npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

# Classical communication enhanced quantum state verification

Wen-Hao Zhang[1,2], Xiao Liu[1,2], Peng Yin[1,2], Xing-Xiang Peng[1,2], Gong-Chu Li[1,2], Xiao-Ye Xu[1,2], Shang Yu[1,2], Zhi-Bo Hou[1,2], Yong-Jian Han[1,2], Jin-Shi Xu[1,2], Zong-Quan Zhou[1,2], Geng Chen[1,2✉], Chuan-Feng Li[1,2✉] and Guang-Can Guo[1,2]

Quantum state verification provides an efficient approach to characterize the reliability of quantum devices for generating certain target states. The figure of merit of a specific strategy is the estimated infidelity $\epsilon$ of the tested state to the target state, given a certain number of performed measurements $n$. Entangled measurements constitute the globally optimal strategy and achieve the scaling that $\epsilon$ is inversely proportional to $n$. Recent advances show that it is possible to achieve the same scaling simply with non-adaptive local measurements; however, the performance is still worse than the globally optimal bound up to a constant factor. In this work, by introducing classical communication, we experimentally implement an adaptive quantum state verification. The constant factor is minimized from ~2.5 to 1.5 in this experiment, which means that only 60% measurements are required to achieve a certain value of $\epsilon$ compared to optimal non-adaptive local strategy. Our results indicate that classical communication significantly enhances the performance of quantum state verification, and leads to an efficiency that further approaches the globally optimal bound.

*npj Quantum Information* (2020)6:103 ; https://doi.org/10.1038/s41534-020-00328-4

## INTRODUCTION

Quantum information science aims to enhance traditional information techniques by introducing the advantage of 'quantumness'. To date, the major subfields in quantum information include quantum computation[1], quantum cryptography[2] and quantum metrology[3,4], which are respectively in pursuit of more efficient computation, more secure communication, and more precise measurement. To achieve these innovations, one needs to manufacture quantum devices and verify that these devices indeed operate as expected. Various techniques have been developed for the task to inspect the quantum states generated from these devices. Quantum state tomography (QST)[5] provides full information about an unknown state by reconstructing the density matrix and constitutes a popular point estimation method. However, the conventional tomographic reconstruction of a state is an exponentially time-consuming and computationally difficult process[6]. In order to reduce the measurement complexity to certify the quantum states, substantial efforts have been made to formalizing more efficient methods. These improved methods normally require prior information or access partial knowledge about the states. On the one hand, it has been found that with prior information about the category of the tested states, compressed sensing[7,8] and matrix product state tomography[9] can be used to simplify the measurement of quantum states. On the other hand, entanglement witnesses can justify the appearance of entanglement with far fewer measurements[10,11]; in a radical case, it is shown that local measurement on few copies is sufficient to certify the appearance of entanglement for multipartite entangled systems[12,13]. Furthermore, when the applied measurements are correlated through classical communication, quantum tomography can be implemented in a significantly more efficient way[14–16].

In quantum information processing, the quantum device is generally designed to generate a specific target state. In this case, the user only needs to confirm that the actual state is sufficiently close to the target state, in the sense that the full knowledge about the exact form of the state is excessive for this requirement. Quantum state verification (QSV) provides an efficient solution applicable to this scenario. As mentioned above, tomography aims to address the following question: What is the state? While QSV addresses a different question: Is the state identical/close to the target state? From a practical point of view, answering this question is sufficient for many quantum information applications. By performing a series of measurements on the output copies of state, QSV reaches a conclusion like 'the device outputs copies of a state that has at least $1-\epsilon$ fidelity with the target, with $1-\delta$ confidence'.

In order to verify a specific quantum state, different kinds of strategies can be constructed, and thus, it is profitable for the user to seek an optimal strategy. Rigorously, this optimization can be achieved by minimizing the number of measurements of $n$ for given values of $\epsilon$ and $\delta$. Similar to the realm of quantum metrology[17,18], an optimal QSV strategy also strives for a $1/n$ scaling of $\epsilon$, with a minimum constant factor before. For QSV, if the target state is a pure state, the best strategy is the projection onto the target state and its complementary space, then the $1/n$ scaling is reached, we call this strategy the globally optimal QSV strategy. Unfortunately, if the target is entangled state, entangled measurements are demanded while they are rare resources and difficult to obtain[19]. Recently, several works have shown that $1/n$ scaling can be achieved with a non-adaptive local (LO) strategy[20–22], the LO here means that the applied measurement operators are separable as oppose to the entangled ones used in globally optimal strategy. However, this non-adaptive LO strategy is still worse than the globally optimal strategy by a constant factor, which represents the number of additional measurements required to compete with the globally optimal strategy.

In this work, we demonstrate adaptive QSV using a photonic apparatus with active bi-directional feed-forward of classical communications between entangled photon pairs based on recent theoretical works[23–25]. The achieved efficiency not only attains the $1/n$ scaling but also further minimizes the constant

[1] CAS Key Laboratory of Quantum Information, University of Science and Technology of China, 230026 Hefei, Anhui, China. [2] CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, 230026 Hefei, Anhui, China. ✉email: chengeng@ustc.edu.cn; cfli@ustc.edu.cn

factor from before. Both bi- and uni-directional classical communications are utilized in our experiment, and the results show that these adaptive strategies significantly outperform the non-adaptive LO strategy. Furthermore, the bi-directional strategy achieves higher efficiency than the uni-directional strategy, and the number of required measurements is reduced by ~40% compared to the non-adaptive LO strategy. Our results indicate that classical communication is beneficial resources in QSV, which enhances the performance to a level comparable with the globally optimal strategy.

## RESULTS

### Theoretical framework

In a QSV task, the verifier is assigned to certify that his on-hand quantum device does produce a series of quantum states ($\sigma_1$, $\sigma_2$, $\sigma_3$, …, $\sigma_n$) satisfying the following inequality:

$$\langle\Psi|\sigma_i|\Psi\rangle > 1-\epsilon\,(i=1,2,\ldots,n). \tag{1}$$

where $|\Psi\rangle$ is the target state that the device is supposed to produce. Equation (1) assumes a different scenario from that of QST, for which all $\sigma_i$ are required to be independent and identically distributed.

Typically, with the probability as $p_l(l=1,\,2,\,\ldots,\,m)$, the verifier randomly performs a two-outcome local measurement $M_l$, which is accepted with certainty when performed on the target state. When all the measurement outcomes are accepted, the verifier can reach a statistical inference that the state from the tested device has a minimum fidelity $1-\epsilon$ to the target state, with a statistical confidence level of $1-\delta$.

For a specific strategy $\Omega = \Sigma_l p_l M_l$, the minimum number of measurements $n$ required to achieve certain values of $\epsilon$ and $\delta$ is then given by[23]

$$n_{\text{local}}^{\Omega} = \frac{\ln(\delta)}{\ln[1-[1-\lambda_2^{\downarrow}(\Omega)]\epsilon]} \overset{\epsilon\to 0}{\approx} \frac{\ln(\delta^{-1})}{[1-\lambda_2^{\downarrow}(\Omega)]\epsilon}. \tag{2}$$

This result indicates that it is possible to achieve the $1/n$ scaling of $\epsilon$ in the QSV of pure entangled states. Furthermore, the verifier can optimize the strategy by minimizing the second largest eigenvalue $\lambda_2^{\downarrow}(\Omega)$, as well as the constant factor $\frac{1}{1-\lambda_2^{\downarrow}(\Omega)}$. For LO strategies with non-adaptive local measurements, the optimal strategy to verify $|\Psi(\theta)\rangle = \cos\theta|HV\rangle - \sin\theta|VH\rangle$ is identified with a minimum $\lambda_2^{\downarrow}(\Omega)$ as[20]

$$\lambda_2^{\downarrow}(\Omega_{\text{LO}}^{\text{opt}}) = \frac{2+\sin 2\theta}{4+\sin 2\theta} \tag{3}$$

The globally optimal strategy can be realized by projecting $\sigma_i$ to the target state $|\Psi\rangle$ and its orthogonal state $|\Psi^{\perp}\rangle$, under which $\lambda_2^{\downarrow}(\Omega)=0$, and thus, the globally optimal bound is calculated as

$$n_{\text{global}}^{\text{opt}} = \frac{\ln(\delta^{-1})}{\epsilon}. \tag{4}$$

For QSV of entangled states, entangled measurements are required to implement the globally optimal strategy, which are sophisticated to perform[26–29]. Therefore, local measurements are preferred from a practical view of point. This realistic contradiction naturally yields a question that how to further minimize the gap between locally and globally optimal strategies with currently accessible techniques.

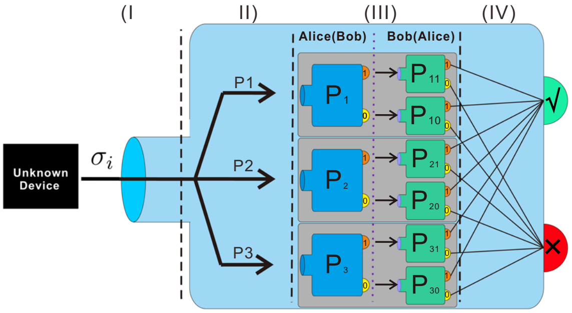

**Fig. 1 Diagram of adaptive QSV with LOCC.** The figure represents the general procedure to implement an adaptive QSV to verify whether an unknown source generates a pure target state. The generated states $\sigma_1$, $\sigma_2$, $\sigma_3$, …, $\sigma_n$ are projected firstly by Alice with a randomly selected measurement setting $\Pi_i$, with a prior probability as $P_i$. The measurement on Bob's side depends on the outcome of Alice's measurement, i.e., if the outcome of $\Pi_i$ is 0 (1), Bob performs measurement $\Pi_{i0}$ ($\Pi_{i1}$) accordingly. Bob's outcome 1 and 0 are coarse-grained as accepted (√) and rejected (×) events, respectively. Similarly, Alice can perform measurements according to Bob's outcome. A bi-directional strategy can be applied by performing these two uni-directional strategies randomly. Through a statistical analysis of the sequence of accepted and rejected events, the verifier can ascertain the largest possible distance between the actual and target states up to some finite statistical confidence.

Recently, a theoretical work generalizes the non-adaptive LO strategy to adaptive versions by introducing classical communication between the two parties sharing entanglement[23]. The elementary adaptive strategy utilizes local measurements and uni-directional classical communication (Uni-LOCC), as diagrammed in Fig. 1. The optimal Uni-LOCC QSV for $|\Psi(\theta)\rangle$ can be implemented by randomly choosing $M_1$, $M_2$ or $M_3$ (see 'Methods' for details) with prior probabilities $\{\frac{1}{2+2\sin^2\theta}, \frac{1}{2+2\sin^2\theta}, \frac{\sin^2\theta}{1+\sin^2\theta}\}$ ($\theta \in (45^{\circ}, 90^{\circ})$), and the corresponding strategy can be written as[23]

$$\Omega_{\rightarrow} = |\Psi(\theta)\rangle\langle\Psi(\theta)| + \frac{\sin^2\theta}{1+\sin^2\theta}|\Psi^{\perp}(\theta)\rangle\langle\Psi^{\perp}(\theta)| + \frac{\cos^2\theta}{1+\sin^2\theta}|VV\rangle\langle VV| + \frac{\sin^2\theta}{1+\sin^2\theta}|HH\rangle\langle HH|. \tag{5}$$

A bi-directional LOCC (Bi-LOCC) strategy can be implemented by randomly switching the role between Alice and Bob, which can be denoted as $\Omega_{\rightleftarrows} = |\Psi(\theta)\rangle\langle\Psi(\theta)| + \frac{1}{3}(I - |\Psi(\theta)\rangle\langle\Psi(\theta)|)$. Although both of these two strategies utilize one-step adaptive measurement, the Bi-LOCC strategy outperforms the Uni-LOCC when $\theta \neq 45^{\circ}$.

When verifying entangled states with local measurements, adaptive strategies $\Omega_{\rightarrow}$ and $\Omega_{\rightleftarrows}$ achieve higher efficiency compared to the non-adaptive LO strategy[23,25]. The efficiency of LO, Uni-LOCC and Bi-LOCC strategies depend on their respective constant-factors $\frac{1}{1-\lambda_2^{\downarrow}(\Omega)}$, which are $2+\sin\theta\cos\theta$, $1+\sin^2\theta$ and 3/2. Although the performance of all these strategies coincides with two-qubit maximally entangled states ($\theta = 45^{\circ}$), the adaptive strategies are still preferred in most practical scenarios, where the realistic states are always different from the maximally entangled ones and actually closer to target states with $\theta \neq 45^{\circ}$.

### Experimental implementation and results

In the above QSV proposals, a valid statement about the tested states is based on the fact that all the outcomes are accepted, while a single appearance of rejection will cease the verification without a quantified conclusion. In practice, the generated states from the quantum devices are unavoidably non-ideal with a limited fidelity to the target state; thus, there is always a certain probability to be rejected in each measurement. Even the probability of single rejection is small, it is natural to observe rejection events in an experiment involving a sequence of measurements. As a result, these original proposals are likely to mistakenly characterize qualified quantum devices as unqualified, which is inadequate for experimental implementation.

By considering the proportion of accepted outcomes, a modified strategy is thus developed here, which is robust to a

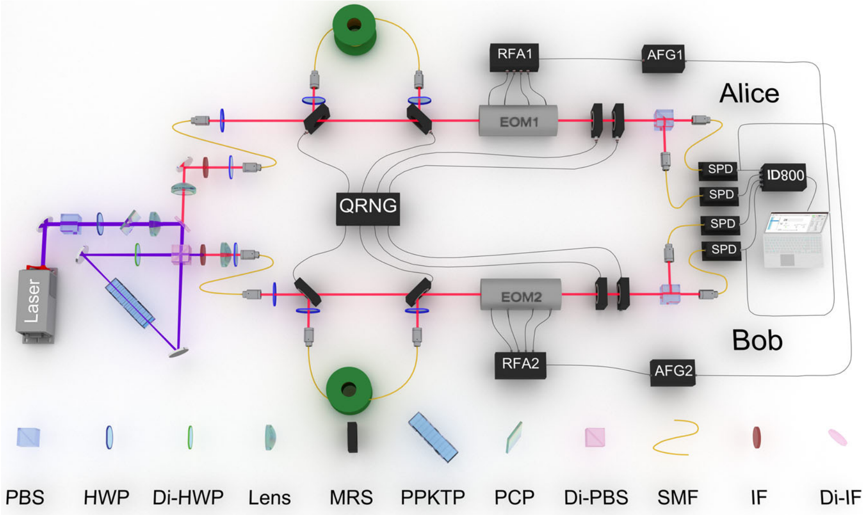

**Fig. 2 Experimental setup.** The setup includes an entanglement source, two sets of MOS and two sets of TPA. The entanglement source is mainly an SI in a triangle configuration, and the generated photon pairs are distributed to two separate parties, namely, Alice and Bob. The MOS consists of two D-Shaped Mirrors mounted in a motorized rotation stage (MRS), and a 100-m single-mode fiber (SMF) for delaying. Each TPA is composed of one electro-optical modulator (EOM) and one standard polarization analyzer, which consists of one half-wave plate (HWP) and one quarter-wave plate (QWP) mounted in MRSes, and a following polarized beam splitter (PBS) with two single-photon detectors (SPDs) at its two exits. For the Uni-LQCC protocol, the MOS on Alice's side is rotated to be open for the passing photon, which is directly measured by TPA with a randomly selected measurement setting. The other photon on Bob's side is reflected in the SMF at Bob's MOS, and then reflected into the TPA after emitting from the SMF. Adaptive processing is realized by using the outcome of Alice's measurement to control the measurement setting of Bob's TPA. Technically, Alice's photon sparks the corresponding SPD and the produced pulse triggers an arbitrary function generator (AFG) to output a recognizable signal for the EOM. After amplifying this signal to an adequate amplitude by a radio-frequency amplifier (RFA), the EOM can be driven to perform a required operation on the passing photon; thus, Bob's measurement is adaptive to the outcomes of Alice's measurement. The coincidence is recorded and analyzed by an ID800 (ID Quantique). The Bi-LQCC protocol can be implemented by randomly switching the role of Alice and Bob. The randomness of the measurement setting and communication direction is realized by controlling the TPA and MOS with the QRNG, respectively. Di dichroic, MMF multi-mode fiber, IF interference filter, SMF single-mode fiber, PCP phase compensation plate, L lens.

certain proportion of rejection events. Quantitatively, we have the corollary that if $\langle\Psi|\sigma_i|\Psi\rangle \le 1-\epsilon$ for all the measured states, the probability for each outcome to be accepted is smaller than $1-(1-\lambda_2^{\downarrow}(\Omega))*\epsilon$. As a result, in the case that the verifier observes an accepted probability $p \ge 1-(1-\lambda_2^{\downarrow}(\Omega))*\epsilon$, it should be concluded that the actual state satisfies Eq. (1) with a confidence level of $1-\delta$, where $\epsilon$ and $\delta$ are calculated from the inequality[12]

$$\delta \le e^{-D\left(\frac{m}{n}||1-(1-\lambda_2^{\downarrow}(\Omega))\epsilon\right)n}, \tag{6}$$

with

$$D(x||y) = x\log\frac{x}{y} + (1-x)\log\frac{1-x}{1-y}, \tag{7}$$

and $m$ results are accepted when $n$ measurements are performed. As a result of this modification, in the case that the final accepted probability $p \ge 1-(1-\lambda_2^{\downarrow}(\Omega))*\epsilon$, the verification can eventually reach a conclusion quantifying the distance between the actual and target states.

Benefiting from this modification, QSV can be applied to realistic non-ideal states, which allows us to experimentally verify two-qubit entangled states using the above adaptive proposals. With the setup shown in Fig. 2, we can perform adaptive QSV. The setup consists of an entangled photon-pair source (see 'Methods' for details), two mechanical optical switcher (MOS) and two high-speed triggered polarization analyzer (TPA). For adaptive QSV, Alice can guide her photon towards the MOS and perform a randomly selected projective measurement by TPA. Afterward, through a uni-directional classical communication, Alice's outcome is sent to Bob to control the measurement performed on the paring photon, which is delayed on Bob's MOS. An opposite adaptive process can also be realized by switching the role of Alice and Bob; and thus, the symmetric adaptive QSV can be executed by randomly selecting the two communication directions with equal probabilities. Technically, this random adaptive operation can be realized by controlling the MOS with a quantum random number generator (QRG), which outputs a binary signal (0 and 1) to decide which MOS transmits the photon directly while the other MOS delays the passing photon. For both Uni- and Bi-LOCC strategies, we use a QRNG to randomly decide the applied setting among $M_1$, $M_2$, $M_3$; therefore, the settings are unknown to the incident photon pairs in prior to the measurement.

In order to confirm the power of classical communication in QSV, three strategies (LO, Uni-LOCC and Bi-LOCC) are utilized to verify a partially entangled state $|\Psi(60^{\circ})\rangle$ and the results are shown in Fig. 3. In Fig. 3a, the results of 50 trials are averaged, which approximately coincide with the theoretical lines for the first few measurements and deviate from the predicted linearity afterward. This deviation mainly results from the difference between verified states and the ideal target state, which leads to rejection outcomes in QSV. In other words, only if the verified states are perfectly identical to the target state, a persistent $1/n$ scaling can be observed in a practical QSV. Since the occurrence rates of rejections are in principle equal for different strategies, a distinct gap in the estimated fidelity can be seen between the adaptive and non-adaptive strategies as predicted in the theory part. These results indicate the power of classical communication in boosting the performance of QSV. However, the practical scaling is not only determined by the optimality of the strategy, but also the quality of the actual state. In this sense, we can only access the intrinsic performance of a strategy by testing an ideal state. Although it is impossible to generate an ideal state in experiment, we can circumvent this difficulty by studying the first few measurements, of which the occurrence of rejections is fairly rare. In Fig. 3b, the first 25 measurements of single trials with all the outputs to be accepted are plotted, accompanied by the

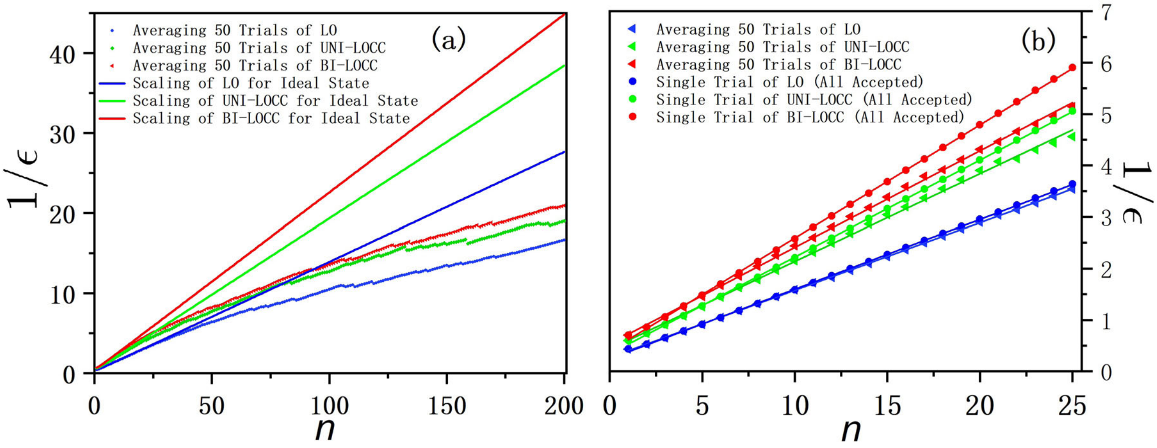

**Fig. 3 Experimental QSV of partially entangled state $|\Psi(60^\circ)\rangle$.** Three strategies (LO, Uni-LOCC and Bi-LOCC) are utilized in this experiment to verify the entangled state $|\Psi(60^\circ)\rangle$. For each strategy, a total of 50 trials of QSV are performed, and each trial contains 200 measurements. In both **a** and **b**, $\delta$ is set to 0.05, and the value of $1/\epsilon$ is plotted against the number of measurement $n$. The averaging results of the 50 trials are shown in **a** together with the theoretical lines for the ideal state. The averaging results suffer from the decoherence and noise of the realistic states and measurements, and thus deviate from the predicted linearity gradually with $n$. To learn the true performance of the applied strategies, the results of single trials in which all the first 25 measurements output acceptance are shown in **b**, together with the averaging results of 50 trials in the same range. For each case in **b**, the data points are linearly fitted and the performance can be quantitatively characterized by the slope of the fitting line. The standard deviation for the averaging data points approximately grows linearly with $n$ and is expressed as $\varepsilon = sn$, with $s$ equal to 0.039, 0.052 and 0.049 for the LO, Uni-LOCC and Bi-LOCC strategies, respectively.

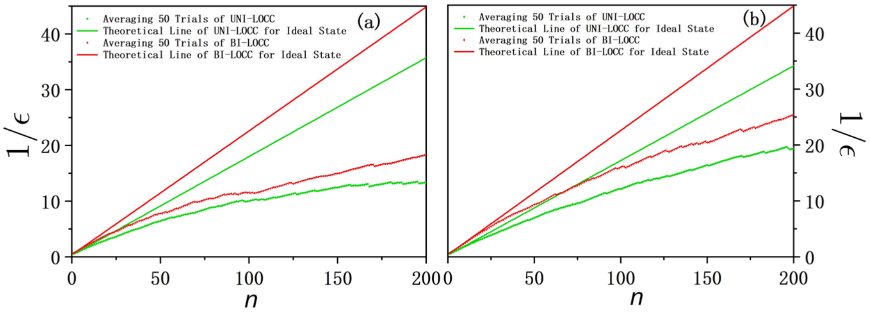

**Fig. 4 Experimental QSV of partially entangled states $|\Psi(70^\circ)\rangle$ and $|\Psi(80^\circ)\rangle$.** Two adaptive strategies, Uni-LOCC and Bi-LOCC, are utilized to study the performance gap between them. In both **a** and **b**, $\delta$ is set to 0.05, and the value of $1/\epsilon$ is plotted against the number of measurement $n$. The averaged results of 50 trials for $|\Psi(70^\circ)\rangle$ and $|\Psi(80^\circ)\rangle$ are shown together with the theoretical lines for ideal states. For both verified states, a distinct gap in the estimated fidelity can be seen between the Uni- and Bi-LOCC strategies. The standard errors for the averaging data points can be approximately expressed as $\varepsilon = sn$ with $s = 0.037$ and 0.035 for UNI- and BI-LOCC strategies in **a**, and $s = 0.045$ and 0.057 for UNI- and BI-LOCC strategies in **b**.

averaged results in Fig. 3a in the same range. The efficiency can be characterized by the slope of linear fitting lines of these data points. For LO, Uni-LOCC and Bi-LOCC strategies, the fitted slope values of the averaged points are 0.13, 0.17 and 0.187, respectively. After eliminating the effects of the state deviations by considering all-accepted single trials, the fitted slope values are 0.135, 0.188 and 0.22 for LO, Uni-LOCC and Bi-LOCC strategies, respectively, and these values are exactly the theoretical predictions for ideal states. As a result, the efficiency of the Bi-LOCC strategy is 1.63 times higher than that of LO and 1.17 times higher than that of Uni-LOCC. In other words, by introducing bi-directional classical communications, only 60% measurements of the non-adaptive LO scenario are required to verify the states to a certain level of fidelity. The performance gap between optimal local strategy and the globally optimal strategy is further minimized. Concretely, the constant factor $\frac{1}{1-\lambda_2^{\downarrow}(\Omega)}$ is reduced to approximately 1.5.

A further study of the performance gap between Uni- and Bi-LOCC strategies is made to verify another two entangled states $|\Psi(70^\circ)\rangle$ and $|\Psi(80^\circ)\rangle$, and the averaged results of 50 trials are shown in Fig. 4. Both results show that Bi-LOCC significantly outperforms Uni-LOCC, and the differences of estimated fidelities are 2.1% and 1.3% for $|\Psi(70^\circ)\rangle$ and $|\Psi(80^\circ)\rangle$, respectively. Classical communication better enhances QSV by transferring the information bi-directionally rather than an ordinary uni-directional configuration.

## DISCUSSION

One main motivation to explore the quantum resources, such as entangled states and measurements, is their potential power to surpass the classical approaches. On the other hand, the fact that the quantum resources are generally complicated to produce and control inspires another interesting question: how to use classical resources exhaustively to approach the bound set by quantum resources? In the task to verify an entangled state, the utilization of entangled measurements constitutes a globally optimal strategy that achieves the best possible efficiency. Surprisingly, one can also construct strategies merely with local measurements and achieve the same scaling. In this experiment, we show that by introducing classical communications into QSV, the performance with local measurements can be further enhanced to approach the globally optimal bound. As a result, to verify the states to a certain level of fidelity, the number of required measurements is only 60% of that for non-adaptive local strategy. Meanwhile, the gap between the locally and globally optimal bound is distinctly reduced, with the constant factor minimized to 1.5 before $1/n$ scaling. Furthermore, recently QSV has been generalized to the adversarial scenario where arbitrary correlated or entangled state preparation is allowed[30,31].

## METHODS

### Generation of entangled photon pairs

In the first part of the setup, tunable two-qubit entangled states are prepared by pumping a nonlinear crystal placed into a phase-stable Sagnac interferometer (SI). Concretely, a 405.4 nm single-mode laser is used to pump a 5-mm long bulk type-II nonlinear periodically poled potassium titanyl phosphate (PPKTP) nonlinear crystal placed into a phase-stable SI to produce polarization-entangled photon pairs at 810.8 nm. A polarized beam splitter (PBS) followed by an HWP and a PCP are used to control the polarization mode of the pump beam. These lenses before and after the SI are used to focus the pump light and collimate the entangled photons, respectively. The interferometer is composed of two highly reflective and polarization-maintaining mirrors, a Di-HWP and a Di-PBS. 'Di' here means it works for both 405.4 and 810.8 nm. The Di-HWP flips the polarization of passing photons, such that the type-II PPKTP can be pumped by the same horizontal light from both clockwise and counter-clockwise directions. Di-IF and LPF (Long pass filter) are used to remove the pump beam light. BPF (bandpass filter) and SMF are used for spectral and spatial filtering, which can significantly increase the fidelity of entangled states. The whole setup, in particular the PPKTP, is sensitive to temperature fluctuations. Placing the PPKTP on a temperature controller (±0.002 °C stability) and sealing the SI with an acrylic box would help improve temperature stability. Polarization-entangled photon pairs are generated in the state $|\Psi(\theta)\rangle = \cos\theta|HV\rangle - \sin\theta|VH\rangle$ ($H$ and $V$ denote the horizontally and vertically polarized components, respectively) and $\theta$ is controlled by the pumping polarization.

### Measurement setting for adaptive QSV

For the QSV of two-qubit pure entangled states, Alice's measurement $\Pi_i$ ($i = 1, 2, 3$) are selected to be Pauli $X$, $Y$ and $Z$ measurements. When the outcome of $X$, $Y$ and $Z$ is 1(0), Bob performs $\Pi_{11} = |\upsilon^+\rangle\langle\upsilon^+|$ $(\Pi_{10} = |\upsilon^-\rangle\langle\upsilon^-|)$, $\Pi_{21} = |\omega^+\rangle\langle\omega^+|$ $(\Pi_{20} = |\omega^-\rangle\langle\omega^-|)$ and $\Pi_{31} = |V\rangle\langle V|$ $(\Pi_{30} = |H\rangle\langle H|)$, respectively, and the vectors are defined as $|\upsilon^\pm\rangle = \sin\theta|H\rangle \mp \cos\theta|V\rangle$ and $|\omega^\pm\rangle = \sin\theta|H\rangle \pm i\cos\theta|V\rangle$. These adaptive measurement settings constitute the optimal Uni-LQCC strategy which has the form[23]

$$\begin{aligned} M_1 &= |+\rangle\langle+|\otimes|\upsilon^+\rangle\langle\upsilon^+| + |-\rangle\langle-|\otimes|\upsilon^-\rangle\langle\upsilon^-|, \\ M_2 &= |R\rangle\langle R|\otimes|\omega^-\rangle\langle\omega^-| + |L\rangle\langle L|\otimes|\omega^+\rangle\langle\omega^+|, \\ M_3 &= |V\rangle\langle V|\otimes|H\rangle\langle H| + |H\rangle\langle H|\otimes|V\rangle\langle V|, \end{aligned} \tag{8}$$

where $|+\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|-\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$ denote the eigenstates of Pauli X operator, $|R\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$ and $|L\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$ denote the eigenstates of Pauli Y operator. In each of these three combined local measurement settings, the choice of Bob's measurement setting is determined by the outcome of Alice's measurement, which can be achieved by controlling the local operation of Bob's EOM according to Alice's outcome.

## DATA AVAILABILITY

The authors declare that all data supporting the findings of this study are available within the article or from the corresponding author upon reasonable request.

Received: 20 February 2020; Accepted: 7 October 2020;
Published online: 15 December 2020

## REFERENCES

1. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring proceedings. In *Proc. 35th Annual Symposium on Foundations of Computer Science* 124–134. https://doi.org/10.1109/SFCS.1994.365700 (IEEE, New York, 1994).
2. Bennett, C. H. & Brassard, G. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India.175–179. (IEEE, New York; 1984).
3. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photonics* **5**, 222 (2011).
4. Braunstein, S. L. Quantum limits on precision measurements of phase. *Phys. Rev. Lett.* **69**, 3598 (1992).
5. James, D. F. V., Kwiat, P. G., Munro, W. J. & White, A. G. Measurement of qubits. *Phys. Rev. A* **64**, 052312 (2001).
6. Hou, Z. et al. Full reconstruction of a 14-qubit state within four hours. *N. J. Phys.* **18**, 083036 (2016).
7. Flammia, S. T., Gross, D., Liu, Y. K. & Eisert, J. Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators. *N. J. Phys.* **14**, 095022 (2012).
8. Gross, D., Liu, Y. K. & Flammia, S. T. Quantum state tomography via compressed sensing. *Phy. Rev. Lett.* **105**, 150401 (2010).
9. Cramer, M. et al. Efficient quantum state tomography. *Nat. Commun.* **1**, 149 (2010).
10. Tóth, G. & Gühne, O. Detecting genuine multipartite entanglement with two local measurements. *Phy. Rev. Lett.* **94**, 060501 (2005).
11. Tóth, G. & Gühne, O. Entanglement detection in the stabilizer formalism. *Phys. Rev. A* **72**, 022340 (2005).
12. Dimić, A. & Dakić, B. Single-copy entanglement detection. *npj Quantum Inf.* **4**, 11 (2018).
13. Saggio, V. et al. Experimental few-copy multipartite entanglement detection. *Nat. Phys.* **15**, 935–940 (2019).
14. Mahler, D. H. et al. Adaptive quantum state tomography improves accuracy quadratically. *Phy. Rev. Lett.* **111**, 183601 (2013).
15. Qi, B. et al. Adaptive quantum state tomography via linear regression estimation: Theory and two-qubit experiment. *npj Quantum Inf.* **3**, 19 (2017).
16. Chapman, R. J., Ferrie, C. & Peruzzo, A. Experimental demonstration of self-guided quantum tomography. *Phys. Rev. Lett.* **117**, 040402 (2016).
17. Chen, G. et al. Heisenberg-scaling measurement of the single-photon Kerr non-linearity using mixed states. *Nat. Commun.* **9**, 93 (2018).
18. Chen, G. et al. Achieving Heisenberg-scaling precision with projective measurement on single photons. *Phys. Rev. Lett.* **121**, 060506 (2018).
19. Gisin, N. Entanglement 25 years after quantum teleportation: testing joint measurements in quantum networks. *Entropy* **21**, 325 (2019).
20. Pallister, S., Linden, N. & Montanaro, A. Optimal verification of entangled states with local measurements. *Phys. Rev. Lett.* **120**, 170502 (2018).
21. 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).
22. Zhang, W.-H. et al. Experimental optimal verification of entangled states using local measurements. *Phys. Rev. Lett.* **125**, 030506 (2020).
23. Wang, K. & Hayashi, M. Optimal verification of two-qubit pure states. *Phys. Rev. A* **100**, 032315 (2019).
24. Li, Z., Han, Y.-G. & Zhu, H. Efficient verification of bipartite pure states. *Phys. Rev. A* **100**, 032316 (2019).
25. Yu, X.-D., Shang, J. & Gühne, O. Optimal verification of general bipartite pure states. *npj Quantum Inf.* **5**, 112 (2019).
26. Lütkenhaus, N., Calsamiglia, J. & Suominen, K. A. Bell measurements for teleportation. *Phys. Rev. A* **59**, 3295 (1999).
27. Vaidman, L. & Yoran, N. Methods for reliable teleportation. *Phys. Rev. A* **59**, 116 (1999).
28. Calsamiglia, J. & Lütkenhaus, N. Maximum efficiency of a linear-optical Bell-state analyzer. *Appl. Phys. B* **72**, 67–71 (2001).
29. Ewert, F. & van Loock, P. 3/4-efficient Bell measurement with passive linear optics and unentangled ancillae. *Phys. Rev. Lett.* **113**, 140403 (2014).
30. Zhu, H. & Hayashi, M. Efficient verification of pure quantum states in the adversarial scenario. *Phy. Rev. Lett.* **123**, 260504 (2019).
31. Zhu, H. & Hayashi, M. General framework for verifying pure quantum states in the adversarial scenario. *Phys. Rev. A* **100**, 062335 (2019).

## ACKNOWLEDGEMENTS

This work was supported by the National Key Research and Development Program of China (Nos. 2016YFA0302700 and 2017YFA0304100), National Natural Science Foundation of China (Grant Nos. 11874344, 61835004, 61327901, 11774335, 91536219 and 11821404), Key Research Program of Frontier Sciences, CAS (No. QYZDY-SSW-SLH003), Anhui Initiative in Quantum Information Technologies (AHY020100 and AHY060300), the Fundamental Research Funds for the Central Universities (Grant No. WK2030020019 and WK2470000026), Science Foundation of the CAS (No. ZDRW-XH-2019-1).

## AUTHOR CONTRIBUTIONS

W.-H.Z. made the calculations assisted by P.Y. and J.-S.X. C.-F.L. and G.C. planned and designed the experiment. W.-H.Z. carried out the experiment assisted by G.C., X.L., G.-C.L., X.-Y.X., S.Y., Z.-B.H., Y.-J.H. and Z.-Q.Z. whereas W.-H.Z. and X.-X.P. designed the computer programs. W.-H.Z. and G.C. analyzed the experimental results and wrote the manuscript. G.-C.G. and C-F.L. supervised the project. All authors discussed the experimental procedures and results.

## COMPETING INTERESTS

The authors declare no competing interests.

## ADDITIONAL INFORMATION

**Correspondence** and requests for materials should be addressed to G.C. or C.-F.L.

**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.