Experimental anonymous quantum conferencing

Citation for published version:
Webb, JW, Ho, J, Grasselli, F, Murta, G, Pickston, A, Ulibarrena, A & Fedrizzi, A 2024, 'Experimental anonymous quantum conferencing', *Optica*, vol. 11, no. 6, pp. 872-875.
https://doi.org/10.1364/OPTICA.514362

Digital Object Identifier (DOI):
10.1364/OPTICA.514362

Published In:
Optica

OPTICA

Experimental anonymous quantum conferencing

JONATHAN W. WEBB,[1] JOSEPH HO,[1] FEDERICO GRASSELLI,[2,3] GLÁUCIA MURTA,[2] ALEXANDER PICKSTON,[1] ANDRES ULIBARRENA,[1] AND ALESSANDRO FEDRIZZI[1,*]

[1]Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK
[2]Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany
[3]Université Paris-Saclay, CEA, CNRS, Institut de Physique Théorique, 91191 Gif-sur-Yvette, France
*a.fedrizzi@hw.ac.uk

Received 30 November 2023; revised 2 May 2024; accepted 7 May 2024; published 17 June 2024

Anonymous quantum conference key agreement (AQCKA) allows a group of users within a network to establish a shared cryptographic key without revealing their participation. Although this can be achieved using bipartite primitives alone, it is costly in the number of network rounds required. By allowing the use of multi-partite entanglement, there is a substantial efficiency improvement. We experimentally implement the AQCKA task in a six-user quantum network using Greenberger–Horne–Zeilinger (GHZ)-state entanglement and obtain a significant resource cost reduction in line with theory when compared to a bipartite-only approach. We also demonstrate that the protocol retains an advantage in a four-user scenario with finite key effects taken into account.

https://doi.org/10.1364/OPTICA.514362

A wide range of modern communication tasks involve group settings where multiple parties communicate, e.g., in a conference call, or in a sensor network [1–7]. These group sessions can be secured cryptographically; in addition one may require anonymity where subgroups can communicate securely without revealing their participation to the wider group. Anonymous group encryption can be built up from pair-wise encryption, which can be made unconditionally secure via quantum key distribution [8]. Multi-partite entanglement can be used to establish a group key between N usersthrough quantum conference key agreement (QCKA) [9–13], which consumes $(N-1)$ times fewer network resources than equivalent pair-wise entanglement schemes. Recently, it has been shown that anonymous quantum conference key agreement (AQCKA) [14] obtains a larger efficiency advantage from multi-partite entanglement with a theoretical maximum of $N(N-1)$ for an N-user network [15]. More so, by increasing the anonymity criteria of this task, an even larger advantage of up to $N(N-1)^2$ can be achieved.

There are different ways to realize a quantum network. A modular approach uses underlying entanglement already present in the network, entangling operations, and local operations to dynamically allocate the desired quantum resources to users [16,17]. A more direct approach to realize a network invokes a central quantum server, which directly generates and distributes entangled resources to required parties [8,12,18]. We consider the task of AQCKA with the direct network approach where N users are connected to the quantum server; see Fig. 1.

AQCKA proceeds as follows. Users are grouped into M keyholders (including a sender) and $N-M$ non-keyholders. The keyholders aim to establish a conference key, coordinated by the sender, while the non-keyholders do not learn the key nor the keyholders' identities. Bipartite resources are distributed in an all-to-all configuration for pair-wise keys to satisfy anonymous subprotocols [8,19]. This ensures anonymity whereby any user adopts the role of sender by first carrying out a subroutine to ensure only one sender is attempting to initialize AQCKA. Upon success, the sender anonymously notifies only the keyholders of the conference key agreement subroutine, which determines how the conference key is distilled securely from the shared entanglement. Once the roles have been assigned, every round requires users to perform measurements on their resource to either distill a raw key or check for eavesdropping. At this stage, users can conduct the remaining steps of the protocol with either bipartite resources or multi-partite resources through either a maximally entangled Greenberger–Horne–Zeilinger (GHZ) state [14,15,20] or a linear cluster [21,22]. Any eavesdropping, or deviation by non-keyholders, introduces noise that is detected during parameter estimation and will lead to the protocol being aborted. Unless the protocol aborts, the sender anonymously broadcasts the information the keyholders require to perform error correction on their respective raw keys, followed by a verification round to ensure the keys are identical. Lastly, the keyholders implement privacy amplification to arrive at the final secret conference key.

We experimentally perform multi-partite and bipartite variants of AQCKA by generating a six-qubit photonic GHZ state that is distributed from a central server, forming a six-user network. To realize each variant, users perform different measurements on the network to distill either Bell pairs for bipartite resources or GHZ states for multi-partite resources. We evaluate the key rate performance in the asymptotic limit for both variants and with two different anonymity conditions in this six-user network. We then implement a fouruser network for a more in-depth analysis of achievable AQCKA key rates and the performance of subprotocols required to establish anonymity in the finite key regime.

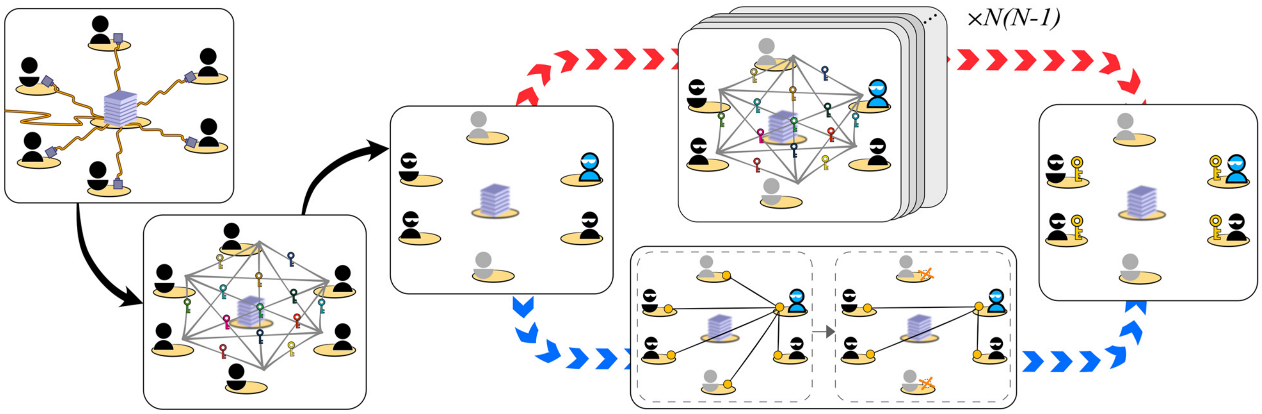

Fig. 1. AQCKA protocol. A quantum server distributes bipartite or multi-partite entanglement to N users. The users perform quantum key distribution with bipartite entanglement to distill $\binom{N}{2}$ unique pair-wise keys. The sender (blue) designates keyholders (black) and non-keyholders (gray) via anonymous messaging primitives. The anonymous conference key can be established by consuming $N(N-1)$ bipartite key bits per conference key bit (red path). Alternatively, by sharing N-party GHZ states and applying a pre-shared measurement sequence, the group can directly obtain up to one conference key bit per GHZ state (blue path).

We prepare the six-photon GHZ state using three entangled-photon-pair sources as shown in Fig. 2. The sources exploit type-II parametric down-conversion using aperiodically poled KTP (aKTP) crystals tailored to produce spectrally separable biphoton states. This suppresses unwanted spectral correlations created in conventional parametric down-conversion sources allowing us to omit narrowband spectral filtering, which improves photon-pair coupling efficiencies [23,24]. All three sources are pumped by a mode-locked laser that produces 1.3 ps pulses at a repetition rate of 80 MHz and center wavelength of 775 nm, creating degenerate telecom photon pairs at 1550 nm. We create polarization-entangled photon pairs by optically pumping the aperiodically poled KTP crystal bidirectionally in a Sagnac configuration [25] to produce the $|\Phi^+\rangle$ Bell state with pair production rate of $\sim 2 \times 10^3$ Hz/mW. Two linear optical fusion gates interfere photons from separate sources in order to create the six-photon GHZ state. The success of these fusion gates is conditioned on the detection of a single photon in each measurement stage; see Fig. 2 for details. We measure an average six-photon rate of 0.67 Hz for a pump power of 300 mW. We also prepare a four-photon GHZ state, using two sources and one fusion gate, measuring a raw four-photon rate of 18 Hz at 40 mW.

To characterize the quality of our GHZ states, we establish a lower-bound fidelity to the ideal state through stabilizer measurements [26]. Our estimated fidelities for the four- and six-photon GHZ states are 0.933(4) and 0.825(5), respectively; see Supplement 1 for further details. In the AQCKA task, both bipartite and multi-partite resources are required from the quantum server, which is distributing GHZ states in every round of the task. When a smaller GHZ state or Bell pair is required, non-keyholders locally measure their photon in the Pauli-X basis to disentangle themselves from the network, whilst keyholders measure in both the Pauli-Z and Pauli-X bases. For example, to obtain a Bell pair resource in a six-party network, four users measure in X and the two remaining users can measure in Z or X, as required by the protocol. As a result, the generation rate of the Bell pairs is the same as the full-sized GHZ state as post-selecting on six-folds is required for the $N = 6$ case.

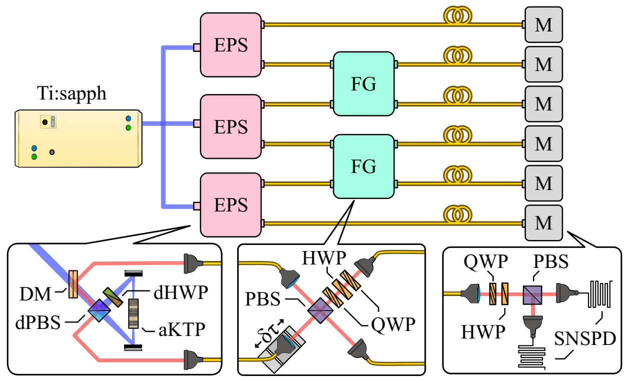

Fig. 2. Experimental setup. A pulsed Ti:sapphire laser pumps three entangled photon-pair sources (EPS). Each EPS embeds an aKTP crystal in a Sagnac configuration consisting of a dual-wavelength polarizing beamsplitter (dPBS), half-wave plate (dHWP), and dichroic mirror (DM). Photon pairs are separated by the dPBS and coupled into single-mode fibers. Fusion gates (FGs) are realized by interfering two photons on a PBS, with a delay stage ($\delta\tau$) to ensure temporal indistinguishability. Two quarter-wave plates (QWPs) and a HWP compensate for phase effects in the FGs. All six photons are then sent to measurement stages (M) featuring a QWP, a HWP, and a PBS whose outputs are fed to superconducting nanowire single-photon detectors (SNSPDs), operating with a nominal quantum efficiency of 80%.

We first evaluate the performance of the AQCKA protocol without multi-partite entanglement, henceforth denoted AQCKA$_B$ and detailed in Supplement 1, by measuring the noise of all 15 configurations of Bell pairs in the six-user network, indexed by q and t, where $q, t \in \{1, \ldots, 6\}$ and $t > q$. In each case we measure the quantum bit error rate ($Q^{q,t}_{Zb}$) and phase error ($Q^{q,t}_{Xb}$), respectively. Each user pair implements the BBM92 protocol [27] to establish secret bipartite keys, whose asymptotic key rate (AKR) is given by $\sigma^{q,t}_{\mathrm{B}} = 1 - h(Q^{q,t}_{Zb}) - h(Q^{q,t}_{Xb})$, where $h(\cdot)$ denotes the binary entropy function. These key rates dictate the overall performance of AQCKA$_B$ as the protocol relies exclusively on the bipartite keys to transmit the conference key directly to the keyholders. In particular, in the asymptotic limit, the amount of bipartite keys used for the initial designation of each users' role becomes negligible—which is also the case for AQCKA with multi-partite entanglement. What impacts the performance of AQCKA_B is the distribution of the conference key to the intended keyholders: for each conference key bit, the protocol consumes $N(N-1)$ bipartite key bits, independently of the number of keyholders. The theoretical scaling is $2(N-1)$ when a network can distribute multiple Bell pairs per round [15]; however, in this work only one Bell pair is obtained per round. The resulting AKR for AQCKA_B is $r_B^{\infty} = 0.0109(2)$; see Supplement 1 for details. We note that the AQCKA approach without multi-partite entanglement does not require anonymity in its quantum phase (when the bipartite keys are established) and can thus rely on conventional QKD primitives. The anonymous distribution of the conference key is then carried out with classical anonymous messaging primitives [19] based on the established bipartite keys.

Next, we evaluate the performance of AQCKA_M exploiting multi-partite entanglement from our six-party GHZ states. Once users are notified of their roles, non-keyholders measure only in the X basis while keyholders measure in either Z for key generation or X for test rounds, according to the prescribed test-key sequence. The group collectively estimate Q_X by announcing their X measurement outcomes using anonymous messaging primitives. Unlike in conventional conference key agreement protocols, the key error rate Q_Z, which is defined as the maximum pair-wise error, is not estimated during the protocol. Instead, the keyholders will use a pre-established Q_Z that is representative of the network, which allows fewer anonymous messaging rounds while allowing error correction to take place; see Supplement 1 for more details on the AQCKA_M protocol. To provide a complete characterization of the network, we measure Q_Z for all possible configurations of keyholders. We obtain the asymptotic key rate using the largest measured Q_Z to ensure the number of keyholders is hidden, of $r_M^{\infty} = 0.235(12)$, which corresponds to an increase over the AQCKA protocol without multi-parite entanglement of $r_M^{\infty}/r_B^{\infty} = 21.6(1.1)$. Theoretically we expect a ratio of 30 for our $N = 6$ network; however, this only holds for symmetric noise. In practice, channel noise will impose a higher penalty on the AQCKA_M protocol, as we must assume the maximal link noise to preserve anonymity.

Using the same data set, we evaluate the performance of a related AQCKA task, denoted "fully AQCKA" in [15], with a stronger anonymity condition where keyholders' identities are now hidden even from each other, except from the sender who designates the keyholders. The immediate consequence of this modification is that the keyholders can no longer use a pre-shared conference key to perform efficient multi-party error correction; instead they must use the costlier bipartite private channels. Similarly, the amount of bipartite resources consumed by the protocol without multi-partite entanglement increases by an additional $(N-1)$ to hide the sender's identity. In this scenario, a maximum multi-partite resource advantage of $N(N-1)^2$ can be obtained, which, for $N = 6$, is 150. However, this advantage quickly diminishes with increasing Q_Z, due to a larger overhead in the required anonymous messaging for error correction. Our noise parameters lead to $r_{\text{fully-}M}^{\infty} = 0.0075(6)$, which equates to a multi-partite resource advantage of 3.42(27), in line with the Q_Z dependence. For further information on this scaling, see Supplement 1.

When a finite number of rounds is performed, the correct designation of the users' roles, the conference key security, and the anonymity of the keyholders cannot be attained with certainty. To account for a small probability of failure, ϵ, for each of these three features, we adopt the ϵ-secure framework introduced in [15] as an extension of QKD composability [28]. In this framework, the conference key length (ℓ) depends on the total protocol rounds (L_{tot}), and on ϵ. For example, the conference key length of AQCKA_M with finite-key effects reads

$$\ell = L \cdot (1-p)\,[1 - h\,(Q_X + \gamma) - h\,(Q_Z)] - L \cdot h(p) - C, \tag{1}$$

where L is the number of multi-partite rounds, p is the fraction of multi-partite rounds used for parameter estimation, and γ is the statistical fluctuation of Q_X. We do not consider statistical fluctuations of Q_Z since the accepted error rate is fixed before running the protocol and does not affect the secrecy of the key. Finally, $C > 0$ is a constant that includes some of the ϵ parameters: $C = \log_2(2(N-1)/\epsilon_{EC}) + 2\log_2(1/2\epsilon_{PA}) + N$. Both γ and L are functions of L_{tot}, p, and the ϵ parameters. The total security parameter of the protocol depends on the ϵ parameters and is fixed to $\epsilon_{tot} = 1 \times 10^{-8}$. See Supplement 1 for more details.

We analyze the finite-key rate (FKR) of AQCKA_M in a smaller network of $N = 4$ users, with three users being keyholders, to increase the raw key generation rate. In L multi-partite rounds, the users share four-photon GHZ states to extract shared key bits. In $L_B = L_{tot} - L$ bipartite rounds, Bell pairs are shared between pairs of users to establish six bipartite keys used for anonymous classical subprotocols. The FKR is defined as the fraction of secure conference key bits established per round (ℓ/L_{tot}). In Fig. 3 we optimized the FKR by numerically maximizing the key length in Eq. (1) over the ϵ parameters and p for a fixed total security parameter. In this set up, we initially measured Q_X and Q_Z to be 0.0304(1) and 0.0160(3), respectively, and use these noise parameters to numerically simulate the FKR, shown as the blue trend line in Fig. 3. Furthermore, we measured $Q_{Zb} = 0.0144(3)$ and extrapolated ℓ', the AQCKA_B FKR (red line in Fig. 3). The definition of ℓ' is given in Supplement 1. We observe that AQCKA_M outperforms AQCKA_B in the finite key regime for $L_{tot} > 2 \times 10^5$.

Ideally, a round constitutes all users detecting one photon in a given time window—we only keep rounds satisfying this outcome. The yellow points in Fig. 3 show the experimentally measured FKR for increasing L_{tot} up to 6.5 M rounds, taking approximately 130 h of measurement time. Each data point has a fixed Q_Z, but a different Q_X found by evaluating the average error in the joint-X

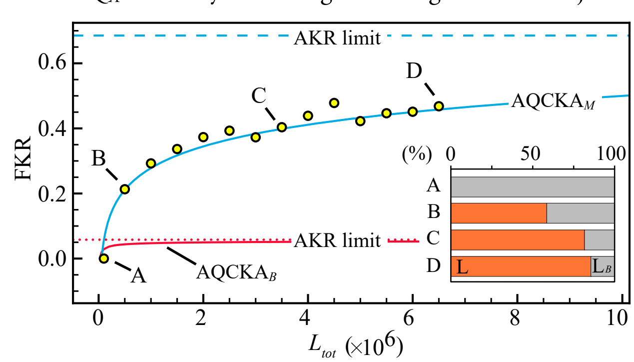

Fig. 3. Finite-key rate performance for AQCKA_M and AQCKA_B versus total rounds L_{tot}. Yellow points are the measured AQCKA_M, blue solid line is the simulated AQCKA_M FKR using fixed noise parameters (see main text) and the red solid line is the simulated result for AQCKA_B FKR. The AKR assuming these noise parameters is shown as the dashed lines for both scenarios. The inset shows the fraction of bipartite (L_B) and multi-partite rounds (L) as a fraction of total rounds L_{tot} for data points A–D of AQCKA_M.

measurements from a random sample of $L \cdot p$ test rounds. We account for finite-key effects even in the pair-wise key generation with the L_B rounds, where Q_{Zb} is also fixed to the maximum pair-wise error rate: 0.0144(3). We highlight four points, labeled A–D, and show in the inset how their respective L_{tot} is decomposed into multi-partite and bipartite rounds. At D, with 6.5 M rounds and an FKR of 0.47, we obtained a secure and anonymous conference key over 2.6 Mbits.

The drastic resource advantage AQCKA_M offers is observed in networks, and similar to our work on network QCKA [13], our premise is that the multi-node network resources are provided in the background, as might be the case in a future quantum Internet. Despite the considerable resource overhead, with current state-of-the-art photon sources it would be faster to generate anonymous conference keys via point-to-point connections. However, at present this approach is limited to trusted-node networks. While the advantage we observed for fully-AQCKA_M was lower than for AQCKA_M, it has a much greater potential for low error rates $Q_Z < 1\%$, which would be the case in a quantum network that incorporates entanglement purification [29–31].

When analyzing AQCKA_M with finite key effects, we find that the number of rounds required for parameter estimation is saturated by a very small fraction of the total rounds. This has the benefit of a greater fraction of total rounds being allocated as multi-partite rounds for distilling a raw key, as well as requiring fewer bipartite rounds for the anonymous classical subprotocols. Nevertheless, this comes at the cost of a larger statistical correction when estimating Q_X, which leads to a larger amount of key reduction in the privacy amplification step. Indeed, even in the regime of $> 1\ M$ total rounds, the majority of rounds are multi-partite rounds used for key generation, yet a fairly modest FKR is obtained. This is due to the statistical correction term, γ, whose value of 0.03 is comparable to the measured Q_X term.

In conventional non-anonymous quantum conference key agreement (QCKA) [12] the statistical correction can be reduced by increasing the share of parameter estimation rounds on the multi-partite entangled state, i.e., by increasing p. However, in AQCKA_M, this would also increase the number of bipartite rounds required to run the anonymous classical subprotocols, which in turn would further decrease the number of multi-partite rounds used for key generation, making this choice disadvantageous. This effect is ascribed to the additional security feature in AQCKA compared to QCKA, i.e., the anonymity of the keyholders. In the AQCKA_B protocol, this behavior is not observed as the pair-wise keys are established with conventional QKD schemes, but distilling the conference key anonymously requires $N(N-1)$ more resources than AQCKA_M.

As quantum networks grow, so does the need for anonymity, and our work highlights the significant resource advantages AQCKA can gain in a network. It is already established that the multi-partite advantage for QCKA also appears in protocols such as quantum secret sharing [32] or distributed sensing [6], and it is very likely that the AQCKA advantage will similarly extend to protocols such as election voting [33,34], distributed parameter estimation [35,36], or multi-party computation. Modifying these protocols for such a resource advantage is the focus of future work.

Funding. Deutsche Forschungsgemeinschaft ((ML4Q) EXC 2004/1-390534769, BR2159/6-1); Engineering and Physical Sciences Research Council (EP/T001011/1).

Acknowledgments. Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 – 390534769 and DFG (Deutsche Forschungsgemeinschaft) Individual Grant BR2159/6- 1.

Disclosures. The authors declare no conflicts of interest.

Data availability. Additional data is available upon request.

Supplemental document. See Supplement 1 for supporting content.

REFERENCES

1. I. Ingemarsson, D. Tang, and C. Wong, IEEE Trans. Inf. Theory **28**, 714 (1982).
2. C. Blundo, A. De Santis, A. Herzberg, *et al.*, in *Advances in Cryptology* (1993), pp. 471–486.
3. M. Burmester and Y. Desmedt, in *Advances in Cryptology* (1995), pp. 275–286.
4. X. Guo, C. R. Breum, J. Borregaard, *et al.*, Nat. Phys. **16**, 281 (2020).
5. P. Kómár, E. M. Kessler, M. Bishof, *et al.*, Nat. Phys. **10**, 582 (2014).
6. L.-Z. Liu, Y.-Z. Zhang, Z.-D. Li, *et al.*, Nat. Photonics **15**, 137 (2021).
7. M. Tubaishat and S. Madria, IEEE Potentials **22**, 20 (2003).
8. Z. Huang, S. K. Joshi, D. Aktas, *et al.*, npj Quantum Inf. **8**, 25 (2022).
9. M. Epping, H. Kampermann, C. Macchiavello, *et al.*, New J. Phys. **19**, 093012 (2017).
10. F. Grasselli, H. Kampermann, and D. Bruß, New J. Phys. **21**, 123002 (2019).
11. G. Murta, F. Grasselli, H. Kampermann, *et al.*, Adv. Quantum Technol. **3**, 2000025 (2020).
12. M. Proietti, J. Ho, F. Grasselli, *et al.*, Sci. Adv. **7**, eabe0395 (2021).
13. A. Pickston, J. Ho, A. Ulibarrena, *et al.*, npj Quantum Inf. **9**, 82 (2023).
14. F. Hahn, J. de Jong, and A. Pappa, PRX Quantum **1**, 020325 (2020).
15. F. Grasselli, G. Murta, J. de Jong, *et al.*, PRX Quantum **3**, 040306 (2022).
16. A. Pirker, J. Wallnöfer, and W. Dür, New J. Phys. **20**, 053054 (2018).
17. F. Hahn, A. Pappa, and J. Eisert, npj Quantum Inf. **5**, 76 (2019).
18. S. Wengerowsky, S. K. Joshi, F. Steinlechner, *et al.*, Nature **564**, 225 (2018).
19. A. Broadbent and A. Tapp, in *Advances in Cryptology (ASIACRYPT)* (2007), pp. 410–426.
20. C. Thalacker, F. Hahn, J. de Jong, *et al.*, New J. Phys. **23**, 083026 (2021).
21. J. de Jong, F. Hahn, J. Eisert, *et al.*, Quantum **7**, 1117 (2023).
22. L. Rückle, J. Budde, J. de Jong, *et al.*, Phys. Rev. Res. **5**, 033222 (2023).
23. F. Graffitti, P. Barrow, M. Proietti, *et al.*, Optica **5**, 514 (2018).
24. A. Pickston, F. Graffitti, P. Barrow, *et al.*, Opt. Express **29**, 6991 (2021).
25. A. Fedrizzi, T. Herbst, A. Poppe, *et al.*, Opt. Express **15**, 15377 (2007).
26. G. Tóth and O. Gühne, Phys. Rev. A **72**, 022340 (2005).
27. C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
28. C. Portmann and R. Renner, Rev. Mod. Phys. **94**, 025008 (2022).
29. J.-W. Pan, C. Simon, Č. Brukner, *et al.*, Nature **410**, 1067 (2001).
30. W. Dür, H. Aschauer, and H.-J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).
31. X.-M. Hu, C.-X. Huang, Y.-B. Sheng, *et al.*, Phys. Rev. Lett. **126**, 010503 (2021).
32. N. Walk and J. Eisert, PRX Quantum **2**, 040339 (2021).
33. F. Centrone, E. Diamanti, and I. Kerenidis, Phys. Rev. Appl. **18**, 014005 (2022).
34. Q. Wang, C. Yu, F. Gao, *et al.*, Phys. Rev. A **94**, 022333 (2016).
35. H. Kasai, Y. Takeuchi, H. Hakoshima, *et al.*, J. Phys. Soc. Jpn. **91**, 074005 (2022).
36. N. Shettell, E. Kashefi, and D. Markham, Phys. Rev. A **105**, L010401 (2022).