Published in final edited form as:
Nat Phys. 2019 June 18; 15(9): 935–940. doi:10.1038/s41567-019-0550-4.

Experimental few-copy multi-particle entanglement detection

Valeria Saggio[1,*], **Aleksandra Dimić**[2], **Chiara Greganti**[1,3], **Lee A. Rozema**[1], **Philip Walther**[1], **Borivoje Dakić**[1,4]

[1]Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria

[2]Faculty of Physics, University of Belgrade, Studentski Trg 12-16, 11000 Belgrade, Serbia

[3]VitreaLab GmbH, Boltzmanngasse 5, A-1090 Vienna, Austria

[4]Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria

Abstract

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, which however require many measurements 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.

[*]Corresponding author, valeria.saggio@univie.ac.at.

Data Availability

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

Author contributions

V.S., C.G., and P.W. designed the experiment. V.S. and C.G. built the setup. V.S. performed data analysis. L.A.R. worked on the detectors. A.D. and B.D. developed the theoretical idea. L.A.R., P.W., and B.D. supervised the project. All authors contributed to writing the paper.

Competing interests

The authors declare they have no competing interests.

Introduction

The reliable verification of quantum entanglement [1] is an essential task for quantum technologies, but it remains a considerable challenge for large-scale quantum systems. The generation of large entangled states [2–9] is required to investigate new quantum phenomena and develop novel applications. At the same time, this makes the problem of reliable verification both more important and significantly more consuming in terms of time and resources. The most exhaustive method for inferring quantum entanglement is to reconstruct density matrices via quantum state tomography [10]. 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 [11] and references therein). Although these techniques show significant improvements with respect to the number of measurement settings [12–15], they still require many detection events (i.e. many copies of the quantum state) to extract expectation values of 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 benchmarking [16], quantum state tomography via compressed sensing [17] and machine learning [18, 19], direct fidelity estimation [20], self-testing methods [21–26], quantum state verification [27, 28], entanglement verification [29–33], 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. In contrast here, 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 [34] 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, is implemented via local measurements only, and does not require the assumption of *independent and identically distributed* (*i.i.d.*) experimental runs.

Furthermore, we show that in certain cases 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, i.e. *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 experiments [2]. We verify the presence of entanglement with at least 99.74% confidence by using around 20 copies of the quantum state and also show that 112 copies suffice to certify genuine six-qubit entanglement with at least 99% confidence. In this way, we lay the foundation for a new efficient and advantageous detection scheme, providing a key tool to characterize quantum devices with minimal resources.

While our work shows similarities with Ref. [34], substantial improvements have been made. Ref. [34] focuses only on reducing the resources down to a single copy of the state, thus finding only some suitable classes of quantum states for which the theory works. Furthermore, a reduction down to a single copy is made possible by increasing the size of the system up to tens of qubits, thus not being practically applicable in realistic situations. In contrast, here we develop a new theory applicable to any quantum state (of arbitrary system size) for which one can construct an entanglement witness. Moreover, Ref. [34] does not discuss different types of entanglement (e.g. genuine multipartite entanglement), while we provide a tool to explicitly distinguish between them. In many cases, this distinction is essential as, for example, genuine multipartite entanglement is required for many quantum information protocols.

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 (i.e. states of the type $|\psi_1\rangle|\psi_2\rangle$). A non-separable state is called *entangled*. For multipartite systems, one can define various types of entanglement [11]. 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, i.e. $\langle W\rangle \geq 0$ for any separable state ρ_{sep}, where $\langle W\rangle = \mathrm{Tr}(W\rho_{sep})$. W is in general not locally accessible (one has to decompose it into the sum of local observables W_k's as $W = \sum_{k=1}^{L} W_k$, where each W_k 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 $\mathfrak{M} = \{M_1, M_2, \ldots, M_L\}$ of binary local multi-particle 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's (each with some probability ε_k) N times from the set $\mathfrak{M}$ and applying each of them to the quantum state, obtaining the outcomes m_k's. The set $\mathfrak{M}$ is tailored such that the probability to obtain success (i.e. 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_e, called *entanglement value*, if a certain entangled state (target state) has been prepared. The entanglement value p_e is strictly greater than the separable bound p_s, i.e. the difference $\delta_0 = p_e - p_s > 0$. In a realistic framework, we can prepare a certain state ρ_{exp} and assume that the application of the M_k's to it returns S successful outcomes. The observed deviation from the separable bound $\delta = p_{\mathrm{obs}} - p_s$ (where p_{obs} is the observed entanglement value) therefore reads

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

It has been shown in [34] that the probability $P(\delta)$ to observe $\delta > 0$ for any separable state is upper bounded as $P(\delta)\ \le e^{-D(p_s+\delta\|p_s)N}$, which goes exponentially fast to zero with the number of copies N. Here $D(x \parallel y) = x\log\frac{x}{y} + 1(1-x)\log\frac{1-x}{1-y}$ is the Kullback-Leibler divergence. Therefore, the confidence $C(\delta)$ of detecting quantum entanglement is lower bounded by $C_{\min}(\delta)$ as follows:

$$C(\delta) = 1 - P(\delta) \ge 1 - e^{-D(p_s + \delta \parallel p_s)N} = C_{\min}(\delta), \qquad (2)$$

and converges exponentially fast to unity in N. From (2) we can estimate the average number of copies N_{av} needed to achieve a certain confidence C_0, meaning that for a target state preparation we find

$$N_{av} \le -K\log\left(1 - C_0\right) = N_{\max}, \qquad (3)$$

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

If δ evaluates to a positive number, we can use (1) to calculate $C_{min}(\delta)$ from (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 [34] for the 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 etc. It is known that in such cases other schemes can lead to inadequate results [35, 36], whereas in our case we never obtain false positives.

Translating entanglement witnesses into the probabilistic framework

Any entanglement witness can be translated into our probabilistic verification protocol. Therefore, our method can detect any type of entanglement (e.g. genuine multipartite, bipartite) for which there exists a corresponding witness. Here we will show how to construct the set $\mathscr{M}$ and find the corresponding separable bound p_s for any entanglement witness (see Methods, Section I 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 $W' = aW + b$. The mean value of this new witness is the probability of success of our protocol, which is upper bounded by p_s for any separable state and achieves $p_e > p_s$ 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 $W = \frac{1}{2}\mathbb{1} - |G\rangle\langle G|$, for which we have $\langle W\rangle \geq 0$ for any biseparable state. This witness W can be easily transformed into the equivalent one $W' = \frac{1}{2}\mathbb{1} + \frac{1}{2}|G\rangle\langle G|$, for which we get $\langle W'\rangle \leq 3/4 = p_s$ for any biseparable state. The graph state can be decomposed as the sum of its stabilizers S_k's as $|G\rangle\langle G| = \frac{1}{2^n}\sum_{k=1}^{2^n} S_k$, where the S_k's are certain products of local Pauli observables. Therefore, the new witness reads $W' = \frac{1}{2^n}\sum_{k=1}^{2^n} M_k$, where $M_k = (\mathbb{1} + S_k)/2$ are the binary observables needed in our probabilistic protocol. The sampling is uniform, i.e. the probabilities equal $\varepsilon_k = 1/2^n$. As the S_k's stabilize the state, $p_e = 1$ for an ideal graph state. This procedure also leads to an estimate of the fidelity $F = \langle G|\rho_{exp}|G\rangle$ between the experimentally generated state ρ_{exp} and the ideal one $\rho_{ideal} = |G\rangle\langle G|$, as in [20]. Note that we can also use our experimental data for quantum state verification [27].

Given p_e and p_s we can obtain the average number of copies needed to achieve a certain confidence C_0 from (3). We get $N_{av} \leq -D(1\|3/4)^{-1}\log(1 - C_0) \approx -3.48\log(1 - C_0)$. Therefore, to achieve confidence of $C_0 = 0.99$ we need at most $N_{\max} \approx 16$ copies of $|G\rangle$, which is a remarkably low number. Furthermore, this number is independent of the system size (i.e. number of qubits n). Notice that different local decompositions of the witness will lead to different scaling constants K in (3), and finding the optimal decomposition is an open challenge [31]. Reduction of resources down to a single copy can be achieved in certain cases [34] by considering a particular dependence of the separable bound on n (see Methods, Section II for a detailed discussion).

Once we have found the M_k's and p_s, we can apply the protocol illustrated in Fig. 1 and find the minimum confidence for entanglement detection.

Entanglement verification tailored 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

$$|Cl_6\rangle = \frac{1}{2}(|H_1H_2H_3H_4H_5H_6\rangle + |H_1H_2H_3V_4V_5V_6\rangle + |V_1V_2V_3H_4H_5H_6\rangle - |V_1V_2V_3V_4V_5V_6\rangle), \quad (4)$$

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:

a) The witness presented in [12], composed of only two measurement settings:

$$W_1 = 3\,\mathbb{1} - 2\left(\prod_{k=1,3,5}\frac{\mathbb{1} + G_k}{2} + \prod_{k=2,4,6}\frac{\mathbb{1} + G_k}{2}\right), \quad (5)$$

where the G_k's (with $k = 1, \ldots, 6$) are the experimental generators of the cluster state [37], listed in the Methods, Section III;

b) The standard witness tailored for our cluster state [38]:

$$W_2 = \frac{1}{2}\,\mathbb{1} - |Cl_6\rangle\langle Cl_6|, \quad (6)$$

which requires $2^6 = 64$ measurement settings (since $|Cl_6\rangle\langle Cl_6| = \frac{1}{2^6}\sum_{k=1}^{2^6} S_k$, 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 be also used to distinguish fully separable and entangled states, i.e. to detect only some entanglement, and the corresponding separable bounds can be evaluated numerically [39]. We can then distinguish two types of separable bounds: one is the so called *biseparable bound* p_{bs}, that can be directly extracted from our translation protocol and is therefore used for detection of genuine six-qubit entanglement, the other one is the *fully separable bound* p_{fs}, which is evaluated numerically and used to detect some entanglement.

Following the procedure shown in the Methods, Section I, we find for W_1 the set $\mathscr{M}_{W_1} = \{M_1 = \prod_{k=1,3,5}\frac{\mathbb{1} + G_k}{2}, M_2 = \prod_{k=2,4,6}\frac{\mathbb{1} + G_k}{2}\}$, where M_1 and M_2 are the binary local observables, and the corresponding biseparable bound is $p_{bsW_1} = 3/4$. For W_2, the binary observables constituting the set $\mathfrak{M}W_2$ are $\frac{\mathbb{1} + S_k}{2}$ (with $k = 1, \ldots, 64$) and the biseparable bound is $p_{bsW_2} = 3/4$ (see the example of the graph state discussed in the previous section). The derived fully separable bounds read $p_{fsW_1} = 9/16$ and $p_{fsW_2} = 5/8$. The entanglement values are $p_{eW_1} = p_{eW_2} = 1$.

The experimental setup

The experimental setup 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 *beam splitters* (BSs). It then pumps three identical single-photon sources, each built in a Sagnac configuration [42–45]. Each source produces a polarization-entangled photon pair at telecommunication wavelengths via collinear type-II *Spontaneous Parametric Down-Conversion* (SPDC), specifically the singlet state $|\psi^-\rangle_{i,j} = (|H_iV_j\rangle - |V_iH_j\rangle)/\sqrt{2}$, where $|H\rangle$, $|V\rangle$ denote the horizontal and vertical photons' polarization states and i, j the photons' spatial modes. A schematic of one single-photon source is shown in Fig. 3b (see Methods, Section IV for details). It is possible to switch between different Bell states with a *half-waveplate* (HWP) placed along one photon path (see Fig. 3b) and/or by rotating the HWP positioned along the pump path right before the source.

In the *Generation stage*, after switching from $|\psi^-\rangle_{1,2}$ and $|\psi^-\rangle_{3,4}$ to $|\phi^-\rangle_{1,2}$ and $|\phi^-\rangle_{3,4}$, and from $|\psi^-\rangle_{5,6}$ to $|\phi^+\rangle_{5,6}$, where $|\phi^\pm\rangle_{i,j} = (|H_iH_j\rangle \pm |V_iV_j\rangle)/\sqrt{2}$, photon pairs from different sources 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 — that enables measurements in different polarization bases, and is then sent to the detection apparatus, which consists of twelve pseudo-number resolving multi-element superconducting detectors [46, 47]. Lenses to adjust the beam size, fibers and manual polarization controllers (to compensate for polarization changes into the fibers) are not shown in the figure. When the HWP in the third photon path is set to perform a Hadamard gate, the simultaneous detection of the six photons at the outputs nominally produces the state (4).

Results

For the witness W_1, we applied $N_{W_1} = 150$ different measurement settings that were randomly sampled from the set $\mathfrak{M}_{W_1}$. For each measurement setting, we acquired data for 40 seconds. In order to ensure that our sampling was random, we only analyzed the first six-photon event in each setting. In 12 of the settings, no six-photon events were detected (see Methods, Section IV), resulting in 138 copies of the state being produced. Fig. 4a,b show plots of the minimum confidence $C_{\min}(\delta_{W_1})$ versus the number of copies N when the fully separable bound p_{fsW_1} and biseparable bound p_{bsW_1} are used, respectively. The points are obtained by plugging the experimentally observed δ_{W_1} into (2) to find $C_{\min}(\delta_{W_1})$.

For the witness W_2, we acquired data in the same manner, randomly choosing $N_{W_2} = 160$ different measurement settings from the set $\mathfrak{M}_{W_2}$. As before, Fig. 4c,d show the increase in the minimum confidence in the full separability (where $p_{fs\,W_2}$ is used) and biseparability (where $p_{bs\,W_2}$ is used) cases, respectively.

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 (2) is a monotonic function in the number of copies because all the binary outcomes evaluate to 1. However, since 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. Fig. 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%. Fig. 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, i.e. 64. As previously discussed, in this last case we can also estimate the fidelity $F = \langle Cl_6 | \rho_{exp} | Cl_6 \rangle = 0.75 \pm 0.06$. The different areas marked with different colours in both plots and the red dotted lines help the 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 ions [3], superconducting circuits [4], or continuous-variable systems [7–9].

Methods

Section I Formal proof for generic witness translation

Here, we show how to translate any entanglement witness into our probabilistic protocol. Conventionally, a witness operator W is normalized such that $\langle W \rangle = \mathrm{Tr}(W\rho_{sep}) \geq 0$ for any separable state ρ_{sep}. An equivalent form reads $W = g_s \mathbb{1} - O$, where O is an Hermitian operator for which $\langle O \rangle = \mathrm{Tr}(O\rho_{sep}) \leq g_s$ holds for any ρ_{sep} [48]. Now, let us consider the local decomposition $O = \sum_{k=1}^{q} W_k$, where q is the number of local settings needed to measure $\langle O \rangle$. We are free to add a constant term to each local component $W'_k = W_k + a\,\mathbb{1}$ such that they become non-negative observables. This transformation leads to the new witness $O' = \sum_{k=1}^{q} W'_k = O + aq\,\mathbb{1}$. We choose $a \geq 0$ to take the minimum possible value. Altogether, we can rewrite the separability condition as

$$\langle O' \rangle = \mathrm{Tr}(O' \rho_{sep}) \leq g_s + aq. \quad (7)$$

Our main aim is to test this inequality in practice via our probabilistic procedure. Note that this inequality is violated for certain entangled (target) state ρ_{ent}, i.e. $\mathrm{Tr}(O' \rho_{ent}) = g_e + aq$, with $g_e - g_s > 0$. We proceed by writing the spectral decomposition $W'_k = \sum_{s=1}^{\mu_k} \lambda_{ks} M_{ks}$, where M_{ks} are eigen-projectors (binary observables), with $\lambda_{ks} > 0$ since W_k's are non-negative operators. The number μ_k counts the non-zero eigenvalues of W_k. Furthermore, we define the constant $\tau = \sum_{k=1}^{q} \sum_{s=1}^{\mu_k} \lambda_{ks}$. We have all we need to set up our verification procedure. As the W_k's are local observables, the binary operators M_{ks}'s are local as well. They constitute the set $\mathfrak{M}$, which contains in total $L = \sum_{k=1}^{q} \mu_k$ elements. The probability weights for M_{ks}'s are set to $\varepsilon_{ks} = \lambda_{ks}/\tau$. For a given copy of a separable state ρ_{sep}, the probability to obtain success for a randomly drawn measurement M_{ks} from the set $\mathfrak{M}$ is given by

$$p = \sum_{k=1}^{q} \sum_{s=1}^{\mu_k} \varepsilon_{ks} \mathrm{Tr}(M_{ks} \rho_{sep}) = \frac{1}{\tau} \sum_{k=1}^{q} \langle W'_k \rangle \leq \frac{1}{\tau}(g_s + aq). \quad (8)$$

Therefore, the separable bound is given by $p_s = \frac{1}{\tau}(g_s + aq)$. Clearly, for the target state preparation we obtain $p_e = \frac{1}{\tau}(g_e + aq)$ with the strict separation $\delta_0 = p_e - p_s = (g_e - g_s)/\tau > 0$. Once we have defined the set $\mathfrak{M}$ and found p_s, 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.

Section II Scaling of resources with the size of the system

The example of the graph state discussed in the section “Translating entanglement witnesses into the probabilistic framework” shows a constant gap between p_s and p_e 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 (we 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 measurement settings, and each setting would demand a large number of copies, whereas our procedure provides reliable detection with a constant overhead. Thus, our method applies even if the number of settings exceeds the number of available copies. A further reduction of copies (even to a single one) was shown for certain classes of large multi-qubit states [34]. More precisely, in [34] examples were presented with $p_s = e^{-\alpha n}$ (where α is a constant), which vanishes exponentially fast in n, while maintaining p_e constant in n. In this case, we can approximate $K \approx 1/(\alpha n)$, thus even a single copy of the quantum state suffices to verify entanglement with high confidence (provided that n is sufficiently large). On the other hand, as long as δ_0 does not vanish when increasing the system size, we still have exponential efficiency of the procedure at the constant rate K. Finally, an interesting case occurs if δ_0 approaches zero as we increase the number of qubits. In this case, we can approximate $K \approx \frac{2p_s(1-p_s)}{\delta_0^2}$, leading to $N_{\max} \approx -\frac{2p_s(1-p_s)}{\delta_0^2}\log(1-C_0)$. Therefore, as long as δ_0^{-2} grows moderately in n, the procedure remains resource-efficient as the size of the system grows.

Section III Generators of the six-qubit cluster state and witness decomposition

Our six-qubit cluster state (4) is uniquely defined by the following six generators [37]:

$$\begin{aligned} &G_1 = Z_1Z_2, \quad G_2 = X_1X_2X_3Z_5, \quad G_3 = Z_2Z_3 \\ &G_4 = Z_4Z_5, \quad G_5 = Z_2X_4X_5X_6, \quad G_6 = Z_5Z_6, \end{aligned} \tag{9}$$

where X and Z are two of the standard Pauli operators. From this set, we can construct all the products of G_k's, and there are in total $2^6 = 64$ independent operators which are called stabilizers. This witness allows one to combine three of the six generators of the cluster state into one measurement setting, reducing the number of measurement settings from six to two. To translate the witness W_1 (see main text) into our procedure, we start with $O = 2\left(\prod_{k=1,3,5}\frac{\mathbb{1}+G_k}{2} + \prod_{k=2,4,6}\frac{\mathbb{1}+G_k}{2}\right)$ and $g_s = 3$. The witness O is already in the spectral form with $M_1 = \prod_{k=1,3,5}\frac{\mathbb{1}+G_k}{2}$ and $M_2 = \prod_{k=2,4,6}\frac{\mathbb{1}+G_k}{2}$ with eigenvalues +1, therefore $a = 0$. We get $\tau = 4$ and the sampling is uniform from the set $\mathfrak{M}_{W_1} = \{M_1, M_2\}$. For the biseparable bound we clearly get $p_{bs\,W1} = 3/4$. For full separability, we used the algorithm presented in [39] to obtain $p_{fs\,W1} = 9/16$.

The translation procedure for the witness W_2 is explained in detail in the main text. For this witness we obtain a biseparable bound of $p_{bs\,W2} = 3/4$. Also in this case, we numerically found the fully separable bound to be $p_{fs\,W2} = 5/8$.

Section IV Experimental details

We implement the random measurements M_k's with our tomography setup. We only analyze measurement results consisting of six-fold coincidence events. When more than one six-fold event is detected during the same measurement setting, we only use the first coincidence event, to ensure that only one copy of the state is used per measurement. We will now give a detailed explanation of Fig. 3a, providing a technical overview of our setup.

Preparation stage—A mode-locked Ti:Sapphire Coherent Mira 900 laser emits pulsed light at a repetition rate of 76 MHz and at an average power of 1.2 W. The pulses have 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 [40]. This approach is referred to as *passive temporal multiplexing* [41]. 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, wherein 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* $KTiOPO_4$ (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. It is composed of a *dichroic mirror* (DM) reflecting the pump and transmitting the photons, a *dual PBS* (DPBS) and a *dual HWP* (DHWP), which work for both pump and photon wavelengths, and a PPKTP. The crystal temperature set to 24° enables photon wavelength degeneracy at 1545.8 nm. The photons generated from the crystal pass through ultra-narrow filters with a bandwidth of 3.2 nm that improve their spectral purity and are eventually coupled into single-mode fibers, not shown in the figure. The residual pump beam is removed using longpass 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 fibers — not shown in the figure — and propagate in free space through the PBSs, before being coupled into fibers again. A HWP placed along the third photon path is used to generate the cluster state.

Detection stage—Photons from each output go to free space again and then pass through a system composed of a motorized QWP and HWP followed by a PBS. They are eventually re-coupled into fibers 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 a pseudo-number resolution and a high detection efficiency (0.87 on average at around 1550 nm). The detectors operate at a temperature of 0.9 K. Photon coincidences are registered using a custom 64-channel time-tagging and logic module.

Our six-fold coincidence rate is primarily affected by coupling losses in the *Generation stage* coming from the propagation of the photons in free space through the PBSs before being coupled again into fibers and filter imperfections. As coupling losses are largest in the second source, we doubled the second source pump power by rotating the HWP placed before the PBS in the *Preparation stage* to compensate. Our final six-fold rate is around 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 seconds. The tomography waveplates are automatized using PCB motors.

Acknowledgments

The authors thank I. Alonso Calafell for help with the detectors and T. Strömberg for helpful discussions. V.S. acknowledges support from the University of Vienna through the Vienna Doctoral School. A.D. acknowledges support from the project no. ON171035 of 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 Co-QuS (W1210-N25), BeyondC (F7113-N38) and NaMuG (P30067-N36), the U.S. Air Force Office of Scientific Research (FA2386-232 17-1-4011), the Austrian Research Promotion Agency (FFG) through the QuantERA ERA-NET Cofund project HiPhoP, and Red Bull GmbH. B.D. acknowledges support from the Foundational Question Institute (FQXi) grant FQXi-MGA-1806 and support from an ESQ Discovery Grant of the Austrian Academy of Sciences (ÖAW).

References

[1]. Arrazola JM, et al. Reliable entanglement verification. Phys Rev A. 2013; 87:062331.

[2]. Wang X-L, et al. Experimental ten-photon entanglement. Phys Rev Lett. 2016; 117:210502. [PubMed: 27911530]

[3]. Monz T, et al. 14-qubit entanglement: Creation and coherence. Phys Rev Lett. 2011; 106:130506. [PubMed: 21517367]

[4]. Song C, et al. 10-qubit entanglement and parallel logic operations with a superconducting circuit. Phys Rev Lett. 2017; 119:180511. [PubMed: 29219550]

[5]. Friis N, et al. Observation of Entangled States of a Fully Controlled 20-Qubit System. Phys Rev X. 2018; 8:021012.

[6]. Wang X-L, et al. 18-Qubit Entanglement with Six Photons' Three degrees of Freedom. Phys Rev Lett. 2018; 120:260502. [PubMed: 30004724]

[7]. Chen M, Menicucci NC, Pfister O. Experimental Realization of Multipartite Entanglement of 60 Modes of a Quantum Optical Frequency Comb. Phys Rev Lett. 2014; 112:120505. [PubMed: 24724640]

[8]. Yoshikawa J-I, et al. Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing. APL Photonics. 2016; 1:060801.

[9]. Cai Y, et al. Multimode entanglement in reconfigurable graph states using optical frequency combs. Nat Comm. 2017; 8:15645–15653.

[10]. James DFV, Kwiat PG, Munro WJ, White G. Measurement of qubits. Phys Rev A. 2001; 64:052312.

[11]. Gühne O, Tóth G. Entanglement detection. Physics Reports. 2009; 474:1–75.

[12]. Tóth G, Gühne O. Detecting genuine multipartite entanglement with two local measurements. Phys Rev Lett. 2005; 94:060501. [PubMed: 15783712]

[13]. Knips L, Schwemmer C, Klein N, Wieśniak M, Weinfurter H. Multipartite entanglement detection with minimal effort. Phys Rev Lett. 2016; 117:210504. [PubMed: 27911541]

[14]. Tran MC, Dakić B, Arnault F, Laskowski W, Paterek T. Quantum entanglement from random measurements. Phys Rev A. 2015; 92:050301.

[15]. Bavaresco J, et al. Measurements in two bases are sufficient for certifying high-dimensional entanglement. Nat Phys. 2018; 14:1032–1037.

[16]. Knill E, et al. Randomized benchmarking of quantum gates. Phys Rev A. 2008; 77:012307.

[17]. Gross D, Liu Y-K, Flammia ST, Becker S, Eisert J. Quantum state tomography via compressed sensing. Phys Rev Lett. 2010; 105:150401. [PubMed: 21230876]

[18]. Montanaro, A. Learning stabilizer states by Bell sampling. 2017. Preprint at http://arXiv.org/abs/1707.04012

[19]. Torlai G, et al. Neural-network quantum state tomography. Nat Phys. 2018; 14:447–450.

[20]. Flammia ST, Liu Y-K. Direct fidelity estimation from few Pauli measurements. Phys Rev Lett. 2011; 106:230501. [PubMed: 21770489]

[21]. Mayers D, Yao A. Self testing quantum apparatus. QIC. 2004; 4:273–286.

[22]. McKague, M. Self-testing graph statesTheory of Quantum Computation, Communication, and Cryptography. Vol. 6745. Springer; Berlin Heidelberg: 2014. 104–120.

[23]. Bancal J-D, Navascués M, Scarani V, Vértesi T, Yang TH. Physical characterization of quantum devices from nonlocal correlations. Phys Rev A. 2015; 91:022115.

[24]. Miller, CA; Shi, Y. Optimal robust quantum self-testing by binary nonlocal XOR games. 2012. Preprint at http://arXiv.org/abs/1207.1819

[25]. Reichardt, BW; Unger, F; Vazirani, U. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. 2012. Preprint at http://arXiv.org/abs/1209.0448

[26]. McKague M, Yang TH, Scarani V. Robust self-testing of the singlet. J Phys: A Math Theor. 2012; 45:455304.

[27]. Takeuchi Y, Morimae T. Verification of many-qubit states. Phys Rev X. 2018; 8:021060.

[28]. Zhu, H; Hayashi, M. Efficient verification of hypergraph states. 2018. Preprint at http://arXiv.org/abs/1806.05565

[29]. Pappa A, Chailloux A, Wehner S, Diamanti E, Kerenidis I. Multipartite entanglement verification resistant against dishonest parties. Phys Rev Lett. 2012; 108:260502. [PubMed: 23004945]

[30]. McCutcheon W, et al. Experimental verification of multipartite entanglement in quantum networks. Nat Comm. 2016; 7:13251–13258.

[31]. Pallister S, Linden N, Montanaro A. Optimal verification of entangled states with local measurements. Phys Rev Lett. 2018; 120:170502. [PubMed: 29756811]

[32]. Schneeloch, J; Tison, CC; Fanto, ML; Alsing, PM; Howland, GA. Quantifying entanglement in a 68-billion dimensional quantum systems. 2018. Preprint at http://arXiv.org/abs/1804.04515

[33]. Barreiro JT, et al. Demonstration of genuine multipartite entanglement with device-independent witnesses. Nat Phys. 2013; 9:559–562.

[34]. Dimić A, Dakić B. Single-copy entanglement detection. npj Quantum Information. 2018; 4:11–18.

[35]. Jungnitsch B, et al. Increasing the statistical significance of entanglement detection in experiments. Phys Rev Lett. 2010; 104:210401. [PubMed: 20867078]

[36]. Blume-Kohout, R. Robust error bars for quantum tomography. 2012. Preprint at http://arXiv.org/abs/1202.5270

[37]. Lu C-Y, et al. Experimental entanglement of six photons in graph states. Nat Phys. 2007; 3:91–95.

[38]. Hein M, Eisert J, Briegel HJ. Multiparty entanglement in graph states. Phys Rev A. 2004; 69:062311.

[39]. Gerke S, Vogel W, Sperling J. Numerical construction of multipartite entanglement witnesses. Phys Rev X. 2018; 8:031047.

[40]. Greganti C, Schiansky P, Alonso Calafell I, Procopio LM, Rozema LA, Walther P. Tuning single-photon sources for telecom multi-photon experiments. Opt Express. 2018; 26:3286–3302. [PubMed: 29401859]

[41]. Broome MA, Almeida MP, Fedrizzi A, White AG. Reducing multi-photon rates in pulsed downconversion by temporal multiplexing. Opt Express. 2011; 19:22698–22708. [PubMed: 22109151]

[42]. Kim T, Fiorentino M, Wong FNC. Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. Phys Rev A. 2006; 73:012316.

[43]. Fedrizzi A, Herbst T, Poppe A, Jennewein T, Zeilinger A. A wavelength-tunable fiber-coupled source of narrowband entangled photons. Opt Express. 2007; 15:15377–15386. [PubMed: 19550823]

[44]. Kuzucu O, Wong FN. Pulsed Sagnac source of narrow-band polarization-entangled photons. Phys Rev A. 2008; 77:032314.

[45]. Jin R-B, et al. Pulsed Sagnac polarization-entangled photon source with a PPKTP crystal at telecom wavelength. Opt Express. 2014; 22:11498–11507. [PubMed: 24921271]

[46]. Natarajan CM, Tanner MG, Hadfield RH. Superconducting nanowire single-photon detectors: physics and applications. Supercond Sci Technol. 2012; 25:063001–063016.

[47]. Marsili F, et al. Detecting single infrared photons with 93% system efficiency. Nat Photon. 2013; 7:210–214.

[48]. Tóth G. Entanglement witnesses in spin models. Phys Rev A. 2005; 71:010301.

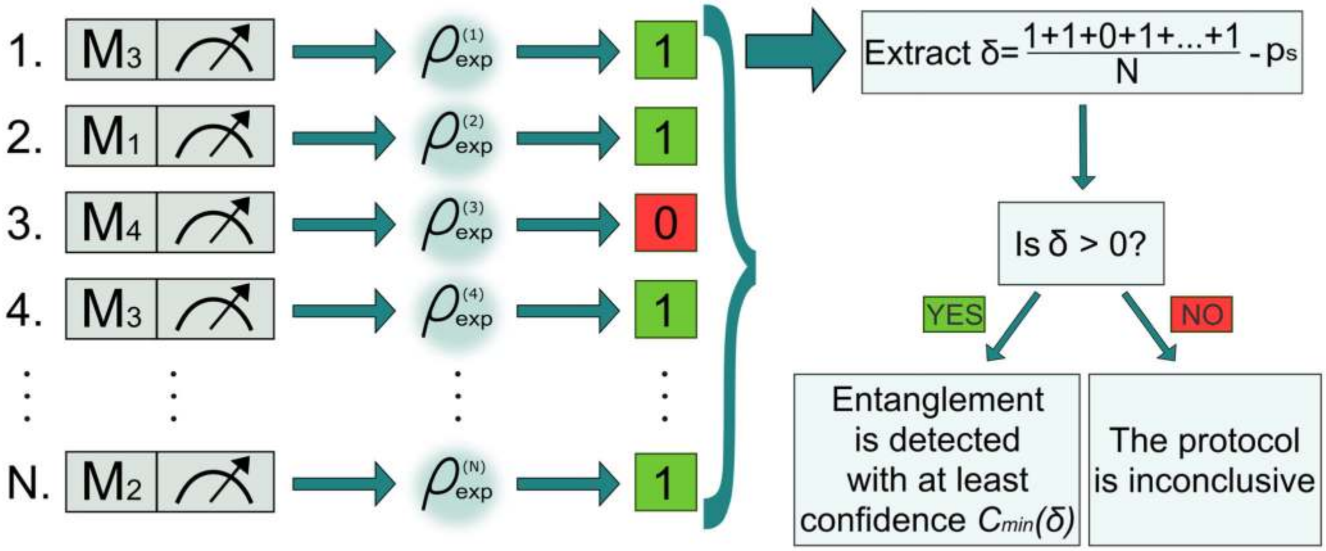
1. M3
2. M1
3. M4
4. M3
N. M2
$\rho_{exp}^{(1)}$
$\rho_{exp}^{(2)}$
$\rho_{exp}^{(3)}$
$\rho_{exp}^{(4)}$
$\rho_{exp}^{(N)}$
1
1
0
1
1
Extract $\delta = \frac{1+1+0+1+...+1}{N} - p_s$
Is δ > 0?
YES
NO
Entanglement is detected with at least confidence $C_{min}(\delta)$
The protocol is inconclusive

Fig. 1. Illustration of the entanglement detection protocol.

The first step consists of randomly drawing from the set $\mathfrak{M}$ the measurements M_k's N times. Next, they are applied to the experimental state ρ_{exp}, which then returns binary outcomes 1 or 0 (success or failure, respectively). The superscripts in ρ_{exp} account for possible variations of the state due to experimental imperfections. After N runs, the protocol returns S successful outcomes. If the deviation $\delta = S/N - p_s > 0$, entanglement is verified in the system with a confidence of at least $C_{\min}(\delta)$. Otherwise, the protocol is inconclusive.

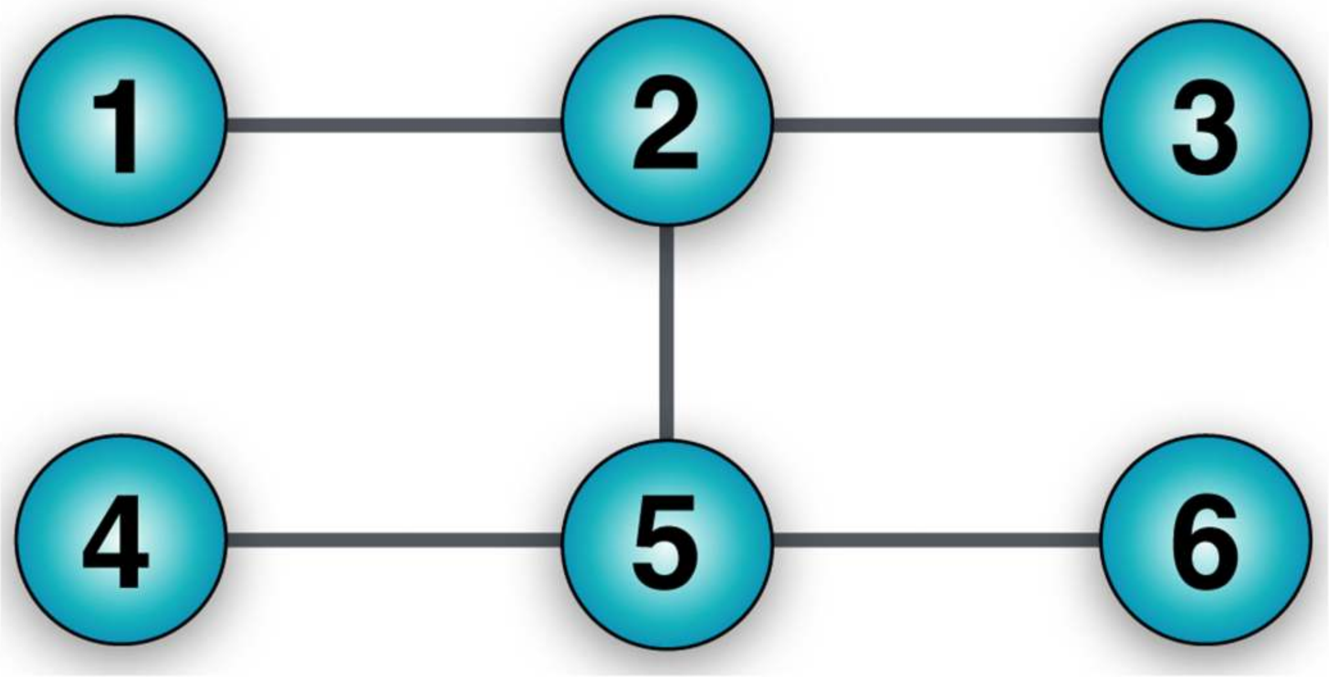

Fig. 2. Schematic of an H-shaped six-qubit cluster state.

The standard way to represent a graph state is to draw a set of vertices and edges. Each vertex is drawn as a disk representing a single qubit prepared in the eigenstate $|+\rangle$ of the Pauli operator X. Edges are solid lines representing pairwise controlled phase gates applied to the connected qubits. As a result of the application of these gates, entanglement is created between the linked qubits.

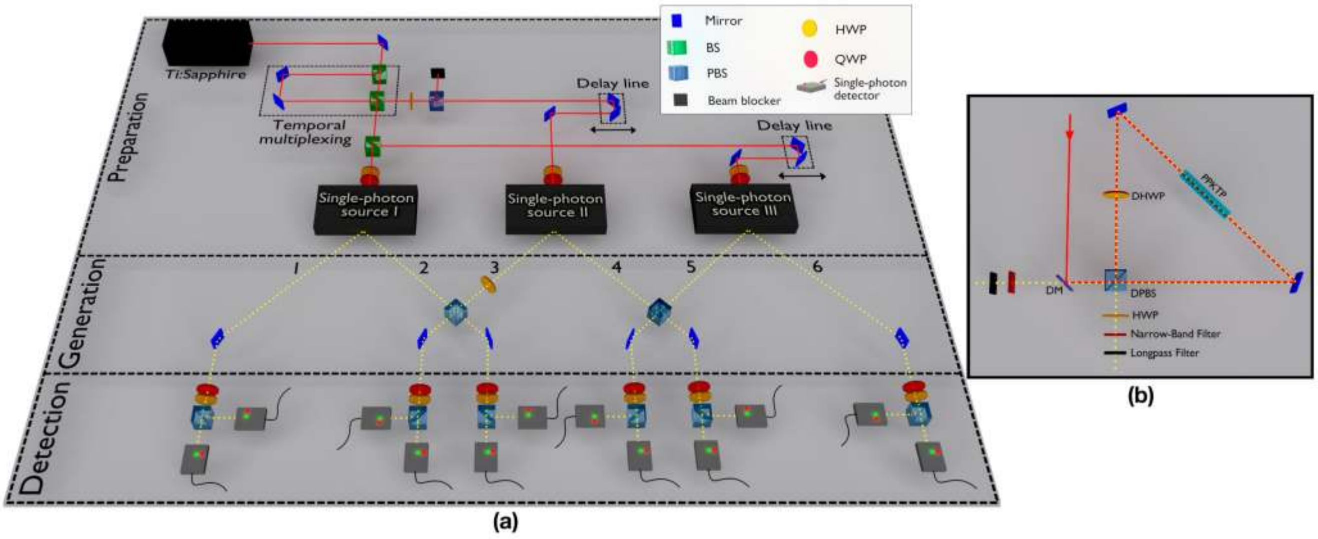

Fig. 3. Experimental setup.

(a) A picosecond Ti:Sapphire laser outputs a beam that is temporally multiplexed to double the repetition rate and reduce contributions from unwanted SPDC high-order emissions. Two beams, equally split at the third BS, pump the first and third single-photon source, while the beam exiting the right output of the second BS passes through a HWP and a PBS before pumping the second source. In this way the power of the second source can be tuned. Movable translation stages are used as delay lines for temporal synchronization. A HWP and a QWP are placed along each beam path to set the needed polarization. Each beam pumps a single-photon source, which emits a polarization-entangled photon pair via type-II SPDC. At each PBS, two photons from different sources interfere. All the photons are then sent to a tomographic system composed of a QWP, a HWP and a PBS. Eventually, photons exiting both outputs of the PBSs reach the single-photon detectors. **(b)** Schematic of a single-photon source. A PPKTP crystal placed into a Sagnac interferometer is used to generate single photons. DM, Dichroic Mirror; DPBS, Dual wavelength PBS; DHWP, Dual wavelength HWP. Narrow-Band and Longpass filters are respectively used to increase the spectral purity of the photons and cut the residual pump.

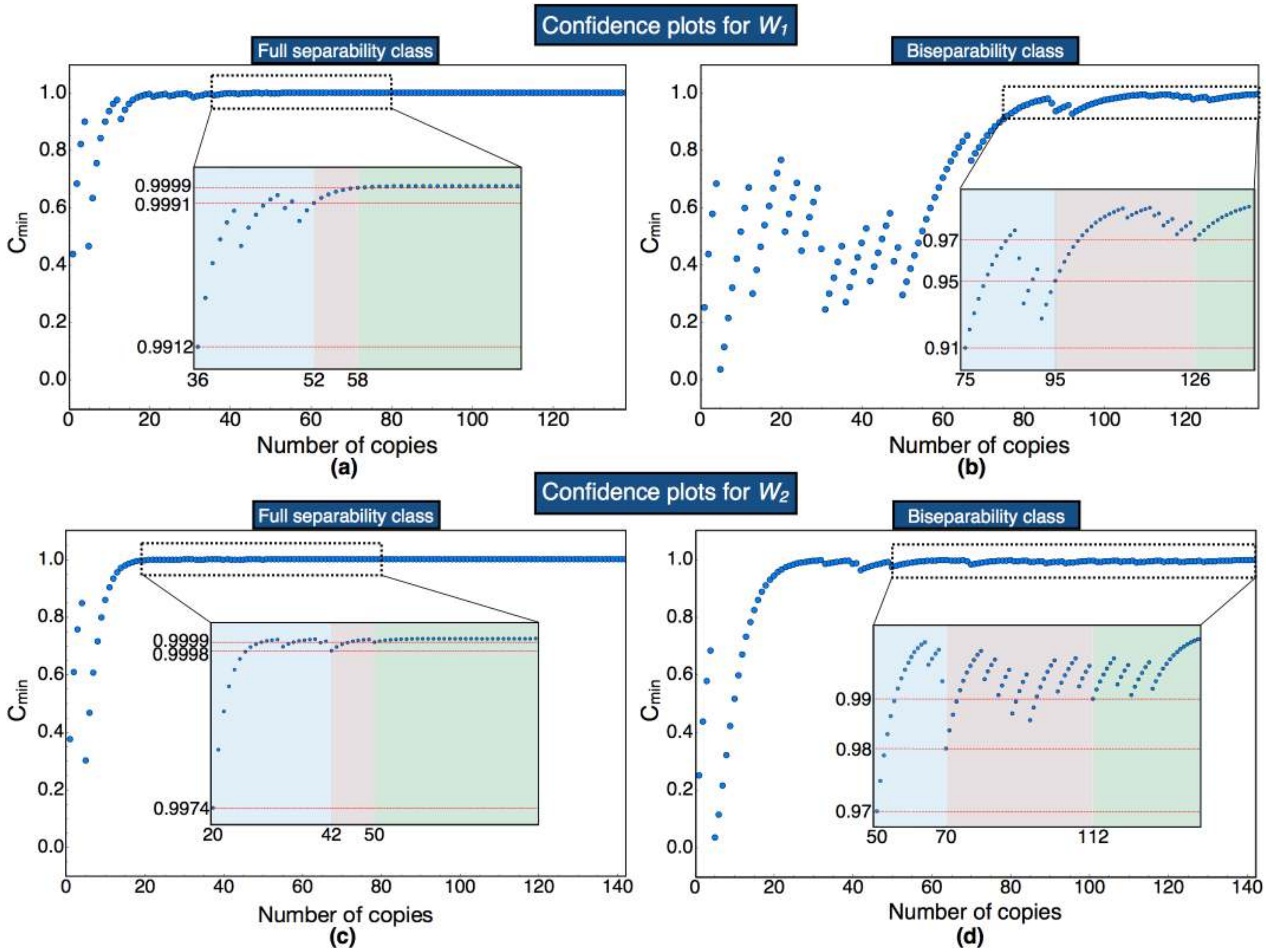

Fig. 4. Growth of confidence of entanglement with the number of copies of the quantum state.

Blue dots represent $C_{\min}$ extracted from (2). **(a)**, **(b)** show the results for the witness W_1, **(c)**, **(d)** for the witness W_2. **(a)** and **(c)** show the minimum confidence when the fully separable bound is used (meaning $C_{\min}(S_{W_1}/N - 9/16)$ and $C_{\min}(S_{W_2}/N - 5/8)$ for **(a)** and **(c)**, respectively) and **(b)**, **(d)** are extracted by using the biseparable bound (meaning $C_{\min}(S_{W_1}/N - 3/4)$ and $C_{\min}(S_{W_2}/N - 3/4)$, respectively). δ_{W_1} and δ_{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 colors indicate different thresholds for the confidence level. Red dotted lines emphasize the different levels.