Experimental verification of multipartite entanglement in the presence of dishonest parties

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

[1]*Department of Electrical and Electronic Engineering, University of Bristol*
[2]*Department of Physics and Astronomy, University College London*
[3]*Faculty of Science, University of Sydney*
[4]*INRIA, Paris Rocquencourt*
[5]*LTCI, CNRS - Télécom ParisTech, Paris, France*
[6]*School of Chemistry and Physics & National Institute for Theoretical Physics, University of KwaZulu-Natal*
[7]*LIAFA, CNRS - Université Paris 7, Paris, France*
[8]*Center for Quantum Technologies, National University of Singapore, Singapore*

Introduction – Multipartite entanglement is a fundamental resource for quantum information tasks in the context of quantum network applications. For instance, the quantum correlations of Greenberger-Horne-Zeilinger (GHZ) states [1] shared between multiple parties allows them to win a nonlocal game with probability 1, which is impossible using classical local theories. Such resources also enable distributed tasks and delegated computation [2], which are essential elements of interactions within quantum networks. One of the main challenges for the future employment of such networks is the necessity to share the underlying entangled states among a large number of parties who wish to perform a distributed computation. In a real-life network, some of these parties may be dishonest, hence it is imperative for any party to be able to verify that the shared state is indeed entangled. This ensures the security of the subsequent computations.

In this work, we design, analyse and implement for the first time a distributed protocol for verifying that an untrusted source shares with multiple parties the GHZ state. We consider any number of dishonest parties that collaborate with the source in order to convince the honest parties that the source creates entanglement while in reality this is not the case. Our verification protocol is based on previous theoretical work [3], where it was shown that multipartite entanglement can be verified in a distributed way between distrustful parties, in an ideal scenario. Under realistic conditions, however, and in particular when the losses associated with the individual parties exceed 50%, that protocol fails. Here, we propose a new protocol that can tolerate high amounts of losses and we examine in detail how the dishonest parties can use the system imperfections in order to increase their cheating probability. Our implementation is based on a state-of-the-art multipartite entangled photon source [4], which can produce 3 and 4-party GHZ states with very high fidelity. This is necessary to be able to demonstrate in practice entanglement verification in the presence of dishonest parties.

The verification protocol – We suppose that a source is sharing a state ρ with n parties and that one of them (the Verifier), wants to verify that the state is the GHZ state, $|G_0^n\rangle = \frac{1}{\sqrt{2}}\big(|0^n\rangle + |1^n\rangle\big)$. First, the Verifier sends to all parties $j \in [n]$ randomly selected inputs $\theta_j \in [0, \pi)$, such that $\sum_j \theta_j$ is a multiple of π. Each party j then measures in basis $\{|+\rangle_\theta, |-\rangle_\theta\} = \{\frac{|0\rangle + e^{i\theta_j}|1\rangle}{\sqrt{2}}, \frac{|0\rangle - e^{i\theta_j}|1\rangle}{\sqrt{2}}\}$ and sends the outcome $Y_j = \{0, 1\}$ to the Verifier. The verification test succeeds if: $\bigoplus_j Y_j = \frac{1}{\pi}\sum_j \theta_j \pmod 2$.

We analyse this test and prove the following statements. First, the GHZ state passes the test with probability 1. Second, the fidelity $F(\rho) = \langle G_0^n|\rho|G_0^n\rangle$ of ρ with respect to the GHZ state can be lower bounded by the pass probability of the test, $P(\rho)$. If all n parties are honest, then $F(\rho) \geq 2P(\rho) - 1$. If the Verifier runs the test in the presence of any number of dishonest parties (say $n - k$ dishonest parties), then any security statement must consider that the dishonest parties may collaborate and apply a joint operation U to their parts of the state that works to their advantage, hence increasing the pass probability of the test. We still manage in this case to lower bound the fidelity as $\max_U F\big((\mathbb{I}_k \otimes U)\rho(\mathbb{I}_k \otimes U^\dagger)\big) \geq 4P(\rho) - 3$, where the identity is on the space of the k honest parties.

Experimental setup and state characterisation – The optical setup used for our experiments is shown in Figure 1. It is based on two microstructured fibre sources of entangled photon pairs [5]. In each of these sources, a loop of fibre is pumped in two directions, such that one direction produces horizontally polarized and the other vertically polarized pairs. These are combined at a polarizing beam-splitter, so that the output is an entangled Bell state, conditional on a single pair being generated. The signal and idler photons are then separated by dichroic mirrors, and the signal photons from the two sources are directed to a polarizing beam-splitter; this has the effect of 'fusing'

the entangled photon pairs into a 4-photon GHZ state [4]. The probability of success of this fusion operation, namely of projecting the state on the 4-photon GHZ, is 50%, where we only consider detection outcomes corresponding to one photon emerging in each mode. All four photons are then coupled into single-mode fibres, which take them to a measurement stage for each party, consisting of a quarter wave-plate, half wave-plate, polarizing beam-splitter, and single-photon counting detectors. With appropriate choices of wave-plate angles, any projective measurement can be made on the polarization of each photon.

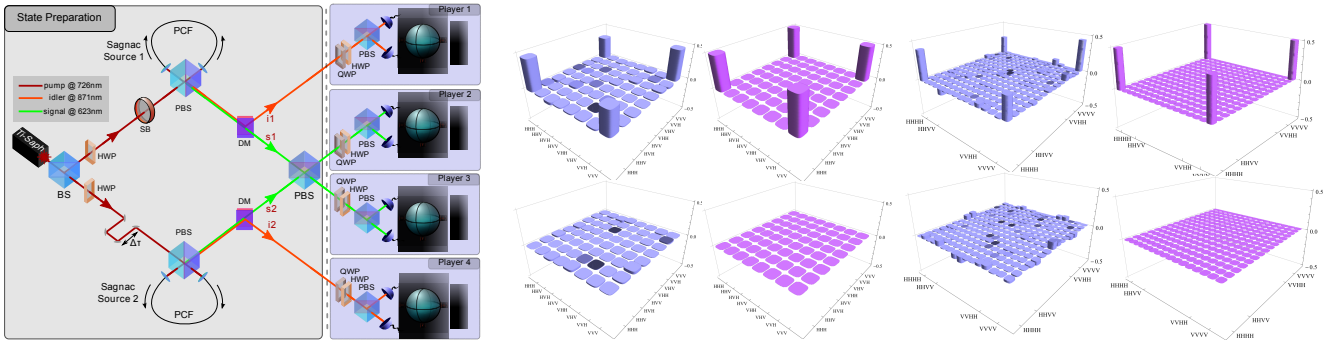

Figure 1: Experimental setup (left) and density matrices (right) for the GHZ-3 (first two columns) and GHZ-4 (last two columns) states, real part (top) and imaginary part (bottom). The tomographic reconstructions of the states appear in blue while the ideal theoretical states appear in purple.

The generation of a 3-photon GHZ state requires only a slight modification to the setup, with one of the fibre loops only pumped in one direction to generate unentangled pairs. The signal is then rotated to $(|H\rangle + |V\rangle)/2$ prior to the fusion operation. The unentangled idler photon is not considered as part of the state but must still be detected to herald the creation of a pair. The resulting density matrices for the 3 and 4-photon GHZ are shown in Figure 1. The achieved fidelities with respect to the ideal states are $F_{\text{GHZ-3}} = 0.81 \pm 0.01$ and $F_{\text{GHZ-4}} = 0.71 \pm 0.01$.

Experimental verification results – Let us first remark that in our protocol it is imperative that the Verifier selects inputs randomly and independently for each copy of the state, to ensure dishonest parties have no prior knowledge of them. Hence, in our experiment, the measurement basis was changed after every detection event. This requirement necessitated the use of automated wave-plate rotators to change the basis, controlled by a computer with access to the incoming data, and contrasts with the usual method of accumulating many detections over a fixed integration time for a measurement, and then examining properties of the obtained ensemble of states.

We performed a series of experimental tests. First, we carried out the verification protocol for the 3-party GHZ state. We used 6000 copies of the state and obtained a pass probability of $83.4\% \pm 0.5\%$. For all honest parties, based on our theoretical analysis we find that this result provides a lower bound of the state fidelity of 0.67 ± 0.01, which is consistent with the value $F_{\text{GHZ-3}}$ measured using state tomography. This value is also sufficient to prove genuine multipartite entanglement (GME), since the fidelity is above 0.5. Furthermore, in the presence of dishonest parties, the pass probability of the test is sufficient to verify entanglement since it exceeds the GME bound of 0.8183 by 3 standard deviations. We emphasize here the difficulty of obtaining in practice the latter result: using the original protocol [3] would not have allowed us to verify entanglement in the dishonest case, since it requires a higher pass probability of $\cos^2(\pi/8) \approx 85.4\%$, while the very high fidelity achieved in our experiment is also crucial to be able to prove entanglement in this case.

Second, we carried our the verification protocol for the 4-party GHZ state. We used 3901 copies of the state and obtained a pass probability of $76.4\% \pm 0.7\%$. For all honest parties, based on our theoretical analysis we find that the lower bound of the state fidelity is 0.53 ± 0.01 in this case, which is just sufficient to show GME. Here, the same could not be shown in the presence of dishonest parties due to the high amount of noise.

Third, for both 3 and 4-party verification protocols, we implemented a cheating strategy, by which one dishonest party is completely disentangled from the other parties and attempts to convince the Verifier that the joint state is a 3 or 4-party GHZ, respectively. In the 3-party case, the dishonest party is able to infer $\theta = \theta_1 + \theta_2 (\text{mod } \pi)$ from her own input θ_3, and tries to guess the parity of the measurement outcomes of the honest parties so that the state passes the test. The pass probability of the test as a function of the value of θ is shown in Figure 2. It is in good agreement with theory and corresponds to an average pass probability equal to $72.3\% \pm 0.8\%$. The corresponding results for the 4-party protocol are also shown in Figure 2 and result in an average pass probability of $66.7\% \pm 0.8\%$.

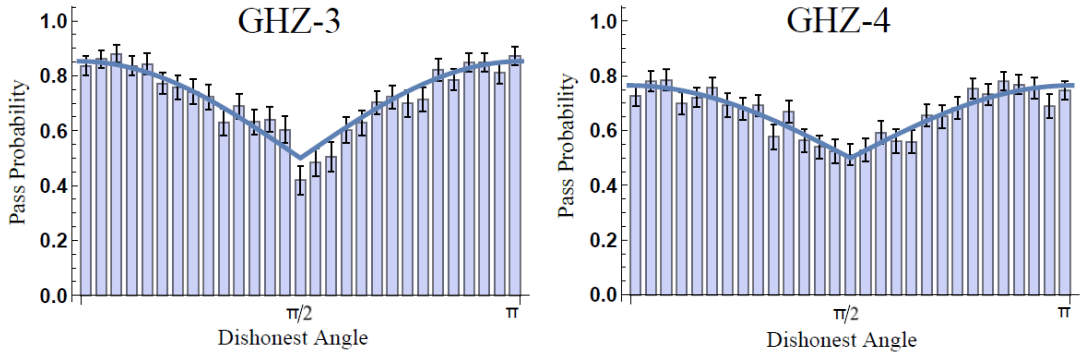

Figure 2: Pass probability as a function of the dishonest angle for GHZ-3 with 2 honest and 1 dishonest party (left) and for GHZ-4 with 3 honest and 1 dishonest party (right). We observe the highest pass probabilities for angles close to 0 and π, while they drop to 50% around $\pi/2$.

Taking into account experimental imperfections – Our experimental verification results show that the pass probability of the verification test is significantly lower when a dishonest party performs her cheating strategy using a separable state than that for an entangled state. This indicates that using a sufficient number of protocol repetitions the Verifier will be able to detect the cheating. However, the dishonest parties may try to take advantage of the experimental imperfections in order to increase their pass probability. For instance, in the cheating strategy corresponding to Figure 2, if the Verifier is willing to accept a loss rate λ, the dishonest party, who is assumed to have perfect equipment, can declare loss whenever θ leads to a low pass probability. Then, the pass probability will increase with λ for both the 3 and 4-party protocols, however it will always remain below the pass probability of the fully entangled state *for any amount of losses*, therefore allowing the Verifier to detect the cheating. It is important to note that this is a unique feature of our new protocol; previous protocols with only two input choices [2, 3] could not tolerate losses higher than 50%, since the dishonest parties could always discard one of the two inputs.

If now the Verifier is willing to accept a certain fail rate from a noisy but entangled state, the dishonest party can take advantage of this fact, by using ideal devices and preparing a perfect but separable state. We experimentally demonstrate this in the 4-party setting. In the cheating strategy implemented before a photon was disentangled from the 4-party GHZ state, therefore keeping the noise level roughly consistent between entangled and separable states; now we directly prepare the 3-party GHZ state (plus an unentangled photon), resulting in a 4-party state with reduced noise. This improves the pass probability from 66.7% to 69%, which is still below the pass probability for the fully entangled state, which is 76.4%. We can show, however, that the verification test ultimately fails if the dishonest party is also allowed to declare losses, in particular, for $\lambda > 1/3$. Hence, for sufficiently high noise and losses, it is not possible to perform in practice the entanglement verification task with our setup.

Conclusion – We provide for the first time an experimental demonstration of multipartite entanglement verification in the presence of dishonest parties. Our theoretical analysis and experimental setup for high-fidelity multipartite entangled state generation allow us to perform a thorough investigation of the role of system imperfections in this setting. Our results are of central importance for securely performing distributed computing tasks within future quantum information networks.

[1] D. M. Greenberger, M. A. Horne and A. Zeilinger, Going beyond Bell's theorem, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, M. Kafatos (Ed.), Kluwer, Dordrecht, 1989, pp. 69–72.
[2] A. Broadbent, J. Fitzsimons and E. Kashefi, Universal blind quantum computation, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* 2009, pp. 517–526.
[3] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti and I. Kerenidis, Multipartite Entanglement Verification Resistant against Dishonest Parties, Phys. Rev. Lett. **108**, 260502 (2012).
[4] B. Bell, A. Clark, M. S. Tame, M. Halder, J. Fulconis, W. Wadsworth and J. Rarity, Experimental characterization of photonic fusion using fiber sources, New J. Phys. **14**, 023021 (2012).
[5] A. Clark, B. Bell, J. Fulconis, M. M. Halder, B. Cemlyn, O. Alibart, C. Xiong, W. J. Wadsworth and J. G Rarity, Intrinsically narrowband pair photon generation in microstructured fibres, New J. Phys. **13**, 065009 (2011).