

ARTICLE OPEN



Towards the standardization of quantum state verification using optimal strategies

Xinhe Jiang^{1,3}, Kun Wang^{2,3}, Kaiyi Qian^{1,3}, Zhaozhong Chen^{1,3}, Zhiyu Chen¹, Liangliang Lu¹, Lijun Xia¹, Fangmin Song¹, Shining Zhu¹ and Xiaosong Ma¹✉

Quantum devices for generating entangled states have been extensively studied and widely used. As so, it becomes necessary to verify that these devices truly work reliably and efficiently as they are specified. Here we experimentally realize the recently proposed two-qubit entangled state verification strategies using both local measurements (nonadaptive) and active feed-forward operations (adaptive) with a photonic platform. About 3283/536 number of copies (N) are required to achieve a 99% confidence to verify the target quantum state for nonadaptive/adaptive strategies. These optimal strategies provide the Heisenberg scaling of the infidelity ϵ as a function of N ($\epsilon \sim N^r$) with the parameter $r = -1$, exceeding the standard quantum limit with $r = -0.5$. We experimentally obtain the scaling parameters of $r = -0.88 \pm 0.03$ and -0.78 ± 0.07 for nonadaptive and adaptive strategies, respectively. Our experimental work could serve as a standardized procedure for the verification of quantum states.

npj Quantum Information (2020)6:90; <https://doi.org/10.1038/s41534-020-00317-7>

INTRODUCTION

Quantum state plays an important role in quantum information processing¹. Quantum devices for creating quantum states are building blocks for quantum technology. Being able to verify these quantum states reliably and efficiently is an essential step towards practical applications of quantum devices². Typically, a quantum device is designed to output some desired state ρ , but the imperfection in the device's construction and noise in the operations may result in the actual output state deviating from it to some random and unknown states σ_i . A standard way to distinguish these two cases is quantum-state tomography^{3–7}. However, this method is both time-consuming and computationally challenging^{8,9}. Non-tomographic approaches have also been proposed to accomplish the task^{10–17}, yet these methods make some assumptions either on the quantum states or on the available operations. It is then natural to ask whether there exists an efficient non-tomographic approach to accomplish the task?

The answer is affirmative. Quantum-state verification protocol checks the device's quality efficiently. Various studies have been explored using local measurements^{14,16,18,19}. Some earlier works considered the verification of maximally entangled states^{20–23}. In the context of hypothesis testing, optimal verification of maximally entangled state is proposed in ref. ²⁰. Under the independent and identically distributed setting, Hayashi et al.²³ discussed the hypothesis testing of the entangled pure states. In a recent work, Pallister et al.²⁴ proposed an optimal strategy to verify non-maximally entangled two-qubit pure states under locally projective and nonadaptive measurements. The locality constraint induces only a constant-factor penalty over the nonlocal strategies. Since then, numerous works have been done along this line of research^{25–31}, targeting on different states and measurements. Especially, the optimal verification strategies under local operations and classical communication are proposed recently^{27–29}, which exhibit better efficiency. We also remark

related works by Dimić and Dakić³², and Saggio et al.³³, in which they developed a generic protocol for efficient entanglement detection using local measurements and with an exponentially growing confidence vs. the number of copies of the quantum state.

In this work, we report an experimental two-qubit-state verification procedure using both optimal nonadaptive (local measurements) and adaptive (active feed-forward operations) strategies with an optical setup. Compared with previous works merely on minimizing the number of measurement settings^{34–36}, we also minimize the number of copies (i.e., coincidence counts (CCs) in our experiment) required to verify the quantum state generated by the quantum device. We perform two tasks—Task A and Task B. With Task A, we obtain a fitting infidelity and the number of copies required to achieve a 99% confidence to verify the quantum state. Task B is performed to estimate the confidence parameter δ and infidelity parameter ϵ vs. the number of copies N . We experimentally compare the scaling of $\delta \cdot N$ and $\epsilon \cdot N$ by applying the nonadaptive strategy²⁴ and adaptive strategy^{27–29} to the two-qubit states. With our methods, we obtain a comprehensive judgment about the quantum state generated by a quantum device. Present experimental and data analysis workflow may be regarded as a standard procedure for quantum-state verification.

RESULTS

Quantum-state verification

Consider a quantum device \mathcal{D} designed to produce the two-qubit pure state

$$|\Psi\rangle = \sin\theta|HH\rangle + \cos\theta|VV\rangle, \quad (1)$$

where $\theta \in [0, \pi/4]$. However, it might work incorrectly and actually outputs independent two-qubit fake states $\sigma_1, \sigma_2, \dots, \sigma_N$ in N runs. The goal of the verifier is to determine the fidelity threshold of

¹National Laboratory of Solid-state Microstructures, School of Physics, Collaborative Innovation Center of Advanced Microstructures, State Key Laboratory for Novel Software Technology, Department of Computer Science and Technology, Nanjing University, Nanjing 210093, China. ²Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China. ³These authors contributed equally: Xinhe Jiang, Kun Wang, Kaiyi Qian, Zhaozhong Chen.

✉email: xiaosong.ma@nju.edu.cn

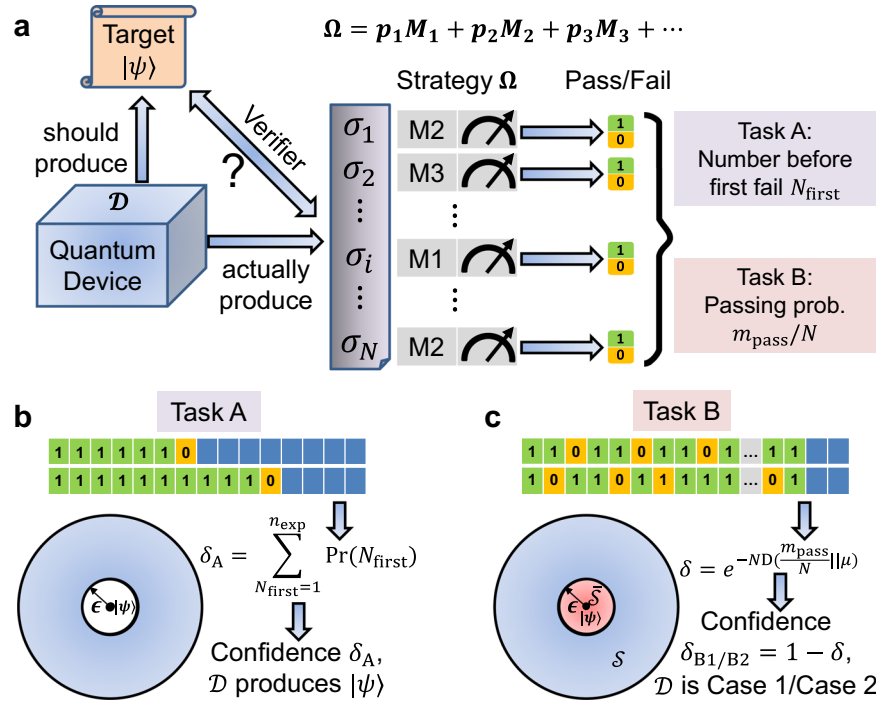


Fig. 1 Illustration of quantum-state verification strategy. **a** Consider a quantum device \mathcal{D} designed to produce the two-qubit pure state $|\psi\rangle$. However, it might work incorrectly and actually outputs two-qubit fake states $\sigma_1, \sigma_2, \dots, \sigma_N$ in N runs. For each copy σ_i , randomly projective measurements $\{M_1, M_2, M_3, \dots\}$ are performed by the verifier based on their corresponding probabilities $\{p_1, p_2, p_3, \dots\}$. Each measurement outputs a binary outcome 1 for pass and 0 for fail. The verifier takes two tasks based on these measurement outcomes. **b** Task A gives the statistics on the number of copies required before finding the first fail event. From these statistics, the verifier obtains the confidence δ_A that the device outputs state $|\psi\rangle$. **c** Task B performs a fixed number (N) of measurements and makes a statistic on the number of copies (m_{pass}/N) passing the test. From these statistics, the verifier can judge with a certain confidence δ_{B1}/δ_{B2} that the device belongs to Case 1 or Case 2.

these fake states to the target state with a certain confidence. We remark that the state for $\theta = \pi/4$ is the maximally entangled state and $\theta = 0$ is the product state. As special cases of the general state in Eq. (1), all the analysis methods presented in the following can be applied to the verification of maximally entangled state and product state. The details of the verification strategies for maximally entangled state and product state are given in Supplementary Notes 1.C and 1.D. Previously, theoretical^{20,23,37} and experimental²¹ works have studied the verification of maximally entangled state. Here we focus mainly on the verification of non-maximally entangled state in the main text, which is more advantageous in certain experiments in comparison to maximally entangled state. For instance, in the context of loophole-free Bell test, non-maximally entangled states require lower detection efficiency than maximally entangled states^{38–41}. The details and experimental results for the verification of maximally entangled state and product state are shown in the Supplementary Notes 2 and 4. To realize the verification of our quantum device, we perform the following two tasks in our experiment (see Fig. 1):

Task A: Performing measurements on the fake states copy-by-copy according to the verification strategy and making statistics on the number of copies required before we find the first fail event. The concept of Task A is shown in Fig. 1b.

Task B: Performing a fixed number (N) of measurements according to verification strategy and making statistics on the number of copies that pass the verification tests. The concept of Task B is shown in Fig. 1c.

Task A is based on the assumption that there exists some $\epsilon > 0$ for which the fidelity $\langle \Psi | \sigma_i | \Psi \rangle$ is either 1 or satisfies $\langle \Psi | \sigma_i | \Psi \rangle \leq 1 - \epsilon$ for all $i \in \{1, \dots, N\}$ (see Fig. 1b). Our task is to determine which is the case for the quantum device. To achieve Task A, we perform binary-outcome measurements from a set of available projectors

to test the state. Each binary-outcome measurement $\{M_l, 1 - M_l\}$ ($l = 1, 2, 3, \dots$) is specified by an operator M_l , corresponding to passing the test. For simplicity, we use M_l to denote the corresponding binary measurement. This measurement is performed with probability p_l . We require the target state $|\Psi\rangle$ always passes the test, i.e., $M_l |\Psi\rangle = |\Psi\rangle$. In the bad case ($\langle \Psi | \sigma_i | \Psi \rangle \leq 1 - \epsilon$), the maximal probability that σ_i can pass the test is given by^{24,25}

$$\max_{\langle \Psi | \sigma_i | \Psi \rangle \leq 1 - \epsilon} \text{Tr}(\Omega \sigma_i) = 1 - [1 - \lambda_2(\Omega)]\epsilon := 1 - \Delta_\epsilon, \quad (2)$$

where $\Omega = \sum_l p_l M_l$ is called an strategy, Δ_ϵ is the probability σ_i fails a test and $\lambda_2(\Omega)$ is the second largest eigenvalue of Ω . Whenever σ_i fails the test, we know immediately that the device works incorrectly. After N runs, σ_i in the incorrect case can pass all these tests with probability being at most $[1 - [1 - \lambda_2(\Omega)]\epsilon]^N$. Hence, to achieve confidence $1 - \delta$, it suffices to conduct N number of measurements satisfying²⁴

$$N \geq \frac{\ln \delta}{\ln[1 - [1 - \lambda_2(\Omega)]\epsilon]} \approx \frac{1}{[1 - \lambda_2(\Omega)]\epsilon} \ln \frac{1}{\delta}. \quad (3)$$

From Eq. (3), we can see that an optimal strategy is obtained by minimizing the second largest eigenvalue $\lambda_2(\Omega)$, with respect to the set of available measurements. Pallister et al.²⁴ proposed an optimal strategy for Task A, using only locally projective measurements. As no classical communication is involved, this strategy (hereafter labeled as Ω_{opt}) is nonadaptive. Later, Wang et al.²⁷, Yu et al.²⁸, and Li et al.²⁹ independently propose the optimal strategy using one-way local operations and classical communication (hereafter labeled as Ω_{opt}^+) for two-qubit pure states. Furthermore, Wang et al.²⁷ also gives the optimal strategy for two-way classical communication. The adaptive strategy allows general local operations and classical communication measurements, and is shown to be more efficient than the strategies based on local measurements. Thus, it is important to realize the

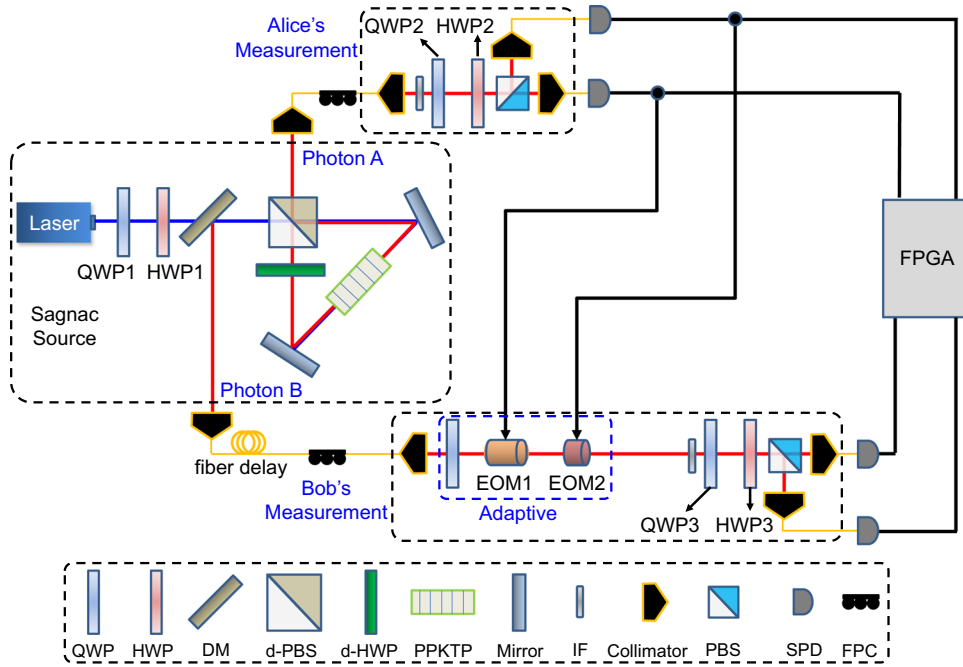


Fig. 2 Experimental setup for optimal verification of two-qubit quantum state. We use a photon pair source based on a Sagnac interferometer to generate various two-qubit quantum state. QWP1 and HWP1 are used for adjusting the relative amplitude of the two counter-propagating pump light. For nonadaptive strategy, the measurement is realized with QWP, HWP, and polarizing beam splitter (PBS) at both Alice's and Bob's site. The adaptive measurement is implemented by real-time feed-forward operation of electro-optic modulators (EOMs), which are triggered by the detection signals recorded with a field-programmable gate array (FPGA). The optical fiber delay is used to compensate the electronic delay from Alice's single photon detector (SPD) to the two EOMs. DM: dichroic mirror; dHWP: dual-wavelength half-wave plate; dPBS: dual-wavelength polarizing beam splitter; FPC: fiber polarization controller; HWP: half-wave plate; IF: 3 nm interference filter centered at 810 nm; PBS: polarizing beam splitter; PPKTP: periodically poled KTiOPO₄; QWP: quarter-wave plate.

adaptive strategy in the experiment. We refer to the Supplementary Notes 1 and 2 for more details on these strategies.

In reality, quantum devices are never perfect. Another practical scenario is to conclude with high confidence that the fidelity of the output states are above or below a certain threshold. To be specific, we want to distinguish the following two cases:

Case 1: \mathcal{D} works correctly— $\forall i, \langle \psi | \sigma_i | \psi \rangle > 1 - \epsilon$. In this case, we regard the device as “good”.

Case 2: \mathcal{D} works incorrectly— $\forall i, \langle \psi | \sigma_i | \psi \rangle \leq 1 - \epsilon$. In this case, we regard the device as “bad”.

We call this Task B (see Fig. 1c), which is different from Task A, as the condition for “ \mathcal{D} works correctly” is less restrictive compared with that of Task A. It turns out that the verification strategies proposed for Task A are readily applicable to Task B. Concretely, we perform the nonadaptive verification strategy Ω_{opt} sequentially in N runs and count the number of passing events m_{pass} . Let X_i be a binary variable corresponding to the event that σ_i passes the test ($X_i = 1$) or not ($X_i = 0$). Thus, we have $m_{\text{pass}} = \sum_{i=1}^N X_i$. Assuming that the device is “good”, then from Eq. (2) we can derive that the passing probability of the generated states is no smaller than $1 - [1 - \lambda_2(\Omega_{\text{opt}})]\epsilon$. We refer to Lemma 3 in the Supplementary Note 3. A for proof. Thus, the expectation of X_i satisfies $\mathbb{E}[X_i] \geq 1 - (1 - \lambda_2(\Omega_{\text{opt}}))\epsilon \equiv \mu$. The independence assumption together with the law of large numbers then guarantee $m_{\text{pass}} \geq N\mu$, when N is sufficiently large. We follow the statistical analysis methods using the Chernoff bound in the context of state verification^{28,32,33,42}, which is related to the security analysis of quantum key distributions^{43,44}. We then upper bound the probability that the device works incorrectly as

$$\delta \equiv e^{-ND\left(\frac{m_{\text{pass}}}{N} \parallel \mu\right)}, \quad (4)$$

where $D(x \parallel y) := x \log_2 \frac{x}{y} + (1-x) \log_2 \frac{1-x}{1-y}$ is the Kullback–Leibler divergence. That is to say, we can conclude with

confidence $\delta_{B1} = 1 - \delta$ that \mathcal{D} belongs to Case 1. Conversely, if the device is “bad”, then using the same argument we can conclude with confidence $\delta_{B2} = 1 - \delta$ that \mathcal{D} belongs to Case 2. Please refer to the Supplementary Note 3 for rigorous proofs and arguments on how to evaluate the performance of the quantum device for these two cases.

To perform Task B with the adaptive strategy $\Omega_{\text{opt}}^{\rightarrow}$, we record the number of passing events $m_{\text{pass}} = \sum_{i=1}^N X_i$. If the device is “good”, the passing probability of the generated states is no smaller than $\mu_s \equiv 1 - [1 - \lambda_4(\Omega_{\text{opt}}^{\rightarrow})]\epsilon$, where $\lambda_4(\Omega_{\text{opt}}^{\rightarrow}) = \sin^2 \theta / (1 + \cos^2 \theta)$ is the smallest eigenvalue of $\Omega_{\text{opt}}^{\rightarrow}$, as proved by Lemma 5 in Supplementary Note 3.B. The independence assumption along with the law of large numbers guarantee that $m_{\text{pass}} \geq N\mu_s$, when N is sufficiently large. On the other hand, if the device is “bad”, we can prove that the passing probability of the generated states is no larger than $\mu_l \equiv 1 - [1 - \lambda_2(\Omega_{\text{opt}}^{\rightarrow})]\epsilon$, where $\lambda_2(\Omega_{\text{opt}}^{\rightarrow}) = \cos^2 \theta / (1 + \cos^2 \theta)$, by Lemma 4 in Supplementary Note 3.B. Again, the independence assumption and the law of large numbers guarantee that $m_{\text{pass}} \leq N\mu_l$, when N is large enough. Therefore, we consider two regions regarding the value of m_{pass} in the adaptive strategy, i.e., the region $m_{\text{pass}} \leq N\mu_s$ and the region $m_{\text{pass}} \geq N\mu_l$. In these regions, we can conclude with $\delta_{B1} = 1 - \delta_l / \delta_s$ that the device belongs to Case 1/Case 2. The expressions for δ_l and δ_s and all the details for applying adaptive strategy to Task B can be found in Supplementary Note 3.B.

Experimental setup and verification procedure

Our two-qubit entangled state is generated based on a type-II spontaneous parametric down-conversion in a 20 mm-long periodically poled potassium titanyl phosphate crystal, embedded in a Sagnac interferometer^{45,46} (see Fig. 2). A continuous-wave external-cavity ultraviolet diode laser at 405 nm is used as the pump light. A half-wave plate (HWP1) and quarter-wave plate

(QWP1) transform the linear polarized light into the appropriate elliptically polarized light to provide the power balance and phase control of the pump field. With an input pump power of ~ 30 mW, we typically obtain 120 kHz CCs.

The target state has the following form

$$|\psi\rangle = \sin\theta|HV\rangle + e^{i\phi}\cos\theta|VH\rangle, \quad (5)$$

where θ and ϕ represent amplitude and phase, respectively. This state is locally equivalent to $|\Psi\rangle$ in Eq. (1) by

$$\mathbb{U} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & e^{i\phi} \\ 1 & 0 \end{pmatrix}. \text{ By using Lemma 1 in Supplementary}$$

Note 1, the optimal strategy for verifying $|\psi\rangle$ is $\Omega_{\text{opt}}' = \mathbb{U}\Omega_{\text{opt}}\mathbb{U}^\dagger$, where Ω_{opt} is the optimal strategy verifying $|\Psi\rangle$ in Eq. (1). In the Supplementary Note 2, we write down explicitly the optimal nonadaptive strategy²⁴ and adaptive strategy^{27–29} for verifying $|\psi\rangle$.

In our experiment, we implement both the nonadaptive and adaptive measurements to realize the verification strategies. There are four settings $\{P_0, P_1, P_2, P_3\}$ for nonadaptive measurements²⁴, while only three settings $\{\tilde{T}_0, \tilde{T}_1, \tilde{T}_2\}$ are required for the adaptive measurements^{27–29}. The exact form of these projectors is given in the Supplementary Note 2. It is noteworthy that the measurements $P_0 = \tilde{T}_0 = |H\rangle\langle H| \otimes |V\rangle\langle V| + |V\rangle\langle V| \otimes |H\rangle\langle H|$ are determined by the standard σ_z basis for both the nonadaptive and adaptive strategies, which are orthogonal and can be realized with a combination of QWP, HWP, and polarization beam splitter. For adaptive measurements, the measurement bases $\tilde{v}_+ = e^{i\phi}\cos\theta|H\rangle + \sin\theta|V\rangle/\tilde{w}_+ = e^{i\phi}\cos\theta|H\rangle - i\sin\theta|V\rangle$ and $\tilde{v}_- = e^{i\phi}\cos\theta|H\rangle - \sin\theta|V\rangle/\tilde{w}_- = e^{i\phi}\cos\theta|H\rangle + i\sin\theta|V\rangle$ at Bob's site are not orthogonal. It is noteworthy that we only implement the one-way adaptive strategy in our experiment. The two-way adaptive strategy is also derived in ref.²⁷. Compared to nonadaptive and one-way adaptive strategy, the two-way adaptive strategy gives improvements on the verification efficiency due to the utilization of more classical communication resources. The implementation of two-way adaptive strategy requires the following: first, Alice performs her measurement and sends her results to Bob; then, Bob performs his measurement according to Alice's outcomes; finally, Alice performs another measurement conditioning on Bob's measurement outcomes. This procedure requires the real-time communications both from Alice to Bob and from Bob to Alice. Besides, the two-way adaptive strategy requires the quantum nondemolition measurement at Alice's site, which is difficult to implement in the current setup. To realize the one-way adaptive strategy, we transmit the results of Alice's measurements to Bob through classical communication channel, which is implemented by real-time feed-forward operations of the electro-optic modulators (EOMs). As shown in Fig. 2, we trigger two EOMs at Bob's site to realize the adaptive measurements based on the results of Alice's measurement. If Alice's outcome is $|+\rangle = (|V\rangle + |H\rangle)/\sqrt{2}$ or $|R\rangle = (|V\rangle + i|H\rangle)/\sqrt{2}$, EOM1 implements the required rotation and EOM2 is identity operation. Conversely, if Alice's outcome is $|-\rangle = (|V\rangle - |H\rangle)/\sqrt{2}$ or $|L\rangle = (|V\rangle - i|H\rangle)/\sqrt{2}$, EOM2 will implement the required rotation and EOM1 is identity operation. Our verification procedure is the following.

- (1) Specifications of quantum device. We adjust the HWP1 and QWP1 of our Sagnac source to generate the desired quantum state.
- (2) Verification using the optimal strategy. In this stage, we generate many copies of the quantum state sequentially with our Sagnac source. These copies are termed as fake states $\{\sigma_i, i=1, 2, \dots, N\}$. Then, we perform the optimal nonadaptive verification strategy to σ_i . From the parameters θ and ϕ of the target state, we can compute the angles of wave plates QWP2 and HWP2, QWP3 and HWP3 for realizing

the projectors $\{P_0, P_1, P_2, P_3\}$ required in the nonadaptive strategy. To implement the adaptive strategy, we employ two EOMs to realize the \tilde{v}_+/\tilde{v}_- and \tilde{w}_+/\tilde{w}_- measurements once receiving Alice's results (refer to Supplementary Note 2.B for the details). Finally, we obtain the timetag data of the photon detection from the field-programmable gate array and extract individual CC, which is regarded as one copy of our target state. We use the timetag experimental technique to record the channel and arrival time of each detected photon for data processing⁴⁷. The time is stored as multiples of the internal time resolution (~ 156 ps). The first data in the timetag is recorded as the starting time t_{i0} . With the increasing of time, we search the required CC between different channels within a fixed coincidence window (0.4 ns). If a single CC is obtained, we record the time of the ended timetag data as t_{i0} . Then, we move to the next time slice $t_{i1} - t_{i1}$ to search for the next CC. This process can be cycled until we find the N -th CC in time slice $t_{iN-1} - t_{iN-1}$. This measurement can be viewed as single-shot measurement of the bipartite state with post selection. The time interval in each slice is about $100 \mu\text{s}$ in our experiment, consistent with the $1/\text{CR}$, CR-coincidence rate. By doing so, we can precisely obtain the number of copies N satisfying the verification requirements. We believe this procedure is suitable in the context of verification protocol, because one wants to verify the quantum state with the minimum amount of copies.

- (3) Data processing. From the measured timetag data, the results for different measurement settings can be obtained. For the nonadaptive strategy, $\{P_0, P_1, P_2, P_3\}$ are chosen randomly with the probabilities $\{\mu_0, \mu_1, \mu_2, \mu_3\}$ ($\mu_0 = \alpha(\theta)$, $\mu_i = (1 - \alpha(\theta))/3$) with $\alpha(\theta) = (2 - \sin(2\theta))/(4 + \sin(2\theta))$. For the adaptive strategy, $\{\tilde{T}_0, \tilde{T}_1, \tilde{T}_2\}$ projectors are randomly chosen according to the probabilities $\{\beta(\theta), (1 - \beta(\theta))/2, (1 - \beta(\theta))/2\}$, where $\beta(\theta) = \cos^2\theta/(1 + \cos^2\theta)$. For Task A, we use CC to decide whether the outcome of each measurement is pass or fail for each σ_i . The passing probabilities for the nonadaptive strategy can be, respectively, expressed as,

$$P_0 = \frac{CC_{HH} + CC_{VH}}{CC_{HH} + CC_{HV} + CC_{VH} + CC_{VV}}, \quad (6)$$

$$P_i = \frac{CC_{\tilde{u}_i\tilde{v}_i} + CC_{\tilde{u}_i\tilde{v}_i} + CC_{\tilde{u}_i\tilde{v}_i} + CC_{\tilde{u}_i\tilde{v}_i}}{CC_{\tilde{u}_i\tilde{v}_i} + CC_{\tilde{u}_i\tilde{v}_i} + CC_{\tilde{u}_i\tilde{v}_i} + CC_{\tilde{u}_i\tilde{v}_i}}.$$

where $i=1, 2, 3$, and $\tilde{u}_i/\tilde{u}_i^\perp$ and $\tilde{v}_i/\tilde{v}_i^\perp$ are the orthogonal bases for each photon and their expressions are given in the Supplementary Note 2.A. For P_0 , if the individual CC is in CC_{HV} or CC_{VH} , it indicates that σ_i passes the test and we set $X_i = 1$; otherwise, it fails to pass the test and we set $X_i = 0$. For $P_i, i=1, 2, 3$, if the individual CC is in $CC_{\tilde{u}_i\tilde{v}_i}$, $CC_{\tilde{u}_i\tilde{v}_i}$, or $CC_{\tilde{u}_i\tilde{v}_i}$, it indicates that σ_i passes the test and we set $X_i = 1$; otherwise, it fails to pass the test and we set $X_i = 0$. For the adaptive strategy, we set the value of the random variables X_i in a similar way.

We increase the number of copies (N) to decide the occurrence of the first failure for Task A and the frequency of passing events for Task B. From these data, we obtain the relationship of the confidence parameter δ , the infidelity parameter ϵ , and the number of copies N . There are certain probabilities that the verifier fail for each measurement. In the worst case, the probability that the verifier fails to assert σ_i is given by $1 - \Delta_\epsilon$, where $\Delta_\epsilon = 1 - \epsilon/(2 + \sin\theta \cos\theta)$ for nonadaptive strategy²⁴ and $\Delta_\epsilon = 1 - \epsilon/(2 - \sin^2\theta)$ for adaptive strategy^{27–29}.

Results and analysis of two-qubit optimal verification

The target state to be verified is the general two-qubit state in Eq. (5), where the parameter $\theta = k\pi/10$ and ϕ is optimized with maximum likelihood estimation method. In this section, we

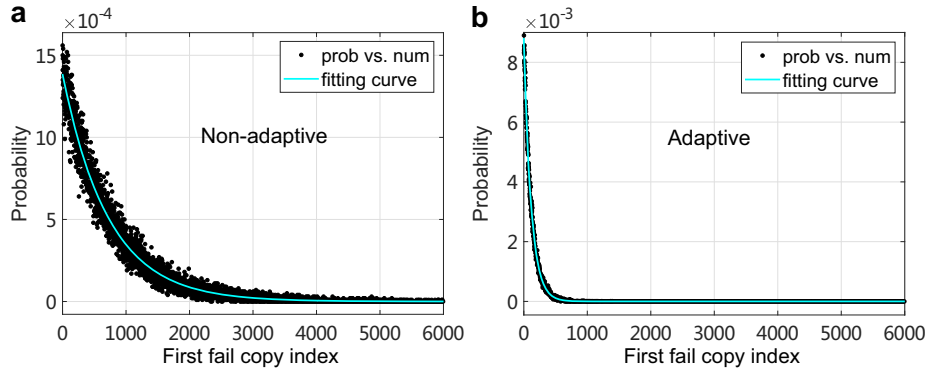


Fig. 3 The distribution of the number required before the first failure. **a** For the nonadaptive strategy. **b** For the adaptive strategy. From the statistics, we obtain the fitting infidelity of $\epsilon_{\text{exp}}^{\text{Non}} = 0.0034(15)$ and $\epsilon_{\text{exp}}^{\text{Adp}} = 0.0121(6)$. The numbers required to achieve a 99% confidence are $n_{\text{exp}}^{\text{Non}} = 3283$ and $n_{\text{exp}}^{\text{Adp}} = 536$, respectively.

present the results of $k=2$ state (termed as k2, see Supplementary Note 2) as an example. The verification results of other states, such as the maximally entangled state and the product state, are presented in Supplementary Note 4. Our theoretical non-maximally target state is specified by $\theta=0.6283$ ($k=2$). In experiment, we obtain $|\psi\rangle = 0.5987|HV\rangle + 0.8010e^{3.2034i}|VH\rangle$ ($\theta=0.6419$, $\phi=3.2034$) as our target state to be verified. To realize the verification strategy, the projective measurement is performed sequentially by randomly choosing the projectors. We take 10,000 rounds for a fixed 6000 number of copies.

Task A: According to this verification task, we make a statistical analysis on the number of measurements required for the first occurrence of failure. According to the geometric distribution, the probability that the n -th measurement (out of n measurements) is the first failure is

$$\Pr(N_{\text{first}} = n) = (1 - \Delta_e)^{n-1} \cdot \Delta_e \quad (7)$$

where $n = 1, 2, 3, \dots$. We then obtain the cumulative probability

$$\delta_A = \sum_{N_{\text{first}}=1}^{n_{\text{exp}}} \Pr(N_{\text{first}}) \quad (8)$$

which is the confidence of the device generating the target state $|\psi\rangle$. In Fig. 3a, we show the distribution of the number N_{first} required before the first failure for the nonadaptive (Non) strategy. From the figure we can see that N_{first} obeys the geometric distribution. We fit the distribution with the function in Eq. (7) and obtain an experimental infidelity $\epsilon_{\text{exp}}^{\text{Non}} = 0.0034(15)$, which is a quantitative estimation of the infidelity for the generated state. From the experimental statistics, we obtain the number $n_{\text{exp}}^{\text{Non}} = 3283$ required to achieve the 99% confidence (i.e., 99% cumulative probability for $N_{\text{first}} \leq n_{\text{exp}}^{\text{Non}}$) of judging the generated states to be the target state in the nonadaptive strategy.

The results for the adaptive (Adp) verification of Task A are shown in Fig. 3b. The experimental fitting infidelity for this distribution is $\epsilon_{\text{exp}}^{\text{Adp}} = 0.0121(6)$. The number required to achieve the same 99% confidence as the nonadaptive strategy is $n_{\text{exp}}^{\text{Adp}} = 536$. It is noteworthy that this nearly six times (i.e., $n_{\text{exp}}^{\text{Non}}/n_{\text{exp}}^{\text{Adp}} \sim 6$) difference of the experimental number required to obtain the 99% confidence is partially because the infidelity with adaptive strategy is approximately four times larger than the nonadaptive strategy. However, the number of copies required to achieve the same confidence by using the adaptive strategy is still about two times fewer than the nonadaptive strategy even if the infidelity of the generated states is the same (see the analysis presented in Supplementary Note 5). This indicates that the adaptive strategy requires a significant lower number of copies to conclude the device output state $|\psi\rangle$ with 99% confidence compared with the nonadaptive one.

Task B: We emphasize that Task B is considered under the assumption that the quantum device is either in Case 1 or in Case 2 as described above. These two cases are complementary and the confidence to assert whether the device belongs to Case 1 or Case 2 can be obtained according to different values of m_{pass} . We refer to the Supplementary Note 3 for detailed information on judging the quantum device for these two cases. For each case, we can reduce the parameter δ by increasing the number of copies of the quantum state. Thus, the confidence $\delta_B = 1 - \delta$ to judge the device belongs to Case 1/Case 2 is obtained. For the nonadaptive strategy, the passing probability m_{pass}/N can finally reach a stable value 0.9986 ± 0.0002 after about 1000 number of copies (see Supplementary Note 6). This value is smaller than the desired passing probability μ when we choose the infidelity ϵ_{min} to be 0.001. In this situation, we conclude the state belongs to Case 2. Conversely, the stable value is larger than the desired passing probability μ when we choose the infidelity ϵ_{max} to be 0.006. In this situation, we conclude the state belongs to Case 1. In Fig. 4, we present the results for the verification of Task B. First, we show the confidence parameter δ vs. the number of copies for the nonadaptive strategy in Fig. 4a, b. With about 6000 copies of quantum state, the δ parameter reaches 0.01 for Case 2. This indicates that the device belongs to Case 1 with probability at most 0.01. In other words, there are at least 99% confidence that we can say the device is in “bad” case after about 6000 measurements. In general, more copies of quantum states are required to reach a same level $\delta = 0.01$ for Case 1, because there are fewer portion for the number of passing events m_{pass} to be chosen in the range of μN to N . From Fig. 4b, we can see that it takes about 17,905 copies of quantum state, to reduce the parameter δ to be below 0.01. At this stage, we can say that the device belongs to Case 2 with probability at most 0.01. That is, there are at least 99% confidence that we can say the device is in “good” case after about 17,905 measurements.

Figure 4c, d are the results of adaptive strategy. For the adaptive strategy, the passing probability m_{pass}/N finally reaches a stable value 0.9914 ± 0.0005 (see Supplementary Note 6), which is smaller than the nonadaptive measurement due to the limited fidelity of the EOMs’ modulation. Correspondingly, the infidelity parameter for the two cases are chosen to be $\epsilon_{\text{min}} = 0.008$ and $\epsilon_{\text{max}} = 0.017$, respectively. We can see from the figure that it takes about 10,429 number of copies for δ_s to be decreased to 0.01 when choosing ϵ_{min} , which indicates that the device belongs to Case 2 with at least 99% confidence after about 10,429 measurements. On the other hand, about 23,645 number of copies are needed for δ_s to be decreased to 0.01 when choosing ϵ_{max} , which indicates that the device belongs to Case 1 with at least 99% confidence after about 23,645 measurements. It is

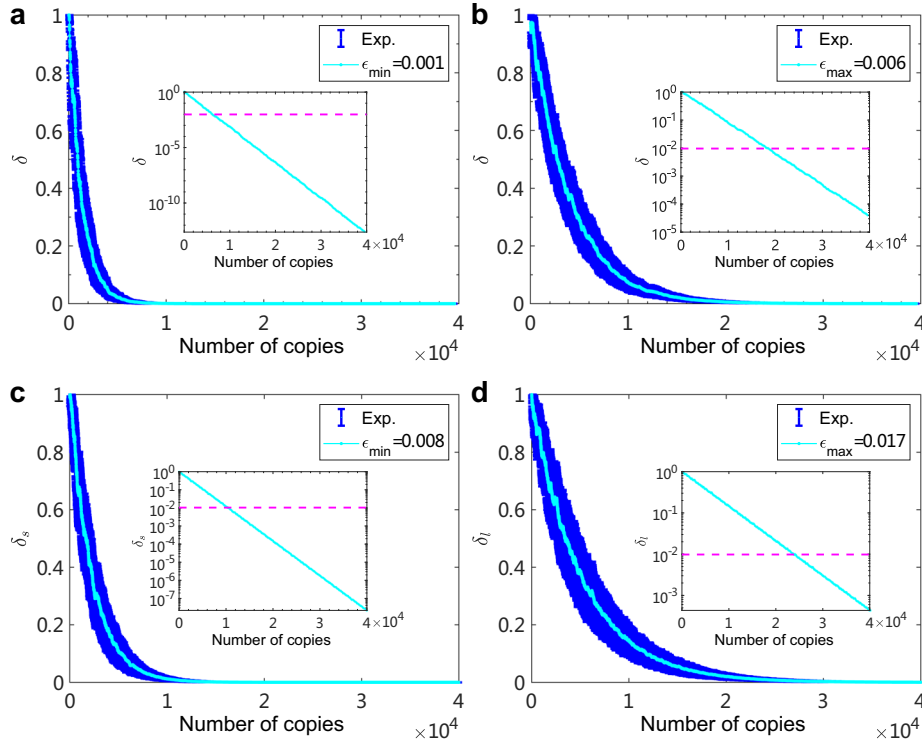


Fig. 4 Experimental results for the verification of Task B. **a, b** Nonadaptive strategy. The confidence parameter δ decreases with the increase of number of copies. After about 6000 copies, δ goes below 0.01 for Case 2 (see inset of **a**). For Case 1 (see inset of **b**), it takes about 17,905 copies to reduce δ below 0.01. **c, d** Adaptive strategy. The number of copies required to reduce δ_s and δ_i to be 0.01 for the two cases are about 10,429 and 23,645, respectively. In general, it takes less number of copies for verifying Case 2, because more space are allowed for the states to be found in the $0-\mu N$ region. The blue is the experimental error bar (Exp.), which is obtained by 100 rounds of measurements for each coincidence. The insets show the log-scale plots, which indicates δ can reach a value below 0.01 with about thousands to tens of thousands of copies.

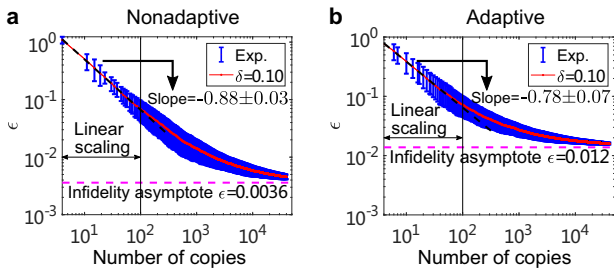


Fig. 5 The variation of infidelity parameter vs. the number of copies. **a** Nonadaptive strategy and **b** adaptive strategy. Here, the data are plotted on a log-log scale. The confidence parameter δ is chosen to be 0.10. The parameter ϵ fast decays to a low value which is asymptotically close to the infidelity 0.0036 (Nonadaptive) and 0.012 (Adaptive) of the generated quantum state when increasing the number of copies. The fitting slopes for the linear scaling region are -0.88 ± 0.03 and -0.78 ± 0.07 for the nonadaptive and adaptive, respectively. The blue symbol is the experimental data with error bar (Exp.), which is obtained by 100 rounds of measurements for each coincidence.

noteworthy that the difference of adaptive and nonadaptive comes from the different descent speed of δ vs. the number of copies N , which results from the differences in passing probabilities and the infidelity parameters. See Supplementary Note 6 for detailed explanations.

From another perspective, we can fix δ and see how the parameter ϵ changes when increasing the number of copies. Figure 5 presents the variation of ϵ vs. the number of copies in the log-log scale when we set the δ to be 0.10. At small number of copies, the infidelity is large and drops fast to a low level when the

number of copies increases to be ~ 100 . The decline becomes slow when the number of copies exceeds 100. It should be noted that the ϵ asymptotically tends to a value of 0.0036 (calculated by $1 - \Delta_\epsilon = 0.9986$) and 0.012 (calculated by $1 - \Delta_\epsilon = 0.9914$) for the nonadaptive and adaptive strategies, respectively. Therefore, we are still in the region of $m_{\text{pass}}/N \geq \mu$. We can also see that the scaling of ϵ vs. N is linear in the small number of copies region. We fit the data in the linear region with $\epsilon \sim N^r$ and obtain a slope $r \sim -0.88 \pm 0.03$ for nonadaptive strategy and $r \sim -0.78 \pm 0.07$ for adaptive strategy. This scaling exceeds the standard quantum limit $\epsilon \sim N^{-0.5}$ scaling^{42,48} for physical parameter estimation. Thus, our method is better for estimating the infidelity parameter ϵ than the classical metrology. It is noteworthy that m_{pass}/N is a good estimation for our state fidelity. If the state fidelity increases, the slope of linear region will decrease to the Heisenberg limit $\epsilon \sim N^{-1}$ in quantum metrology (see Supplementary Note 6).

Comparison with standard quantum-state tomography

The advantage of the optimal verification strategy lies in that it requires fewer number of measurement settings and, more importantly, the number of copies to estimate the quantum states generated by a quantum device. In standard quantum-state tomography⁴⁹, the minimum number of settings required for a complete reconstruction of the density matrix is 3^n , where n is the number of qubits. For two-qubit system, the standard tomography will cost nine settings whereas the present verification strategy only needs four and three measurement settings for the nonadaptive and adaptive strategies, respectively. To quantitatively compare the verification strategy with the standard tomography, we show the scaling of the parameters δ and ϵ vs. the number of copies N in Fig. 6. For each number of copies, the

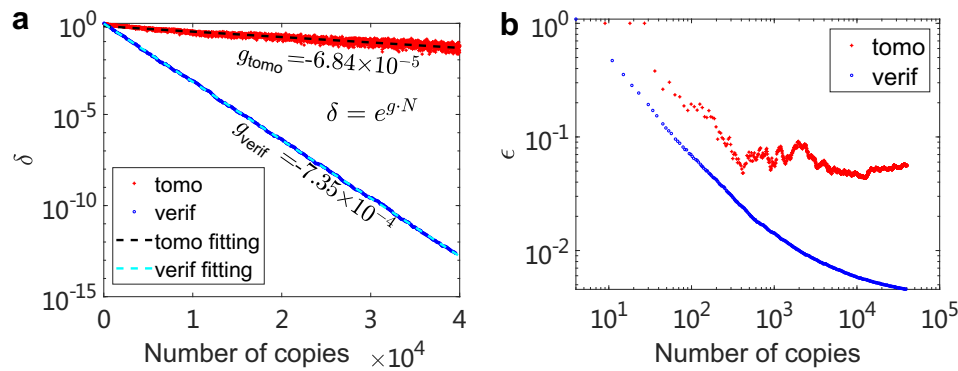


Fig. 6 Comparison of standard quantum-state tomography and present verification strategy. In the figure, we give the variation of **a** δ and **b** ϵ vs. the number of copies N by using standard quantum-state tomography (tomo) and present verification strategy (verif). For standard tomography, the fidelity $F \pm \Delta F$ is first obtained from the reconstructed density matrix of each copy N . Then confidence parameter δ is estimated by assuming normal distribution of the fidelity with mean F and SD ΔF . The infidelity parameter ϵ is estimated by $\epsilon = 1 - F$. It is noteworthy that the experimental data symbols shown in **a** looks like lines due to the dense data points.

fidelity estimation $F \pm \Delta F$ can be obtained by the standard quantum-state tomography. The δ of standard tomography is calculated by the confidence assuming normal distribution of the fidelity with mean F and SD ΔF . The ϵ of standard tomography is calculated by $\epsilon = 1 - F$. The result of verification strategy is taken from the data in Figs. 4 and 5 for the nonadaptive strategy. For δ vs. N , we fit the curve with equation $\delta = e^{g \cdot N}$, where g is the scaling of $\log(\delta)$ with N . We obtain $g_{\text{tomo}} = -6.84 \times 10^{-5}$ for the standard tomography and $g_{\text{verif}} = -7.35 \times 10^{-4}$ for the verification strategy. This indicates that present verification strategy achieves better confidence than standard quantum-state tomography given the same number of copies. For ϵ vs. N , as shown in Fig. 6b, the standard tomography will finally reach a saturation value when increasing the number of copies. With the same number of copies N , the verification strategy obtains a smaller ϵ , which indicates that the verification strategy can give a better estimation for the state fidelity than the standard quantum-state tomography when small number of quantum states are available for a quantum device.

DISCUSSION

Our work, including experiment, data processing and analysis framework, can be used as a standardized procedure for verifying quantum states. In Task A, we give an estimation of the infidelity parameter ϵ_{exp} of the generated states and the confidence δ_A to produce the target quantum state by detecting certain number of copies. With the ϵ_{exp} obtained from Task A, we can choose ϵ_{max} or ϵ_{min} which divides our device to be Case 1 or Case 2. Task B is performed based on the chosen ϵ_{min} and ϵ_{max} . We can have an estimation for the scaling of the confidence parameter δ vs. the number of copies N based on the analysis method of Task B. With a chosen δ , we can also have an estimation for the scaling of the infidelity parameter ϵ vs. N . With these steps, we can have a comprehensive judgment about how well our device really works.

In summary, we report experimental demonstrations for the optimal two-qubit pure state verification strategy with and without adaptive measurements. We give a clear discrimination and comprehensive analysis for the quantum states generated by a quantum device. Two tasks are proposed for practical applications of the verification strategy. The variation of confidence and infidelity parameter with the number of copies for the generated quantum states are presented. The obtained experimental results are in good agreement with the theoretical predictions. Furthermore, our experimental framework offers a precise estimation on the reliability and stability of quantum devices. This ability enables our framework to serve as a standard

tool for analyzing quantum devices. Our experimental framework can also be extended to other platforms.

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.

CODE AVAILABILITY

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

Received: 20 February 2020; Accepted: 26 August 2020;

Published online: 27 October 2020

REFERENCES

- Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, UK, 2010).
- Paris, M. & Rehacek, J. *Quantum State Estimation*. Vol. 649 (Springer, 2004).
- Sugiyama, T., Turner, P. S. & Murao, M. Precision-guaranteed quantum tomography. *Phys. Rev. Lett.* **111**, 160406 (2013).
- Gross, D., Liu, Y.-K., Flammia, S. T., Becker, S. & Eisert, J. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.* **105**, 150401 (2010).
- Haah, J., Harrow, A. W., Ji, Z., Wu, X. & Yu, N. Sample-optimal tomography of quantum states. In *Proc. 48th Annual ACM Symposium on Theory of Computing*, STOC 2016, 913–925 (ACM, New York, 2016).
- Donnell, R. & Wright, J. Efficient quantum tomography. In *Proc. 48th Annual ACM Symposium on Theory of Computing*, STOC 2016, 899–912 (ACM, New York, 2016).
- Donnell, R. & Wright, J. Efficient quantum tomography II. In *Proc. 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, 962–974 (ACM, New York, 2017).
- Häffner, H. et al. Scalable multiparticle entanglement of trapped ions. *Nature* **438**, 643–646 (2005).
- Carolan, J. et al. On the experimental verification of quantum complexity in linear optics. *Nat. Photonics* **8**, 621–626 (2014).
- Tóth, G. & Gühne, O. Detecting genuine multipartite entanglement with two local measurements. *Phys. Rev. Lett.* **94**, 060501 (2005).
- Flammia, S. T. & Liu, Y.-K. Direct fidelity estimation from few Pauli measurements. *Phys. Rev. Lett.* **106**, 230501 (2011).
- da Silva, M. P., Landon-Cardinal, O. & Poulin, D. Practical characterization of quantum devices without tomography. *Phys. Rev. Lett.* **107**, 210404 (2011).
- Aolita, L., Gogolin, C., Kliesch, M. & Eisert, J. Reliable quantum certification of photonic state preparations. *Nat. Commun.* **6**, 8498 (2015).
- Hayashi, M. & Morimae, T. Verifiable measurement-only blind quantum computing with stabilizer testing. *Phys. Rev. Lett.* **115**, 220502 (2015).
- McCutcheon, W. et al. Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* **7**, 13251 (2016).

16. Takeuchi, Y. & Morimae, T. Verification of many-qubit states. *Phys. Rev. X* **8**, 021060 (2018).
17. Bădescu, C., Donnell, R. & Wright, J. Quantum state certification. In *Proc. 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, 503–514 (ACM, New York, 2019).
18. Morimae, T., Takeuchi, Y. & Hayashi, M. Verification of hypergraph states. *Phys. Rev. A* **96**, 062321 (2017).
19. Takeuchi, Y., Mantri, A., Morimae, T., Mizutani, A. & Fitzsimons, J. F. Resource-efficient verification of quantum computing using Serfling's bound. *npj Quantum Inf.* **5**, 27 (2019).
20. Hayashi, M., Matsumoto, K. & Tsuda, Y. A study of LOCC-detection of a maximally entangled state using hypothesis testing. *J. Phys. A Math. Gen.* **39**, 14427–14446 (2006).
21. Hayashi, M. et al. Hypothesis testing for an entangled state produced by spontaneous parametric down-conversion. *Phys. Rev. A* **74**, 062321 (2006).
22. Hayashi, M., Tomita, A. & Matsumoto, K. Statistical analysis of testing of an entangled state based on the Poisson distribution framework. *N. J. Phys.* **10**, 043029 (2008).
23. Hayashi, M. Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing. *N. J. Phys.* **11**, 043028 (2009).
24. Pallister, S., Linden, N. & Montanaro, A. Optimal verification of entangled states with local measurements. *Phys. Rev. Lett.* **120**, 170502 (2018).
25. Zhu, H. & Hayashi, M. Efficient verification of hypergraph states. *Phys. Rev. Appl.* **12**, 054047 (2019).
26. Zhu, H. & Hayashi, M. Efficient verification of pure quantum states in the adversarial scenario. *Phys. Rev. Lett.* **123**, 260504 (2019).
27. Wang, K. & Hayashi, M. Optimal verification of two-qubit pure states. *Phys. Rev. A* **100**, 032315 (2019).
28. Yu, X.-D., Shang, J. & Gühne, O. Optimal verification of general bipartite pure states. *npj Quantum Inf.* **5**, 112 (2019).
29. Li, Z., Han, Y.-G. & Zhu, H. Efficient verification of bipartite pure states. *Phys. Rev. A* **100**, 032316 (2019).
30. Liu, Y.-C., Yu, X.-D., Shang, J., Zhu, H. & Zhang, X. Efficient verification of Dicke states. *Phys. Rev. Appl.* **12**, 044020 (2019).
31. Li, Z., Han, Y.-G. & Zhu, H. Optimal verification of Greenberger-Horne-Zeilinger states. *Phys. Rev. Applied* **13**, 054002 (2020).
32. Đimić, A. & Dakić, B. Single-copy entanglement detection. *npj Quantum Inf.* **4**, 11 (2018).
33. Saggio, V. et al. Experimental few-copy multipartite entanglement detection. *Nat. Phys.* **15**, 935–940 (2019).
34. Knips, L., Schwemmer, C., Klein, N., Wieśniak, M. & Weinfurter, H. Multipartite entanglement detection with minimal effort. *Phys. Rev. Lett.* **117**, 210504 (2016).
35. Bavaresco, J. et al. Measurements in two bases are sufficient for certifying high-dimensional entanglement. *Nat. Phys.* **14**, 1032–1037 (2018).
36. Friis, N., Vitagliano, G., Malik, M. & Huber, M. Entanglement certification from theory to experiment. *Nat. Rev. Phys.* **1**, 72–87 (2019).
37. Zhu, H. & Hayashi, M. Optimal verification and fidelity estimation of maximally entangled states. *Phys. Rev. A* **99**, 052346 (2019).
38. Eberhard, P. H. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A* **47**, R747–R750 (1993).
39. Giustina, M. et al. Bell violation using entangled photons without the fair-sampling assumption. *Nature* **497**, 227–230 (2013).
40. Giustina, M. et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
41. Shalm, L. K. et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
42. Zhang, W.-H. et al. Experimental optimal verification of entangled states using local measurements. *Phys. Rev. Lett.* **125**, 030506 (2020).
43. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
44. Hayashi, M. & Nakayama, R. Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths. *N. J. Phys.* **16**, 063009 (2014).
45. 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).
46. Fedrizzi, A., Herbst, T., Poppe, A., Jennewein, T. & Zeilinger, A. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Express* **15**, 15377–15386 (2007).
47. UQDevices. Time tag and logic user manual. Version 2.1. <https://uqdevices.com/documentation/> (2017).
48. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photonics* **5**, 222–229 (2011).
49. Altepeter, J. B., Jeffrey, E. R. & Kwiat, P. In *Advances In Atomic, Molecular, and Optical Physics*. 52, 105–159 (Academic Press, 2005).

ACKNOWLEDGEMENTS

We thank B. Dakić for the helpful discussions. This work was supported by the National Key Research and Development Program of China (numbers 2017YFA0303704 and 2019YFA0308704), the National Natural Science Foundation of China (numbers 11674170 and 11690032), NSFC-BRICS (number 61961146001), the Natural Science Foundation of Jiangsu Province (number BK20170010), the Leading-edge technology Program of Jiangsu Natural Science Foundation (number BK20192001), the program for Innovative Talents and Entrepreneur in Jiangsu, and the Fundamental Research Funds for the Central Universities.

AUTHOR CONTRIBUTIONS

X.-H.J., K.-Y.Q., Z.-Z.C., Z.-Y.C., and X.-S.M. designed and performed the experiment. K. W. performed the theoretical analysis. X.-H.J. and K.-Y.Q. analyzed the data. X.-H.J., K. W., and X.-S.M. wrote the paper with input from all authors. All authors discussed the results and read the manuscript. F.-M.S., S.-N.Z., and X.-S.M. supervised the work. X.-H. J., K.W., K.-Y.Q. and Z.-Z.C. contributed equally to this work.

COMPETING INTERESTS

A patent application related to this work is filed by Nanjing University on 29 May 2020 in China. The application number is 202010475173.4 (Patent in China). The status of the application is now under patent pending.

ADDITIONAL INFORMATION

Supplementary information is available for this paper at <https://doi.org/10.1038/s41534-020-00317-7>.

Correspondence and requests for materials should be addressed to X.M.

Reprints and permission information is available at <http://www.nature.com/reprints>

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



Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2020