nature COMMUNICATIONS

ARTICLE

Received 12 Mar 2016 | Accepted 13 Sep 2016 | Published 9 Nov 2016

DOI: 10.1038/ncomms13251 OPEN

Experimental verification of multipartite entanglement in quantum networks

W. McCutcheon[1], A. Pappa[2], B.A. Bell[1], A. McMillan[1], A. Chailloux[3], T. Lawson[4], M. Mafu[5], D. Markham[4], E. Diamanti[4], I. Kerenidis[6,7], J.G. Rarity[1] & M.S. Tame[8,9]

Multipartite entangled states are a fundamental resource for a wide range of quantum information processing tasks. In particular, in quantum networks, it is essential for the parties involved to be able to verify if entanglement is present before they carry out a given distributed task. Here we design and experimentally demonstrate a protocol that allows any party in a network to check if a source is distributing a genuinely multipartite entangled state, even in the presence of untrusted parties. The protocol remains secure against dishonest behaviour of the source and other parties, including the use of system imperfections to their advantage. We demonstrate the verification protocol in a three- and four-party setting using polarization-entangled photons, highlighting its potential for realistic photonic quantum communication and networking applications.

[1] Quantum Engineering Technology Laboratory, Department of Electrical and Electronic Engineering, University of Bristol, Woodland Road, Bristol BS8 1UB, UK. [2] School of Informatics, University of Edinburgh, Edinburgh EH89AB, UK. [3] INRIA, Paris Rocquencourt, SECRET Project Team, Paris 75589, France. [4] LTCI, CNRS, Telecom ParisTech, Université Paris-Saclay, 75013 Paris, France. [5] Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16, Palapye, Botswana. [6] CNRS IRIF, Université Paris 7, Paris 75013 France. [7] Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore. [8] School of Chemistry and Physics, University of KwaZulu-Natal, Durban 4001, South Africa. [9] National Institute for Theoretical Physics, University of KwaZulu-Natal, Durban 4001, South Africa. Correspondence and requests for materials should be addressed to A.P. (email: annapappa@gmail.com) or to M.S.T. (email: markstame@gmail.com).

Entanglement plays a key role in the study and development of quantum information theory and is a vital component in quantum networks[1–5]. The advantage provided by entangled states can be observed, for example, when the quantum correlations of the n-party Greenberger–Horne–Zeilinger (GHZ) state[6] are used to win a nonlocal game with probability 1, while any classical local theory can win the game with probability at most 3/4 (see ref. 7). In a more general setting, multipartite entangled states allow the parties in a network to perform distributed tasks that outperform their classical counterparts[8], to delegate quantum computation to untrusted servers[9], or to compute through the measurement-based quantum computation model[10]. It is therefore vital for parties in a quantum network to be able to verify that a state is entangled, especially in the presence of untrusted parties and by performing only local operations and classical communication.

A protocol for verifying that an untrusted source creates and shares the n-qubit multipartite entangled GHZ state, $|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$, with n parties has recently been proposed[11]. In the verification protocol, the goal of the honest parties is to determine how close the state they share is to the ideal GHZ state and verify whether or not it contains genuine multipartite entanglement (GME)—entanglement that can only exist if all qubits were involved in the creation of the state[1]. On the other hand, any number of dishonest parties that may collaborate with the untrusted source are trying to 'cheat' by convincing the honest parties that the state they share is close to the ideal GHZ state and contains GME when this may not be the case. Verifying GME in multipartite GHZ states in this way is relevant to a wide variety of protocols in distributed quantum computation and quantum communication. While distributed quantum computation is at an early stage of development experimentally[12–14], many schemes for using multipartite GHZ states in distributed quantum communication have already been demonstrated, including quantum secret sharing[15], open-destination teleportation[16] and multiparty quantum key distribution[17,18]. This makes the entanglement verification protocol relevant for distributed quantum communication with present technology.

In order for a quantum protocol to be practical, however, it must take into account system imperfections, including loss and noise, throughout the protocol (generation, transmission and detection of the quantum state). In the previous work[11], it was shown that by using a suitable protocol, the closeness of a shared resource state to a GHZ state and the presence of GME can be verified in a distributed way between untrusted parties under perfect experimental conditions. However, the protocol is not tolerant to arbitrary loss and in fact it cannot be used for a loss rate that exceeds 50%.

In this work, we design and experimentally demonstrate a protocol that outperforms the original one in ref. 11. We examine quantitatively how a dishonest party can use system imperfections to boost their chances of cheating and show our protocol defends against such tactics. We demonstrate both the original and new protocols using a source of polarization-entangled photons, which produces three- and four-party GHZ states, and examine the performance of the protocols under realistic experimental conditions. Our results are perfectly adapted to photonic quantum networks and can be used to reliably verify multipartite entanglement in a real-world quantum communication setting. To achieve verification of a state in an untrusted setting, the protocols exploit the capability of GHZ states to produce extremal correlations, which are unobtainable by any quantum state that is not locally equivalent to the GHZ state. This property has been shown to bound state fidelities in the fully device-independent setting of nonlocality via self-testing[19–21]. In addition, a related recent study[22] has proposed a method to detect multipartite entanglement in the 'steering' setting, in which some of the devices are known to be untrusted (or defective), by using one-sided device-independent entanglement witnesses. Our protocols extend beyond these methods by allowing the amount of entanglement to be quantified in terms of an appropriate fidelity measure in a setting where some unknown parties are untrusted, as well as providing a method for dealing with loss and other inefficiencies in the system. This makes our protocols and analysis more appropriate for a realistic network setting.

Results

The verification protocol. The network scenario we consider consists of a source that shares an n-qubit state ρ with n parties, where each party receives a qubit. One of the parties, a 'Verifier', would like to verify how close this shared state is to the ideal state and whether or not it contains GME. The protocol to do this is as follows: first, the Verifier generates random angles $\theta_j \in [0,\pi)$ for all parties including themselves ($j \in [n]$), such that $\sum_j \theta_j$ is a multiple of π. The angles are then sent out to all the parties in the network. When party j receives their angle from the Verifier, they measure in the basis $\{|+_{\theta_j}\rangle, |-_{\theta_j}\rangle\} = \{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_j}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - e^{i\theta_j}|1\rangle)\}$ and send the outcome $Y_j = \{0, 1\}$ to the Verifier. A flow diagram of the protocol is shown in Fig. 1a, where the order in which the angles are sent out and outcomes returned is irrelevant and it is assumed that the Verifier and each of the parties share a secure private channel for the communication. This can be achieved by using either a one-time pad or quantum key distribution[3], making the communication secure even in the presence of a quantum computer. The state passes the test when the following condition is satisfied: if the sum of the randomly chosen angles is an even multiple of π, there must be an even number of 1 outcomes for Y_j, and if the sum is an odd multiple of π, there must be an odd number of 1 outcomes for Y_j. We can write this condition as

$$\oplus_j Y_j = \frac{1}{\pi}\sum_j \theta_j \qquad (\mathrm{mod}\ 2). \tag{1}$$

For an ideal n-qubit GHZ state, the test succeeds with probability 1 (see Supplementary Note 1). Moreover, it can be shown that the fidelity $F(\rho) = \langle \mathrm{GHZ}_n|\rho|\mathrm{GHZ}_n\rangle$ of a shared state ρ with respect to an ideal GHZ state can be lower bounded by a function of the probability of the state passing the test, $P(\rho)$. If we first suppose that all n parties are honest, then $F(\rho) \geq 2P(\rho) - 1$ (see Supplementary Note 1). Furthermore, we can say that GME is present for a state ρ when $F(\rho) > 1/2$ with respect to an ideal GHZ state[23], and therefore GME can be verified when the pass probability is $P(\rho) > 3/4$. This verification protocol, that we will call the 'θ-protocol', is a generalization of the protocol in ref. 11, called the 'XY-protocol', where the angles θ_j are fixed as either 0 or $\pi/2$, corresponding to measurements in the Pauli X or Y basis. In the honest case and under ideal conditions, the lower bound for the fidelity is the same in both protocols.

When the Verifier runs the test in the presence of $n-k$ dishonest parties, the dishonest parties can always collaborate and apply a local or joint operation U to their part of the state. This encompasses the different ways in which the dishonest parties may try to cheat in the most general setting. Hence, we look at a fidelity measure given by $F'(\rho) = \max_U F((\mathbb{I}_k \otimes U_{n-k})\rho(\mathbb{I}_k \otimes U^\dagger_{n-k}))$, and lower bound it by the pass probability as $F'(\rho) \geq 4P(\rho) - 3$ for both the θ and XY protocols (see Supplementary Note 1). This gives directly a bound of $P(\rho) > 7/8 = 0.875$ to observe GME. However, by concentrating on attacks for the case $F'(\rho) = 1/2$, tighter analysis

can be performed (see Supplementary Note 1), where the GME bound can be shown to be $P(\rho)\geq 1/2+1/\pi\approx 0.818$ for the θ-protocol and $P(\rho)\geq\cos^2(\pi/8)\approx 0.854$ for the XY protocol. The θ-protocol is more sensitive to detecting cheating and hence can be used to verify GME more broadly in realistic implementations where the resources are not ideal.

The above bounds do not account for loss. To analyse cheating strategies, which take advantage of loss, we must allow the dishonest parties (which have potentially perfect control of the source and their equipment) to choose to declare 'loss' at any point. In particular, they may do this when they are asked to make measurements that would reduce the probability of success, making the round invalid, which can skew the statistics in favour of passing to the advantage of the dishonest parties. This may change the fidelity and GME bounds above. We address this to find GME bounds in the case of loss in our photonic realization.

Experimental setup. The optical setup used to perform the verification protocols is shown in Fig. 1b. The source of GHZ states consists of two micro-structured photonic crystal fibres (PCFs), each of which produces a photon pair by spontaneous four-wave mixing, with the signal wavelength at 623 nm and the idler at 871 nm (see Supplementary Note 2). To generate entangled pairs of photons, each fibre loop is placed in a Sagnac configuration, where it is pumped in both directions. When the pump pulse entering the Sagnac loop is in diagonal polarization, conditional on a single pair being generated by the pump laser, the state exiting the polarizing beamsplitter (PBS) of the loop is in the Bell state $\frac{1}{\sqrt{2}}\left(|H\rangle_{\rm s}|H\rangle_{\rm i}+|V\rangle_{\rm s}|V\rangle_{\rm i}\right)$, with s and i indicating the signal and idler photons, respectively[24,25]. The signal and idler photons of each source are then separated into individual spatial modes by dichroic mirrors, after which the two signal photons are overlapped at a PBS that performs a parity check, or 'fusion' operation[26,27]. We postselect with 50% probability the detection outcomes in which one signal photon emerges from each output mode of the PBS, which projects the state onto the four-photon GHZ state

$$\frac{1}{\sqrt{2}}\left(|H\rangle_{\rm i_1}|H\rangle_{\rm s_1}|H\rangle_{\rm s_2}|H\rangle_{\rm i_2}+|V\rangle_{\rm i_1}|V\rangle_{\rm s_1}|V\rangle_{\rm s_2}|V\rangle_{\rm i_2}\right). \quad (2)$$

All four photons are then coupled into single-mode fibres, which take them to measurement stages representing the parties in the network. With appropriate angle choices of the wave plates included in these stages, any projective measurement can be made by the parties on the polarization state of their photon[28]. In our experiment, the successful generation of the state is conditional on the detection of four photons in separate modes, that is, postselected. In principle, it is possible to move beyond postselection in our setup, where the GHZ states are generated deterministically. This can be achieved by the addition of a quantum non-demolition measurement of the photon number in the modes after the fusion operation. While technically challenging, quantum non-demolition measurements are possible for photons, for instance as theoretically shown[29,30] and experimentally demonstrated[31]. By using postselection, we are able to give a proof-of-principle demonstration of the protocols and gain important information about their performance in such a scenario, including the impact of loss.

In our experiments, we use both a three- and a four-photon GHZ state. The generation of the three-photon state requires only a slight modification to the setup, with one of the PCFs pumped in just one direction to generate unentangled pairs (see Supplementary Note 2). Before carrying out the verification protocols, we first characterize our experimental GHZ states by performing quantum state tomography[28]. The resulting density matrices for the three- and four-photon GHZ states are shown in Fig. 2 and have corresponding fidelities $F_{\rm GHZ_3}=0.80\pm 0.01$ and $F_{\rm GHZ_4}=0.70\pm 0.01$ with respect to the ideal states. These fidelities compare well with other recent experiments using photons (see Table 1) and are limited mainly by dephasing from the fusion operation[26] and higher-order emission (see Supplementary Note 2). The errors have been calculated using maximum likelihood estimation and a Monte Carlo method with Poissonian noise on the count statistics, which is the dominant source of error in our photonic experiment[28].

Entanglement verification. To demonstrate the verification of multipartite entanglement, we use the polarization degree of freedom of the photons generated in our optical setup. The computational basis states sent out to the parties are therefore defined as $|0\rangle=|H\rangle$ and $|1\rangle=|V\rangle$ for a given photon. Furthermore, the verification protocol relies on a randomly selected set of angles being distributed by the Verifier for each state being tested. To ensure dishonest parties have no prior knowledge, the set of angles is changed after every detection of a copy of the state, that is, we perform single-shot measurements in our experiment. To achieve this, we use automated wave-plate rotators to change the measurement basis defined by the randomized angles for each state. The rotators are controlled by a computer with access to the incoming coincidence data. This approach is needed to provide a faithful demonstration of the protocol and is technologically more advanced than the usual method used in photonic quantum information experiments, where many detections are accumulated over a fixed integration time for a given measurement basis and properties then inferred from the ensemble of states. We now analyse the performance of the XY and θ verification protocols for the three- and four-party GHZ states.

Verification of three-party GHZ. The XY verification protocol was initially carried out using the three-photon GHZ state, with all parties behaving honestly. The first two angles θ_j were randomly chosen to be either 0 or $\pi/2$, with the third angle representing the Verifier being decided so that $\sum_j\theta_j$ is a multiple of π. After repeating the protocol on 6,000 copies of the state, the pass probability was found to be 0.838 ± 0.005. Similarly, the θ-protocol was carried out, with the first two angles chosen uniformly at random from the continuous range $[0,\pi)$. After 6,000 copies of the state were prepared and measured, the pass probability was found to be 0.834 ± 0.005.

Using the relation between the fidelity and the pass probability, $F(\rho)\geq 2P(\rho)-1$, the Verifier can conclude that the fidelity with respect to an ideal GHZ state is at least 0.676 ± 0.010 for the XY-protocol and at least 0.668 ± 0.010 for the θ-protocol. These values are consistent with the value obtained using state tomography. Despite the non-ideal experimental resource, the lower bound on the fidelity is clearly above 1/2 and therefore sufficient for the Verifier to verify GME in this all honest case.

More importantly, the θ-protocol enables the Verifier to verify GME even when they do not trust all of the parties. Indeed, the experimental value of the pass probability, 0.834, exceeds by more than 3 s.d. the GME bound of 0.818 for the dishonest case. We remark that for verifying GME in these conditions, we crucially used the fact that our three-qubit GHZ state has very high fidelity and that the θ-protocol has improved tolerance to noise. In fact, the Verifier is not able to verify GME using the XY-protocol, since the experimental value of 0.838 does not exceed the GME bound of 0.854.

Theoretical verification of three-party GHZ with losses. We now investigate the impact of loss on the performance

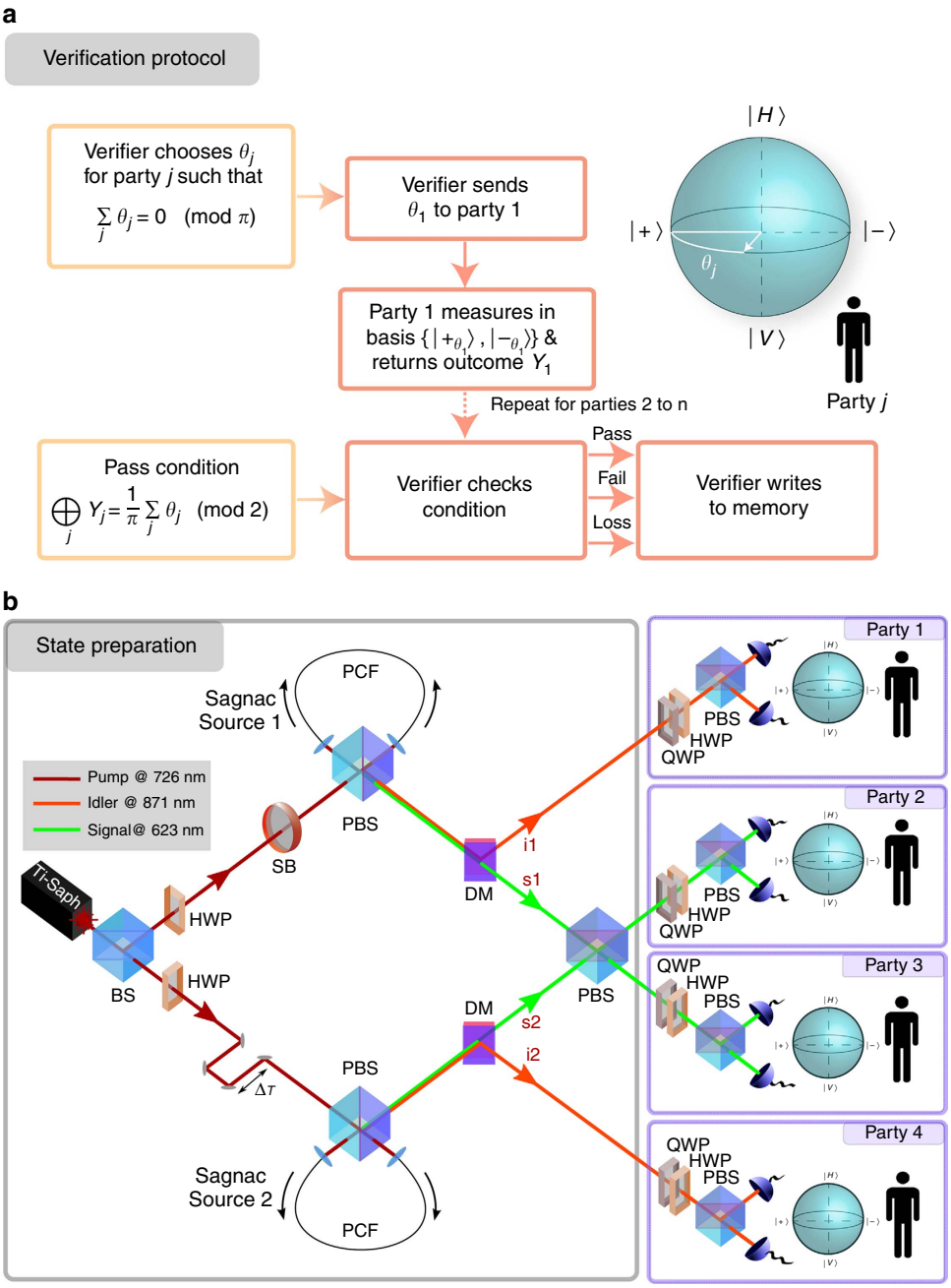

Figure 1 | The verification protocol and experimental setup. (**a**) A flow diagram showing the steps of the verification protocol. (**b**) The experimental setup for state preparation, consisting of a femto-second laser (Spectra-Physics Tsunami) filtered to give 1.7 nm bandwidth pulses at 726 nm. The laser beam is split by a beamsplitter into two modes with the polarization set to diagonal by half-wave plates. One mode undergoes a temporal offset, ΔT, using a translation stage and the other a phase rotation using a Soleil–Babinet compensator. The modes each enter a PCF source via a PBS in a Sagnac configuration, enabling pumping in both directions. The sources generate non-degenerate entangled signal and idler photon pairs by spontaneous four-wave mixing. Temperature tuning in one of the sources is used to match the spectra of the resulting signal photons in the other source. The entangled photon pairs exit the sources via the PBS and due to their non-degenerate wavelengths they are separated by dichroic mirrors and filtered with $\Delta\lambda_s = 40$ nm at $\lambda_s = 623$ nm (tunable $\Delta\lambda_i = 2$ nm at $\lambda_i = 871$ nm) in the signal (idler) to remove any remaining light from the pump laser. The signal photons from each pair interfere at a PBS and all photons are collected into single-mode fibres. Pairs of automated half- and quarter-wave plates on each of the four output modes from the fibres allow arbitrary rotations to be made before the modes are split by PBSs and the light is detected by eight silicon avalanche photodiode detectors. The protocol's software (outlined in panel (**a**)) is linked to an eight-channel coincidence counting box (Qumet MT-30A) and the automated wave plates to set each unique measurement basis for the parties and detect single-shot four-fold coincidences.

of the verification protocols. In this setting, the Verifier is willing to accept up to a certain loss rate from each party. When a party declares loss, the specific run of the protocol is aborted and the Verifier moves on to testing the next copy of the resource state. A dishonest party, who may not have the maximum allowed loss rate in their system, or may even have no loss at all, can increase the overall pass probability of the state by declaring loss whenever the probability to pass a specific measurement request from the Verifier is low.

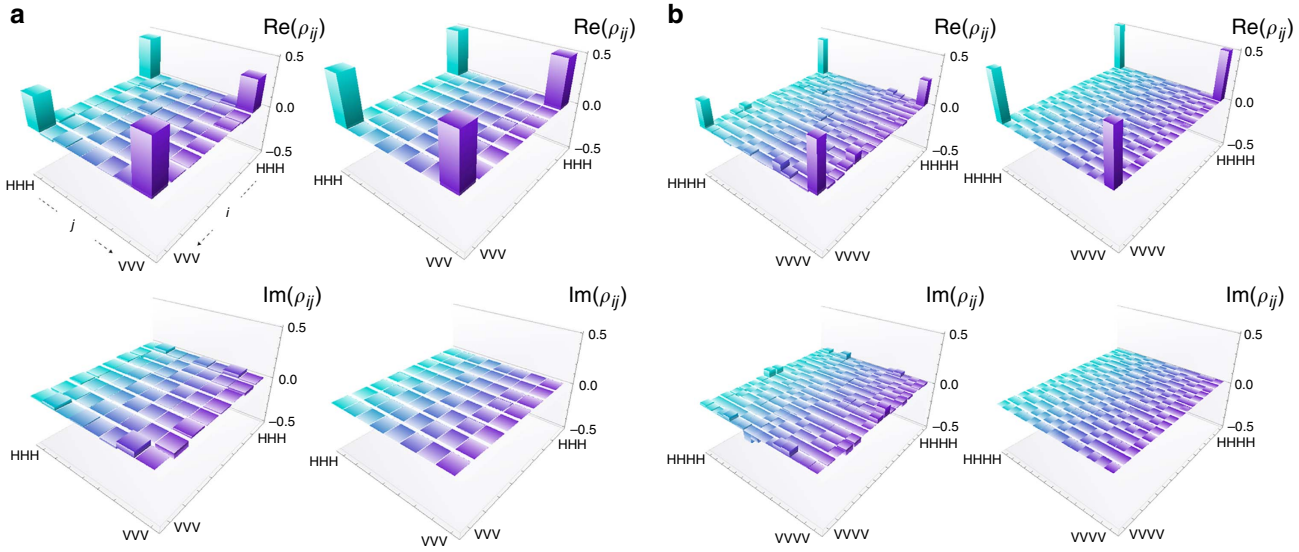

Figure 2 | Tomographic reconstruction of the three- and four-photon GHZ states used in the protocols. (**a**) Three-photon GHZ state (left column) and ideal case (right column). (**b**) Four-photon GHZ state (left column) and ideal case (right column). Top row corresponds to the real parts and bottom row corresponds to the imaginary parts. The density matrix elements are given by $\rho_{ij} = \langle i|\rho_{\text{exp}}|j\rangle$, where ρ_{exp} is the reconstructed experimental density matrix.

Table 1 | Comparison of GHZ fidelities.

Three-photon GHZ fidelity	Four-photon GHZ fidelity
$F = 0.80 \pm 0.01$, This work	$F = 0.70 \pm 0.01$, This work
$F = 0.768 \pm 0.015$, K. Resch *et al.*[33]	$F = 0.840 \pm 0.007$, Z. Zhao *et al.*[34]
$F = 0.74 \pm 0.01$, X.-Q. Zhou *et al.*[35]	$F = 0.66 \pm 0.01$, B. Bell *et al.*[27]
$F = 0.811 \pm 0.002$, H.-X. Lu *et al.*[36]	$F = 0.833 \pm 0.004$, X.-L. Wang *et al.*[37]
$F = 0.93 \pm 0.01$, R.B. Patel *et al.*[38]	

The table shows the fidelity of recent three-photon and four-photon GHZ states from other experiments, and includes the fidelities from this work (top row).

For example, a non-GME state can have pass probability 1 for the *XY*-protocol when the allowed loss rate is 50%. In this case, the source can share a state of the form $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \otimes |+\rangle$, where the third qubit is sent to a dishonest party. Then, when the latter is asked to measure in the Pauli X basis, the party always answers correctly; while when asked to measure in the Pauli Y basis, it declares loss. Of course, such a strategy would alert the Verifier that the party is cheating, since the party is always declaring loss when asked to measure in the Y basis, while when asked to measure in the X basis, the party always measures the $|+\rangle$ eigenstate. However, if the source and the dishonest party are collaborating, and the source is able to create and share any Bell pair with the two honest parties, then the test can be passed each time without the cheating detected. The dishonest strategy would go as follows: the source sends randomly one of the four states $\{\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle), \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle), \frac{1}{\sqrt{2}}(|HH\rangle + i|VV\rangle), \frac{1}{\sqrt{2}}(|HH\rangle - i|VV\rangle)\}$ and tells the dishonest party which one was sent, so that the latter can coordinate its actions. For the first state, the party replies 0 only for the X basis; for the second state, it replies 1 only for the X basis; for the third, it replies 1 only for the Y basis; and for the fourth, it replies 0 only for the Y basis.

More generally, we can analytically find the GME bound as a function of the loss rate for both protocols and describe optimal cheating strategies to achieve these bounds with non-GME states. The optimal cheating strategy for the *XY*-protocol consists of the source rotating the non-GME state that is sent to the honest parties in a specific way depending on the amount of loss allowed, and informing the dishonest party about the rotation. For zero loss, the optimal state is the $\pi/4$-rotated Bell pair $\frac{1}{\sqrt{2}}(|HH\rangle + e^{i\frac{\pi}{4}}|VV\rangle)$, while for 50% loss, the optimal state is the Bell pair $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$. For any loss, λ, in between, the dishonest strategy is a probabilistic mixture of these two strategies; it consists of sending the Bell pair with probability 2λ (and discarding the rounds in which the dishonest party is asked to measure Y), and the $\pi/4$-rotated Bell pair with probability $1-2\lambda$. In both, the strategy mentioned in the previous paragraph for avoiding detection of the dishonest party's cheating is required. On the other hand, the optimal strategy for the θ-protocol is having the source send a rotated Bell pair with the dishonest party declaring loss for the angles that have the lowest pass probability (see Supplementary Note 1).

The upper bounds of the pass probability for the optimal cheating strategies using a non-GME state are shown as the solid turquoise and purple upper curves in Fig. 3, for the *XY* and θ-protocol, respectively. Specifically for the case of no loss, we recover the GME bounds of 0.854 and 0.818 for the *XY*- and θ-protocol, respectively. The GME bound for the *XY*-protocol reaches 1 for 50% loss, while the GME bound for the θ-protocol reaches 1 only at 100% loss.

Experimental verification of three-party GHZ with losses. In Fig. 3a, one can see the experimental value of 0.834 ± 0.005 when there is no loss for the θ-protocol enables the Verifier to verify GME in the presence of up to $\sim$5% loss—once the loss increases past 5%, the Verifier can no longer guarantee the shared experimental state has GME. Again, this loss tolerance is only possible due to the high fidelity of our three-party GHZ state and the fact that our θ-protocol has a better behaviour with respect to loss. The tolerance to loss can be further improved using experimental states with higher fidelities. However, it is interesting to note that 5% loss corresponds to $\sim$1 km of optical fibre, which already makes the protocol relevant to a quantum network within a small area, such as a city or government facility,

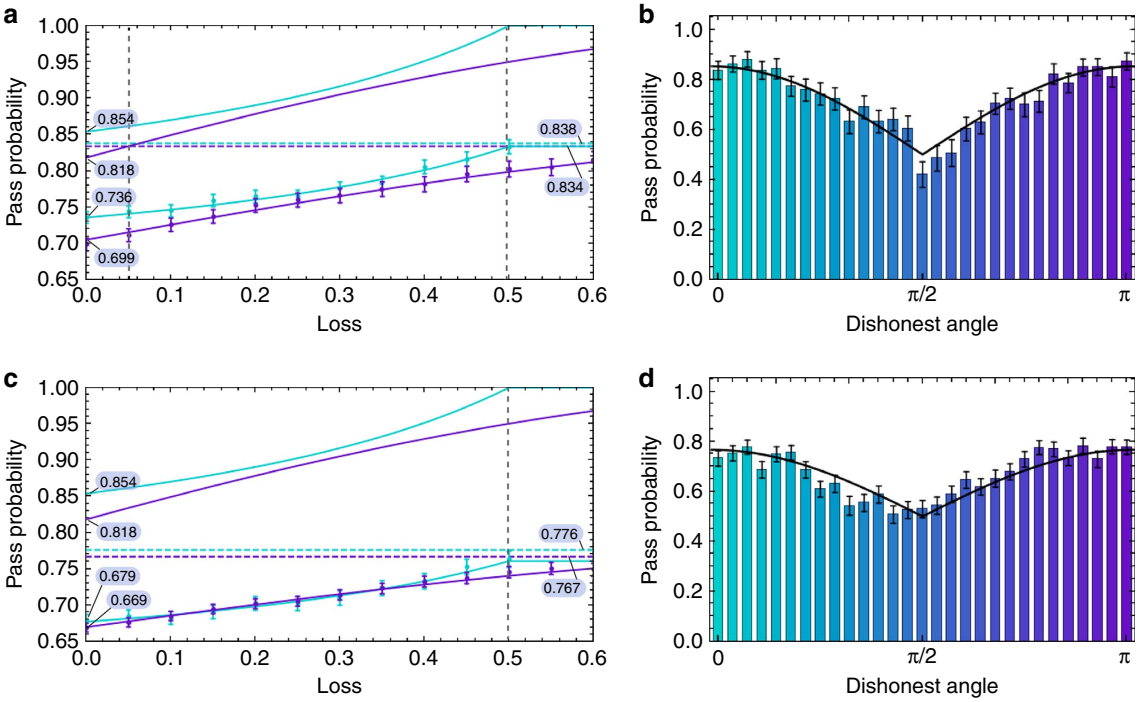

Figure 3 | Pass probabilities as a function of loss for one dishonest party in a three- and four-party setting. (**a**,**b**) correspond to the three-party setting, and (**c**,**d**) correspond to the four-party setting. The upper curves in **a** and **c** show the ideal theoretical case for the GME bound for the θ-protocol (purple curve) and a cheating strategy for the *XY*-protocol (turquoise curve) that always performs better. Note that the *XY*-protocol cannot be used here for verification as the non-GME dishonest value is always above the honest value. The lower solid curves in **a** and **c** correspond to the experimental results obtained for the three- and four-photon GHZ state, respectively. In both panels, the dashed lines correspond to the honest experimental values when there is no loss (turquoise for the *XY*-protocol and purple for the θ-protocol). (**a**,**c**) clearly show that the θ-protocol can tolerate loss $\gtrapprox 0.5$ in the ideal case. (**b**,**d**) show the optimal pass probability that the dishonest party can obtain when running the θ-protocol with no loss, for a given dishonest angle θ, for the three-party and four-party case, respectively. In all plots, the curves are a best fit to the data. All error bars represent the standard deviation and are calculated using a Monte Carlo method with Poissonian noise on the count statistics[28].

where a number of quantum communication protocols could be carried out over the network, such as, for instance quantum secret sharing[15], telecloning[32] and open destination teleportation[16].

Implementation of dishonest strategies for three-party GHZ. To maximize the pass probabilities of the protocols using a non-GME state, the source needs to appropriately rotate the state that is sent to the honest parties depending on the amount of loss allowed. We implemented this strategy for a single dishonest party by using a complementary method, where the source creates a three-qubit GHZ state and gets the dishonest party to perform a projective measurement that creates the necessary rotated non-GME state between the honest parties. This strategy was performed experimentally for both protocols on 3,000 copies of the three-qubit GHZ state. Since in our experiment, the GHZ states are created by postselection, the loss corresponds to the allowed percentage of tests in which the dishonest party can claim they lost their qubit during transmission of the corresponding photon from the source.

The pass probabilities are shown as a function of loss by the solid turquoise and purple lower curves in Fig. 3a. They show the same trend as the previous curves but are shifted lower due to the non-ideal experimental state. For the no loss case, we obtain a pass probability of 0.736 ± 0.008 for the *XY*-protocol. For the θ-protocol, the pass probability depends on the dishonest party's measurement request θ: for no loss, the experimental results are shown in Fig. 3b, from which we obtain an average pass probability of 0.699 ± 0.009. When loss is included, the dishonest party's cheating strategy leads to a higher pass probability, since the dishonest party claims loss when the angle given to him by the Verifier is close to $\pi/2$, corresponding to the minimum pass probability shown in Fig. 3b. Similar to the discussion in the example of the *XY*-protocol, the source collaborates with the dishonest party and applies a rotation to the shared state, so that the declared lost angles appear uniform and not always around $\pi/2$.

Verification of four-party GHZ. To check the performance of the protocols for a higher number of parties, the verification tests were carried out using the four-photon GHZ state generated in our experiment, now with three angles chosen randomly, and the fourth depending on the condition that $\sum_j \theta_j$ is a multiple of π. Again, we start with the all honest case where any of the parties may be the Verifier. For the *XY*-protocol, with all θ_j equal to 0 or $\pi/2$, the pass probability for 6,000 copies of the state was found to be 0.776 ± 0.005. For the θ-protocol, using 6,000 copies, the pass probability was found to be 0.767 ± 0.005.

As in the three-party case, the Verifier can conclude that the fidelity with respect to an ideal GHZ state is at least 0.552 ± 0.010 for the *XY*-protocol and at least 0.534 ± 0.010 for the θ-protocol, therefore just sufficient for the Verifier to verify that GME is present in the state. Again, the high fidelity of our experimental state is crucial for this result. Nevertheless, none of the two protocols can confirm GME in the presence of dishonest parties since the pass probabilities are below the GME bounds of 0.854 and 0.818, respectively.

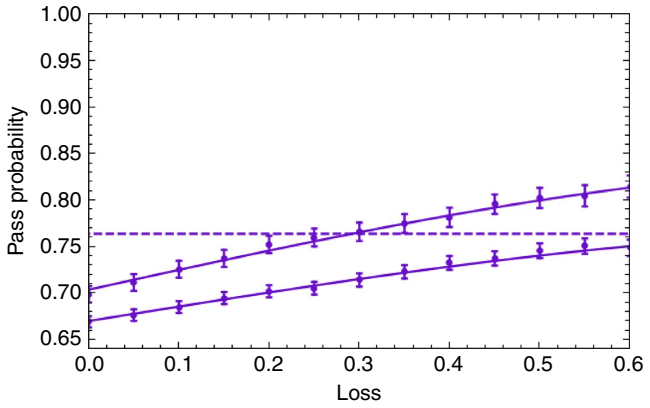

Figure 4 | Impact of noise and loss on the pass probability of the θ-verification protocol in a four-party setting. The lower curve corresponds to a biseparable state (four-qubit GHZ state with a projective measurement on the dishonest qubit) and the upper curve corresponds to a biseparable state (three-qubit GHZ state and an unentangled qubit for the dishonest player) that has less noise. The dashed line corresponds to the honest case. All error bars represent the standard deviation and are calculated using a Monte Carlo method with Poissonian noise on the count statistics[28].

Implementation of dishonest strategies for four-party GHZ. The dishonest strategies that are used to implement the two verification protocols for different amounts of loss are the same as in the three-party case. However, we proceed in two different ways for a single dishonest party. First, we have the source create our non-ideal four-qubit GHZ state and then allow the dishonest party to perform the dishonest projective measurement to create a non-GME state. When there is no loss, we obtain a pass probability of 0.679 ± 0.008 for the XY-protocol and 0.669 ± 0.008 for the θ-protocol (averaged over the dishonest angle θ, as shown in the histogram of Fig. 3d). When loss is included, the pass probabilities of both the XY- and θ-protocols increase, as the dishonest party uses the loss to their advantage (see Fig. 3c). A second way to implement the dishonest strategy is to have the source create the non-ideal three-qubit GHZ state for the honest parties and the dishonest party hold an unentangled photon. This results in a four-party non-GME state with reduced noise—as the dephasing from the entangled pair of the second PCF is no longer present[26]. We perform the θ-protocol with this better-quality resource state and see that the pass probability increases from 0.669 ± 0.005 to 0.698 ± 0.008 for the no loss case and remains higher when loss is included (see Fig. 4). Note that despite the second strategy having higher pass probabilities, these are still below the GME bound shown in Fig. 3c (upper purple curve).

The comparison of the two strategies shows that the projection method is not necessarily optimal for the dishonest party due to phase noise in the experimental state. Note also that as the pass probability of the experimental state in the honest case (dotted purple line in Fig. 3c) is below the GME bound, the Verifier is not able to verify GME for this four-party setting for any amount of loss. Verification of GME is achieved in our experiment only in the three-party setting. However, four-party verification could be achieved using experimental states with higher fidelities, and even with our non-ideal three-party GHZ state, we have been able to provide the first proof-of-principle demonstration of our GME verification protocol.

Discussion

The results we have presented are situated in a realistic context of distributed communication over photonic quantum networks: we have shown that it is possible for a party in such a network to verify the presence of GME in a shared resource, even when some of the parties are not trusted, including the source of the resource itself. This distrustful setting sets particularly stringent conditions on what can be shown in practice. With our state-of-the-art optical setup that produces high-fidelity three- and four-photon GHZ states, we were able to show, for the three-party case, that this verification process is possible using a carefully constructed protocol, for up to 5% loss, under the most strict security conditions. Clearly, the loss tolerance of the system can be further improved by using states with even higher fidelities. This would also enable the implementation of the verification protocols for a larger number of qubits.

It is important to remark that our verification protocols go beyond merely detecting entanglement; they also link the outcome of the verification tests to the state that is actually used by the honest parties of the network with respect to their ideal target state. This is non trivial and of great importance in a realistic setting where such resources are subsequently used by the parties in distributed computation and communication applications executed over the network. Such applications may also require multipartite entangled states other than the GHZ states studied in this work. We expect that our verification protocols should indeed be applicable to other types of useful states such as, for instance, stabilizer states.

Data availability. All relevant data are available from the authors.

References

1. Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81,** 865 (2009).
2. Kimble, H. J. The quantum internet. *Nature* **453,** 1023–1030 (2008).
3. Scarani, V. *et al.* The practical security of quantum key distribution. *Rev. Mod. Phys.* **81,** 1301 (2009).
4. Chiribella, G., D'Ariano, G. M. & Perinotti, P. Theoretical framework for quantum networks. *Phys. Rev. A* **80,** 022339 (2009).
5. Perseguers, S., Lapeyre, G. J. Jr, Cavalcanti, D., Lewenstein, M. & Acin, A. Distribution of entanglement in large-scale quantum networks. *Rep. Prog. Phys* **76,** 096001 (2013).
6. Greenberger, D. M., Horne, M. A. & Zeilinger, A. Going beyond Bell's theorem. in *Bell's Theorem, Quantum Theory, and Conceptions of the UniverseKafatos, M. (Ed.) 69–72 (Kluwer, 1989).*
7. Mermin, N. D. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.* **65,** 1838 (1990).
8. Buhrman, H., Cleve, R., Massar, S. & de Wolf, R. Nonlocality and communication complexity. *Rev. Mod. Phys.* **82,** 665 (2010).
9. Broadbent, A., Fitzsimons, J. & Kashefi, E. in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 517–526 (2009).
10. Raussendorf, R. & Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett.* **86,** 5188 (2001).
11. Pappa, A., Chailloux, A., Wehner, S., Diamanti, E. & Kerenidis, I. Multipartite entanglement verification resistant against dishonest parties. *Phys. Rev. Lett.* **108,** 260502 (2012).
12. Barz, S. *et al.* Experimental demonstration of blind quantum computing. *Science* **335,** 303–308 (2012).
13. Barz, S., Fitzsimons, J. F., Kashefi, E. & Walther, P. Experimental verification of quantum computation, Nat. *Phys* **9,** 727–731 (2013).
14. Greganti, C., Roehsner, M.-C., Barz, S., Morimae, T. & Walther, P. Demonstration of measurement-only blind quantum computing. *New J. Phys.* **18,** 013020 (2016).
15. Tittel, W., Zbinden, H. & Gisin, N. Experimental demonstration of quantum secret sharing. *Phys. Rev. A* **63,** 042301 (2001).
16. Zhao, Z. *et al.* Experimental demonstration of five-photon entanglement and open-destination teleportation. *Nature* **430,** 54–58 (2004).
17. Chen, Y.-A. *et al.* Experimental quantum secret sharing and third-man quantum cryptography. *Phys. Rev. Lett.* **95,** 200502 (2005).
18. Adamson, R. B. A., Fortescue, B., Lo, H. K. & Steinberg, A. M. Experimental implementation of a three-party quantum key distribution protocol. *IEEE Conf. Las. Elec. Opt.*, QMA3 (2006).
19. Mayers, D. & Yao, A. Self testing quantum apparatus. *QIC* **4,** 273–286 (2004).
20. Pal, K. F., Vertesi, T. & Navascues, M. Device-independent tomography of multipartite quantum states. *Phys. Rev. A* **90,** 042340 (2014).

21. McKague, M. *Self-Testing Graph States, Proceedings of Theory of Quantum Computation, Communication, and Cryptography,* Vol. 6745, 104–120 (Springer, 2011).
22. Cavalcanti, D. *et al.* Detection of entanglement in asymmetric quantum networks and multipartite quantum steering. *Nat. Commun.* **6,** 7941 (2015).
23. Toth, G. & Guehne, O. Detecting genuine multipartite entanglement with two local measurements. *Phys. Rev. Lett.* **94,** 060501 (2005).
24. Halder, M. *et al.* Nonclassical 2-photon interference with separate intrinsically narrowband fibre sources. *Opt Express* **17,** 4670–4676 (2009).
25. Clark, A. *et al.* Intrinsically narrowband pair photon generation in microstructured fibres. *New J. Phys.* **13,** 065009 (2011).
26. Bell, B. *et al.* Experimental characterization of photonic fusion using fiber sources. *New J. Phys.* **14,** 023021 (2012).
27. Bell, B. A. *et al.* Experimental characterization of universal one-way quantum computing. *New J. Phys.* **15,** 053030 (2013).
28. James, D. F. V., Kwiat, P. G., Munro, W. J. & White, A. G. Measurement of qubits. *Phys. Rev. A* **64,** 052312 (2001).
29. Imoto, N., Haus, H. A. & Yamamoto, Y. Quantum nondemolition measurement of the photon number via the optical Kerr effect. *Phys. Rev. A* **32,** 2287 (1985).
30. Xiao, Y.-F. *et al.* Quantum nondemolition measurement of photon number via optical Kerr effect in an ultra-high-Q microtoroid cavity. *Opt. Exp.* **16,** 21462–21475 (2008).
31. Guerlin, C. *et al.* Progressive field-state collapse and quantum non-demolition photon counting. *Nature* **448,** 889–893 (2007).
32. Radmark, M., Zukowski, M. & Bourennane, M. Experimental high fidelity six-photon entangled state for telecloning protocols. *New J. Phys.* **11,** 103016 (2009).
33. Resch, K., Walther, P. & Zeilinger, A. Full characterization of a three-photon GHZ state using quantum state tomography. *Phys. Rev. Lett.* **94,** 070402 (2005).
34. Zhao, Z. *et al.* Experimental violation of local realism by four-photon Greenberger-Horne-Zeilinger entanglement. *Phys. Rev. Lett.* **91,** 180401 (2003).
35. Zhou, X.-Q. *et al.* Greenberger-Horne-Zeilinger-type violation of local realism by mixed states. *Phys. Rev. A* **78,** 012112 (2008).
36. Lu, H.-X., Zhang, J., Wang, X.-Q., Li, Y.-D. & Wang, C.-Y. Experimental high-intensity three-photon entangled source. *Phys. Rev. A* **78,** 033819 (2008).
37. Wang, X.-L. *et al.* Experimental ten-photon entanglement. Preprint at http://arxiv.org/abs/1605.08547 (2016).
38. Patel, R. B., Ho, J., Ferreyrol, F., Ralph, T. C. & Pryde, G. J. A quantum Fredkin gate. *Sci. Adv.* **2,** e1501531 (2016).

Acknowledgements

This work was supported by the UK's Engineering and Physical Sciences Research Council, ERC grants 247462 QUOWSS and QCC, EU FP7 grant 600838 QWAD, the Ville de Paris Emergences project CiQWii, the ANR project COMB, the Ile-de-France Region project QUIN and the South African National Research Foundation.

Author contributions

A.P., A.C., T.L., D.M., E.D. and I.K. conceived the entanglement verification scheme, W.M., A.P., B.A.B., A.M., J.G.R. and M.S.T. developed the experimental layout and methodology. W.M., B.A.B. and A.M. performed the experiments. M.S.T. led the project. All authors discussed the results and participated in the manuscript preparation.

Additional information

Supplementary Information accompanies this paper at http://www.nature.com/naturecommunications

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: McCutcheon, W. *et al.* Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* **7**, 13251 doi: 10.1038/ncomms13251 (2016).

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.