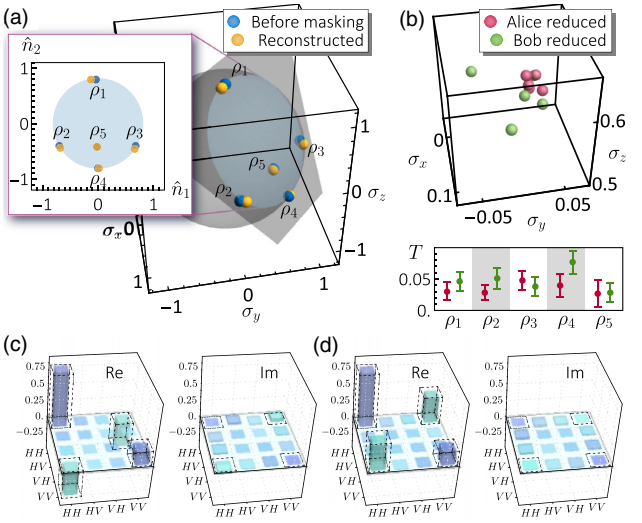

FIG. 2. Masking of a qubit disk. (a) The maskable disk is the intersection of the plane $x + y + z = 1$ and the unit ball. Pure states $\rho_1 \sim \rho_4$ and mixed state ρ_5 fall on the disk. The blue and orange points denote the initial states deduced from quantum state tomography and the reconstructed final states, respectively. The inset shows a projection of these states on the maskable disk, and the axes are defined as $\hat{n}_1 = (-\hat{x} + \hat{y})/\sqrt{2}$ and $\hat{n}_2 = (-\hat{x} - \hat{y} + 2\hat{z})/\sqrt{6}$. (b) Experimentally determined marginal states after masking, and the trace distance from their theoretical values. (c) and (d) The density matrix of the bipartite state resulted from masking ρ_1 and ρ_4. Solid and dashed bars denote the experimental values and theoretical predictions, respectively.

Furthermore, we observe the zero Haar measure of the maskable set, that is, the thickness of the maskable disk is infinitesimal. We verify this property on the masker $\mathcal{U}_0^0$, realized by setting the orientations of all the three wave plates in the masking machine to 0°. The corresponding maskable disks are every latitudinal plane on the Bloch sphere. Experimentally, the reference states $\psi_0 = \sin(\phi/2)|H\rangle + \cos(\phi/2)|V\rangle$ on latitude ϕ, with ϕ setting to 0°,30°, and 60°, are selected. We then prepare some states shifted from ψ_0 along a parallel or a meridian, cast $\mathcal{U}_0^0$, and take tomography on these states. The marginal states of Bob, ρ^B, are obtained from the reconstructed bipartite density matrices, and compared with the theoretical value, $\rho_0^B = \mathrm{Tr}_A(\mathcal{U}_0^0|\psi_0\rangle\langle\psi_0| \otimes |0\rangle\langle 0|\mathcal{U}_0^{0\dagger})$ to determine the result of masking. Our results in Fig. 3 shows that when the shift is along a parallel, ρ^B remains invariant, which can be revealed by the vanishing $T(\rho^B, \rho_0^B)$. Consequently, the state still belongs to the maskable set. However, a shift along a meridian always induces nonzero $T(\rho^B, \rho_0^B)$ regardless of ϕ, indicating failure of qubit masking because extra information is transmitted to the marginal state of Bob. We note that the residual error in the longitudinal data is mainly due to the imperfect overlapping of the two-photon wave function on the PBS, which is caused by the spectral difference between the two type-II parametric photons [34].

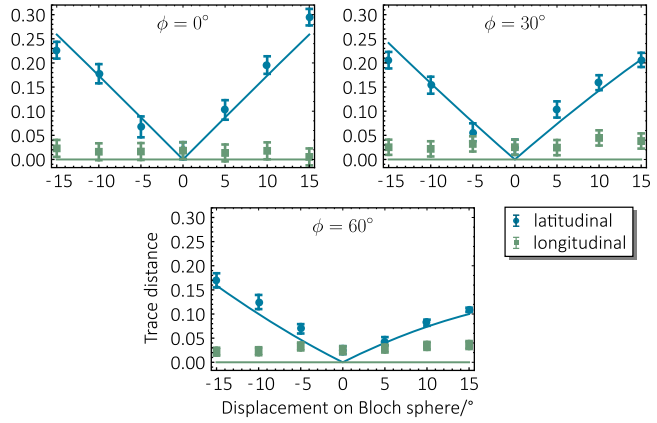

FIG. 3. Zero measure of maskable sets. The maskable disks are encircled by the line of constant latitudes ϕ on the Bloch sphere. Each plot shows the trace distance of Bob's marginal density matrices from the reference state, when Alice slightly shifts the initial state away from a reference point on different latitudes. The cases of displacement along a parallel or a meridian on the Bloch sphere are plotted, respectively, in green and cyan points (experimental data) and curves (theoretical values). The error bars correspond to the 1σ standard deviation, deduced from a Poissonian counting statistics.

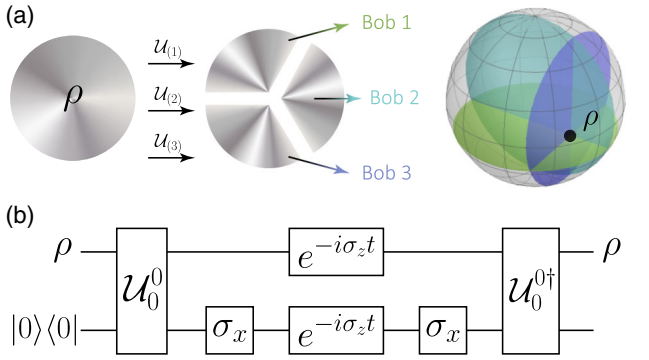

FIG. 4. Application of QIM. (a) Sharing of a secret state among multiple recipients. Alice masks a secret quantum state ρ using three maskers $\mathcal{U}_i$, and send one resulting marginal state to Bob$_i$, respectively. From the information of the marginal states and the masker informed by Alice, every Bob independently interprets the possible disk that contains the masked states. The original state is pinned at the intersection of the three disks. (b) Protecting quantum information in a noisy channel. Given only access to the quantum channels with phase errors $\exp(-i\sigma_z t)$, a qubit can still be correctly transmitted using QIM based on the masker $\mathcal{U}_0^0$.

Discussion.—Our photonic masking machine is based on the qubit photon fusion gate, but the adopted method here is also capable of masking qudit states. To this end, we can encode each digit of the qudit on a qubit, akin to the practice in the quantum factoring algorithm [35,36], and mask every qubit independently. A rigorous account for the qudit state masking is deferred to Sec. IIB of the Supplemental Material [27]. Moreover, because the fusion gate only requires time-correlated photons, the masking machine will work for not only the parametric photon pairs, but also for paused weak coherent light as one input mode, providing the other input mode is genuine single photon with the same wavelength and repetition rate (cf. Supplemental Material [27], Sec. IIC). These features suggest that QIM may be useful in bright single-photon source-based quantum information processing tasks.

QIM has some practical merits in addition to the theoretical significance. As a proof-of-concept application, we utilize the infinitely many d-dimensional maskable sets to experimentally demonstrate quantum secret sharing [22,37–40]. As is shown in Fig. 4(a), Alice masks a quantum state using the masking machine tuned to three different maskers $\mathcal{U}_{(i)}$, and sends each resulting qubit to a recipient, Bob$i$, respectively. The Bobs can only use their marginal state to restrict the masked state onto a disk, and have to cooperate together and comparing their results to reveal the concealed information: upon comparison, the three disks will intersect at a single point in the Bloch sphere. We explain the experimental details, the security of the secret sharing, and its application in image reconstruction in Sec. IID of the Supplemental Material [27]. Owing to the geometric representation of the maskable set, our scheme does not rely on entanglement between the recipients and suffer from decoherence. It also works smoothly for the mixed state. Moreover, it requires no Pauli-type correction at the receiver's side, thus is applicable even when the sender has no access to classical communication after masking.

The quantum information processing protocols based on QIM also have intimate connection with fault tolerance. Because the quantum information is transferred to the nonlocal correlation after masking, it acquires additional resilience to some common-mode noise. An example is shown in Fig. 4(b). Suppose we are given access to two identical, noisy quantum channels, which will apply a random phase error $e^{-i\sigma_z t}$ on the input state. To correctly transmit a qubit state, we can mask it with $\mathcal{U}_0^0$, and apply σ_x on the auxiliary qubit before sending the two qubits through the channel. After the transmission, the original quantum state can be recovered by applying σ_x again on the auxiliary qubit and using the inverse isometry $\mathcal{U}_0^{0\dagger}$. Since the protocol resembles the celebrated spin echo effect (with the noise applied simultaneously on two quanta), it is plausible to expect that it will find further applications in the near future.

Going beyond the no-go theorem, we have provided both the geometric properties of QIM, and the recipe for implementing QIM on photonic architectures. We have demonstrated QIM on our photonic qubit masking machine to meticulously test the theoretical predictions, and show that quantum information can be concealed in and restored from nonlocal correlations. The masking machine is extensible, versatile, and applicable in tasks like quantum secret sharing and quantum communication. This work deepens our comprehension of the tie between QIM and the

basic axioms of the quantum nature, and sheds lights on its future applications in quantum information processing.

This work was supported by the National Key Research and Development Program of China (Grants No. 2016YFA0302700, No. 2017YFA0304100), the National Natural Science Foundation of China (Grants No. 61725504, No. U19A2075, No. 12065021, No. 61805227, No. 61975195, No. 11765016, No. 11774335, and No. 11821404), Key Research Program of Frontier Sciences, CAS (Grant No. QYZDY-SSW-SLH003), Science Foundation of the CAS (Grant No. ZDRW-XH-2019-1), the Fundamental Research Funds for the Central Universities (Grants No. WK2470000026, No. WK2030380017), Anhui Initiative in Quantum Information Technologies (Grants No. AHY020100, and No. AHY060300). J. L. C. was supported by the National Natural Science Foundations of China (Grants No. 11875167 and No. 12075001). X. B. L. was supported by the Natural Science Foundation of Jiangxi Province (Grant No. 20202BAB201010).

Z. H. L., X. B. L., and K. S. contributed equally to this work.

*libobeijing2008@163.com
†chenjl@nankai.edu.cn
‡jsxu@ustc.edu.cn
§cfli@ustc.edu.cn

[1] C. H. Bennett and D. P. DiVincenzo, Nature (London) **404**, 247 (2000).
[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[3] K. Modi, A. K. Pati, A. Sen(De), and U. Sen, Phys. Rev. Lett. **120**, 230501 (2018).
[4] E. Schrödinger, Phys. Rev. **28**, 1049 (1926).
[5] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[6] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[7] A. Kalev and I. Hen, Phys. Rev. Lett. **100**, 210502 (2008).
[8] A. K. Pati and S. L. Braunstein, Nature (London) **404**, 164 (2000).
[9] J. R. Samal, A. K. Pati, and A. Kumar, Phys. Rev. Lett. **106**, 080401 (2011).
[10] S. L. Braunstein and A. K. Pati, Phys. Rev. Lett. **98**, 080502 (2007).
[11] X.-B. Liang, B. Li, and S.-M. Fei, Phys. Rev. A **100**, 030304 (R) (2019).
[12] B. Li, S.-H. Jiang, X.-B. Liang, X. Li-Jost, H. Fan, and S.-M. Fei, Phys. Rev. A **99**, 052343 (2019).
[13] M.-S. Li and K. Modi, Phys. Rev. A **102**, 022418 (2020).
[14] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
[15] A. Lamas-Linare, C. Simon, J. C. Howell, and D. Bouwmeester, Science **296**, 712 (2002).
[16] M.-S. Li and Y.-L. Wang, Phys. Rev. A **98**, 062306 (2018).
[17] F. Ding and X. Hu, Phys. Rev. A **102**, 042404 (2020).
[18] U. Pereg, C. Deppe, and H. Boche, arXiv:2006.05925.
[19] G. Tian, S. Yu, F. Gao, Q. Wen, and C. H. Oh, Phys. Rev. A **91**, 052314 (2015).
[20] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[21] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[22] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[23] S. H. Lie and H. Jeong, Phys. Rev. A **101**, 052322 (2020).
[24] X.-B. Liang, B. Li, S.-M. Fei, and H. Fan, Phys. Rev. A **101**, 042321 (2020).
[25] G. Mahler and V. A. Weberruss, in *Quantum Networks* (Springer, Berlin, 1995).
[26] G. Kimura, Phys. Lett. A **314**, 339 (2003).
[27] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.126.170505 for the proof of propositions and experimental details in the main text, which also includes Ref. [28].
[28] Y. Shih, in *An Introduction to Quantum Optics: Photon and Biphoton Physics* (CRC Press, Boca Raton, 2018).
[29] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
[30] T. P. Bodiya and L.-M. Duan, Phys. Rev. Lett. **97**, 143601 (2006).
[31] B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. A **63**, 032303 (2001).
[32] B. Dakić, Y. O. Lipp, X. Ma, M. Ringbauer, S. Kropatschek, S. Barz, T. Paterek, V. Vedral, A. Zeilinger, C. Brukner, and P. Walther, Nat. Phys. **8**, 666 (2012).
[33] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Informationn: 10th Anniversary Edition* (Cambridge University Press, Cambridge, England, 2010).
[34] W. P. Grice and I. A. Walmsley, Phys. Rev. A **56**, 1627 (1997).
[35] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, 1994), p. 124.
[36] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien, Nat. Photonics **6**, 773 (2012).
[37] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[38] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[39] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[40] B. P. Williams, J. M. Lukens, N. A. Peters, B. Qi, and W. P. Grice, Phys. Rev. A **99**, 062311 (2019).