APPLIED PHYSICS

Experimental sample-efficient and device-independent GHZ state certification

Laura dos Santos Martins[1]*, Nicolas Laurent-Puig[1]*, Simon Neves[2], Uta I. Meyer[1], Ivan Šupić[1], Damian Markham[1], Eleni Diamanti[1]

The certification of quantum resources is a critical tool in the development of quantum information processing. In particular, quantum state verification is a fundamental building block for communication and computation applications, determining whether the involved parties can trust the resources at hand or whether the application should be aborted. Self-testing methods have been used to tackle such verification tasks in a device-independent (DI) setting. However, these approaches commonly consider the limit of large (asymptotic), independent and identically distributed (IID) samples, which weakens the DI claim and poses serious challenges to their experimental implementation. Here, we overcome these challenges by adopting a theoretical protocol, enabling the certification of quantum states in the few-copies and non-IID regime and by leveraging a high-fidelity multipartite entangled photon source. This allows us to show the efficient and DI certification of a single copy of a four-qubit GHZ state that can readily be used for the robust and reliable implementation of quantum information tasks.

INTRODUCTION

The certification of entangled quantum states is one of the most important quantum information primitives as entangled states are very often the crucial resource for quantum information applications, so that their certification can, in turn, ensure the reliable running of the associated application (*1*, *2*). Examples of such resources are cluster states offering a platform for universal measurement–based quantum computation (*3*); stabilizer states for error correction (*4*); and Greenberger–Horne–Zeilinger (GHZ) states for anonymous communication (*5*), quantum metrology (*6*), leader election (*7*), and more.

When entangled states are intended for use in a given application, their certification should meet three key requirements. First, it must output a state that can be used for a given application, without additional assumptions. Given that measurements in quantum theory are destructive and irreversible, it is crucial to certify the quality of quantum states without destroying them. Second, certification should ideally not rely on complete trust in the measurement devices as faulty assumptions about their structure could compromise security, implying that it should be, at least to some degree, device independent (DI). Last, the certification process must account for possible memory effects, thereby avoiding the assumption that the source produces independent and identical copies in every round of the experiment. In addition to the requirements imposed by the applications, certification should also prioritize efficiency in terms of both energy consumption and invested time. Quantum resources are inherently costly, underscoring the significance of verifying quantum systems using the fewest possible samples or measurements while still achieving robust confidence in the results. This not only minimizes the time, cost, and computational resources needed for verification but also mitigates the potential introduction of errors by external factors, narrowing the time window during which errors may occur.

Bell nonlocality, aside from being a fundamentally nonclassical phenomenon used to invalidate locally causal theories, offers an elegant solution for device-independent (DI) certification (*8*). This approach enables certification despite lacking control over the measurement devices, with self-testing results pinpointing specific quantum experiments based solely on observed measurement correlations (*9*). While traditionally expressed as mathematical theorems linking quantum setups with correlation probabilities obtained through infinite repetitions, recent advancements demonstrate the practical utility of such self-testing results in finite regimes, enabling protocols for sample-efficient DI certification of quantum states without the need for the independent and identically distributed (IID) assumption (*10*).

Such DI certification protocols pose substantial experimental challenges and hence have been largely unexplored in practice. Recent experiments have certified states when measurement devices are trusted (i.e., not DI) (*11*), even when some parties act dishonestly (*12*). In the DI setting, there have been experiments robustly self-testing states (*13*, *14*) or verifying entanglement properties (*15*), but these assume IID and are only valid in the large copy (asymptotic) limit. No experiment, so far, satisfies our three requirements for the certification of entangled quantum states. Here, we experimentally demonstrate the DI certification of a single copy of a four-partite GHZ state, completely free of the IID assumption. Our demonstration relies upon and expands the sample-efficient protocol of (*10*) and leverages the characteristics of a high-performance multipartite entangled photon source (*16*). We analyze the protocol in terms of the achieved certified optimized fidelity measure and show that our implementation opens the way to carrying out efficient and reliable quantum information tasks.

RESULTS

A DI protocol in the non-IID scenario

The objective of our certification protocol is to quantitatively assess the proximity of a state, σ_c, generated by an uncharacterized source to the target state $|\mathrm{GHZ}\rangle = (|HHHH\rangle + |VVVV\rangle)/\sqrt{2}$, without direct measurement. Ideally, the source should consistently produce multiple copies of the state $|\mathrm{GHZ}\rangle$. However, due to its uncharacterized nature, it is possible that, over N rounds, the produced state, σ^N, may exhibit

[1]Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, Paris F-75005, France. [2]FEMTO-ST Institute/Optics Department, Université Marie et Louis Pasteur, 15B avenue des Montboucons, 25030 Besançon Cedex, France.
*Corresponding author. Email: laura_smartins@hotmail.com (L.d.S.M.); nicolas.laurent-puig@lip6.fr (N.L.-P.)

correlations or even entanglement across rounds. In our protocol, on the basis of (*10*), we perform measurements over $N-1$ rounds and use the obtained results to estimate the proximity of an unmeasured copy to the target state, as illustrated in Fig. 1. Operating in a DI scenario, where measurements are uncharacterized and conform to a Bell scenario, we only have access to input-output correlations. For this reason, our approach involves testing the violation of a Bell inequality, which self-tests the target state: A high Bell violation implies that all $N-1$ measured copies are close to the target state. Given the random selection of the unmeasured copy, we can infer with high confidence that it is also close to the target state.

The fact that we operate in a DI scenario leads to a few caveats in our certification protocol. Unlike in many other approaches to quantum certification tasks [see, e.g., (*17*)], the fidelity between states cannot serve as a standard metric in this setting. Under DI conditions, our protocol is limited to certifying states up to local isometries, at best. Therefore, to address the uncertainty inherent in treating all measurement devices as black boxes, we propose using extractability as an appropriate metric, as suggested in (*18*). Extractability represents fidelity optimized over all possible local isometries. A high extractability indicates the presence of an isometry capable of aligning the measured state closely with the target state. As all other copies are measured, the extractability of the unmeasured copy is estimated conditionally on the outcomes of the performed measurements. In this sense, the certified extractability is conditional, or, in other words, it characterizes the conditional state

$$\tilde{\sigma}_c = \frac{1}{p_{1,\ldots,c-1,c+1,\ldots,N}} \mathrm{Tr}_{1,\ldots,c-1,c+1,\ldots,N}\left[\left(\bigotimes_{k=1}^{N\setminus\{c\}} M_{\mathbf{o}_k|\mathbf{i}_k}\right)\sigma^N\right] \tag{1}$$

where σ^N is the state over N rounds, $M_{\mathbf{o}_k|\mathbf{i}_k}$ represents the measurement performed on the kth copy giving outcome $\mathbf{o}_k$, and $p_{1,\ldots,c-1,c+1,\ldots,N} = \mathrm{Tr}\left[\left(\bigotimes_{k=1}^{N\setminus\{c\}} M_{\mathbf{o}_k|\mathbf{i}_k}\right)\sigma^N\right]$. This approach guarantees that the conditional state of the unmeasured copy is independent from all the other copies produced in the measurement rounds, which allows us to define the appropriate figure of merit for a non-IID DI quantum state certification protocol and formally express its final goal. We wish to claim, with a confidence level $1-\delta$, whether the extractability of the conditional state, $\tilde{\sigma}_c$, from the target state, $|\mathrm{GHZ}\rangle$, is bigger than some value $1-\eta$, with $\eta \in [0,1]$, which can be written as

$$\Xi\left(\tilde{\sigma}_c, |\mathrm{GHZ}\rangle\right) = \max_{\Phi} \mathcal{F}\left(\Phi\left[\tilde{\sigma}_c\right], |\mathrm{GHZ}\rangle\right) \geq 1-\eta \tag{2}$$

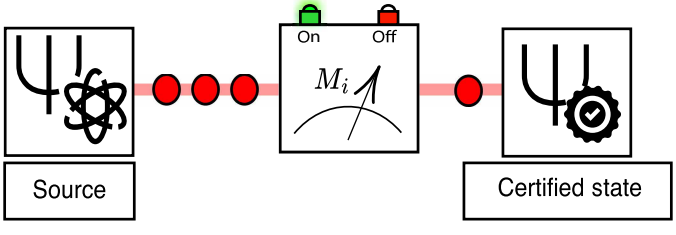

Fig. 1. DI quantum state certification scheme. The source generates N states, out of which $N-1$ are used as a verification set and are measured according to Bell nonlocality tests. The outcomes resulting from these measurements are used to evaluate whether the remaining unmeasured sample is certified to be close to the target state.

where Φ is an arbitrary local isometry and the fidelity of a state σ with respect to the target state $|\psi\rangle$ is defined as $\mathcal{F}(\sigma, |\psi\rangle) = \langle\psi|\sigma|\psi\rangle$.

To properly estimate the extractability of the GHZ state from the unmeasured copy, we must first carefully choose a Bell inequality that self-tests the target state. In other words, the selected Bell inequality should be maximally violated only by the $|\mathrm{GHZ}\rangle$ state (up to local isometries). This selection determines the Bell test to which the copies will be subjected during the measurement rounds. Furthermore, we can rely on robust self-testing statements based on a Bell inequality to establish a lower bound on the extractability of the underlying quantum state, $\Xi\left(\tilde{\sigma}_c, |\mathrm{GHZ}\rangle\right)$, from the observed violation of the inequality, β. Moving from a general self-testing framework to a well-defined certification protocol, it is useful to reframe the scenario as a nonlocal game derived from the Bell inequality. In this context, after establishing the appropriate winning and losing outcomes (where winning corresponds to those outcomes that contribute to violation of the Bell inequality), only the target state (up to local isometries) achieves the optimal quantum winning probability, p_{QM}. Although self-testing statements are typically designed for IID sources, we can leverage the robustness statement to determine the maximal winning probability for states with limited extractability.

After the copies are measured and given a score for their performance in all $N-1$ rounds (they score one if they get a winning result, zero if not), we can add them up to determine the overall score, N_{win}, and deduce the resulting verification pass rate, $P = N_{\mathrm{win}}/(N-1)$.

For a given desired extractability $1-\eta$ (Eq. 2) and confidence level $1-\delta$, the number of copies required is determined by two parameters ϵ_1, ϵ_2 that are related to the violation of the Bell inequality in the ideal case. In the protocol, ϵ_1 fixes the required pass rate: our claim on extractability holds when $P \geq p_{\mathrm{QM}} - \epsilon_1$. This is then related to the desired extractability through ϵ_2, via $c\eta = \epsilon_2 > \epsilon_1$, where c is a constant coming from self-testing, linking the extractability to β [see (*10*) and the Supplementary Materials]. The role of ϵ_2 is to allow for a gap in the requested pass rate and the desired extractability so that our goal can be achieved for finite N. The requested number of copies N is chosen so that the following is satisfied

$$\delta \leq \left(\frac{1}{N} + \frac{N-1}{N} e^{-D(p_1\|p_2)}\right)^N \tag{3}$$

where $D(a\|b) = a\log(a/b) + (1-a)\log\left[(1-a)/(1-b)\right]$ is the Kullback-Leibler divergence and $p_i = p_{\mathrm{QM}} - \epsilon_i$; see the Supplementary Materials for a detailed description of the protocol.

Choosing the Bell measurement operator

As explained above, a crucial step for experimentally demonstrating the certification of a GHZ state is to select the most appropriate Bell operator. To this end, we studied the performance of three different candidates: two Bell operators, proven to have very tight self-testing bounds in terms of robustness (*13*, *19*, *20*) (see Materials and Methods and Eqs. 5 and 6) and the following Mermin-like operator (*21*)

$$\begin{aligned} B_{Mermin} = {} & A_0B_0C_0D_0 - A_1B_1C_0D_0 \\ & - A_1B_0C_1D_0 - A_1B_0C_0D_1 \\ & + A_1B_1C_1D_1 - A_0B_1C_1D_0 \\ & - A_0B_1C_0D_1 - A_0B_0C_1D_1 \end{aligned} \tag{4}$$

where $A_0, B_0, C_0, D_0 = X$ and $A_1, B_1, C_1, D_1 = Y$. The motivation behind this choice is the fact that its quantum bound, β_Q, saturates the algebraic bound, $\beta_{algebraic}$, leading to a maximum success probability of $p_{QM} = 1$. However, to our knowledge, the only self-testing bound for a Mermin inequality existing in the literature is restricted to a tripartite system (*18*). For this reason, we computed for this work a self-testing bound for the four-partite case, relying on the numerical method described in (*19*) (see the Supplementary Materials for more details).

To compare the different Bell operators fairly, we consider a quantum state described as a statistical mixture of a GHZ state and white noise, mathematically expressed as $\rho = (1-\alpha)\rho_{GHZ} + \frac{\alpha}{16}\mathbb{1}$. We calculate the pass rate (as a probability in this case), P, and subsequently fix the winning probability threshold, $p_1 = P$, for each operator, as a function of the noise characterizing the state we want to certify, α. This allows us to study the behavior of the remaining parameters, captured in inequality (*3*). For this analysis, three main figures of merit stand out for their significance: The maximum extractability one can certify how many samples one needs to measure to complete the protocol and the confidence level associated with the results. In Fig. 2, we analyze the behavior of the different operators from the perspective of the parameters mentioned above (further details are given in Materials and Methods). In all three plots, it is clear that the Mermin operator outperforms the others, providing not only a substantial advantage in terms of sample efficiency, by almost two orders of magnitude, but also an overall better performance, regarding how close we can certify a state with respect to the target state. It is therefore the one that we use to device-independently certify the four-partite GHZ state.

Experimental results

To experimentally demonstrate the DI certification of a quantum state, we use a compact and high-performance four-party GHZ state source on the basis of spontaneous parametric down conversion (SPDC) in a layered-Sagnac interferometer configuration (see Fig. 3) (*16*). Once the states are generated, we transmit each of the four photons to the measurement apparatus and run the protocol described above. After the protocol is successfully completed, we use all the recorded measurement outcomes, except for one corresponding to a single copy randomly selected, to calculate the pass rate P. After setting the desired confidence level, $1-\delta$, we use the total number of copies, N, to numerically invert inequality (*3*) and compute the solution for the maximum certified extractability that fulfills the condition $\epsilon_2 > \epsilon_1$ (a detailed description of the data acquisition and its analysis is given in Materials and Methods).

The results are shown in Fig. 4. The certified extractability with respect to the total number of copies follows the overall expected behavior outlined by the simulation (full) curves, apart from standard experimental fluctuations. The abrupt reductions in certified extractability occur when a sequence of successive winning rounds is interrupted by the measurement of a losing outcome, resulting in a characteristic seesaw pattern. The plot on the left illustrates that, by tuning the confidence level, we can reduce the number of samples required to achieve the same certification level. However, this trade-off vanishes for large samples as the certified extractability always converges to the self-testing bound. These results show the experimental DI certification of a four-qubit GHZ state with an extractability of $\Xi(\tilde{\sigma}_c, |GHZ\rangle) \geq 0.896$, for a total of 4643 verified samples and a confidence level of $1-\delta = 0.99$, in a non-IID scenario. This demonstration is only possible due to the high-fidelity states produced with our experimental setup, yielding an average success probability of $P = 0.973$.

It is clear that the collection of additional samples would allow us to get closer to the self-testing bound of $\Xi_{max}(\tilde{\sigma}_c, |GHZ\rangle) \geq 0.919$, assuming that the average passing probability of P would remain unchanged. However, a significant increase of the acquired statistics can be experimentally challenging due to the accumulation of the recovery time associated with updating each black box's setting. This motivates the consideration of a less conservative trust scenario, in which, instead of a one-to-one input-to-output correspondence, we record multiple outcomes within the 15-s acquisition time associated with each classical input. Using postprocessing techniques, we can decompose the results obtained within the acquisition window into multiple near-single-shot measurements, mimicking the recording of a single output for each input. A randomization of the decomposed events provides the opportunity to simulate the implementation of the protocol for a larger sample, using experimental data (see Materials and Methods for more details about the data acquisition and analysis). The resulting dataset, shown in Fig. 4 (right), is further explored by testing different state generation rates, ranging from 6 to 101 Hz, which result in varying degrees of high-order SPDC emissions, consequently affecting the certified extractability, ranging from 0.923 to 0.820, respectively. This analysis highlights the range of capabilities in which our multipartite entanglement source can operate

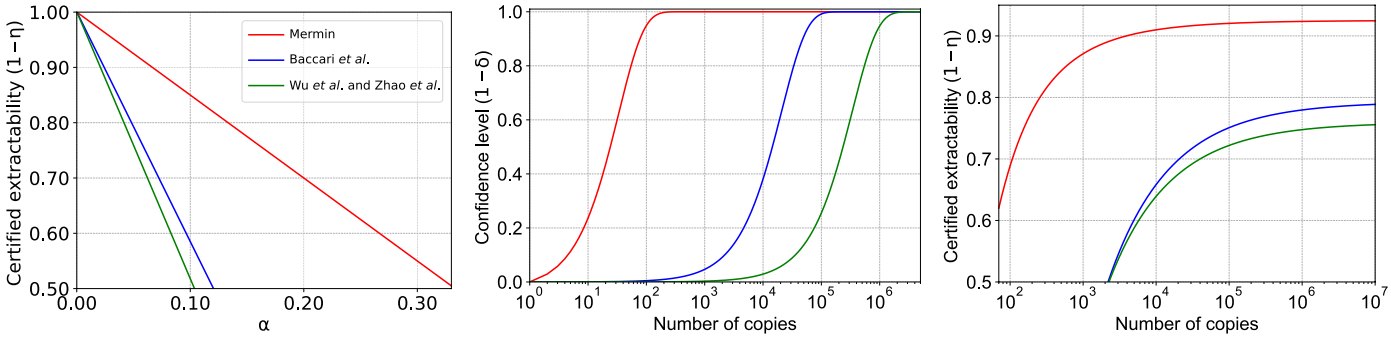

Fig. 2. Performance of three distinct Bell operators in the certification of a four-qubit GHZ state. Green and blue lines refer to operators proposed in (*13*, *19*, *20*) (see also Eqs. 5 and 6 in Materials and Methods), respectively, for robust self-testing purposes; red line corresponds to the Mermin operator (Eq. 4). Left: Maximum certified extractability, $1-\eta$, as a function of the certified quantum state noise, α, for a confidence level of $1-\delta = 0.99$, and setting $\epsilon_1 = \epsilon_2$, which is only possible in the limit of $N \to \infty$. Middle: Confidence level, $1-\delta$, as a function of the total number of copies required for the certification task, N, for a certified infidelity of $\eta = 0.25$ and for $\alpha = 0.05$. Right: Certified extractability, $1-\eta$, as a function of the total number of copies required for the certification task, N, for a fixed $1-\delta = 0.99$, $\alpha = 0.05$.

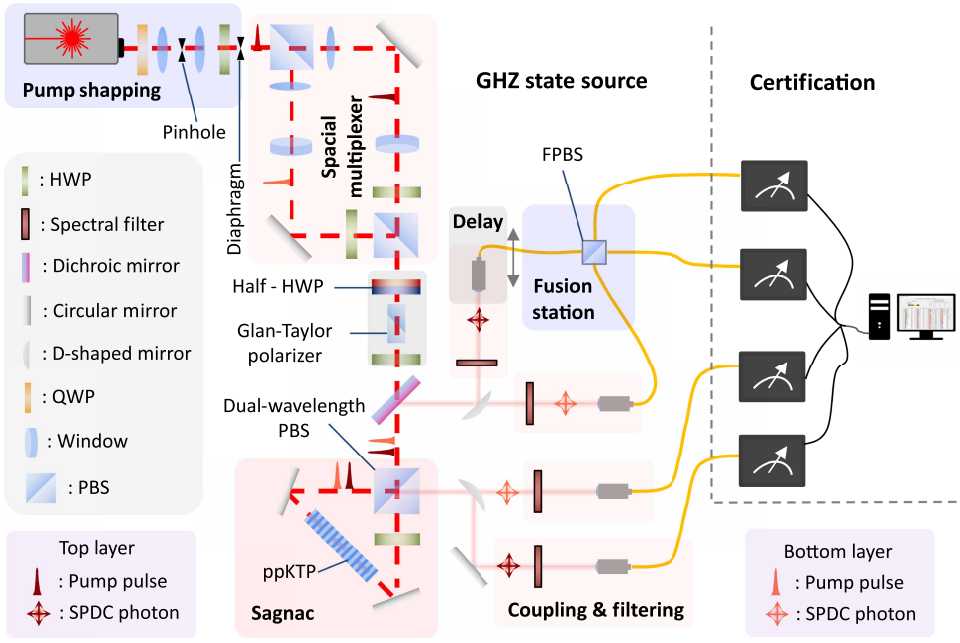

Fig. 3. Experimental setup. Laser pump: A Ti:sapphire laser (3.4-W average power) emits 2-ps pulses at 775 nm with a repetition rate of 76 MHz. Spatial mode shaping: The pump is prepared in a Gaussian spatial mode. Spatial multiplexer: Each pulse is split into two parallel beams (top and bottom layers) with horizontal and vertical polarizations, respectively. Polarization shaping: Both layers are diagonally polarized to maximize the fidelity of the output Bell states. Sagnac interferometer: Polarization-entangled photon pairs are probabilistically generated via type II SPDC in a 30-mm-long periodically poled potassium titanyl phosphate (ppKTP) crystal (46.2-μm poling period), producing the state $(|H\rangle_s|V\rangle_i + e^{i\theta}|V\rangle_s|H\rangle_i)/\sqrt{2}$. Coupling and filtering: After separation with a dichroic mirror and 1100-nm long-pass and 1.3-nm ultra-narrowband filters, bottom-layer photons are reflected by half-circle mirrors, while top-layer photons are transmitted. All photons are coupled into single-mode fibers using 12-mm focal-length lenses. Fusion station: A mechanical delay aligns the arrival of both idler photons at a fibered polarizing beam splitter (FPBS). Conditioned on fourfold coincidences and transmission to different FPBS outputs, a four-photon GHZ state $(|HHHH\rangle + e^{i\delta}|VVVV\rangle)/\sqrt{2}$ is generated. Certification: Measurement inputs and outputs from four black-box devices are used to compute the winning score over multiple rounds, certifying the proximity to the target GHZ state; HPW, half-wave plate; QWP, quarter-wave plate; PBS, polarizing beam splitter.

and shows a clear convergence of the certified extractability toward the self-testing bound, which is only possible due to the marked increase of copies to $N \sim 4 \times 10^5$. Although this approach does not strictly follow the protocol, it shows that, as long as the stability of the setup is maintained, it is possible to saturate the self-testing bound.

DISCUSSION

It is worth noting that, although the Mermin operator provides the best certification results among those we analyzed, this does not mean that they cannot be further improved. It is possible that the self-testing bound that we found is not optimal in terms of robustness, i.e., that a tighter bound exists. Furthermore, there might exist operators, other than the ones that we analyzed, yielding a more favorable combination of robust self-testing bound parameters and maximum probability of winning, p_{QM}. Because the GHZ state certification protocol heavily relies on such parameters, this suggests that the same experimental data can potentially produce even better results. Additionally, to implement the non-IID DI certification protocol, we must guarantee the precise isolation of one single random event from the whole sample. One possibility could be to use an optical switch. While this method allows for the selection of some states, accurately discerning the presence of one and only one state would prove challenging due to the postselected nature of states produced by SPDC and their inherent high-order emissions. Furthermore, in a DI scenario, the certification of extractability must account for any local isometries introduced by elements such as optical fibers or distinct measurement stations. The introduction of a physically distinct path for certified samples, an inevitable consequence of using an optical switch, would require prior certification of both the channel and the new measurement devices, leading to a circular dependency. Alternatively, although conceptually close to verification, postprocessing analysis techniques are a viable solution (see Materials and Methods for details), particularly given the absence of a specific protocol to use the certified state. However, the integration of this protocol as a subroutine in a quantum information task would likely require the incorporation of quantum memories. Moreover, our primary limitation in recording a large sample, while guaranteeing a one-to-one input-to-output correspondence, is the active control of the Mermin settings. More specifically, the experimental realization of each black box involves controlling the rotation of wave plates with mechanical motors. Adjusting their configuration requires waiting for their response time before measuring, which is accumulated over all classical inputs, leads to time-consuming implementations. Alternatively, a passive choice mechanism or electro-optic modulators (*22*) could accelerate the protocol execution, making it more efficient.

Our work demonstrates a proof-of-principle framework for DI certification of multipartite entangled states in a fully non-IID scenario, addressing key challenges encountered in real-world

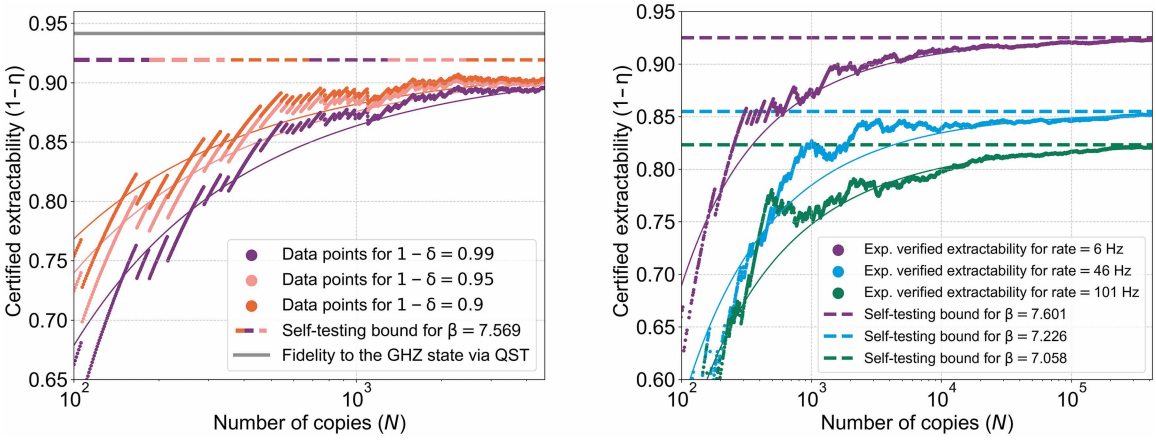

Fig. 4. Experimental certified extractability of a four-qubit GHZ state with respect to the total number of samples, *N*. Full simulation curves consider the winning probability threshold to be $p_1 = N_{\text{win}} / (N^{\max} - 1)$. The dashed horizontal lines refer to the self-testing bounds, determined by the measured inequality violations, β, representing the maximum obtainable certified extractability in the limit of $N \to \infty$. Left: Non-IID DI protocol implementation for different confidence levels, $1 - \delta$. Each classical input is associated with one single output. Dataset taken for a pump power of 240 mW, yielding an average state generation rate of 6 Hz. The full horizontal gray line refers to the fidelity estimated via quantum state tomography (QST) ($\mathcal{F} = 94.15\%$) and shows the correctness of the protocol. Right: Protocol implementation for different rates: 6 Hz (purple), 46 Hz (blue), and 101 Hz (green). Each input is associated with multiple outcomes recorded within an acquisition time of 15 s. The confidence level is fixed to $1 - \delta = 0.99$.

implementations. While the primary aim is to showcase the feasibility and robustness of the protocol, it is important to note that such implementations inherently rely on certain experimental assumptions and may involve potential loopholes (see Table 1 for an overview). These include the locality loophole and detection loophole, both of which are necessary to fulfill the theoretical requirements of device independence. The locality loophole arises when there is a possibility of communication or causal influence between measurement stations, which can undermine the no-signaling and measurement independence conditions. Addressing this loophole is typically done through strict space-like separation between players (*23*). Although this loophole is not directly addressed in our work, given that our focus is on demonstrating the feasibility of DI certification rather than testing foundational quantum principles, we consider it is reasonable to rely on proper isolation of the laboratory setup to mitigate any risks of communication, as has been proposed in previous studies (*24*). The detection loophole, on the other hand, refers to the possibility that measurement outcomes could be biased because of detection inefficiencies. Heralded sources based on alternative physical platforms (*23*) can bypass this issue. However, photonic experiments face substantial challenges, including losses and the probabilistic nature of GHZ state generation, particularly when postselection is involved. Incorporating "no-click" events as valid outcomes could theoretically address this loophole, but the low effective detection efficiency in our probabilistic source renders this approach unfeasible. Consequently, we adopt the fair sampling assumption, a common practice in photonic quantum information experiments (*15*). Despite these assumptions, our work marks a substantial advancement by addressing the challenges of non-IID scenarios, an aspect that has been largely overlooked in prior DI certification studies. Table 1 provides a comparative summary of these studies, highlighting the loopholes that they address and the methodologies used. By tackling the non-IID scenario, our framework broadens the robustness and applicability of DI protocols, paving the way for future, more stringent implementations. A detailed discussion of these experimental assumptions and the specific measures taken to address them can be found in the Supplementary Materials.

Table 1. Overview of DI implementations of quantum state certification protocols, highlighting the specific loopholes addressed in each reference. (S) and (P) refer to superconducting and photonic systems, respectively.

Ref.	Locality	Detection	IID
This work	✗	✗	✓
Wu *et al.* (*23*) (S)	✗	✓	✗
Wu *et al.* (*23*) (P)	✓	✗	✗
Xu *et al.* (*14*)	✗	✗	✗
Zang *et al.* (*15*)	✗	✓*	✗

*The authors show that the measurement devices satisfy the weak fair sampling assumption (*26*).

This work reinforces the validity of the DI certification of quantum states as a valuable fundamental resource for a wide range of quantum information applications. We emphasize the practicality of our protocol in providing a rigorous framework in which a finite number of samples can yield meaningful results, without further assuming identical and independent distribution for all produced copies. Furthermore, it is instructive to observe the impact the number of samples has on the robustness of our results. This is particularly clear when comparing the purple data points in the two plots in Fig. 4; for a similar passing probability and the same confidence level, the certified extractability increases by 3% with 10 times more samples. In other words, while the theory is able to characterize the few-copies regime, demanding confidence levels and extractability requirements can only be achieved for relatively large samples. In general, the ability to experimentally demonstrate the DI certification of such a high extractability level paves the way to the reliable and robust use of

quantum information systems in practical, real-world settings. Note. At the time of finalizing this work, we became aware of parallel and independent work on experimental quantum state certification by Antesberger *et al.* (*25*).

MATERIALS AND METHODS

Self-testing bounds

The self-testing bound plays a pivotal role in our implementation of the quantum state certification protocol as it affects not only the sample efficiency but also the lower bound for the certified extractability. For this purpose, as mentioned in Results section, we consider two options, introduced in (*13*, *19*, *20*), alongside the Mermin operator (Eq. 4). The Bell operator, derived from Baccari *et al.* (*19*), holds substantial potential for its tight self-testing bound, and it can be written as

$$\begin{aligned} B_{\text{Baccari}} &= 3\left(A_0B_0C_0D_0 + A_1B_0C_0D_0\right) \\ &+ \left(A_0B_1 - A_1B_1\right) + \left(A_0C_1 - A_1C_1\right) + \left(A_0D_1 - A_1D_1\right) \end{aligned} \tag{5}$$

The subsequent operator, originating from Wu *et al.* and Zhao *et al.* (*13*, *20*), offers comparable advantages, it was demonstrated to be even tighter than the first one, and it is defined as

$$\begin{aligned} B_{Zhao_1} &= \left(A_0 + A_1\right)B_1C_1D_1 \\ &+ \left(A_0 - A_1\right)B_0 + B_0C_0 + B_0D_0 \end{aligned} \tag{6}$$

For GHZ states, the optimal quantum bounds, for both operators mentioned above, can be achieved by taking $A_0 = \frac{X+Z}{\sqrt{2}}$, $A_1 = \frac{X-Z}{\sqrt{2}}$, and B_i, C_i, D_i defined as X (Z) for $i = 0$ ($i = 1$). Last, we take the Mermin operator, defined in Eq. 4, because of its optimal maximum success probability of $p_{\text{QM}} = 1$.

To compare the different options, we consider the robust self-testing statement to be of the form (see the Supplementary Materials for more details)

$$\Xi(\sigma, |\text{GHZ}\rangle) \geq s\beta + \mu \tag{7}$$

where $s, \mu \in \mathbb{R}$, for all states σ achieving a violation greater than β. The lower bound of each inequality, determined by the values of s and μ (see Table 2), is illustrated in Fig. 5.

The Mermin operator displays the tightest bound from a robust self-testing perspective, suggesting that it is likely the most appropriate operator for the certification protocol. However, because the lower bound on the extractability provided by the DI quantum state certification protocol also depends on the maximum probability of winning the nonlocal game with a quantum strategy, p_{QM}, we observe that the advantage of the Mermin operator becomes even more predominant than one would think by simply comparing the self-testing bounds (see Fig. 2). This indicates that the robust self-testing analysis does not contain all the necessary information for the choice of the most favorable operator for the DI certification of a quantum state. This point is further reinforced by the observed inversion in the performance assessment of the Bell inequalities from (*13*, *19*, *20*), depending on the evaluation metric. While a self-testing analysis suggests that (*19*) (green line) outperforms (*13*, *20*) (blue line) by requiring a smaller relative violation to achieve the same extractability bound, the protocol adopted in this work, when considering sample efficiency and maximum certified extractability, leads to the opposite conclusion. Moreover, although the results in Fig. 2 (left) depend on the type of noise affecting the quantum state and slight performance variations may occur for different states, this approach clearly provides valuable insights into the assessment of different Bell tests for quantum state certification.

Table 2. Numerical self-testing bound parameters for the three different operators considered for the DI quantum state certification protocol.

4-Qubit GHZ	s	μ	β_Q	β_C
$\mathbf{B}_{\text{Baccari}}$	0.4897	−3.1552	$6\sqrt{2}$	6
$\mathbf{B}_{\text{Zhao}_1}$	1	$-1-2\sqrt{2}$	$2\sqrt{2}+2$	4
$\mathbf{B}_{\text{Mermin}}$	0.1875	−0.5	8	4

Data collection and analysis

We conducted the experiment for three different pump power settings, associated with different state generation rates: 6, 46, and 101 Hz. For each of these configurations, we collected more than 4×10^5 states over a fixed acquisition window of 15 s per randomly selected classical input. To implement the non-IID DI certification protocol, we must guarantee the precise isolation of one single random event from the whole sample. For this purpose, we rely on postprocessing analysis techniques. Using a high-performance time tagger, we can record the precise time-stamps associated with each detected event. With this capability, we can replay the full experiment and decompose each of the 15-s acquisitions into multiple ultrashort measurements, such that each of them records, on average, one single output. Two different methods are taken to analyze the resulting data. First, we take each 15-s window and randomly select one out of the full set of recorded outcomes, guaranteeing a true one-to-one input-to-output correspondence in the nonlocal game (Fig. 4, left). While this

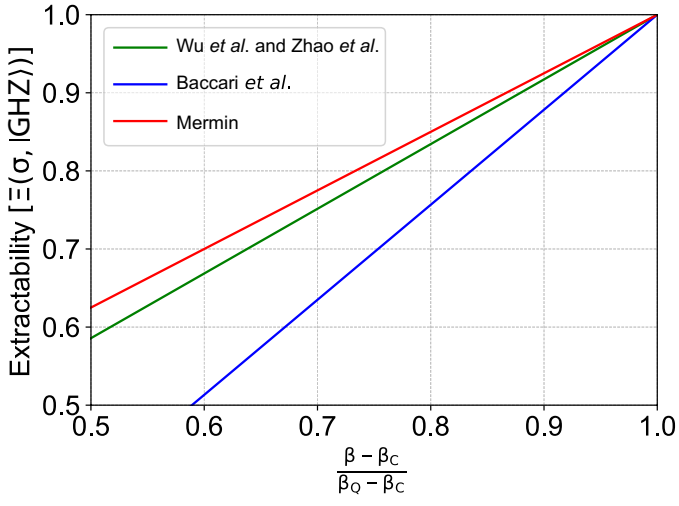

Fig. 5. Lower bound of the extractability from the target GHZ state as a function of the normalized violation $\frac{\beta-\beta_C}{\beta_Q-\beta_C}$. Green and blue lines refer to inequalities proposed in (*13*, *19*, *20*), respectively (Eqs. 5 and 6), and the red line corresponds to the Mermin inequality (Eq. 4).

approach discards a substantial portion of the recorded events and limits the number of measured samples, N, to the total number of randomly generated inputs throughout the experiment, it reflects a faithful implementation of the protocol. Alternatively, we consider the full dataset resulting from the decomposition of each classical input into as many inputs as the total number of recorded outputs within the 15-s acquisition window (Fig. 4, right). As mentioned in Results section, while this last approach does not strictly follow the protocol, it allows to use the full dataset to simulate a considerably larger sample. This approach enables us to keep the acquisition time for the entire dataset within a reasonable range, considering our limited measurement-setting update rate of 1.4 Hz. While it could be experimentally feasible to take 5×10^5 samples at this speed, we believe that our alternative method is still useful to demonstrate the convergence to the self-testing bound with a less demanding data acquisition. For both approaches, we can use a random number generator to select a single copy to be certified and, consequently, excluded from the verification analysis. It is worth noting that high-order emissions hamper the isolation of individual single events. Each time one of these is selected to be certified, we restart the random selection until we discard one and only one copy for each classical input.

Supplementary Materials

This PDF file includes:

Notes S1 to S4
Fig. S1
Table S1

REFERENCES

1. H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).
2. J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, E. Kashefi, Quantum certification and benchmarking. *Nat. Rev. Phys.* **2**, 382–390 (2020).
3. R. Raussendorf, H. J. Briegel, A one-way quantum computer. *Phys. Rev. Lett.* **86**, 5188–5191 (2001).
4. D. Gottesman, "Stabilizer codes and quantum error correction," thesis, California Institute of Technology (1997).
5. M. Christandl, S. Wehner, "Quantum anonymous transmissions," in *International Conference on the Theory and Application of Cryptology and Information Security* (Springer, 2005), pp. 217–235.
6. V. Giovannetti, S. Lloyd, L. Maccone, Advances in quantum metrology. *Nat. Photonics* **5**, 222–229 (2011).
7. S. Tani, H. Kobayashi, K. Matsumoto, Exact quantum algorithms for the leader election problem. *ACM Trans. Comput. Theory* **4**, 1–24 (2012).
8. N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, Bell nonlocality. *Rev. Modern Phys.* **86**, 419–478 (2014).
9. I. Šupić, J. Bowles, Self-testing of quantum systems: A review. *Quantum* **4**, 337 (2020).
10. A. Gočanin, I. Šupić, B. Dakić, Sample-efficient device-independent quantum state verification and certification. *PRX Quantum* **3**, 010317 (2022).
11. W.-H. Zhang, C. Zhang, Z. Chen, X.-X. Peng, X.-Y. Xu, P. Yin, S. Yu, X.-J. Ye, Y.-J. Han, J.-S. Xu, G. Chen, C.-F. Li, G.-C. Guo, Experimental optimal verification of entangled states using local measurements. *Phys. Rev. Lett.* **125**, 030506 (2020).
12. W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. G. Rarity, M. S. Tame, Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* **7**, 13251 (2016).
13. D. Wu, Q. Zhao, X.-M. Gu, H.-S. Zhong, Y. Zhou, L.-C. Peng, J. Qin, Y.-H. Luo, K. Chen, L. Li, N.-L. Liu, C.-Y. Lu, J.-W. Pan, Robust self-testing of multiparticle entanglement. *Phys. Rev. Lett.* **127**, 230503 (2021).
14. J.-M. Xu, Q. Zhou, Y.-X. Yang, Z.-M. Cheng, X.-Y. Xu, Z.-C. Ren, X.-L. Wang, H.-T. Wang, Experimental self-testing for photonic graph states. *Opt. Express* **30**, 101–111 (2022).
15. C. Zhang, W.-H. Zhang, P. Sekatski, J.-D. Bancal, M. Zwerger, P. Yin, G.-C. Li, X.-X. Peng, L. Chen, Y.-J. Han, J.-S. Xu, Y.-F. Huang, G. Chen, C.-F. Li, G.-C. Guo, Certification of genuine multipartite entanglement with general and robust device-independent witnesses. *Phys. Rev. Lett.* **129**, 190503 (2022).
16. L. dos Santos Martins, N. Laurent-Puig, P. Lefebvre, S. Neves, E. Diamanti, Realizing a compact, high-fidelity, telecom-wavelength source of multipartite entangled photons. arXiv:2407.00802 (2024).
17. H. Zhu, M. Hayashi, Efficient verification of pure quantum states in the adversarial scenario. *Phys. Rev. Lett.* **123**, 260504 (2019).
18. J. Kaniewski, Analytic and nearly optimal self-testing bounds for the clauser-horne-shimony-holt and mermin inequalities. *Phys. Rev. Lett.* **117**, 070402 (2016).
19. F. Baccari, R. Augusiak, I. Šupić, J. Tura, A. Acín, Scalable bell inequalities for qubit graph states and robust self-testing. *Phys. Rev. Lett.* **124**, 020402 (2020).
20. Q. Zhao, Y. Zhou, Constructing multipartite Bell inequalities from stabilizers. *Phys. Rev. Res.* **4**, 043215 (2022).
21. A. Cabello, O. Gühne, D. Rodríguez, Mermin inequalities for perfect correlations. *Phys. Rev. A* **77**, 062106 (2008).
22. G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger, Violation of bell's inequality under strict einstein locality conditions. *Phys. Rev. Lett.* **81**, 5039–5043 (1998).
23. D. Wu, Q. Zhao, C. Wang, L. Huang, Y.-F. Jiang, B. Bai, Y. Zhou, X.-M. Gu, F.-M. Liu, Y.-Q. Mao, Q.-C. Sun, M.-C. Chen, J. Zhang, C.-Z. Peng, X.-B. Zhu, Q. Zhang, C.-Y. Lu, J.-W. Pan, Closing the locality and detection loopholes in multiparticle entanglement self-testing. *Phys. Rev. Lett.* **128**, 250401 (2022).
24. S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, Random num bers certified by bell's theorem. *Nature* **464**, 1021–1024 (2010).
25. M. Antesberger, M. M. E. Schmid, H. Cao, B. Dakić, L. A. Rozema, P. Walther, Efficient and device independent active quantum state certification. arXiv:2407.13913 (2024).
26. D. Orsucci, J.-D. Bancal, N. Sangouard, P. Sekatski, How post-selection affects device-independent claims un der the fair sampling assumption. *Quantum* **4**, 238 (2020).

Acknowledgments: We thank H. Silvério for fruitful discussions and technical support.
Funding: We acknowledge financial support from the European Union's Horizon 2020 framework programme under the Marie Skłodowska Curie innovation training network project AppQInfo, grant no. 956071 (L.d.S.M.); the Horizon Europe research and innovation programme under the project QSNP, grant no. 101114043 (E.D.); the European Research Council Starting Grant QUSCO, grant no. 758911 (N.L.-P., E.D., and S.N.); the PEPR integrated projects QCommTestbed, ANR-22-PETQ-0011 (E.D.), and EPiQ, ANR-22-PETQ-0007 (I.Š., D.M., and U.I.M.); and the HQI project, ANR-22-PNCQ-000 (D.M. and U.I.M.), which are part of Plan France 2030.
Author contributions: L.d.S.M., S.N., and N.L.-P. designed and implemented the experimental setup. L.d.S.M. and N.L.-P. performed the measurements. Data processing was carried out by L.d.S.M. and N.L.-P., with input from I.Š. Simulations and theoretical analysis were conducted by L.d.S.M. and N.L.-P., with contributions from U.I.M. and I.Š. The manuscript was written by L.d.S.M. and N.L.-P., with contributions from I.Š., D.M., and E.D. The project was supervised by I.Š., D.M., and E.D. **Competing interests:** The authors declare that they have no competing interests.
Data, code, and materials availability: All data and code needed to evaluate and reproduce the results in the paper are present in the paper and/or the Supplementary Materials and are available online for the data: https://doi.org/10.5061/dryad.z08kprrv4 and for the code: https://doi.org/10.5281/zenodo.18769412. This study did not generate new materials.

Submitted 8 July 2025
Accepted 2 March 2026
Published 3 April 2026
10.1126/sciadv.aea4292

ScienceAdvances

Experimental sample-efficient and device-independent GHZ state certification

Laura dos Santos Martins, Nicolas Laurent-Puig, Simon Neves, Uta I. Meyer, Ivan Šupi#, Damian Markham, and Eleni Diamanti

Sci. Adv. **12** (14), eaea4292. DOI: 10.1126/sciadv.aea4292