# ARTICLE     OPEN

# Experimental demonstration of robust self-testing for bipartite entangled states

Wen-Hao Zhang[1,2], Geng Chen[1,2], Peng Yin[1,2], Xing-Xiang Peng[1,2], Xiao-Min Hu[1,2], Zhi-Bo Hou[1,2], Zhi-Yuan Zhou[1,2], Shang Yu[1,2], Xiang-Jun Ye[1,2], Zong-Quan Zhou[1,2], Xiao-Ye Xu[1,2], Jian-Shun Tang[1,2], Jin-Shi Xu[1,2], Yong-Jian Han[1,2], Bi-Heng Liu ⬤[1,2], Chuan-Feng Li[1,2] and Guang-Can Guo[1,2]

Quantum entanglement is the key resource for quantum information processing. Device-independent certification of entangled states is a long standing open question, which arouses the concept of self-testing. The central aim of self-testing is to certify the state and measurements of quantum systems without any knowledge of their inner workings, even when the used devices cannot be trusted. Specifically, utilizing Bell's theorem, one can infer the appearance of certain entangled state when the maximum violation is observed, e.g., to self-test singlet state using CHSH inequality. In this work, by constructing a versatile entanglement source, we experimentally demonstrate a generalized self-testing proposal for various bipartite entangled states up to four dimensions. We show that the high-quality generated states can approach the maximum violations of the utilized Bell inequalities, and thus, their Schmidt coefficients can be precisely inferred by self-testing them into respective target states with near-unity fidelities. Our results indicate the superior completeness and robustness of this method and promote self-testing as a practical tool for developing quantum techniques.

npj Quantum Information (2019)5:4 ; https://doi.org/10.1038/s41534-018-0120-0

## INTRODUCTION

In contrast to theoretical schemes of quantum information processing (QIP), where the imperfections of the involved devices are generally not taken into account, practically we often do not have sufficient knowledge of the internal physical structure, or the used devices cannot be trusted. The researches on this topic open a new realm of quantum science, namely, "device-independent" science,[1–9] in which no assumptions are made about the states under observation, the experimental measurement devices, or even the dimensionality of the Hilbert spaces where such elements are defined. In this case, the only way to study the system is to perform local measurements and analyze the statistical results. It seems to be an impossible task if we still want to identify the state and measurements under consideration. However, assuming quantum mechanics to be the underlying theory and within the no-signalling constraints, a purely classical user can still infer the degree of sharing entanglement due to the violation of the Bell inequalities,[10–12] simply by querying the devices with classical inputs and observing the correlations in the classical outputs.

Such a device-independent certification of quantum systems is titled "self-testing", which was first proposed by Mayers and Yao to certify the presence of a quantum state and the structure of a set of experimental measurement operators.[13] In the past decade, although different quantum features, such as the dimension of the underlying Hilbert space,[14,15] the binary observable[16] or the overlap between measurements[17] can also be tested device-independently, most previous researches focus on the problem of certifying the quantum entangled state that is shared between the

devices.[18–22] In particular, intensive studies have been devoted to the maximally entangled "singlet" state, which is the cornerstone for QIP. Meanwhile, a large amount of progress has been made overall on the self-testing of other forms of entangled states. For example, Yang and Navascué propose a complete self-testing certification of all partially entangled pure two-qubit states.[23,24] In addition, the maximally entangled pair of qutrits,[25] the partially entangled pair of qutrits that violates maximally the CGLMP3 inequality,[26,27] a small class of higher-dimensional partially entangled pairs of qudits,[28] and multi-partite entangled states[6,29] and graph states[30] are also shown to be self-testable. Another interesting application is the possibility of self-testing a quantum computation, which consists of self-testing a quantum state and a sequence of operations applied to this state.[31]

Self-testing aims to device-independent certifications of entangled states from measured Bell correlation. A typical self-testing protocol generally contains two steps, namely, self-testing criterion and self-testing bound. A self-testing criterion underlies the entire protocol, with which one can uniquely infer the presence of a particular ensemble of entangled states, when observing the maximal violation of certain Bell inequality. These states should be different from each other by only a local unitary transformation, which does not change the Bell correlations. In a self-testing language, all the states in this ensemble have the same Schmidt coefficients and are identical up to local isometries. The state certification becomes much more complex if a non-maximal violation occurs in a black-box scenario. This non-maximal violation can result from a strongly nonlocal state with a non-optimal measurement, or a weakly nonlocal state with a (nearly) optimal state. As a result, one cannot infer the Schmidt

[1]CAS Key Laboratory of Quantum Information, University of Science and Technology of China, 230026 Hefei, China and [2]Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, 230026 Hefei, Anhui, China
Correspondence: Geng Chen (chengeng@ustc.edu.cn) or C-F. Li (cfli@ustc.edu.cn)

coefficients of the tested state from the given criterion. It is of practical significance if one can still give a commitment about the lowest possible fidelity to the target state violating the inequality maximally, namely, self-testing bound. Combining the criterion and this lower bound, self-testing can be used to test the quality of entanglement in a device-independent way.

Previous self-testing protocols for entangled states are limited to several special maximally entangled states of low-dimension. A further generalization to non-maximally entangled states[32] and multidimensional quantum entanglement[33–35] enables self-testing to be a more powerful tool in practical quantum information processes. Recently, A. Coladangelo et al.[36] have provided a general method to self-test all pure bipartite entangled states by constructing explicit correlations, which can be achieved exclusively by measurements on a unique quantum state (up to local isometries). In other words, this generalized method allows complete certifications not only for singlet state, but also for any pure bipartite entangled state of arbitrary dimensions. The criterion presented above is still a proof of ideal self-testing, which only considers ideal situations in which the correlations are exact. Practically, however, the robustness to statistical noises and experimental imperfections is essential for self-testing proposals. Despite of considerable progresses made in self-testing theory, the relevant experimental work is very rare due to the weak robustness. Recently, self-testing has been used to estimate the quality of a large-scale integrated entanglement source.[37] Nevertheless, it is necessary to verify the reliability of a certain self-testing criterion and relevant lower bound before utilizing them. In this work, under the fair sampling assumption, we implement a proof-of-concept experiment of Coladangelo's complete self-testing protocol with various entangled states up to four dimensions. We show that even in the appearance of practical imperfections, we can give a trustable description of the tested states, i.e., to quantify how far the tested state from the pure target state can be, in terms of fidelity, when the violation is not maximal.

## RESULTS

### Theoretical framework

The self-testing of arbitrary entangled two-qubit systems was resolved by Yang and Navascué.[23] In their work, they considered a scenario in which Alice and Bob share a pure two-qubit entangled state $|\varphi\rangle$, and one can record the probabilities in a [{2, 2}, {2, 2}] Bell measurement, in which both Alice and Bob have two possible measurement settings with binary outcomes.

For a general two-qubit entangled state

$$|\varphi_{\text{target}}(\theta)\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle, \tag{1}$$

it has been proved that it can maximally violate a particular family of Bell inequalities,[32] parametrized as

$$\beta(a) = aA_0 + A_0(B_0 + B_1) + A_1(B_0 - B_1), \tag{2}$$

where $0 \leq a \leq 2$ and the maximum quantum violation of it is $b(a) = \sqrt{8 + 2a^2}$.

If such Bell correlations are duplicated by Alice and Bob on an unknown state $|\varphi\rangle$, it is possible to construct an isometry satisfying that follows equations[23]

$$\Phi(|\varphi\rangle) = |\varphi_{\text{target}}(\theta)\rangle \tag{3}$$

$$\Phi([\Pi_A \otimes \Pi_B]|\varphi\rangle) = [M_A \otimes M_B]|\varphi_{\text{target}}(\theta)\rangle. \tag{4}$$

$\Pi_A$, $M_A$ and $\Pi_B$, $M_B$ here stand for projective operators on the Alice and Bob sides.

From these relations, it can be concluded that these Bell correlations can self-test $|\varphi_{\text{target}}(\theta)\rangle$. Intuitively, self-testing means proving the existence of local isometries which extract the target state $|\varphi_{\text{target}}(\theta)\rangle$ from the physical state $|\varphi\rangle$.

Hereby, Yang and Navascué gave the criterion to self-test all pure two-qubit states: When one observes a Bell correlation causing $b(a_0) - \langle\beta(a_0)\rangle = 0$, the corresponding quantum state is identical, up to local isometries, to a certain entangled state $|\varphi_{\text{target}}(\theta)\rangle$ and and $\theta$ is determined by the following equation:

$$\tan 2\theta = \sqrt{\frac{4 - (a_0)^2}{2(a_0)^2}}. \tag{5}$$

Hence, it is proved that any pure two-qubit state can be self-tested,[23] since its violation of Bell inequality Eq. (2) is unique, up to local isometry. The authors also show that it is possible to generalize this method to bipartite high-dimensional maximally entangled states. However, it is still unclear whether arbitrary pure bipartite entangled state is self-testable.

Recently, A. Coladangelo et al. successfully addressed this long-standing open question by constructing explicit correlations built on the framework outlined by Yang and Navascués.[36] The concrete process of this self-testing process is illustrated by Fig. 1. The uncharacterized devices are assigned to Alice and Bob, and they share a pure state $|\psi\rangle$ which is identical to (up to local isometries):

$$|\psi_{\text{target}}\rangle = \sum_{i=1}^{d-1} c_i|ii\rangle. \tag{6}$$
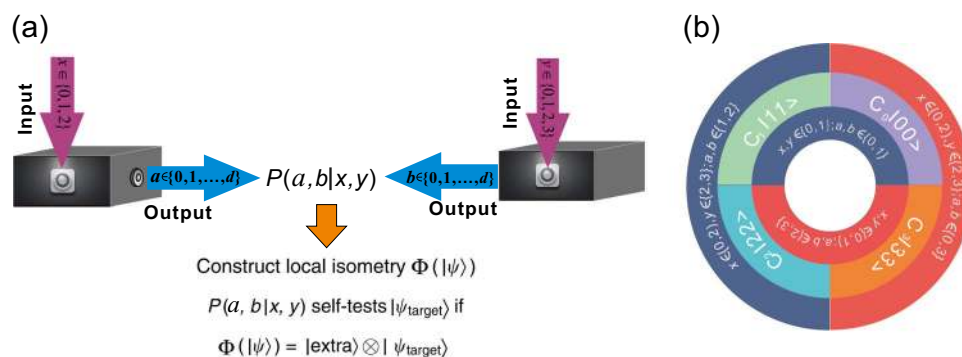


**Fig. 1** Self-testing proposals. **a** The scheme to self-test an arbitrary pure bipartite entangled state: measurement inputs and outputs from a [{3, d}, {4, d}] Bell experiment are recorded, by which one can estimate the correlations of the Bell experiment and construct a local isometry $\Phi$. We conclude that the correlations self-test $|\psi_{\text{target}}\rangle$ on the condition of $\Phi(|\psi\rangle) = |\text{auxiliary}\rangle \otimes |\psi_{\text{target}}\rangle$. **b** The specific strategy to self-test a four-dimensional state in Eq. (6). This joint state is decomposed into four $2 \times 2$ blocks, and each block can be self-tested according to the measurement strategy illustrated, while the whole state can be self-tested by combining these results
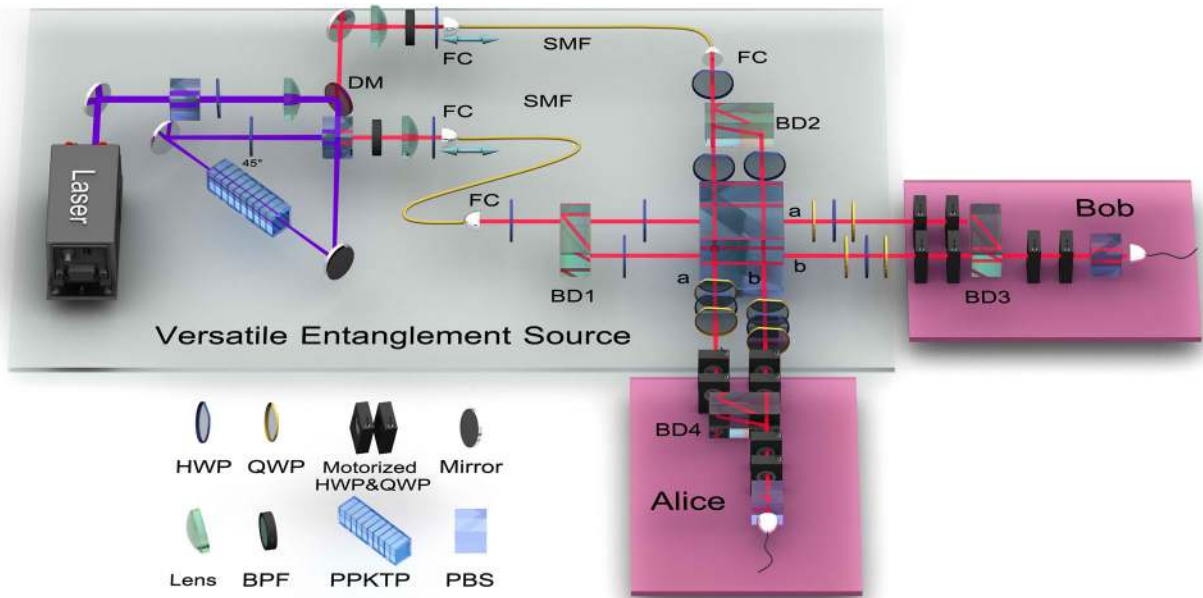
**Fig. 2** Experimental setup to self-test pure unknown bipartite systems. The setup includes an entanglement source and a measurement apparatus for self-testing. In brief, entangled photon pairs are generated by pumping a periodically poled KTP (PPKTP) crystal in a polarization Sagnac interferometer (SI), and then they are encoded into polarization and path modes to produce high-dimensional entanglement. A hybrid measurement apparatus can perform arbitrary projective measurements on polarization and path modes. BD beam displacer, HWP half wave plate, QWP quarter wave plate, DM dichroic mirror, BPF bandpass filter, PBS polarized beam splitter, SMF single mode fiber

Initially they receive the inputs $x$ and $y$ deciding their choice of measurement settings and return the outcomes $a$ and $b$, respectively. Consider a [{3, $d$}, {4, $d$}] Bell scenario, in which Alice has three possible measurement settings and Bob has four, all of which have $d$ possible outcomes. The measured statistics are recorded in the form of probabilities $P(a, b|x, y)$. Similarly to two-qubit scenario, if the [{3, $d$}, {4, $d$}] quantum correlations for bipartite entangled state of qudits are reproduced through local measurements on a joint state $|\psi\rangle$, it is possible to construct a local isometry $\Phi$ such that $\Phi(|\psi\rangle) = |\text{auxiliary}\rangle \otimes |\psi_{\text{target}}\rangle$. The central idea to self-test high-dimensional states is to decompose $|\psi\rangle$ into two series of $2 \times 2$ blocks, and thus, each block can be self-tested through the two-qubit criterion described above.[23] Referring to the four-dimensional states we test in the experiment, this decomposition can be implemented as shown in Fig. 1b. Grouping $P(a, b|x, y)$ elements of which $x, y \in 0, 1$, with $a, b \in 0, 1$ and $2, 3$, one can self-test $c_0|00\rangle + c_1|11\rangle$ and $c_2|22\rangle + c_3|33\rangle$, respectively. Similarly, using measurement settings $x \in 0, 2$ and $y \in 2, 3$, one can self-test $c_1|11\rangle + c_2|22\rangle$ and $c_0|00\rangle + c_3|33\rangle$. Such a decomposition procedure can determine the relative ratio of the two modes in each block. The weight of each block in the joint state can be further estimated by the total photon counting on this block, and eventually, the form of the tested state can be inferred.

Experimental implementation and results

In order to implement this generalized self-testing criterion, a versatile entangled photon-pair source is constructed which can generate bipartite states up to four dimensions, as shown in Fig. 2. Initially entangled photon pairs are generated by pumping a PPKTP crystal in a Sagnac interferometer (SI).[38] Afterward, both photons are encoded into polarization and path modes, and therefore, the joint two-photon can be flexibly prepared into the product, two-qubit, two-qutrit, and two-qudit entangled states (see Methods for details). Accordingly, the detecting apparatus is also properly designed in order to perform projective measurements on these two modes. Profiting from this setup, we can implement both self-testing and state tomography on the tested unknown states.

As discussed above, the two-qubit self-testing criterion is the foundation for the entire theoretical frame. First, we test various of two-qubit states through [{2, 2}, {2, 2}] Bell measurements. In the experiment, we initially generate four two-qubit entangled states $\rho_j$ ($j = 0, 1, 2, 3$), each of which is close to a pure state $|\varphi_{\text{target}}(\theta_j)\rangle$. The value of $\theta_j$ is selected to maximize the fidelity $\langle\varphi_{\text{target}}(\theta_j)|\rho_j|\varphi_{\text{target}}(\theta_j)\rangle$.

For each $\rho_j$, three randomly generated local operators are applied, leading to a ensemble three unknown states $\rho_{j(k)}$ ($k = 0, 1, 2$) that we want to self-test. For a certain $\rho_{j(k)}$, we perform Bell measurements and measure its violation $\langle\beta(a_j)\rangle$ with $a_j = 2/\sqrt{2\tan^2(2\theta_j) + 1}$ (the inverse function of Eq. (5)). As $b(a_j) - \langle\beta(a_j)\rangle$ approaches 0, a self-testing conclusion can then be reached that the tested state have the same Schmidt coefficients with $|\varphi_{\text{target}}(\theta_j)\rangle$. In principle, the three states in each ensemble all violate the inequality $\beta(a_j)$ maximally. In practical experiment, due to the imperfections in state preparing and unitary transformations, each realistic state is slightly mixed and the measured ultimate violation approaches $b(a_j)$ with a tiny difference. When these imperfections are negligibly small, we can either assume the tested state to be an ideally pure state and infer the Schmidt coefficients of it from the given self-testing criterion, or give a lowest possible fidelity $F_S$ to the target state according to the self-testing bound (blue squares in Fig. 3).

For four target states investigated here, we give the self-testing bounds through a semidefinite program (SDP) following the method of refs [22,23], and the results are shown in Fig. 3. The self-testing bound suggests a nearly unity fidelity when the observed violation approaches the maximum. The tightness of the calculated bound becomes weaker when the tested states tend to be a product state. This is expected because, as $a$ increases, the range of tolerable error gets smaller since the local bound and quantum bound coincide at $a = 2$.[22]
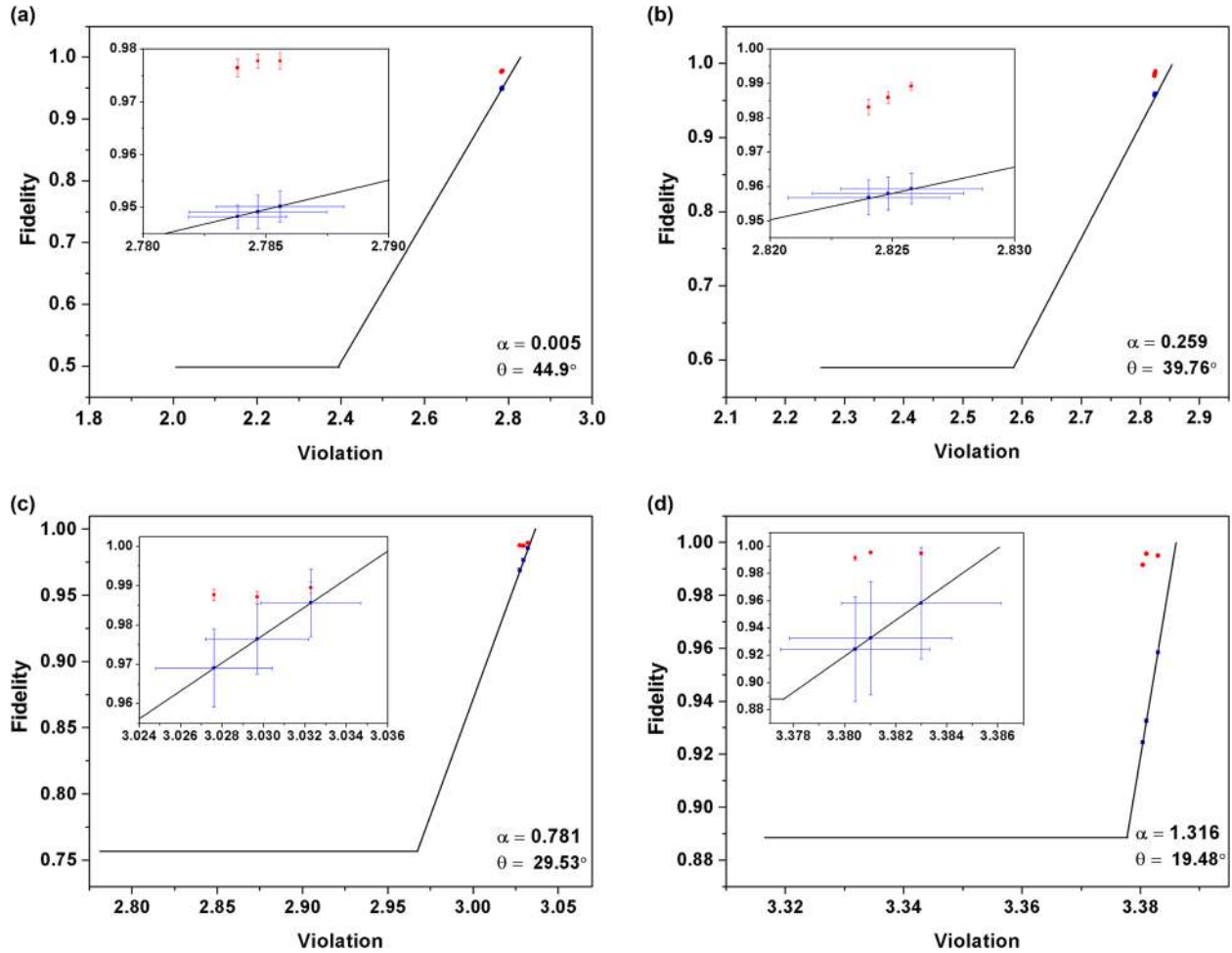
**Fig. 3** Self-testing results for four groups of two-qubit states. For each subgraph, we experimentally generate a two-qubit state $\rho_j$ ($j = 0, 1, 2, 3$), which is supposed to be a pure target state $|\varphi_{\text{target}}(\theta_j)\rangle$ which maximally violates a certain inequality $\beta(a_j)$. To each $\rho_j$, three unitary local operators are applied, resulting in a series of tested states $\rho_{j(k)}$ ($k = 0, 1, 2$), which can be self-tested by measuring the violation of $\beta(a_j)$. A self-testing bound, which describes the minimum possible fidelity to $|\varphi_{\text{target}}(\theta_j)\rangle$, is plotted as the function of the violation of $\beta(a_j)$ (the solid line). Therefore, corresponding to the measured violation for each tested state, in theory there exists a minimum possible fidelity $F_S$, as labeled by the blue square on the self-testing bound. In order to verify the reliability of this self-testing protocol, the density matrix of $\rho_{j(k)}$ is reconstructed through a state tomography process, and its actual fidelity $F_T$ to $|\varphi_{\text{target}}(\theta_j)\rangle$ (labeled by red circles) is well above $F_S$. The insets show partial enlarged details of the data points

These self-testing conclusions can be verified by measuring the the actual fidelity $F_T$ of $\rho_{j(k)}$ to its corresponding target state $|\varphi_{\text{target}}(\theta_j)\rangle$, which can be calculated as $F_T = \langle\varphi_{\text{target}}(\theta_j)|\rho_{j(k)}|\varphi_{\text{target}}(\theta_j)\rangle$. For each $\rho_{j(k)}$, the density matrix is reconstructed through a state tomography process. These actual fidelities are also labeled in Fig. 3 (red circles in Fig. 3), all of which are well above $F_S$ on self-testing bound. This result clearly suggests that the given self-testing criterion is valid for device-independent certification of two-qubit pure states, and the lower fidelity bound is also reliable for entanglement quality verification in a black-box scenario.

For high-dimensional scenarios, we decompose the joint state into several $2 \times 2$ blocks, each of which can be self-tested into a pure target state with high fidelity, similar to the procedures implemented for two-qubit scenarios. The probabilities needed to self-test these blocks are measured according to the strategy shown in Fig. 1b. When $d = 4$, in the self-testing process, Alice has 12 possible projective measurements, and Bob has 16, which results in a total of 192 values of P(a, b|x, y) (see Supplementary Note 1 for details). For each block, 16 values of P(a, b|x, y) are recorded and the parameter $a$ is ascertained to minimize $b(a) - \langle\beta(a)\rangle$, and thus, the pure target state for each block is determined.

Totally, 64 measurements are required to self-test the four decomposed blocks to be the closest pure target states. The summation of the counts in each group of 16 projective measurements can be used as the weight of the corresponding block. Therefore, the four two-qubit target states comprise the joint target state $|\psi_{\text{target}}\rangle$ with respective weights. Considering the fact that only a non-maximum violation is attained in self-testing each block, this inferred joint states should also deviate from the actual tested states. In principle, a high-dimensional self-testing bound can also be obtained from an SDP method. However, due to the appearance of significantly higher order moments in the expression of fidelity, the computing complexity is far beyond the limits of a single computer (see Supplementary Note 3 for details). Nevertheless, we can still verify the reliability of the self-testing results by measuring the density matrix of the tested state and calculating its fidelity $F_T$ to inferred target state $|\psi_{\text{target}}\rangle$. We investigate totally 10 high-dimensional bipartite entangled states (see Supplementary Note 2 for details), and the self-testing results of their pure target states are shown in Fig. 4. The tested states are all approximately identical (up to local isometries) to $|\psi_{\text{target}}\rangle$ with a high fidelity $F_T$.
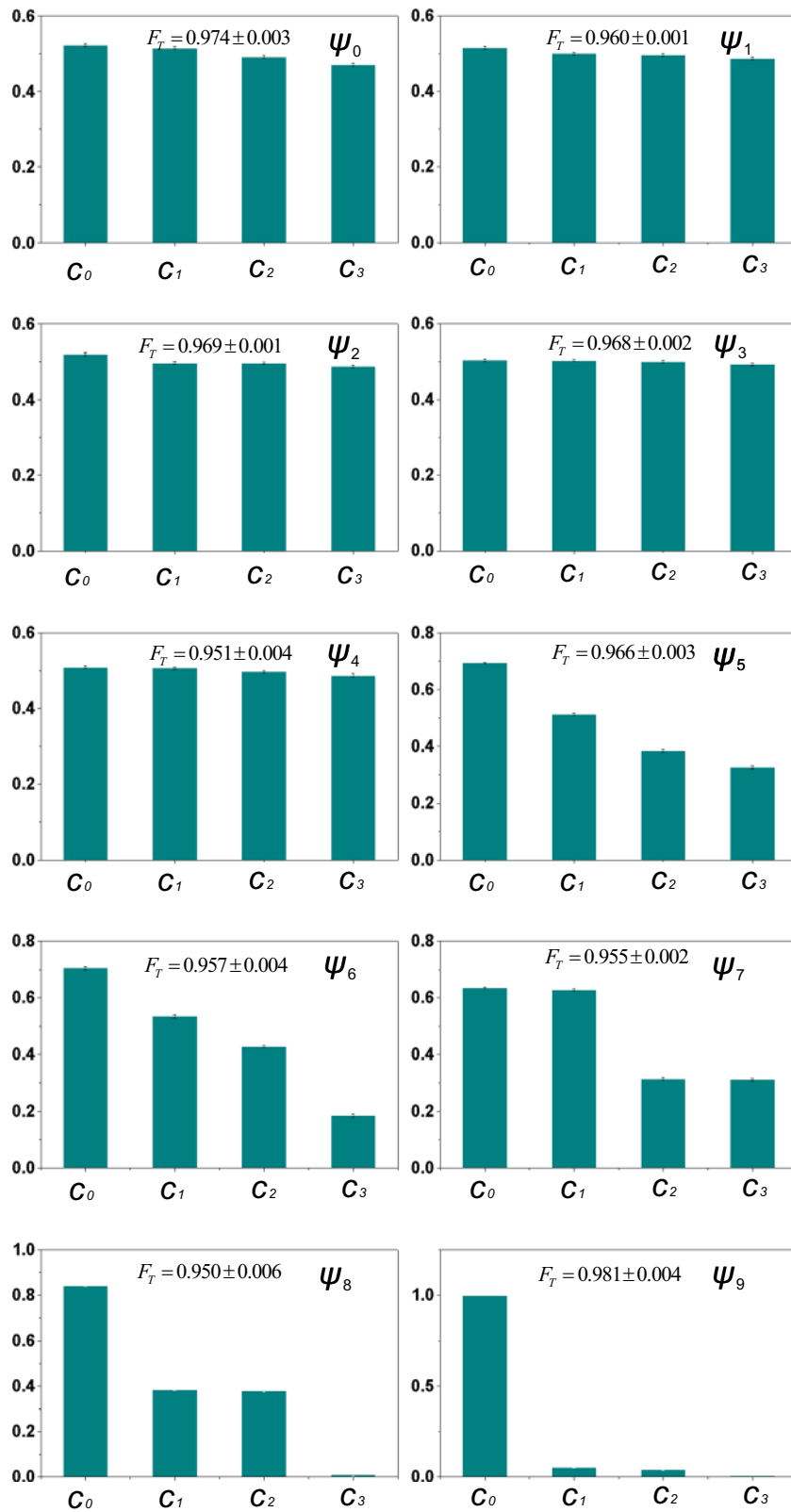
**Fig. 4** Self-testing of high-dimensional bipartite states. Through a [{3, $d$}, {4, $d$}] Bell experiment, totally 10 pure states are self-tested. Approximately, $|\psi_0\rangle$ is a maximally entangled two-qudit state, and $|\psi_{1,2,3,4}\rangle$ are transformations of it through local unitary operations. $|\psi_{5,6,7}\rangle$ are partially entangled two-qudit states, and $|\psi_8\rangle$ is a partially entangled two-qutrit states, while $|\psi_9\rangle$ is close to a product state. Each state is self-tested into a close pure target state of which the four coefficients are shown in the histogram. The actual fidelity $F_T$ of each tested state to its target state is also shown. For all the tested states, $F_T$ is above 0.95, indicating the ability to infer the Schmidt coefficients of high-dimensional entangled states through self-testing

Device-independent certifications require no-signalling constraints[39] on the devices, which can be tested through the influence of the measurement of Alice (Bob) side on Bob (Alice) side.[12] Concretely, no-signalling constraints require the following relations to be satisfied:

$$\sum_{b=0}^{d-1} P(a,b|x,y) = \sum_{b=0}^{d-1} P(a,b|x,y') \quad \text{for all} \quad a,x,y,y' \tag{7}$$

$$\sum_{a=0}^{d-1} P(a,b|x,y) = \sum_{a=0}^{d-1} P(a,b|x',y) \quad \text{for all} \quad b,y,x,x'. \tag{8}$$

In experiment, all the 192 probabilities need to be recorded to verify above equations. In Supplementary Note 4, we give the results when the tested state is $|\psi_0\rangle$.

## DISCUSSION

Normally, a self-testing criterion is feasible for an ideal case where the involved Bell inequality can be maximally violated by a pure target state. However, due to unavoidable errors in experiment, the realistic states cannot attain the maximum violation, and thus, it becomes difficult to give an exact description about the states. Fortunately, it is still possible to lower-bound the fidelity to the pure target state as the function of Bell violation. Especially, we show that when the utilized Bell inequalities are almost maximally violated, the generated states from our versatile entanglement source can be self-tested into respective target states with pretty high fidelities. We shall note that, as an initial experimental work for self-testing, our experiment constitutes to the proof of principle studies of self-testing. How to close the loopholes of Bell measurement in self-testing, such as detection, locality, and freewill loopholes, are interesting open questions for future works.

There are several ways that a purely classical user can certify the quantum state of a system, among which the standard quantum tomography is the most widely used method. However, it depends on characterization of the degrees of freedom under study and the corresponding measurements, thereby, it becomes invalid if the devices cannot be trusted. Furthermore, it requires performing and storing data from an exponentially large number of projection measurements. Recently, Chapman et al. proposed a self-guided method which exhibits better robustness and precision for quantum state certification.[40] Unsurprisingly, all of these benefits rely on the ability to fully characterize the measurement apparatus. The presence of self-testing suggests that the state certification can also be implemented in a device-independent way. Two main obstacles preventing self-testing from practical applications are the weak robustness and an extremely small quantity of self-testable states, and thus, the relevant experimental work is very rare. Thanks to the consecutive efforts by Yang, Navascué', Coladangelo, Goh and Scarani, a complete self-testing proposal has been raised for all pure bipartite quantum states utilizing a [{3, d}, {4, d}] Bell measurement. We experimentally demonstrate this proposal with our high-quality entanglement source and measurement apparatus. For all of the tested scenarios, the obtained results exhibit excellent precision and robustness. Due to this significant progress, self-testing can now be applied to realistic quantum technologies.

## METHODS

### Versatile entanglement source

The versatile entanglement source consists of two main parts. One part is responsible for the generation of polarization entangled photon pairs, and the other part is in charge of entangling the two photons in both polarization and path modes to form high-dimensional states. In the first part, a 405 nm continuous-wave diode laser with polarization set by a half-wave plate is used to pump a 4 mm-long PPKTP crystal inside an SI to generate polarization-entangled photons. The photon pairs are in the state $\cos\theta|HH\rangle + \sin\theta|VV\rangle$ ($H$ and $V$ denote the horizontal and vertical polarized components, respectively) and $\theta$ is controlled by the pumping polarization. The visibility of the maximally entangled state is larger than 0.985. These photon pairs are then sent into the second part by two single mode fibers, and the polarization is maintained by two HWPs before and after each fiber. The relative phase difference due to the birefringence in single mode fibers can be compensated when adjusting the interference between the pairs of BDs. The path mode is then created by BD1 and BD2, which causes an ~4 mm separation between the $H$ and $V$ components at 810 nm. At this stage the path mode is entangled with the polarization mode, and therefore, the joint state remains two-dimensional. After BD1 and BD2, an HWP is inserted on each path and totally four HWPs are employed for state-preparing. A centering PBS, serving as a Bell-state synthesizer,[41] leads to a coincidence registration of a single photon at each output and generates polarization entanglement on both path modes ($a$ and $b$). This is because, there is no way, even in principle, to distinguish between the two possibilities $|HH\rangle$ and $|VV\rangle$ if all the other information (such as time, frequency, and spatial mode) is erased. The arriving time of the two photons on PBS is accurately synchronized by adjusting the position of the FC collimator and the indistinguishability is tested by measuring the visibility of the Hong–Ou–Mandel interference. The main limiting factor for this visibility is the bandwidth difference from the type II SPDC process, which results in a best visibility of the polarization entanglement as ~0.975. The number of dimensions of the outcome states after the PBS can be selected by the alignments of the four state-preparing HWPs after BD1 and BD2. Concretely, when the four HWPs are set to be 0° or 45°, the outcome is a path mode entangled state $\cos\theta|aa\rangle + \sin\theta|bb\rangle$. When HWPs rotate single $H$ or $V$ polarized photons to a superposition state $\alpha|H\rangle + \beta|V\rangle$ ($\alpha, \beta \neq 0$), the result is a two-qutrit state $|\psi\rangle(d=3) = c_0|00\rangle + c_1|11\rangle + c_2|22\rangle$. When both $H$ and $V$ polarized photons are rotated to be superposition states, we can finally obtain a two-qudit state $|\psi\rangle(d=4) = c_0|00\rangle + c_1|11\rangle + c_2|22\rangle + c_3|33\rangle$. All of the coefficients $c_i$ are decided by the rotating angle of the four HWPs and the value of $\theta$. The encoding rule uses 0, 1, 2, 3 to denote $|Ha\rangle$, $|Va\rangle$, $|Hb\rangle$, $|Vb\rangle$ components, respectively. In order to attain a larger state space, local unitary operations can be applied by the waveplate sets after the crossing PBS, which lead to other entangled states of the same dimensions.

### Measurement apparatus

The measurement apparatus in this experiment is properly designed so as to perform both high-dimensional quantum tomography and self-testing. On both the Alice and Bob sides, the measurement apparatuses have an array of QWP-HWP on both the $a$ and $b$ paths, which is in charge of making projective measurements on the polarization mode. A subsequent BD (BD3 and BD4) combines the two separated paths, and a QWP-HWP set with a PBS are responsible for the measurements on the path mode. All the waveplates are mounted in the programmable motorized rotation stages. It is obvious that the two pairs of BDs compose Mach–Zehnder-like interferometers. The distance between two BDs in one pair is about 40 cm, and the optical phase is stabilized by isolating the entire setup from the environment by a sealed box. Each BD used here is selected to be most compatible with its partner thus a high interference visibility of above 0.999 can be attained. The used four BDs are selected from a total number of 12 same products. For a four-dimensional state, we perform 256 joint projective measurements for state tomography and 64 for self-testing.

## AUTHOR CONTRIBUTIONS

## ADDITIONAL INFORMATION

**Supplementary information** accompanies the paper on the *npj Quantum Information* website (https://doi.org/10.1038/s41534-018-0120-0).

**Competing interests:** The authors declare no competing interests.

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

## REFERENCES

1. Acín, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
2. Acín, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
3. Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.* **2**, 238 (2011).
4. Pironio, S. et al. Random numbers certified by Bell's theorem. *Nature* **464**, 1021 (2010).
5. Lunghi, T. et al. Self-testing quantum random number generator. *Phys. Rev. Lett.* **114**, 150501 (2015).
6. Pál, K. F., Vértesi, T. & Navascués, M. Device-independent tomography of multipartite quantum states. *Phys. Rev. A* **90**, 042340 (2014).
7. Chen, S. L., Budroni, C., Liang, Y. C. & Chen, Y. N. Natural framework for device-independent quantification of quantum steerability, measurement incompatibility, and self-testing. *Phys. Rev. Lett.* **116**, 242401 (2016).
8. Rabelo, R., Zhi, L. Y. & Scarani, V. Device-independent bounds for Hardy's experiment. *Phys. Rev. Lett.* **109**, 180401 (2012).
9. Rabelo, R., Ho, M., Cavalcanti, D., Brunner, N. & Scarani, V. Device-independent certification of entangled measurements. *Phys. Rev. Lett.* **107**, 050502 (2011).
10. Bell, J. On the einstein podolsky rosen paradox. *Physics* **1**, 195 (1964).
11. Popescu, S. & Rohrlich, D. Which states violate Bell's inequality maximally? *Phys. Lett. A* **169**, 411 (1992).
12. Brunner, N. et al. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419 (2014).
13. Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Inf. Comput.* **4**, 273 (2004).
14. Brunner, N. et al. Testing the dimension of Hilbert spaces. *Phys. Rev. Lett.* **100**, 210503 (2008).
15. Gallego, R., Brunner, N., Hadley, C. & Acín, A. Device-independent tests of classical and quantum dimensions. *Phys. Rev. Lett.* **105**, 230501 (2010).
16. Kaniewski, J. Self-testing of binary observables based on commutation. *Phys. Rev. A* **95**, 062323 (2017).
17. McKague, M., Yang, T. H. & Scarani, V. Robust self-testing of the singlet. *J. Phys. A* **45**, 455304 (2012).
18. Kaniewski, J. Analytic and nearly optimal self-testing bounds for the Clauser–Horne–Shimony–Holt and Mermin Inequalities. *Phys. Rev. Lett.* **117**, 070402 (2016).
19. Moroder, T., Bancal, J. D., Liang, Y. C., Hofmann, M. & Gühne, O. Device-independent entanglement quantification and related applications. *Phys. Rev. Lett.* **111**, 030501 (2013).
20. Bardyn, C. E. et al. Device-independent state estimation based on Bells inequalities. *Phys. Rev. A* **80**, 062327 (2009).
21. Navascués, M., Pironio, S. & Acín, A. Bounding the set of quantum correlations. *Phys. Rev. Lett.* **98**, 010401 (2007).
22. Bancal, J. D., Navascués, M., Scarani, V., Vértesi, T. & Yang, T. H. Physical characterization of quantum devices from nonlocal correlations. *Phys. Rev. A* **91**, 022115 (2015).
23. Yang, T. H. & Vértesi, T. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A* **87**, 050102 (2013).
24. Bamps, C. & Pironio, S. Sum-of-squares decompositions for a family of Clauser–Horne–Shimony–Holt-like inequalities and their application to self-testing. *Phys. Rev. A* **91**, 052111 (2015).
25. Salavrakos, A. et al. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.* **119**, 040402 (2017).
26. Yang, T. H., Vértesi, T., Bancal, J.-D., Scarani, V. & Navascués, M. Robust and versatile black-box certification of quantum devices. *Phys. Rev. Lett.* **113**, 040401 (2014).
27. Acín, A., Durt, T., Gisin, N. & Latorre, J. I. Quantum nonlocality in two three-level systems. *Phys. Rev. A* **65**, 052325 (2002).
28. Coladangelo, A. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. *Quantum Inf. Comput.* **17**, 831–865 (2017).
29. Liang, Y. C. et al. Family of Bell-like Inequalities as device-independent witnesses for entanglement depth. *Phys. Rev. Lett.* **114**, 190401 (2015).
30. McKague, M. Self-testing graph states. In: Bacon, D., Martin-Delgado, M. & Roetteler, M. (eds.), *Conference on Quantum Computation, Communication, and Cryptography* (Springer, Berlin, Heidelberg, 2011).
31. Magniez, F., Mayers, D., Mosca, M. & Ollivier, H. Self-testing of quantum circuits. In: Bugliesi, M., Preneel, B., Sassone, V. & Wegener, I. (eds.), *International Colloquium on Automata, Languages, and Programming*. 72–83 (Springer, Berlin, Heidelberg, 2006).
32. Acín, A., Massar, S. & Pironio, S. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.* **108**, 100402 (2012).
33. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys. Rev. Lett.* **70**, 1895 (1993).
34. Bennett, C. H. & Wiesner, S. J. Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. *Phys. Rev. Lett.* **69**, 2881–C2884 (1992).
35. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–C663 (1991).
36. Coladangelo, A. et al. All pure bipartite entangled states can be self-tested. *Nat. Commun.* **8**, 15485 (2017).
37. Wang, J. W. et al. Multidimensional quantum entanglement with large-scale integrated optics. *Science* **360**, 285–291 (2018).
38. Fedrizzi, A., Herbst, T., Poppe, A., Jennewein, T. & Zeilinger, A. A wavelength-tunable fibercoupled source of narrowband entangled photons. *Opt. Exp.* **15**, 15377–15386 (2007).
39. Popescu, S. & Rohrlich, D. Quantum nonlocality as an axiom. *Found. Phys.* **24**, 379 (1994).
40. Chapman, R. J., Ferrie, C. & Peruzzo, A. Experimental demonstration of self-guided quantum tomography. *Phys. Rev. Lett.* **117**, 040402 (2016).
41. Kim, Y. H. et al. Experimental entanglement concentration and universal Bell-state synthesizer. *Phys. Rev. A* **67**, 010301 (2003).