Experimental few-copy multipartite entanglement detection

Valeria Saggio1*, Aleksandra Dimić2, Chiara Greganti1,3, Lee A. Rozema1, Philip Walther1 and Borivoje Dakić1,4

Many future quantum technologies rely on the generation of entangled states. Quantum devices will require verification of their operation below some error threshold, but the reliable detection of quantum entanglement remains a considerable challenge for large-scale quantum systems. Well-established techniques for this task rely on the measurement of expectation values of entanglement witnesses; however these require many measurement settings to be extracted. Here, we develop a generic framework for efficient entanglement detection that translates any entanglement witness into a resource-efficient probabilistic scheme, whose confidence grows exponentially with the number of individual detection events, namely copies of the quantum state. To benchmark our findings, we experimentally verify the presence of entanglement in a photonic six-qubit cluster state generated using three single-photon sources operating at telecommunication wavelengths. We find that the presence of entanglement can be certified with at least 99.74% confidence by detecting 20 copies of the quantum state. Additionally, we show that genuine six-qubit entanglement is verified with at least 99% confidence by using 112 copies of the state. Our protocol can be carried out with a remarkably low number of copies and in the presence of experimental imperfections, making it a practical and applicable method to verify large-scale quantum devices.

The reliable verification of quantum entanglement1 is an essential task for quantum technologies, but it remains a considerable challenge for large-scale quantum systems. The generation of large entangled states2–9 is required to investigate quantum state tomography10. However, the number of measurement settings required to characterize a generic quantum state grows exponentially with the size of the system, making this approach unfeasible for large devices. In many cases, the full density matrix is not needed and alternative approaches for entanglement detection, such as witness-based methods, have been developed (see ref. 11 and references therein). Although these techniques show significant improvements with respect to the number of measurement settings12–15, they still require many detection events (that is, many copies of the quantum state) to extract expectation values of the different operators used to construct a witness. Moreover, almost all the standard techniques assume that every detection event is identical and independent, a situation that is challenging to achieve in practice. For these reasons, as large quantum devices move closer to practical realization, novel methods are urgently needed that are both reliable and resource-efficient.

In the past few years, new approaches exploiting various random sampling techniques have been developed, such as randomized benchmarking16, quantum state tomography via compressed sensing17 and machine learning18,19, direct fidelity estimation20, self-testing methods21–24, quantum state verification25–28, entanglement verification29–31 and many others. Most of these techniques are focused on minimizing the number of measurement settings, while an increasing number of copies is needed when higher accuracy in parameter estimation (for example, the expectation value of an entanglement witness) is required. These parameters are compared to a certain threshold to conclude whether or not the state is entangled. Here, in contrast, instead of doing parameter estimation with a certain accuracy, we ask the following: given a certain number of experimental runs, what is the statistical significance that the state is entangled? Remarkably, in this case it has been shown in ref. 24 that even a single copy of the quantum state can be considered as a meaningful resource for entanglement detection. Although parameter estimation reveals much more information about the actual state, it requires significantly more resources than our protocol. Here we develop a generic framework to translate any entanglement witness into a reliable and resource-efficient procedure and apply it to a real experimental situation. We show that our approach detects entanglement with an exponentially growing confidence in the number of copies of the quantum state, implemented via local measurements only, and does not require the assumption of independent and identically distributed (i.i.d.) experimental runs.

Furthermore, we show, in certain cases, that our procedure works even if the number of available copies is less than the total number of measurement settings needed to extract the mean value of the witness operator, that is, even if the corresponding witness-based method is not logically possible. We demonstrate the applicability of our method by validating the presence of quantum entanglement in a six-photon cluster state. This state, produced for the first time at telecommunication wavelengths, is generated with three high-quality single-photon sources and detected with pseudo-number resolving superconducting nanowire detectors. We obtain a fidelity between the produced state and the ideal one of 0.75 ± 0.06, which is equivalent to fidelities obtained in state-of-the-art photonic experiments1. We verify the presence of entanglement with at least
Probabilistic entanglement verification

We start by clarifying some basic definitions and types of entanglement. A bipartite quantum state is called separable if it is a mixture of product states (that is, states of the type $|\psi_1\rangle \otimes |\psi_2\rangle$). A non-separable state is called entangled. For multipartite systems, one can define various types of entanglement. For a multipartite quantum system, we say that the state is biseparable if we can divide the system into two parts, such that the state is separable with respect to such bipartition. If this is not possible, the state exhibits genuine multipartite entanglement. Full separability refers to separability across any bipartition of the system.

In the standard witness-based approach (a witness operator always specifies the type of entanglement), the presence of entanglement is verified by measuring the mean value of the witness operator $W$ to be less than zero, that is $\langle W \rangle \leq 0$ for any separable state $\rho_{sep}$, where $\langle W \rangle = \text{Tr}(W \rho_{sep})$. $W$ is in general not locally accessible (one has to decompose it into the sum of local observables $W_i$ as $W = \sum_{i=1}^{L} W_i$, where each $W_i$ needs to be measured in a separate experimental run), requiring one to estimate several mean values and therefore demanding a large number of copies. Thus, this technique is not reliable when few copies are available. Moreover, for a limited number of copies $N$, one has to use $L$ independent measurement settings and ensure that for every individual detection event the source provides exactly the same copy of the quantum state (this is the i.i.d. assumption). Neither of these two requirements is very practical.

We overcome both of these difficulties by using a probabilistic framework for entanglement detection. More precisely, our protocol is centred on a set $\mathcal{M} = \{M_1, M_2, \ldots, M_L\}$ of binary local observables, which we will show can be derived for any entanglement witness. Each $M_k$ (with $k = 1, \ldots, L$) returns a binary outcome $m_k = 1, 0$, associated with the success or failure of the measurement, respectively. The procedure consists of randomly drawing the measurements $M_k$ (each with some probability $e_k$) $N$ times from the set $\mathcal{M}$ and applying each of them to the quantum state, obtaining the outcomes $m_k$. The set $\mathcal{M}$ is tailored such that the probability to obtain success (that is, to get $m_k = 1$ for a randomly chosen $M_k$) for any separable state is upper bounded by a certain value $p_s < 1$, that we call separable bound. On the other hand, the probability of success is maximized to $p_s$, called the entanglement value, if a certain entangled state (target state) has been prepared. The entanglement value $p_s$ is strictly greater than the separable bound $p_s$, that is, the difference $\delta_s = p_s - p_s > 0$. In a realistic framework, we can prepare a certain state $\rho_{sep}$ and assume that the application of the measurements $M_k$ to it returns $S$ successful outcomes. The observed deviation from the separable bound $\delta = p_{obs} - p_s$ (where $p_{obs}$ is the observed entanglement value) therefore reads

$$\delta = \frac{S}{N} - p_s$$ (1)

It has been shown in ref. 31 that the probability $P(\delta)$ to observe $\delta > 0$ for any separable state is upper bounded as $P(\delta) \leq e^{-D(p_s + \delta_0 \| p_s)N}$, which goes exponentially fast to zero with the number of copies $N$. Here $D(x\|y) = x \log 2 + (1-x) \log 2 -x$ is the Kullback–Leibler divergence. Therefore, the confidence $C(\delta)$ of detecting quantum entanglement is lower bounded by $C_{min}(\delta)$ as follows:

$$C(\delta) = 1 - P(\delta) \geq 1 - e^{-D(p_s + \delta_0 \| p_s)N} = C_{min}(\delta)$$ (2)

and converges exponentially fast to unity in $N$. From equation (2) we can estimate the average number of copies $N_{av}$ needed to achieve a certain confidence $C_{av}$ meaning that for a target state preparation we find

$$N_{av} \leq K \log (1-C_0) = N_{max}$$ (3)

which grows logarithmically at the rate of $K = D(p_s + \delta_0 \| p_s)^{-1}$ as $C_0$ approaches unity.

If $\delta$ evaluates to a positive number, we can use equation (1) to calculate $C_{max}(\delta)$ from equation (2). We summarize the entanglement detection procedure in Fig. 1.

Additionally, due to random sampling of the measurement settings, our protocol does not require the i.i.d. assumption (see ref. 34 for proof). This is an important feature of our procedure as the experimental state is necessarily subject to variations over time due to experimental conditions such as source drift and so on. It is known that in such cases other schemes can lead to inadequate results, whereas in our case we never obtain false positives.

Translation of entanglement witnesses

Any entanglement witness can be translated into our probabilistic verification protocol. Therefore, our method can detect any type of entanglement (for example, genuine multipartite, bipartite) for which there exists a corresponding witness. Here we will show how to construct the set $\mathcal{M}$ and find the corresponding separable bound $p_s$ for any entanglement witness (see first section of the Methods for the detailed proof). We start with the observation that for every witness $W$, one can define a new equivalent one $W'$, whose mean value
is always positive and bounded by 1, by using the equivalence transformation \( W = a W + b \). The mean value of this new witness is the probability of success of our protocol, which is upper bounded by \( p \), for any separable state and achieves \( p > p \), for a certain entangled state. To illustrate the translation procedure, we consider the example of multipartite entanglement detection in an \( n \)-qubit graph state \( |G \rangle \) via the witness \( W = \frac{1}{2} - |G \rangle \langle G | \), for which we have \( \langle W \rangle \geq 0 \) for any biseparable state. This witness \( W \) can be easily transformed into the equivalent one, \( W' = \frac{1}{2} + \frac{1}{2} |G \rangle \langle G | \), for which we get \( \langle W' \rangle \leq \frac{1}{2} = p \) for any biseparable state. The graph state can be decomposed as the sum of its stabilizers \( S_k \) as \( |G \rangle \langle G | = \frac{1}{2} \sum_{k=1}^{n!} S_k \), where \( S_k \) are certain products of local Pauli observables. Therefore, the new witness reads \( W' = \frac{1}{2} \sum_{k=1}^{n!} M_k \), where \( M_k = (1 + S_k)/2 \) are the binary observables needed in our probabilistic protocol. The sampling is uniform; that is, the probabilities equal \( \exp(-\langle W' \rangle) \), which is an upper bound of the so-called biseparable bound. Reduction of resources down to a single copy can be achieved in certain cases by considering a particular dependence of the separable bound on \( n \) (see second section of the Methods).

Once we have the measurements \( M_i \) and the separable bound \( p_s \), we can apply the protocol illustrated in Fig. 1 and find the minimum confidence for entanglement detection.

**Entanglement verification for a six-qubit cluster state**

We will now translate two different witnesses, tailored for our experimental state, into our probabilistic framework. Our ideal experimental six-qubit cluster state is

\[
|Cl_6 \rangle = \frac{1}{2} (|H_1 H_2 H_3 H_4 H_5 H_6 \rangle + |H_1 H_2 H_3 V_4 V_5 V_6 \rangle + |V_1 V_2 V_3 V_4 H_5 H_6 \rangle - |V_1 V_2 V_3 V_4 V_5 V_6 \rangle)
\]

which is equivalent to the state shown in Fig. 2 up to local unitary transformations.

We consider the two following witnesses, defined to detect genuine six-qubit entanglement:

- The witness presented in ref. 12, composed of only two measurement settings:
  \[
  W_1 = 31 - 2 \left( \prod_{k=1,3,5} \frac{1 + G_k}{2} + \prod_{k=2,4,6} \frac{1 + G_k}{2} \right)
  \]
  where \( G_k \) (with \( k = 1, \ldots, 6 \)) are the experimental generators of the cluster state\(^{49}\), listed in the third section of the Methods;
  - The standard witness tailored for our cluster state\(^{48}\):
  \[
  W_2 = \frac{1}{2} I - |Cl_6 \rangle \langle Cl_6 |
  \]

which requires \( 2^{16} = 64 \) measurement settings (because \( |Cl_6 \rangle \langle Cl_6 | = \frac{1}{2} \sum_{k=1}^{n!} S_k \), analogously to the previous graph state example).

For both witnesses \( \langle W_1 \rangle, \langle W_2 \rangle \geq 0 \) for any biseparable state, thus allowing detection of genuine six-qubit entanglement. Nevertheless, both can also be used to distinguish fully separable and entangled states, that is, to detect only some entanglement, and the corresponding separable bounds can be evaluated numerically\(^{48}\). We can then distinguish two types of separable bound: one is the so-called biseparable bound \( p_s \), which can be directly extracted from our translation protocol and is therefore used for detection of genuine six-qubit entanglement; the other is the fully separable bound \( p_s \), which is evaluated numerically and used to detect some entanglement.

Following the procedure shown in the first section of the Methods we find for \( W_1 \) the set \( \mathcal{M}_{W_1} = \left\{ M_i = \prod_{k=1,3,5} \left( \frac{1 + G_k}{2} \right), M_2 = \prod_{k=2,4,6} \left( \frac{1 + G_k}{2} \right) \right\} \), where \( M_i \) and \( M_2 \) are the local observables and the corresponding biseparable bound is \( p_{bs W_1} = \frac{1}{2} \). For \( W_2 \), the binary observables constituting the set \( \mathcal{M}_{W_2} = \left\{ \prod_{k=1}^{64} \frac{1 + G_k}{2} \right\} \) (with \( k = 1, \ldots, 64 \)) and the biseparable bound is \( p_{bs W_2} = \frac{1}{2} \) (see the example of the graph state discussed in the previous section). The derived fully separable bounds read \( p_{fs W_1} = \frac{2}{16} \) and \( p_{fs W_2} = \frac{2}{8} \). The entanglement values are \( p_{W_1} = p_{W_2} = 1 \).

**Experimental set-up**

The experimental set-up used for the cluster state generation is shown in Fig. 3a.

In the ‘Preparation’ stage, a Ti:sapphire pulsed laser is temporally multiplexed\(^{40,41}\) to a repetition rate of 152 MHz with two beamsplitters (BSs). It then pumps three identical single-photon sources, each built in a Sagnac configuration\(^{42,43}\). Each source produces a polarization-entangled photon pair at telecommunication wavelengths via collinear type-II spontaneous parametric downconversion (SPDC), specifically the singlet state \( |\psi^- \rangle_{ij} = (|H_i V_j \rangle - |V_i H_j \rangle)/\sqrt{2} \), where \( |H \rangle \) and \( |V \rangle \) denote the horizontal and vertical photons’ polarization states and \( i,j \) are the photons’ spatial modes. A schematic of one single-photon source is shown in Fig. 3b (see fourth section of the Methods for details). It is possible to switch between different Bell states with a half-waveplate (HW) placed along one photon path (Fig. 3b) and/or by rotating the HW at a certain angle immediately before the source.

In the ‘Generation’ stage, after switching from \( |\psi^- \rangle_{12} \) and \( |\psi^- \rangle_{34} \) to \( |\phi^+ \rangle_{12} \) and \( |\phi^+ \rangle_{34} \), and from \( |\psi^- \rangle_{56} \) to \( |\phi^+ \rangle_{56} \), where \( |\phi^\pm \rangle_{ij} = (|H_i H_j \rangle \pm |V_i V_j \rangle)/\sqrt{2} \), photon pairs from different sources are generated into the equivalent one, \( W' = \frac{1}{2} + \frac{1}{2} |G \rangle \langle G | \), for which we get \( \langle W' \rangle \leq \frac{1}{2} = p \) for any biseparable state. The graph state can be decomposed as the sum of its stabilizers \( S_k \) as \( |G \rangle \langle G | = \frac{1}{2} \sum_{k=1}^{n!} S_k \), where \( S_k \) are certain products of local Pauli observables. Therefore, the new witness reads \( W' = \frac{1}{2} \sum_{k=1}^{n!} M_k \), where \( M_k = (1 + S_k)/2 \) are the binary observables needed in our probabilistic protocol. The sampling is uniform; that is, the probabilities equal \( \exp(-\langle W' \rangle) \), which is an upper bound of the so-called biseparable bound. Reduction of resources down to a single copy can be achieved in certain cases by considering a particular dependence of the separable bound on \( n \) (see second section of the Methods).

Once we have the measurements \( M_i \) and the separable bound \( p_s \), we can apply the protocol illustrated in Fig. 1 and find the minimum confidence for entanglement detection.

**Entanglement verification for a six-qubit cluster state**

We will now translate two different witnesses, tailored for our experimental state, into our probabilistic framework. Our ideal experimental six-qubit cluster state is

\[
|Cl_6 \rangle = \frac{1}{2} (|H_1 H_2 H_3 H_4 H_5 H_6 \rangle + |H_1 H_2 H_3 V_4 V_5 V_6 \rangle + |V_1 V_2 V_3 V_4 H_5 H_6 \rangle - |V_1 V_2 V_3 V_4 V_5 V_6 \rangle)
\]

which is equivalent to the state shown in Fig. 2 up to local unitary transformations.

We consider the two following witnesses, defined to detect genuine six-qubit entanglement:

- The witness presented in ref. 12, composed of only two measurement settings:
  \[
  W_1 = 31 - 2 \left( \prod_{k=1,3,5} \frac{1 + G_k}{2} + \prod_{k=2,4,6} \frac{1 + G_k}{2} \right)
  \]
  where \( G_k \) (with \( k = 1, \ldots, 6 \)) are the experimental generators of the cluster state\(^{49}\), listed in the third section of the Methods;
  - The standard witness tailored for our cluster state\(^{48}\):
  \[
  W_2 = \frac{1}{2} I - |Cl_6 \rangle \langle Cl_6 |
  \]
interfere at two polarizing BSs (PBSs), at which they are temporally synchronized with the help of delay lines placed along the second and third pump paths. A HWP placed in the path of the third photon is needed to generate the target cluster state.

In the ‘Detection’ stage, each photon passes through a tomographic system—composed of a motorized quarter-waveplate (QWP) and HWP followed by a PBS—which enables measurements in different polarization bases, and is then sent to the detection apparatus, which consists of twelve pseudo-number resolving multi-element superconducting detectors46,47. Lenses to adjust the photon momentum are used) cases, respectively. The points are obtained by plugging the experimental plots confirm the efficiency of our entanglement verification method by showing an exponential growth of the confidence. The insets show that the confidence stabilizes towards a certain value with $N$. For the ideal state (cluster state with fidelity of 1), the expression for the minimum confidence in equation (2) is a monotonic function in the number of copies because all the binary outcomes evaluate to 1. However, because usual technical imperfections decrease the fidelity, occasional events with the binary outcome 0 can occur at random. This will occasionally pull the confidence down, while an outcome 1 will pull it up. Obviously, the fluctuations in the confidence values are linked to the number of measured copies, such that a higher number of copies suppresses these fluctuations. All of this can be seen in Fig. 4.

In Fig. 4a the confidence stabilizes to at least 99.12% with only 36 copies. Already, 58 copies suffice to exclude full separability in the system with at least 99.99% confidence. Figure 4b shows verification of genuine six-qubit entanglement with at least 91% confidence with 75 copies, and already 126 copies suffice to reach at least 97%.

In Fig. 4c we see that only 20 copies suffice to reveal the presence of entanglement with at least 99.74% confidence, and 50 copies provide more than 99.99%. Figure 4d shows that biseparability can be excluded with more than 97% confidence with 50 copies, and 112 copies provide more than 99%. Interestingly, in contrast to the standard witness-based method, in this case our protocol works with fewer copies than the total number of measurement settings, that is 64. As previously discussed, in this last case we can also estimate the fidelity $F = \langle Cl | \rho_{ex} | Cl \rangle = 0.75 \pm 0.06$. The different areas marked with different colours in both plots and the red dotted lines help with visualization of the different confidence levels.

In our new approach we bypass the measurement of mean values. Our results clearly show that we are able to detect entanglement with a very high confidence using only a few copies of the quantum state. The practicability of our method may prove essential for entanglement detection in large-scale systems in future experiments. It should also be advantageous to apply our techniques to entanglement verification in other physical systems, such as trapped ions1, superconducting circuits4 or continuous-variable systems7–9.
Fig. 4 | Growth of confidence of entanglement with the number of copies of the quantum state. (a–d), where plots in (a) and (c) show the minimum confidence when the fully separable bound is used ($C_{\min}(S_{W_1}/N-\frac{1}{2})$) and $C_{\min}(S_{W_1}/N-\frac{3}{2})$ for (a) and (c), respectively) and the plots in (b) and (d) are extracted by using the biseparable bound ($C_{\min}(S_{W_2}/N-\frac{1}{2})$ and $C_{\min}(S_{W_2}/N-\frac{3}{2})$ respectively). Blue dots represent $C_{\min}$ extracted from equation (2). $\delta_{W_1}$ and $\delta_{W_2}$ are positive for all the points in the four plots. The region in which the confidence stabilizes is highlighted and shown in the insets, where areas marked with different colours indicate different thresholds for the confidence level. Red dotted lines emphasize the different levels.

Online content
Any methods, additional references, Nature Research reporting summaries, source data, statements of code and data availability and associated accession codes are available at https://doi.org/10.1038/s41567-019-0550-4.

Received: 2 October 2018; Accepted: 9 May 2019; Published online: 24 June 2019

References
1. Arrazola, J. M. et al. Reliable entanglement verification. Phys. Rev. A 87, 062331 (2013).
2. Wang, X.-L. et al. Experimental ten-photon entanglement. Phys. Rev. Lett. 117, 210502 (2016).
3. Monz, T. et al. 14-qubit entanglement: creation and coherence. Phys. Rev. Lett. 106, 130506 (2011).
4. Song, C. et al. 10-qubit entanglement and parallel logic operations with a superconducting circuit. Phys. Rev. Lett. 119, 180511 (2017).
5. Friis, N. et al. Observation of entangled states of a fully controlled 20-qubit system. Phys. Rev. X 8, 021012 (2018).
6. Wang, X.-L. et al. 18-qubit entanglement with six photons’ three degrees of freedom. Phys. Rev. Lett. 120, 260502 (2018).
7. Chen, M., Menicucci, N. C. & Pfister, O. Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb. Phys. Rev. Lett. 112, 120505 (2014).
8. Yoshikawa, J.-I. et al. Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing. APL Photon. 1, 060801 (2016).
9. Cai, Y. et al. Multimode entanglement in reconfigurable graph states using optical frequency combs. Nat. Commun. 8, 15645–15653 (2017).
10. James, D. F. V., Kwiat, P. G., Munro, W. J. & White, A. G. Measurement of multipartite entanglement of 60 modes of a quantum optical frequency comb. Phys. Rev. Lett. 112, 120505 (2014).
11. Knips, L., Schwemmer, C., Klein, N., Wieśniak, M. & Weinfurter, H. Multipartite entanglement detection with minimal effort. Phys. Rev. Lett. 117, 210504 (2016).
12. Tran, M. C., Đakić, B., Arnault, F., Laskowski, W. & Paterek, T. Quantum entanglement from random measurements. Phys. Rev. A 92, 050301 (2015).
13. Knill, L., Schwemmer, C., Klein, N., Wieśniak, M. & Weinfurter, H. Multipartite entanglement detection with minimal effort. Phys. Rev. Lett. 117, 210504 (2016).
14. Tran, M. C., Đakić, B., Arnault, F., Laskowski, W. & Paterek, T. Quantum entanglement from random measurements. Phys. Rev. A 92, 050301 (2015).
15. Bavaresco, J. et al. Measurements in two bases are sufficient for certifying high-dimensional entanglement. Nat. Phys. 14, 1032–1037 (2018).
16. Knill, L. et al. Randomized benchmarking of quantum gates. Phys. Rev. A 77, 012307 (2008).
17. Gross, D., Liu, Y.-K., Flammia, S. T., Becker, S. & Eisert, J. Quantum state tomography via compressed sensing. Phys. Rev. Lett. 105, 150401 (2010).
18. Montanaro, A. Learning stabilizer states by Bell sampling. Preprint at https://arXiv.org/abs/1707.04012 (2017).
19. Torlai, G. et al. Neural-network quantum state tomography. Nat. Phys. 14, 447–450 (2018).
20. Flammini, S. T. & Liu, Y.-K. Direct fidelity estimation from few Pauli measurements. Phys. Rev. Lett. 106, 230501 (2011).
21. Mayers, D. & Yao, A. Self testing quantum apparatus. QIC 4, 273–286 (2004).
22. McGauley, M. in Theory of Quantum Computation, Communication, and Cryptography Vol. 6745 (eds Bacon, D., Martin-Delgado, M. & Roettler, M) 104–120 (Springer, 2014).
23. Bancal, J.-D., Navascués, M., Scarani, V., Vértesi, T. & Yang, T. H. Physical characterization of quantum devices from nonlocal correlations. Phys. Rev. A 91, 022115 (2015).
24. Müller, C. A. & Shi, Y. Optimal robust quantum self-testing by binary nonlocal XOR games. Preprint at https://arXiv.org/abs/1207.1819 (2012).
25. Reichardt, B. W., Unger, F. & Vazirani, U. A classical leash for a quantum system: command of quantum systems via rigidity of CHSH games. Preprint at https://arXiv.org/abs/1209.0448 (2012).
26. McGauley, M., Yang, T. H. & Scarani, V. Robust self-testing of the singlet. J. Phys. A: Math. Theor. 45, 455304 (2012).
27. Takeuchi, Y. & Morimae, T. Verification of many-qubit states. Phys. Rev. X 8, 021060 (2018).
28. Zhu, H. & Hayashi, M. Efficient verification of hypergraph states. Preprint at https://arXiv.org/abs/1806.05565 (2018).
29. Pappa, A., Chailloux, A., Wehner, S., Diamanti, E. & Kerenidis, I. Multiparty entanglement verification resistant against dishonest parties. Phys. Rev. Lett. 108, 260502 (2012).
30. McCutcheon, W. et al. Experimental verification of multiparticle entanglement in quantum networks. Nat. Commun. 7, 13251–13258 (2016).
31. Pallister, S., Linden, N. & Montanaro, A. Optimal verification of entangled states with local measurements. Phys. Rev. Lett. 120, 170502 (2018).
32. Schneeloch, J., Tison, C. C., Fanto, M. L., Alsing, P. M. & Howland, G. A. Quantifying entanglement in a 68-billion dimensional quantum systems. Preprint at https://arXiv.org/abs/1804.09515 (2018).
33. Barreiro, J. T. et al. Demonstration of genuine multiparticle entanglement with device-independent witnesses. Nat. Phys. 9, 559–562 (2013).
34. Dimić, A. & Dakić, B. Single-copy entanglement detection. npj Quantum Inf. 4, 11–18 (2018).
35. Jungnitsch, B. et al. Increasing the statistical significance of entanglement detection in experiments. Phys. Rev. Lett. 104, 210401 (2010).
36. Blume-Kohout, R. Robust error bars for quantum tomography. Preprint at https://arXiv.org/abs/1202.5270 (2012).
37. Lu, C.-Y. et al. Experimental entanglement of six photons in graph states. Nat. Phys. 3, 91–95 (2007).
38. Hein, M., Eisert, J. & Briegel, H. J. Multiparty entanglement in graph states. Phys. Rev. A 69, 062311 (2004).
39. Gerke, S., Vogel, W. & Sterfling, J. Numerical construction of multipartite entanglement witnesses. Phys. Rev. X 8, 031047 (2018).
40. Greganti, C. et al. Tuning single-photon sources for telecom multi-photon experiments. Opt. Express 26, 3286–3302 (2018).
41. Broome, M. A., Almeida, M. P., Fedrizzi, A. & White, A. G. Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing. Opt. Express 19, 22698–22708 (2011).
42. Kim, T., Fiorentino, M. & Wong, F. N. C. Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. Phys. Rev. A 73, 012316 (2006).
43. Fedrizzi, A., Herbst, T., Poppe, A., Jennnewein, T. & Zeilinger, A. A wavelength-tunable fiber-coupled source of narrowband entangled photons. Opt. Express 15, 15377–15386 (2007).
44. Kuzucu, O. & Wong, F. N. Pulsed Sagnac entangled-photon source with a fiber-coupled system: command of quantum systems via rigidity of CHSH games. Preprint at https://arXiv.org/abs/1810.04515 (2018).
45. Jin, R.-B. et al. Pulsed Sagnac polarization-entangled photon source with a PPMT crystal at telecom wavelengths. Opt. Express 22, 11498–11507 (2014).
46. Natarajan, C. M., Tanner, M. G. & Hadfield, R. H. Superconducting nanowire single-photon detectors: physics and applications. Supercond. Sci. Technol. 25, 063001–063016 (2012).
47. Marsili, F. et al. Detecting single infrared photons with 93% system efficiency. Nat. Photon. 7, 210–214 (2013).

Acknowledgements
The authors thank I. Alonso Calafell for help with the detectors and T. Strömbberg for helpful discussions. V.S. acknowledges support from the University of Vienna through the Vienna Doctoral School. A.D. acknowledges support from project no. ON171035 of the Serbian Ministry of Education and Science and from the scholarship awarded from The Austrian Agency for International Cooperation in Education and Research (OeAD-GmbH). L.A.R. acknowledges support from the Templeton World Charity Foundation (fellowship no. TWCF0194). P.W. acknowledges support from the European Commission through ErBeStA (no. 800942), from the Austrian Science Fund (FWF) through CoQuS GmbH). L.A.R. acknowledges support from the Templeton World Charity Foundation (fellowship no. TWCF0194). P.W. acknowledges support from the European Commission through ErBeStA (no. 800942), from the Austrian Science Fund (FWF) through CoQuS (W1210-N25), BeyondC (F7113-N38) and NaMuG (P30067-N36), the US Air Force Office of Scientific Research (FA2386-232-17-1-4011), the Austrian Research Promotion Agency (FFG) through the QuantiERE ERA-NET Cofund project HiPhoP, and Red Bull. B.D. acknowledges support from the Foundational Question Institute (FQXi) grant FQXi-MGA-1806 and from an ESQ Discovery Grant of the Austrian Academy of Sciences.

Author contributions
V.S., C.G. and P.W. designed the experiment. V.S. and C.G. built the set-up. V.S. performed the experiment. V.S. and C.G. wrote the paper. L.A.R., P.W. and B.D. supervised the project. All authors contributed to writing the paper.

Competing interests
The authors declare no competing interests.

Additional information
Reprints and permissions information is available at www.nature.com/reprints. Correspondence and requests for materials should be addressed to V.S.

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

© The Author(s), under exclusive licence to Springer Nature Limited 2019
Methods

Formal proof for generic witness translation. Here, we show how to translate any entanglement witnessed in our probabilistic protocol. Conventionally, a witness operator \( W \) is normalized such that \( \text{Tr}(W W^\dagger) \geq 0 \) for any separable state \( \rho_{\text{sep}} \). An equivalent form reads \( W = a I - O \), where \( O \) is a Hermitean operator for which \( \text{Tr}(O \rho_{\text{sep}}) \leq g \) holds for any \( \rho_{\text{sep}} \) (ref. 48). Now, let us consider the local decomposition \( O = \sum_i W_i q_i \), where \( q_i \) is the number of local settings needed to measure \( O \). We are free to add a constant term to each local component \( W_i = \tilde{W} + a q_i \) such that they become non-negative observables. This transformation leads to the new witness \( O' = \sum_i W_i' q_i \). We choose \( a \geq 0 \) to take the minimum possible value. Altogether, we can rewrite the separability condition as

\[
\text{Tr}(O \rho_{\text{sep}}) \leq g + a q
\]

(1)

Our main aim is to test this inequality in practice via our probabilistic procedure. Note that this inequality is violated for a certain entangled (target) state \( \rho_{\text{target}} \) that is \( \text{Tr}(O \rho_{\text{target}}) \geq g + a q \). We proceed by writing the spectral decomposition \( W = \sum_i \lambda_i M_i \), where \( M_i \) are eigen-projectors (binary observables), with \( \lambda_i > 0 \) because \( W_i \) are non-negative operators. The number \( \mu_i \) counts the non-zero eigenvalues of \( W_i \). Furthermore, we define the constant \( \tau = \sum_i \lambda_i / \mu_i q_i \). We have all we need to set up our verification procedure. As the \( W_i \) are local observables, the binary operators \( M_i \) are local as well. They constitute the set \( \mathcal{M} \), which contains in total \( L = \sum_i \mu_i \) elements. The probability weights for \( M_i \) are set to \( \gamma_i = \lambda_i / \mu_i q_i \). For a given copy of a separable state \( \rho_{\text{sep}} \), the probability to obtain success for a randomly drawn measurement \( M_i \) from the set \( \mathcal{M} \) is given by

\[
p = \sum_{k=1}^{L} \sum_{l=1}^{K} \gamma_k \frac{\text{Tr}(M_k \rho_{l})}{\tau} 
\]

Therefore, the separable bound is given by \( p = \sum_{k=1}^{L} \gamma_k (g + a q) \). Clearly, for the target state preparation we obtain \( p = \sum_{k=1}^{L} \gamma_k (g + a q) \) with the strict separation \( \lambda_i = p_i - p_i = (g - g) / q_i > 0 \). Once we have defined the set \( \mathcal{M} \) and found \( p \), we can apply the protocol illustrated in Fig. 1 and find the minimum confidence for detecting quantum entanglement. We would like to point out that our protocol could possibly be applied to the device-independent entanglement witnesses as well. In this case our procedure would need to be adapted to a device-independent framework.

Scaling of resources with the size of the system. The example of the graph state discussed in the section "Translation of entanglement witnesses" shows a constant gap between \( p_c \) and \( p_t \) that does not depend on the number of qubits \( n \). For this reason, the number of required copies needed to achieve a certain confidence does not grow with the number of qubits (recall that only 16 copies are required to achieve 99% confidence, regardless of the number of qubits). In this case, the standard witness-based approach would require \( 2^n \) to achieve 99% confidence, regardless of the number of qubits. In this case, the pulse has a central wavelength of 772.9 nm and a duration of 2.1 ps. The first two BSs along the pump path are used to double the repetition rate of the laser and decrease at the same time the power of each pulse, such that unwanted contributions from SPDC higher-order emissions are reduced. This approach is referred to as passive temporal multiplexing. One output of the second BS is sent to a third BS, which equally splits the pump power. The other one passes through a HWP and a PBS, where the reflected port is stopped by a beam block. This allows us to adjust the pump power along this path if needed. The two output beams from the third BS and the one from the PBS go through a HWP and a QWP so that polarization can be adjusted, and are then used to pump three single-photon sources. Delay lines in the second and third beam paths are needed later for temporal synchronization. A photon pair is generated from each source via collinear type-II SPDC from a 30-mm-long periodically poled KTiOPO₄ (PPKTP) crystal placed into a Sagnac interferometer, which has the advantages of compactness and phase stability. A schematic of a single-photon source is shown in Fig. 3b. This is composed of a DM reflecting the pump and transmitting the photons, a DBPS and a DHWP, which work for both pump and photon wavelengths, and a PPKTP. The crystal temperature, set to 24°C enables photon wavelength degeneracy at 1.545.8 nm. The photons generated from the crystal pass through ultranarrow filters with a bandwidth of 3.2 nm that improve their spectral purity and are eventually coupled into single-mode fibres (not shown in the figure). The residual pump beam is removed using long-pass filters.

Generation stage. Each pair of photons coming from different sources is sent to a PBS, at which it has been temporally synchronized using the delay lines discussed above. The photons exit in fibres—not shown in the figure—and propagate in free space through the PBSs, before being coupled into fibres again. A HWP set to 22.5° placed along the third photon path is used to generate the cluster state.

Detection stage. Photons from each output again pass to free space and then through a system composed of a motorized QWP and HWP followed by a PBS. They are eventually re-coupled into fibres and sent to a detection system composed of 12 multi-element superconducting detectors. Each multi-element detector is made up of four nanowires on the same chip, allowing for pseudo-number resolution and a high detection efficiency (0.87 on average at around 1.530 nm). The detectors operate at a temperature of 9.8 K. Photon coincidences are registered using a custom 64-channel time-tagging and logic module.

Our sixfold coincidence rate is primarily affected by coupling losses at the generation stage coming from propagation of the photons in free space through the PBSs before being coupled again into fibres, and also filter imperfections. As coupling losses are largest in the second source, we double the second source pump power by rotating the HWP placed before the PBS at the preparation stage to compensate. Our final sixfold rate is ~0.1 Hz. To maximize the probability that each measurement detects at least one copy of the state in every basis, we set the measurement time to 40 s. The tomography waveplates are automated using PCB motors.

Data availability

The data that support the plots within this paper and other findings of this study are available from the corresponding author on request.

References

48. Töth, G. Entanglement witnesses in spin models. Phys. Rev. A 71, 010301 (2005).